ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Introduction on Security Engineering

Dr. Puthanveetil Deepthi
Associate Professor, Department of Engineering Physics, Presidency University, Bangalore, India,
Email Id-deepthi.pr@presidencyuniversity.in

ABSTRACT: ***Strong security measures are now essential as businesses increasingly depend on sophisticated technical systems to store, analyse, and send sensitive data. Designing, putting into place, and maintaining safe systems that can resist a variety of attacks is the focus of the field of security engineering. This abstract examines the discipline of security engineering and emphasises its importance in light of a changing threat environment. The main issues that contemporary threats, such as sophisticated cyberattacks, data breaches, and the introduction of new attack vectors, present are first identified. These difficulties highlight the need for proactive security measures that go above and beyond traditional methods. The main ideas and techniques used in security engineering are further explored in the abstract. These include access control, cryptography, secure system design, risk assessment, and management, and incident response planning. The multidisciplinary character of security engineering is emphasised since complete protection requires cooperation between engineers, IT specialists, security analysts, and stakeholders.***

KEYWORDS: ***Cryptography, Risk Management, Security Engineering, Security Analysts***.

INTRODUCTION

Additionally, this abstract explores how security engineering is changing as a result of technological improvements and the intelligence of hostile actors rising. It emphasises the value of ongoing surveillance, threat information, and adaptable defence systems to quickly identify and counter new threats. In order to secure privacy and compliance, the abstract emphasises the need of security engineering alignment with legal, ethical, and regulatory frameworks. It also discusses the value of user education and awareness in creating a culture of security awareness inside organisations. This abstract concludes by emphasising the crucial role that security engineering plays in defending systems and data against an ever-evolving threat environment. Organisations may increase their resilience and lessen the effects of possible security breaches by implementing proactive tactics, using cutting-edge technology, and cultivating a culture of security.

The goal of security engineering is to create reliable systems that can withstand malicious intent, human mistake, and mishap. As a discipline, it focuses on the instruments, procedures, and techniques required for the design, implementation, testing, and adaptation of existing systems as their environment changes [1]–[3]. Cross-disciplinary understanding in areas such as cryptography, computer security, hardware tamper-resistance, formal techniques, economics, applied psychology, organisations, and legislation are all necessary for security engineering. Skills in system engineering, from business process analysis to software engineering to assessment and testing, are equally crucial, but they are insufficient since they only address mistake and misfortune rather than malicious intent.

Critical assurance requirements are included in many security systems. Their failure may put people's lives and the environment in danger as with nuclear safety and control systems, cause significant harm to the nation's financial system cash registers and other bank systems, threaten people's right to privacy (medical record systems), jeopardise the viability of entire industries (pay-TV), and make crime easier (burglar and car alarms). Economic progress may be seriously hampered even by the notion that a system is more susceptible than it really is paying with a credit card online.

According to the traditional wisdom, security is concerned with making sure that certain things don't happen, while software engineering is concerned with making sure that they occur e.g., "John can read this file". The truth is far more nuanced. Every system has a different set of security needs. User authentication, transaction integrity and accountability, fault tolerance, message secrecy, and covertness are often combined. But many systems fail because of improper

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

protection of the proper items or improper protection of the proper things. This means that getting protection correctly requires a variety of processes.

You must determine what needs to be protected and how to achieve it. Additionally, you must make sure that those who will protect and maintain the system are adequately motivated. I'll lay out a framework for thinking about this in the part after this. Then, I will quickly look at four application areas: a bank, an air force base, a hospital, and the house, to demonstrate the variety of diverse things that security systems have to accomplish. We will be able to try some definitions after we have provided some specific instances of the material that security engineers must comprehend and construct.

Designing, putting into practice, and managing secure systems are the main objectives of the field of security engineering. In order to safeguard computer systems, networks, and data from unauthorized access, abuse, and threats, it comprises a number of concepts, strategies, and best practices. Security breaches and cyberattacks pose serious hazards to people, businesses, and even whole countries in the linked world of today, when information is essential to every part of our lives. By creating strong and resilient systems that can resist and defend against a variety of attacks, security engineering tries to reduce these risks. To balance usability, functionality, and security is the main objective of security engineering. It entails spotting possible weaknesses and dangers, creating defences, and incorporating them into system design and execution. By being proactive, security is made to be a fundamental and essential element of the system rather than an afterthought. Network security, information security, software security, physical security, cryptography, access control, incident response, and risk management are all included in the vast field of security engineering. It uses a multidisciplinary strategy that combines concepts from politics, computer science, engineering, mathematics, and other fields.

Because threats and assaults are always changing, the area of security engineering is continually developing. Security experts must keep up with the most recent developments in technology and trends since new vulnerabilities and attack routes are often discovered. Additionally, as technology develops, new difficulties appear, such as the need to secure cloud-based systems, IoT gadgets, and AI applications.

Security engineering is used by businesses in a variety of sectors, such as government organisations, financial institutions, healthcare providers, and technology firms, to safeguard their sensitive data and important assets. They may protect their systems, maintain confidence with their stakeholders, and adhere to applicable legislation and standards by using efficient security engineering practices. Security engineering is a critical discipline that protects systems, networks, and data from vulnerabilities and attacks. Security engineers work to create safe systems that safeguard data and reduce risks by using methodical methodologies, best practices, and cutting-edge technology. As a result, they assist create a safer and more secure digital environment.

DISCUSSION

A Framework

Four factors need to work together for security engineering to be effective. There is policy, which outlines what you must accomplish. The cyphers are one such method.

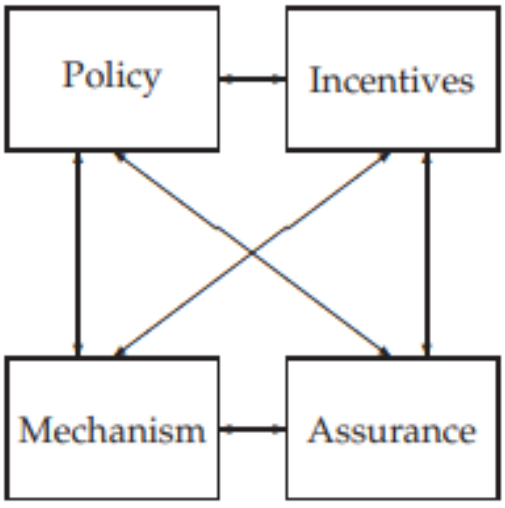

Figure 1: Security Engineering Analysis Framework.

You construct equipment such as access controls, hardware tamper-resistance, and other tools to carry out the policy. The degree of confidence you can have

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

on any specific mechanism provides assurance. Finally, there is incentive, which serves as both a motivation for system guards and maintainers to do their duties effectively and a drive for attackers to attempt to circumvent your security measures [4]–[7]. These all work together (see Figure-1).

Let's use the 9/11 terrorist attacks as an example. Knives with blades up to three inches were allowed at the time, and as far as we know, the screeners performed their job of keeping weapons and explosives off. The hijackers' success in getting knives past airport security was not due to a mechanical failure, but rather a policy one. Since then, the policy has altered, first outlawing all knives and subsequently most weapons baseball bats are now prohibited but whisky bottles are allowed it has also changed its mind on numerous specifics butane lighters were formerly prohibited but are now permitted again. Due to items like composite blades and non-nitrogen explosives, the mechanism is weak. The level of assurance is consistently inadequate; several tonnes of innocuous passenger belongings are discarded each month, while only about half of all weapons that are accidentally or purposefully brought past screening are removed.

Serious experts highlight significant issues with priorities. For instance, the TSA has spent $14.7 billion on intrusive passenger screening, which is mostly ineffectual, but $100 million would substantially reduce danger if cockpit doors were strengthened. The majority of ground personnel are not checked, according to the president of the Airline Pilots Security Alliance, and little effort is made to protect planes that are left parked overnight. There isn't much that can stop a bad man from wheeling steps up to an aircraft and planting a bomb inside since most aeroplanes don't have locks; if he had flying abilities and enough chutzpah, he could submit a flight plan and take off with the plane. However, vetting employees and watching over aircraft are simply not priorities.

Simply put, the incentives for decision-makers prefer visible restrictions above those that are efficient. The outcome is what Bruce Schneier refers to as "security theatre"measures intended to elicit a sense of security rather than actual protection. Politicians who want to scare up the vote, journalists who want to sell more publications, businesses who want to sell more goods, government officials who want to expand their empires, and security experts who want to win grants all have a motive to overestimate the danger posed by terrorism. The end result of all this is that the overreaction is mostly to blame for the harm that terrorists do to democratic nations. Fortunately, over time, electorates understand this. The public's response to the 7/7 bombings in Britain, where the IRA struck us sporadically for a decade, was mostly a shrug.

Security engineers must be aware of all of this in order to identify risks and dangers in content, make accurate predictions of what could go wrong, and provide sound guidance to customers. That relies on having a thorough awareness of what has gone wrong over time with different systems, as well as what kinds of assaults have been used, their results, and how they were prevented (if it was beneficial to do so). There are several case histories in this book. In Part III, I'll focus exclusively on terrorism. For the time being, I'll present a few succinct instances of intriguing security systems and what they are intended to prevent in order to set the stage. While many of the phrases used in security engineering are clear-cut, others are deceptive or even debatable. Use the index to locate the appropriate chapters, where you may discover more thorough descriptions of technical words. I'll attempt to identify the key issues in this part [8]–[11].

We must first define what we mean by "system" in order to go on. In actuality, this might mean:

1. A product or component, such as a smartcard, a cryptographic protocol, or the PC's hardware;
2. A combination of the aforementioned elements as well as an operating system, communications, and other components that make up an organization's infrastructure;
3. The aforementioned plus one or more apps (such as a word processor, music player, browser, accounts/payroll software, and so on);
4. All of the aforementioned, plus IT personnel;
5. Any or all of the aforementioned, plus management and internal users;
6. Any or all of the aforementioned, as well as clients and other outside users.

A common source of mistakes and vulnerabilities is the ambiguity between the aforementioned concepts.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

In general, the first and sometimes the second are the areas of concentration for the vendor and evaluator communities, while the sixth and occasionally the fifth are the areas of focus for businesses. We shall see several instances of hardware-based security-advertised systems that really crashed when a certain program was executed or when the device was utilised in a manner that the creators hadn't intended. One of the main reasons for security failure is the lack of the human elements, and therefore the neglect of usability difficulties. As a result, we will often employ definition 6, and it should be evident from the context when we adopt a more limited interpretation.

Lack of understanding of the players and their claims is what causes the following set of issues. We often find phrases like "Alice authenticates herself to Bob" in the literature on security and cryptology since it's a practice that security protocol principals be designated by names picked with (typically) consecutive initial letters, much like storms. This greatly improves readability, but often at the price of accuracy. Do we mean that Alice demonstrates to Bob that her name is Alice or that she demonstrates that she has a certain qualification? Do we mean Alice the person doing the authentication, or Alice's agent, a smartcard or software tool? In that scenario, are we certain it's Alice and not Cherie, to whom Alice may have loaned her card, David, who may have stolen it, or Eve, whose computer was hacked? A corporeal person (human, extraterrestrial, etc.) in any capacity, such as that of an operator, principal, or victim, is referred to as a "subject." I'll use the term "person" to refer to either a real person or a legal entity, such as a business or a government.

An organisation that uses a security system has a principle. This thing might be a topic, a person, a role, or even a piece of technology like a computer, a smartcard, or a terminal that reads credit cards. A primary may also be a communication channel (which, depending on the situation, might be a cryptographic key or a port number). A principle may also be a compound of other principals; examples include a group (Bob or Alice), a conjunction (Bob and Alice operating together), a compound role (Alice serving as Bob's manager), and a delegation (Bob acting on Alice's behalf while she is away). A word of caution: roles and groups are not the same. A group is a collection of principles, but a role is a collection of responsibilities taken on successively by various people (e.g., "the officer of the watch on the USS Nimitz" or "the president of the Icelandic Medical Association for the time being"). A primary may be thought of from many perspectives; for instance, "Bob acting for Alice in her absence" might also imply "Bob's smartcard representing Bob who is acting for Alice in her absence" or "Bob operating Alice's smartcard in her absence." I'll be more precise if we need to think about further specifics.

The definition of the term "identity" is debatable. I'll use it to denote a correspondence between the names of two principles to indicate that they relate to the same person or piece of machinery when we need to be extra cautious. It may be crucial to know, for instance, that the Bob in "Alice acting as Bob's manager" is the same Bob as "Bob acting as Charlie's manager" and "Bob as branch manager signing a bank draught jointly with David." identification is often misused to signify nothing more than a "name," a misuse that is reinforced by terms like "user identity" and "citizen's identity card." I sometimes fall back on using this colloquial language in situations when there is no chance of being unclear in order to avoid seeming pompous.

The terms trustworthy and dependable are often used interchangeably. The following scenario demonstrates the difference: if an NSA employee is seen in a bathroom selling sensitive information to a Chinese official, we may refer to him as "trusted but not trustworthy" (assuming his operation was not authorised). In the following, we'll utilise the NSA definition, which states that a trustworthy system or component is one that won't fail whereas a trusted system or component is one whose failure might compromise the security policy.

Be aware that there are several more ways to define trust. According to the UK military, trusted system components are those "whose integrity cannot be assured by external observation of their behaviour while in operation." A trusted system may be "a system which won't get me fired if it gets hacked on my watch" or even "a system which we can insure," according to other definitions, which often have to do with whether a certain system is sanctioned by authority. Neither of these definitions will be used by

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

me. I'll be clear when we refer to a system that is authorised, insured, or not failure-evident.

Another bag of worms is unlocked by the notion of confidentiality vs privacy versus secrecy. While there is no denying that these phrases are related, they are not the same. It is not my confidentially that has been violated if my neighbour trims some ivy at our shared fence so that his kids may poke fun at my pets and peer into my yard. Furthermore, the obligation to maintain silence on the affairs of a former employer is one of trust, not of privacy.

CONCLUSION

Security engineering has a lot of terminological ambiguity, most of which is caused by the conflict factor. The term "security" is excessively overused and often signifies very different things to various individuals. For a company, it can mean having the power to keep an eye on every employee's email and online use; for the workers, it might mean having the freedom to use email and the internet without being watched. We may anticipate a rise in disputes, muddle, and misleading language usage as time goes on and security features are utilised more and more by those in charge of a system's design to obtain a competitive edge over other users. The security engineer should become sensitive to the many shades of meaning that everyday words take on in various contexts and be able to formalise what the security policy and aim are in reality. The protection aims must always be made clear in order to ensure effective security design, which might be annoying for customers who want to get away with anything.

REFERENCES

[1] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. Mcquaid, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," *Natl. Inst. Stand. Technol.*, 2021.

[2] P. M. Beach, L. O. Mailloux, B. T. Langhals, and R. F. Mills, "Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2930718.

[3] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Adaptable, model-driven security engineering for SaaS cloud-based applications," *Autom. Softw. Eng.*, 2014, doi: 10.1007/s10515-013-0133-z.

[4] G. McGraw, R. Bonett, H. Figueroa, and V. Shepardson, "Security engineering for machine learning," *Computer (Long. Beach. Calif).*, 2019, doi: 10.1109/MC.2019.2909955.

[5] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," *Future Internet*. 2019. doi: 10.3390/fi11030073.

[6] D. Mažeika and R. Butleris, "Integrating Security Requirements Engineering into MBSE: Profile and Guidelines," *Secur. Commun. Networks*, 2020, doi: 10.1155/2020/5137625.

[7] Á. Török and Z. Pethő, "Introducing safety and security co-engineering related research orientations in the field of automotive security," *Period. Polytech. Transp. Eng.*, 2020, doi: 10.3311/PPTR.15850.

[8] M. A. Simonyi, "What Is Security?," in *Securing Windows NT/2000*, 2020. doi: 10.1201/9781420031461-4.

[9] C. Bynoe, "What Security Means to Me," *J. Intell. Conflict, Warf.*, 2021, doi: 10.21810/jicw.v3i3.2574.

[10] R. Anderson, "What Is Security Engineering?," in *Security Engineering*, 2020. doi: 10.1002/9781119644682.ch1.

[11] C. Bueger, "What is maritime security?," *Mar. Policy*, 2015, doi: 10.1016/j.marpol.2014.12.005.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Understanding Usability and Psychology

Mr. Soundra Prashanth
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-prashanth.sp@presidencyuniversity.in

ABSTRACT: ***In security engineering, usability and psychology are vital because they have an impact on the efficacy and acceptability of security methods and systems. This abstract examines the relationship between usability and psychology in the context of security engineering, emphasising the significance of this relationship and its influence on user behaviour, decision-making, and overall security posture. Usability describes how simple, effective, and efficient a system or interface is to use. Usability in security engineering focuses on creating security measures that are user-friendly and do not hinder users' experience or productivity. The chance of user circumvention due to annoyance or misunderstanding is decreased and user compliance is increased by a well-designed, user-friendly security system. Users can easily comprehend and engage with safe systems because to usability concepts including simplicity, consistency, and feedback. This abstract emphasises how important it is for security engineering to take usability and psychology into account. Security experts may build safe systems that are simple to use, effective, and in line with users' mental models by using user-centered design principles and psychological insights. Overall security and resilience against threats and vulnerabilities are increased as a result of this strategy, which also increases user acceptability, engagement, and compliance.***

KEYWORDS: ***Antagonistic, Authentication Systems, Phishing, Psychology.***

INTRODUCTION

Contrarily, psychology explores the cognitive and behavioural aspects of human nature. In security engineering, an understanding of human psychology is essential since human mistakes and weaknesses often result in security breaches. Users' vulnerability to phishing attempts, weak passwords, and other security threats is influenced by psychological variables such cognitive biases, social engineering, and decision-making heuristics. Security engineers may build systems that fit with users' mental models, expectations, and motivations by analysing these psychological variables. This will encourage users to adopt more secure behaviour.

A user-centered strategy is necessary for the combination of usability and psychology in security engineering. To find usability issues, cognitive biases, and behavioural patterns, user research, usability testing, and feedback analysis are conducted. This information guides the development and use of security measures such access control procedures, authentication systems, and security awareness training. Security engineers may create systems that are both safe and easy to use, enhancing user satisfaction and encouraging a security-conscious culture. This is done by taking usability and psychology into account.

At least as much as technology, many actual assaults take use of psychology. Phishing, when victims are tricked into logging on to what looks to be a legitimate website but is really intended to steal their credentials, is the kind of online crime that is expanding the quickest. Because most online protection mechanisms are not nearly as intuitively usable or as challenging to forge convincingly as their real-world equivalents, online frauds like phishing are frequently easier to commit and harder to detect than comparable real-world frauds. It is much simpler for thieves to build a fake bank website that passes casual inspection than it is for them to build a fake bank in a shopping mall [1]–[3].

In order to cope with deceit in face-to-face situations, we have developed social and psychological skills over millions of years, but they are of little value to us when we get an email asking us to do an action.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Making excellent usage easier than poor use, or beneficial asymmetry in usability, seems to be more difficult. There are a few instances of asymmetry in real world objects: Using a knife to peel potatoes is far more difficult than using a potato peeler. Less suitable for murder. Nevertheless, a significant portion of the asymmetry on which we rely in our day-to-day operations doesn't merely depend on formal trades which may be readily mechanised, but on a mix of physical items, human judgement, and the underlying social norms. I'll go into more detail about this in Chapter 3's Introduction. Therefore, the danger of forging these messages increases when our interactions with companies, banks, and the government become more formalised via online communication and we lose both a physical and personal environment.

Today, deception in all its forms poses the biggest danger to internet security. It may be used to get passwords, corrupt private data, or even influence financial operations. Pretexting calling someone who possesses the information under a false pretence, often by claiming to be someone who is authorised to be told it is the most popular method used by private investigators to obtain personal information. Social engineering is a term that has been used to describe such assaults in general. There are a lot of different tastes. The Bruce Schneier quotation at the beginning of this chapter was taken from a story on a stock fraud in which a fake news release said that a company's CEO had quit and that its profits would be restated. When this was reported by many wire agencies, the stock fell 61% before the fraud was discovered. Hoaxes and scams have always existed, but the Internet makes some of them more accessible and allows others to be repackaged in ways that may go beyond our current regulations whether they be laws, corporate policies, or even just common sense. For some time, we will be playing catch-up.

People's increased proficiency with technology is another factor contributing to the rise in social engineering-based assaults. Design professionals get increasingly interested in psychological manipulation of system users or operators as they understand how to defend against simpler technical assaults. Thus, the only need for a security engineer is a rudimentary understanding of psychology and "security usability," and one of the major possibilities for the research community is to better understand how and why things operate. Designing and creating user-centered systems, products, and interfaces requires the integration of the domains of usability and psychology. Psychology studies how people perceive, interpret, and interact with technology, whereas usability focuses on making goods and systems simple to use and effective. Usability is a metric for how easily consumers can pick up a product and utilise it to accomplish their objectives quickly and effectively while still having a good time. It includes a variety of elements, including user pleasure, efficiency, learnability, effectiveness, and mistake avoidance. Systems that are usable are clear, simple to use, and created with the user's requirements and expectations in mind [4].

In contrast, psychology explores the cognitive and behavioural aspects of human-computer interaction. It looks at how people utilise information, make choices, and react to various stimuli in a digital setting. Designing interfaces that are in line with users' mental models, cognitive capabilities, and preferences requires a thorough understanding of human psychology. The fields of cognitive psychology, human factors, ergonomics, and user experience (UX) design are all relevant to usability and psychology. It contains guidelines, ideas, and approaches to assess, enhance, and maximise how people engage with technology. Researchers and practitioners may gain insights into human behaviour, cognitive processes, and user expectations by integrating psychological concepts into usability design. This information may help designers create user-friendly interfaces, compelling information displays, and seamless user experiences. Usability and psychology support critical business results in addition to raising user enjoyment and productivity. Users are more inclined to embrace products and systems that are simple to use and provide a pleasant user experience, which will boost

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

customer loyalty and produce better levels of user engagement.

Some of the most important approaches used in the subject include user interface (UI) design, user research, usability testing, and user-centered design. In order to find usability problems and obtain input for improvement, usability testing entails watching people interact with a system. Through methods including surveys, interviews, and user observations, user research entails acquiring information on user requirements, behaviours, and preferences. By putting the user at the centre of the design process, user-centered design makes sure that the system or product is developed with their needs and objectives in mind. The goal of UI design is to provide user interfaces that are simple to use and aesthetically attractive. In order to design user-centered and successful goods, systems, and interfaces, the sciences of usability and psychology are linked. Designers and researchers may optimise usability and improve the entire user experience by studying human behaviour, cognitive processes, and user expectations. In the end, using usability and psychology principles results in products that are simple to use, effective, and enjoyable, which is advantageous for both consumers and companies.

DISCUSSION

Attacks Based on Psychology

Although it is becoming more common, hacking systems via their users is not new. Military and intelligence outfits have long targeted one other's personnel; the majority of the previous Soviet Union's intelligence achievements These were the sort of Union. Private detective services are not far behind. Pretexting is the standard method of assault for this kind [5], [6].

a) ***Pretexting:***

My colleagues conducted an experiment in England in 1996 to ascertain the danger that pretexting poses to medical privacy. We provided training to the employees of a health authority, a district-owned health insurer that paid for medical services for a population of around 250,000 people. A typical private eye would pose as a doctor attending to a patient in need of emergency treatment, but he would be easily identified since the phone number he provided was not that of the hospital where he claimed to work. (A detailed account of the incident is provided in the chapter on multilateral security.) Averaging 30 fraudulent pretext calls every week, we found them. Sadly, we were unable to convince the UK government to require this training of employees of health authorities.

A lot of privacy is compromised when there are 30 assaults each week, 52 weeks in a year, and 200 health authorities in England. Pretexting is illegal in many nations, including the USA, the UK, and many others, although it is nonetheless a source of income in both. Describes an example of a similar situation where a debt collector for General Motors was punished for tricking government employees into handing over 250 people's home addresses over the phone. The release of Kevin Mitnick's "Art of Deception," perhaps the most terrifying security book ever, occurred in 2002. When released from jail, Mitnick revealed how practically all of his escapades had included social engineering. Mitnick, who received substantial news attention when he was caught and found guilty for hacking phone networks, revealed this following his imprisonment. His usual attack was pretending to be a coworker and asking for "help" like a password from a phone company employee. Sales training programs have long taught techniques for getting past a company's switchboard and gaining its employees' confidence; Mitnick honed these skills by utilising them to get over security measures, and his book details a remarkable array of ruses.

When it was revealed that Patricia Dunn, the chairperson of Hewlett-Packard, had engaged private investigators who had used pretexting to collect the phone records of other board members of whom she was suspicious and of journalists she regarded antagonistic, pretexting became international top news in September 2006. She was compelled to step down. The California Attorney General charged her and three private investigators with felonies and issued arrest warrants for them the following month. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

accusations included internet crime, wire fraud, stealing computer data, and unauthorised use of personally identifiable information. Charges against her were dismissed in March 2007; one reason for this was that she had cancer. Her co-defendants received community service after entering a no contest plea to lesser charges of false wire communications, a misdemeanour.

But solving the issue is challenging. Despite ongoing media attention over pretexting, the IRS was the subject of an audit in 2007 by the Treasury Inspector General for Tax Administration. The IRS was contacted by 102 employees at various levels, who were instructed to change their passwords to a known value and provide their user ids.62 did so. Now that over 100,000 IRS workers have access to tax return information, there might be 60,000 US taxpayers who are deceived into allowing someone to invade your financial privacy. Worse however, this occurred despite audit tests that were conducted similarly in 2001 and 2004.

Numerous federal agencies, including Homeland Security, want to conduct phishing attacks on their own employees in order to evaluate the success of security training. The privacy authorities in the UK launched a crackdown and filed charges against a private detective organisation that provided blagging services to prestigious legal firms. Operational security is the term used in the military to describe the process of thwarting efforts by outsiders to coerce your people into disclosing information. Limiting access and enforcing rigorous guidelines on who may share highly valuable secrets such as unreleased financial data, unpatentable industrial discoveries, or military plans depend on protecting them. regulations alone are not sufficient; you also need to teach all employees who have access to personal information and explain the rationale behind the regulations. In our example of medical privacy, we taught personnel to avoid pretexting and instructed them not to discuss medical data over the phone unless they had made the call themselves and had gotten the number from the phone directory, not from a caller. The message is sent loudly and clearly once a few pretexting efforts have been met, identified, and destroyed by the staff. Senior leaders are often the most difficult to teach; one firm sent a USB memory stick to the finance directors of 500 publicly-quoted businesses with the message, "For Your Chance to Attend the Party of a Lifetime," and 46% of them inserted it into their computers [7], [8] .

Rules for intelligence agencies are substantially stricter. The majority of operational security work is spent on educating personnel about inappropriate behaviour and fostering a culture of caution that verges on anonymity. Furthermore, a spymaster cannot depend on a strong detection culture to emerge on its own since foreign intelligence services contact spooks far less often than private investigators visit medical record clerks. To make sure that his staff takes the paranoid business seriously, he has to have his own red squad monitor them continuously. Some operational security procedures, such avoiding throwing confidential materials in the garbage, are plain sense. The necessity to teach the individuals you trust, especially if they are longtime friends, is less clear.

An embarrassing email leak that seemed to originate from the UK Prime Minister's office and was initially attributed to "hackers" was revealed to have been the work of a private investigator known as "Benji the Binman," who gained instant notoriety [8]. Most governments now follow a set of protocols that classify sensitive material as "classified" and limit who may access it by requiring background checks and special training. The creation of various protective systems, which I'll address later in the chapter on Multilevel Security, has resulted from this, even if it can often become obscenely bureaucratic and inefficient. It nevertheless provides a valuable foundation for thinking about operational security. I cover them in the chapter on Banking and Bookkeeping. Disciplines employed by banks to stop a rogue from convincing a manager to pay him money are similar in spirit but vary in specifics.

Pretexting is often used to target businesses, but it is beginning to be used more frequently against people. As of this writing in 2007, the following is the current

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

fraud in the USA: You get a phone call from a nasty person posing as a court official informing you that you have been chosen for jury service and requesting your SSN and birthdate. He applies for a credit card in your name if you instruct him to. He threatens to arrest and jail you if you tell him to leave. Not everyone has the self-assurance and legal expertise necessary to fend against this sort of trick.

b) ***Phishing:***

In many respects, phishing is more difficult for a business to manage than pretexting since, like the previous scam I discussed, the victims are your customers rather than your workers. The ordinary client need a lot of training, so you can't just design for them. You are asking for major legal issues if your security systems are inaccessible to those who don't speak English well, are dyslexic, or have learning disabilities, at least if you do business in developed nations. Bank phishing assaults first appeared in 2003, with six recorded attempts. Early cyberattacks were primitive and avaricious; they resembled bank websites and demanded a wide range of data, including ATM PINs. They were also poorly written in English. Most clients smelled rat. In order to get the victim to log in and claim that they hadn't, the attackers now use superior psychology. They often recycle real bank emails, changing just the URLs, or they send a message like "Thank you for adding a new email address to your PayPal account." Customers are likely to have their accounts emptied if they click the supplied URL instead of entering www.paypal.com or utilising an existing bookmark.

Losses are increasing very quickly (perhaps $200 million in the US in 2006, £35 million or $70 million in the UK), albeit they are difficult to pinpoint precisely since some banks attempt to blame the client and/or alter the accounting standards to prevent reporting frauds. There is still space for expansion in the phishing industry. One bank in the UK incurred the most of losses in 2006, although there may have been six or seven major victims in the USA. The temptation is obvious when stealing a password enables you to alter the target's email and street addresses to your own, and then use their credit card to get a widescreen TV. We are only just beginning to see large-scale assaults on companies like eBay and Amazon, but I'm confident we will see many more.

A variety of elements determine whether you are targeted whether you are a bank or an online retail company. Some of it has to do with how weak others perceive you to be; banks that go after fraudsters fiercely and persistently in court, long beyond the limit of economic reason, tend to be able to stave off assaults. The phishermen also favour institutions with lax internal controls that permit speedy transfers of huge sums of money overseas, with ineffective intrusion alarms, slow verification of the authorization of suspicious payments, and lax recovery efforts. The remainder of this chapter will discuss how to convince users to select strong passwords and input them correctly as well as how to prevent users from giving them to other parties. I'll start by discussing some fundamental psychology that is pertinent to this topic. A short section on CAPTCHAs, which websites employ to verify that a user is human and not a robot, will follow. These tests provide another perspective on the distinctions between human brains and software.

c) ***Insights from Psychology Research:***

As with security economics during the previous five years, I anticipate that research on the intersection of security and psychology will grow significantly over the next five years. This is not merely a result of the rise in assaults that target users in addition to or in instead of technology. For instance, much of terrorism involves influencing people's perceptions of danger, and even outside of the context of national security, many protective measures are marketed using scare tactics. Psychology is a vast field that encompasses everything from neuroscience to therapeutic subjects and crosses over into related fields like philosophy, artificial intelligence, and sociology.

Our knowledge of the mind is significantly less comprehensive than that of computers despite having been researched for a much longer period of time because the brain is so much more complicated. One fundamental issue, the nature of consciousness, remains unsolved. Although we are aware that "the mind is what the brain does," the processes behind our

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

sense of self and personal history are still largely unknown. However, there is a wealth of knowledge on how the mind and brain operate, and I anticipate that if psychologists and security experts collaborate on actual challenges, we will gain many insightful understandings.

d) ***What the Brain Does Worse Than the Computer:***

Cognitive psychology examines our thought processes, memories, decision-making processes, and even daydreaming. There are several well-known effects, such as how much simpler it is to remember information that is repeated repeatedly and when it is stored in context. The majority of these ideas, meanwhile, are not well known among system developers. George Miller's finding that the human short-term memory can handle roughly seven (plus or minus two) simultaneous selections, for instance, is well known. As a consequence, many designers restrict menu options to about five. But this is not the proper inference to make. After remembering where to look, people seek for information by scanning. Once you have located the necessary menu, scanning 10 items is just twice as difficult as scanning five. With spoken menus, when the typical user has trouble coping with more than three or four selections, there is a genuine limit to the size of the menu.

The empirical information amassed via the iterative development of deployed systems as well as lab studies has greatly advanced our understanding in this sector. Because of this, the focus of attention has shifted from applied psychology to the field of human-computer interaction (HCI) research. Researchers in human-computer interaction (HCI) have learned how to model and measure human performance, such as perception, motor control, memory, and problem-solving, as well as how people's mental models of systems operate. They have also developed an understanding of the techniques (such as task analysis and cognitive walkthrough) that we can use to investigate how people learn to use and comprehend systems.

In order to turn these ploughshares into swords the bad guys are already working on it, security experts must discover a solution. There are certain very evident opportunities for improvement. For instance, the safety research community has worked hard to characterise the mistakes users make while using machinery. According to error research, it is true that "to err is human" and that there are predictable types of human error that have their roots in the functioning of cognition. We are susceptible when the incorrect model is activated due to the schemata, or mental models, that let humans identify persons, sounds, and ideas so much better than computers do. Depending on where they occur in the "stack," human errors produced when operating equipment may be roughly divided into three categories: slip-ups and errors at the level of ability, errors at the level of rules, and errors at the level of cognition.

CONCLUSION

In conclusion, the creation of user-centered designs that improve the usability and user experience of goods, systems, and interfaces requires the combination of usability and psychology. Designers and researchers may create user interfaces that are clear, effective, and rewarding by taking cognitive and behavioural factors into account. Usability makes ensuring that goods are simple to understand and use, allowing consumers to accomplish their objectives quickly and effectively. It includes elements like user happiness, efficiency, learnability, and mistake avoidance. Usability problems may be found and fixed by using usability principles and doing usability tests, which enhances user performance and happiness.

Psychology sheds light on how people think about, utilise, and interact with technology. Designers may develop interfaces that fit users' mental models and preferences by studying human behaviour, cognitive processes, and user expectations. The total user experience is improved by using psychology to provide interesting interactions, easy navigation, and effective information display. There are various advantages to usability and psychology working together. Interfaces that are easy to use and straightforward boost user pleasure, engagement, and productivity. Products that provide a great user

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

experience are more likely to be adopted and kept in use by users. Delivering user-centered designs that satisfy client wants and preferences is another way for firms to achieve a competitive edge. As technology develops and user expectations shift, the fields of usability and psychology continue to adapt. The enhancement of usability and user experience in the digital sphere is facilitated by ongoing study and developments in user research methodology, UI design approaches, and usability assessment technologies.

In conclusion, combining usability and psychology is essential for developing products and user interfaces that are simple to use, effective, and pleasing to people. Designers may create intuitive and captivating experiences that satisfy user wants and expectations by taking into account human behaviour and cognitive processes. The employment of usability and psychological concepts ultimately results in higher user happiness, higher adoption rates, and more prosperous business outcomes in the digital sphere.

REFERENCES

[1] R. J. Anderson, "Usability and Psychology," *Secur. Eng. A Guid. to Build. Dependable Distrib. Syst.*, 2008.

[2] R. Anderson, "Psychology and Usability," in *Security Engineering*, 2020. doi: 10.1002/9781119644682.ch3.

[3] S. Jang and J. Y. Yun, "User experience and usability of physical controls(home button) on front of smartphones," *Arch. Des. Res.*, 2020, doi: 10.15187/adr.2020.05.33.2.137.

[4] M. Hertzum, "Usability Testing: A Practitioner's Guide to Evaluating the User Experience," *Synth. Lect. Human-Centered Informatics*, 2020, doi: 10.2200/s00987ed1v01y202001hci045.

[5] Rachna Dhamija, "Usability, Psychology, and Security, UPSEC 2008," *Usability, Psychology, and Security, UPSEC 2008*. 2008.

[6] R. Anderson and T. Moore, "Information security: Where computer science, economics and psychology meet," *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, 2009, doi: 10.1098/rsta.2009.0027.

[7] T. Whalen, "Security as if people mattered," *IEEE Secur. Priv.*, 2011, doi: 10.1109/MSP.2011.92.

[8] J. D. Still, A. Cain, and D. Schuster, "Human-centered authentication guidelines," *Inf. Comput. Secur.*, 2017, doi: 10.1108/ICS-04-2016-0034.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Brief Study on System Issues and CAPTCHAs

Dr. Bolanthur Vittaldasa Prabhu
Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-bvprabhu@presidencyuniversity.in

ABSTRACT: ***System security is crucial in the modern digital environment to safeguard sensitive data and stop unauthorised access. However, as security measures advance, enemies constantly create fresh ways to get around them. This abstract investigates the systemic problems that exist and how CAPTCHAs (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) may help to solve them. A variety of vulnerabilities, such as malicious assaults, data breaches, and unauthorised access, are included in system problems. In order to breach systems and obtain unauthorised access, adversaries use a variety of strategies, including software vulnerabilities, social engineering, and brute-force assaults. These system flaws pose serious threats to people, businesses, and even national security, underscoring the urgent need for strong security measures. System flaws significantly increase the danger to the integrity and security of digital systems. CAPTCHAs provide a way to stop automated assaults and confirm human identity, but they need to be built properly to strike a balance between usability and security. Researchers and practitioners may work to design robust and user-friendly systems in the face of growing threats by comprehending the difficulties and investigating alternate security solutions.***

KEYWORDS: ***Security Engineers, Security Tools, Social Engineering, System Security.***

INTRODUCTION

One such security mechanism that seeks to differentiate between actual human users and artificial bots trying to attack systems is the CAPTCHA. CAPTCHAs ask users to answer questions or solve problems that are relatively simple for people to understand but difficult for computers. CAPTCHAs aid in preventing automated assaults like brute-force password cracking and automated account creation by confirming the user's human identity. However, there are certain difficulties with using CAPTCHAs. The harmony between usability and security is one major issue. Overly complicated or challenging CAPTCHAs might annoy genuine users and provide a negative user experience. Additionally, improvements in AI and machine learning have made it possible for opponents to create sophisticated bots that can get around certain CAPTCHAs, decreasing their effectiveness. This presentation also examines CAPTCHA alternatives, including risk-based authentication and biometrics, which employ user attributes and contextual data to confirm identities. These methods seek to provide an authentication procedure that is more fluid and user-friendly while retaining a high degree of security. The significance of a multi-layered security strategy is emphasised in the study's conclusion in order to successfully alleviate system concerns. While CAPTCHAs are helpful in thwarting automated assaults, it is best to combine them with additional security measures for more complete defence. Future studies should concentrate on creating novel, flexible security methods that can solve changing system problems while preserving good user experience.

Systems in the digital era have a number of difficulties relating to user experience, privacy, and security. The danger presented by automated bots and malicious software is one concern that has grown in importance. These automated entities have the ability to disrupt services, engage in unauthorised behaviour, and exploit system flaws. The usage of CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is one generally accepted way to reduce this issue. Security tools called CAPTCHAs are used to confirm that a user is human

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

and not a computer program. They often give users tasks or assessments that need cognitive capacities like to those of humans to complete. By prohibiting automated bots from getting unauthorised access or carrying out nefarious deeds, CAPTCHAs operate as a defence against them.

The main purpose of CAPTCHAs is to distinguish between human users and automated bots. Human users can understand and react to the challenges, whereas automated bots have difficulty passing the tests because they lack human-like perception, reasoning, and problem-solving skills. In a variety of online contexts, including user registration, comment forms, online surveys, and transaction verification, CAPTCHAs are often employed. Although CAPTCHAs are a useful security tool, there are still several difficulties and system problems with them. The following are some noteworthy features:

User Experience:

CAPTCHAs may sometimes be difficult for human users as well. The examinations can be difficult to understand or complete, which would be frustrating and inconvenient. Especially for users with visual impairments or cognitive limits, complex CAPTCHAs with distorted characters or unclear instructions might cause accessibility problems. For CAPTCHAs to be successfully implemented, the correct balance between security and user experience must be struck.

Usability:

User-friendly CAPTCHA designs should be used to make sure that the tests are simple to comprehend and solve. Users may give up on the job or look for other services as a consequence of poorly designed CAPTCHAs with unclear or deceptive instructions.

Accessibility:

The accessibility requirements of all users, including those with impairments, must be taken into account. Alternative CAPTCHA tests or accessible versions should be made available to assist users who may have trouble with the conventional CAPTCHA tests. This may include solutions like audio CAPTCHAs or other types of verification.

Evolving Bots:

Automated bots and malevolent actors modify their strategies to get around CAPTCHAs as they advance in sophistication. There have been cases when sophisticated bots have been able to get around certain kinds of CAPTCHAs utilising artificial intelligence and machine learning algorithms. In order to keep ahead of automated attacks, CAPTCHA strategies must constantly advance as a result of the continual conflict between attackers and CAPTCHA creators.

Scalability:

Systems that deal with a lot of traffic or user interactions must integrate CAPTCHAs. It's crucial to make sure that CAPTCHA tests can grow effectively without degrading system responsiveness or frustrating users.

User Privacy:

During the verification process, certain CAPTCHA providers may gather user information or behavioural patterns. Addressing privacy issues and making ensuring that user data is handled safely and in accordance with applicable legislation are crucial. In order to solve security issues with automated bots and dangerous malware, CAPTCHAs are essential. System designers must carefully consider user experience, accessibility, and growing bot capabilities even if they provide an efficient defence mechanism. CAPTCHAs may be a crucial component of a system's security measures by balancing security, usability, and privacy, safeguarding against automated attacks while delivering a great user experience for authorized human users.

DISCUSSION

Although phishing is the password issue that is receiving the most attention from the general public, and psychology is the most popular area of study, there are a variety of other situations where attackers attempt to obtain or guess passwords or compromise systems in other ways. I'll also quickly touch on some technical concerns with password entering and storage here for the purpose of completeness [1], [2]. The main system problem, as I previously said, was whether it

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

was feasible to limit the amount of password guesses. When guessing is not restricted, such as with ATM PINs, security engineers refer to password systems as being "offline." Originally, this referred to systems where a user could retrieve the password file and take it elsewhere in order to attempt to guess the passwords of other users, including more privileged users. The phrases are now hardly accurate. Some offline systems, such as the smartcards used in an increasing number of countries for ATMs and retail transactions, restrict password guesses by checking the PIN stored on the smartcard chip and relying on its tamper-resistance.

Many online systems do not have the ability to limit guesses. For instance, if you log in using Kerberos, an adversary who taps the line can see your key, which is encrypted with your password, flowing from the server to your client, as well as data, which is encrypted with that key, flowing on the line. She can then take her time trying out all possible passwords.

However, there are additional and interrelated system-level design problems than password guessability. I'll go through a few threat model and technological protection-related challenges in this part that you may want to think about the next time you construct a password system [3]–[7]. Just as we can only discuss the soundness of a security protocol in the context of a particular threat model, we can only determine the soundness of a certain password scheme by taking into account the kind of assaults we are attempting to thwart. These broadly speaking are

a) **Targeted attack on one account:** A hacker attempts to determine a specific user's password. To cause trouble directly, he would attempt to figure out Bill Gates' bank account PIN or a rival's workplace login password. Spear phishing is the term used when this includes sending emails.
b) **Attempt to penetrate any account on a system:** The hacker attempts to get in as any system user. This is a typical instance of a phisherman attempting to get a password from any user of an online banking service provided by a target bank.
c) **Attempt to penetrate any account on any system:** The intrusive party just cares that they have an account on any system inside a specified domain. Examples include criminals attempting to guess passwords on an online service so they can use the hacked account to spread spam or utilise its web space to temporarily host a phishing website. The standard operating procedure is to test one or two widely used passwords (such "password1") on a huge number of accounts that have been chosen at random. Other potential attackers include teenagers searching for a place to store pornographic material or a private investigator charged with gaining access to a company's intranet who is seeking a beachhead in the form of a login to an arbitrary computer inside their domain.

The attacker could want to block the authorised user from accessing the system. This might apply to all accounts or just one specific one.

Can You Deny Service?

In many banks, a terminal and user account are frozen after three unsuccessful password tries; an administrator then has to revive them. In a military system, this may be highly risky since an adversary who gained access to the network could launch a service denial assault using a flood of erroneous login attempts; if the adversary had a list of all the user names on a computer, he could even entirely disable it. Nowadays, a lot of commercial websites don't restrict guessing due to the possibilities of such an attack.

You must take into account both the scenario in which someone attacks one of your customers and the scenario in which someone attacks your whole system when determining if this may be an issue. Can a wave of erroneous login attempts put your service offline? Could you be the target of espionage? Or, can you rapidly disable account blocking in the case that such an attack happens? What kind of assaults could happen if you do turn it off?

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Protecting Oneself or Others?

No one should be allowed to utilise a service at another person's cost in certain systems, such mobile phone and cash machine systems. It is presumpted that the attackers are already authorised system users. So systems are or at least should be carefully built such that access to one user's password will not jeopardise the accounts of other identified users. Whereas a user who selects a password that is simple to decipher simply does damage. Hence, it is easier to accept a broad range of password strengths.

Keep in mind that people's passwords are often simple for their wives or partners to decipher hence, consideration should be given to concerns like what happens when an unfaithful partner seeks retribution. However, many systems do not provide a significant level of user isolation. Although operating systems like Unix and Windows may have been created to guard against unintentional interference by other users, they are not hardened to guard against malicious activities taken by other users who are capable of doing so. They have several known weaknesses, and new ones are continuously being posted online. A capable adversary who is able to get a single account on a networked computer system that is not properly maintained may often swiftly rise to the position of system administrator and carry out his own will from there.

Attacks on Password Entry

a) Interface Design

Occasionally, the issue is careless interface design. A thief may easily see a user enter her PIN before removing her pocketbook from her shopping bag since certain popular cash machines featured vertical keyboards that were at head height. The keyboards were created for males, so they were at a decent height for them, but because women and men in many nations are a few inches shorter, they were rather exposed. One of these devices required the user to look at the screen via a small slot in order to "protect client privacy." Your PIN wasn't secret, but your balance was! Similar issues plague many pay phones, and shoulder surfing of calling card information, as it's called in the business, has become commonplace in certain places like busy US railway stations and airports.

When entering a card number or PIN in a public area, I often conceal my dialling hand with my body or with my other hand. However, you shouldn't build systems based on the premise that all of your customers would do this. As hiding a PIN from others is seen as a visible show of mistrust, many individuals find it unpleasant to do so. This unease may be made worse if a buddy is close and the person is waiting in line at the grocery store. However, in court cases where I've testified as an expert witness, only a small percentage of customers shield their PIN effectively enough to protect it from an overhead camera. In the UK, for instance, banks claim that 20% of users never shield their PIN when entering it. And wait till the evildoers begin using infrared imaging.

b) Eavesdropping

Using caution while entering passwords might prevent criminal men from seeing you use your calling card at an airport phone. However, it won't prevent further eavesdropping attempts. The newest tactic used by criminals is to provide free Wi-Fi in public areas while collecting website users' credentials. Passwords put into the numerous websites that don't utilise encryption are easy to get, and utilising a middleperson attack, you may obtain passwords typed into the majority of those that do.

Such assaults have existed for a very long time. In the past, a hotel manager may have abused the keypad on his switchboard to record the keystrokes you made on the phone in your room. By doing this, he may learn the credit card number you used, and if it wasn't the one you used to pay your hotel bill, he may be able to steal money from your account with much less risk. Additionally, many networked computer systems in businesses still transmit passwords in plain sight via local area networks, making them harvestable by anybody with network programming skills or access to sniffer equipment. There are still a lot of unprotected computers I'll explain in the next chapter how Windows utilizes the Kerberos authentication protocol to stop this.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

c) Technical Defeats of Password Retry Counters

Many children learn that by resolving each ring in sequence of looseness, a bicycle combination lock can often be opened in a matter of minutes. The same strategy was effective against several computer systems. When a password was incorrect, the PDP-10 TENEX operating system examined the passwords one character at a time and stopped. A timed attack was now possible since the attacker could repeatedly store a guess at a password in memory at a convenient position, verify it as part of a file access request, and then watch to see how long it took for the request to be denied. A mistake in the first character would be reported fairly immediately, a mistake in the second would take a bit longer to report, a mistake in the third would take much longer, and so on.

So, instead of a password of N letters chosen at random from an alphabet of A characters requiring an average of AN/2 guesses, it took AN/2 guesses. Keep in mind that the more the system you're constructing now may be remembered for in thirty years is the more noteworthy security failures. In the field of embedded systems, the same errors are often made. With one remote automobile locking system, the red warning light on the receiver illuminated as soon as an incorrect byte was communicated from the key fob. With certain smartcards, it has been feasible to figure out the customer PIN by testing every input value and observing the card's power use. If the input was incorrect, a reset command would then be sent. The explanation was that writing to the EEPROM memory that contained the PIN retry counter resulted in a current spike of several milliamps, which could be detected in time to reset the card before the write was complete. These implementation specifics are crucial.

d) Attacks on Password Storage

Wherever passwords are kept, they have often been insecure. A terrible fault in an operating system update from the 1980s allowed anybody who typed the erroneous password and received the message "sorry, wrong password" to just click carriage return to get access to the machine. Almost a hundred U.S. government systems in Germany were using unlicensed copies of the software and did not receive the patch, which allowed hackers to gain access and steal data that they are rumoured to have sold to the KGB. This was quickly discovered, and a patch was sent out.

A U.K. bank suffered from yet another terrible programming blunder, giving all of its clients the same PIN unintentionally. It occurred as a result of the typical PIN creation equipment in use at the time, which required the bank programr to first generate and store an encrypted PIN before using a different command to print out a clear version on a PIN mailer. Due to a problem, each client received the identical encrypted PIN. No one at the bank had access to anybody else's PIN other than their own due to the stringent PIN handling protocols, therefore the error wasn't discovered until thousands of client cards had been sent out[8], [9].

And further risk comes from auditing. Users often enter the "username, password" sequence out of order in systems that keep track of unsuccessful password attempts, therefore the log typically includes a lot of passwords. If the logs are not properly safeguarded, assaults are simple. One may reasonably assume that this string is a password for one of the system's legitimate user names if they see an audit record of a failed login with the nonexistent user name e5gv,8yp.

CAPTCHAs

Recently, efforts have been made to create defence systems that rely more on the brain's strengths than its flaws. Passfaces was one early effort; it is an authentication system that displays users with nine faces, only one of which is of a person they are familiar with. Users must choose the correct face repeatedly to log in [356]. People are incredibly excellent at identifying other people's faces, but they are terrible at describing them, which means you could design a system where it was almost impossible for users to reveal their passwords, whether intentionally or accidentally. The selection of a sequence of spots on a picture is another broad proposition that is simple to memorise but difficult to reveal. Both kinds of systems

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

make intentional offline disclosure and shoulder surfing more difficult [10]–[12].

The CAPTCHA, which stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart," is the most successful invention in this sector. These are the little visual puzzles that are sometimes required to post to a blog or sign up for a free email account. You have undoubtedly seen these before. The concept is that a computer program creates some random text and then distorts it such that the user must understand it. Programs do a worse job of interpreting altered text than humans do. Using CAPTCHAs wisely may make it more difficult for attackers to attempt a few basic passwords with each of a huge number of existing accounts. CAPTCHAs originally saw widespread usage in 2003 to discourage spammers from using scripts to establish thousands of accounts on free email services.

Luis von Ahn and colleagues created the CAPTCHA [1304]. It was influenced by Alan Turing's famous test to determine if a machine was intelligent, in which a person was invited to attempt to distinguish between a computer and a human in separate rooms. The test's innovative design enables a computer to distinguish between humans and machines by putting one of AI's well-known "hard problems," like the identification of distorted text against a noisy backdrop, to use. It is proposed that figuring out the CAPTCHA is similar to resolving the AI issue.

The progress of attack and defence for the CAPTCHA is accelerating quickly, as is the case with any new security technology. Early systems presented several picture identification challenges that turned out not to be all that difficult. Additionally, there are potential protocol-level assaults. Von Ahn said in 2001 that, in principle, a spammer might use a porn site to solve them by charging users to access free porn. Since then, this has become a folk tale, and finally, it began to happen in October 2007 when spammers built a game where you had to solve one CAPTCHA after another to undress a lady. The first commercial CAPTCHA-breaking tools entered the market in the same month as well.

Finally, the technology may be used in potentially advantageous new ways with authentication and authorization rules. An intriguing illustration comes from German banks, who are implementing an anti-phishing measure in which, if you authorise a payment online, the bank sends you the payee, the amount, and your date of birth, integrated into a CAPTCHA that also contains a challenge, such as "if you want to authorise this payment please enter the thirteenth password from your list." This allows them to verify actual amounts and recipients using a static set of one-time passwords by assuring that a real-time man-in-the-middle attack would need a person in the loop. It may be a more advanced technology than the CAP calculator, and it won't need inputting transaction information twice, which would be more cumbersome. If it succeeds, only time will tell.

CONCLUSION

In many secure systems, usability is one of the most crucial and challenging design issues. The majority of actual assaults now target the user, despite it having long been disregarded as having less technological glitter than operating systems or cryptographic methods. The most dangerous threat to online banking systems is phishing, which is also beginning to affect other websites. Other sorts of trickery are also expected to become more prevalent as technological security increases and criminals turn their attention to users. Passwords were a major subject of the early research on security usability. When creating a password system, it's important to consider not just if users could reuse passwords but also whether they need to be safeguarded from one another, whether they can be instructed and held accountable, and whether accounts can be frozen after a certain number of incorrect guesses. You must also think about technological security concerns including whether passwords may be stolen by malicious software, fake terminals, or network eavesdropping, as well as if attackers would target a specific account or be content with breaking any account on a system or a network.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

REFERENCES

[1] Z. Nouri and M. Rezaei, "Deep-CAPTCHA: A Deep Learning Based CAPTCHA Solver for Vulnerability Assessment," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3633354.

[2] N. Roshanbin and J. Miller, "A survey and analysis of current CAPTCHA approaches," *J. Web Eng.*, 2013.

[3] S. M. R. Saadat Beheshti, P. Liatsis, and M. Rajarajan, "A CAPTCHA model based on visual psychophysics: Using the brain to distinguish between human users and automated computer bots," *Comput. Secur.*, 2017, doi: 10.1016/j.cose.2017.08.006.

[4] J. Tam, S. Hyde, J. Simsa, and L. Von Ahn, "Breaking audio CAPTCHAs," in *Advances in Neural Information Processing Systems 21 - Proceedings of the 2008 Conference*, 2009.

[5] T. V. Laptyeva, S. Flach, and K. Kladko, "The weak-password problem: Chaos, criticality, and encrypted p-CAPTCHAs," *EPL*, 2011, doi: 10.1209/0295-5075/95/50007.

[6] M. K. Sadar, P. A. Tijare, and S. N. Sawalkar, "Review on Captcha : Graphical Password for Security," *Int. J. Res. Advent Technol.*, 2015.

[7] M. Al-Fawa'reh, M. Qasaimeh, I. Abuarja, and M. Al-Fayoumi, "Mitigating deep learning attacks against text image captcha using arabic scheme," *Int. J. Commun. Antenna Propag.*, 2021, doi: 10.15866/irecap.v11i4.20375.

[8] K. Loganathan and D. Saranya, "An Extensive Web Security through Cloud Based Double Layer Password Encryption (DLPE) Algorithm for Secured Management Systems," in *2021 International Conference on System, Computation, Automation and Networking, ICSCAN 2021*, 2021. doi: 10.1109/ICSCAN53069.2021.9526381.

[9] A. Abuarqoub, "D-FAP: Dual-factor authentication protocol for mobile cloud connected devices," *J. Sens. Actuator Networks*, 2020, doi: 10.3390/jsan9010001.

[10] C. Li, X. Chen, H. Wang, P. Wang, Y. Zhang, and W. Wang, "End-to-end attack on text-based CAPTCHAs based on cycle-consistent generative adversarial network," *Neurocomputing*, 2021, doi: 10.1016/j.neucom.2020.11.057.

[11] H. Weng *et al.*, "Towards understanding the security of modern image captchas and underground captcha-solving services," *Big Data Min. Anal.*, 2019, doi: 10.26599/BDMA.2019.9020001.

[12] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2003, doi: 10.1007/3-540-39200-9_18.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Discussion on Protocols

Dr. Surendrakumar Malor
Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-coe@presidencyuniversity.in

ABSTRACT: ***The study of security protocols is the field of security engineering's deep unifying subject, if there is one. A few protocols have previously been seen informally; I've already described challenge-response authentication and Kerberos. Since this book is about engineering, I will also provide several instances of how protocols go wrong. A typical security system is made up of a number of principals, including individuals, businesses, computers, and magnetic card readers. These principals may interact with one another by phone, email, radio, infrared, and by carrying data on tangible objects like bank cards and transportation tickets. The guidelines that control these communications are the security protocols. Typically, they are built to withstand harmful actions like forgers changing the information on railway tickets, hostile countries blocking radio, or individuals lying on the phone. Since defending against every conceivable attack is sometimes prohibitively costly, rules are generally created based on presumptions about the dangers. For instance, the login protocol, which requires a user to input a password into a device, presumes that she can do so on the correct device. This made sense when computers in the office were hardwired, but it makes far less sense now that employees access websites over the Internet. In order to evaluate a protocol, one must first determine if the threat model is realistic. Does the protocol address it, secondly?***

KEYWORDS: ***Cryptographic Technologies, Encryption, Kerberos, Protocols.***

INTRODUCTION

Some protocols are really straightforward, like swiping a badge through a scanner to enter a building. They often include interaction and may or may not include technological solutions like encryption. For instance, the customary wine-waiter protocol in a restaurant when we order a bottle of fine wine offers some privacy (the other diners at our table are not informed of the price), some integrity (we can be sure we got the right bottle and that it wasn't switched for, or refilled with, cheap plonk), and non-repudiation (it is difficult for the diner to later claim that the wine was off). Blaze provides further examples from a variety of applications, including ticket checking, aviation security, and voting. The technological side of things may make protocols considerably more complicated. Numerous protocols govern how customers interact with cash registers and retail terminals, how a cash register or terminal talks to the bank that operates it, how the bank talks to the network operator, how money is settled between banks, how encryption keys are set up between the various cards and machines, and what kinds of alarm messages (like instructions to capture a card) may be transmitted. These protocols must all function together in a big, complicated system.

Frequently, a seemingly innocent design decision reveals a significant issue. For instance, some banks inscribed the customer's PIN on the card's magnetic strip after encrypting it with a key that was only known to their cash registers and central computers. The concept was to allow the cash machine to check PINs locally in order to save communications costs and even enable a limited service to be offered while the cash machine was down. A programr who was tinkering with a card reader used in a building access control system found that he could change the magnetic strip of his own bank card by replacing his own bank account number with his wife's after this system had been in use for many years without incident. The changed card and his personal PIN may then be used to withdraw funds from her account. Over the course of many years, he stole hundreds of thousands of dollars after realising that this allowed him to take money from any other customer's account as well. The impacted institutions were had to spend millions on new system upgrades. Additionally, certain security changes might take years. For

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

example, whereas America has not yet switched from magnetic-strip cards to smartcards, most of Europe has done so as of the time of writing. To enable purchases from American retailers by European cards and vice versa, old and new systems must coexist. Because the security features of the two systems don't precisely align, counterfeit European credit cards are often used in magnetic-strip cash machines in other nations, creating chances for thieves.

Protocols in Security Engineering

Protocols are essential in the area of security engineering for creating secure communication and guaranteeing the availability, confidentiality, and integrity of data. In order to ensure security, protocols provide a set of guidelines for the transmission of data between entities, such as computers, devices, or systems [1]–[4].

Here are a few frequently used security engineering protocols:

Secure Sockets Layer (SSL) / Transport Layer Security (TLS):

Cryptographic technologies like SSL and TLS are used to protect network communications. They provide data integrity, authentication, and encryption for protocols including HTTP (HTTPS), SMTP, and FTP. The SSL/TLS protocols provide secure channels of communication between clients and servers, guarding against spying, manipulation, and unauthorised access.

Internet Protocol Security (IPSec):

In order to protect IP communications at the network layer, IPSec is a protocol suite. In order to safeguard network communication between computers or networks, it offers authentication, encryption, and data integrity for IP packets. A secure virtual private network (VPN) or secure communication between network devices may be established using IPSec.

Secure Shell (SSH):

SSH is a mechanism for safe remote login and untrusted network command execution. It offers data integrity, encryption, and authentication for safe file transfers and remote access to computers. SSH is often used for secure server and network device management.

SFTP, or Secure File Transfer Protocol:

The File Transfer Protocol (FTP) has a secure variant known as SFTP. It offers network-based secure file transfer capabilities, preserving data security and privacy. SFTP is a well-liked option for secure file transfers since it makes use of SSH for authentication and encryption.

Virtual Private Network (VPN) Protocols:

Secure private networks are built using VPN protocols like OpenVPN, L2TP/IPSec, and PPTP across open networks like the internet. VPNs provide secure tunnels between networks or devices to enable resource access and secure communication. For network communication, VPN protocols provide secrecy, integrity, and authentication.

Domain Name System Security Extensions (DNSSEC):

The DNS (Domain Name System) protocol addition DNSSEC provides security capabilities to stop DNS spoofing and manipulation. To guarantee the integrity and validity of DNS data and defend against DNS-related threats, it makes use of digital signatures.

Kerberos:

A network authentication system called Kerberos is used to securely authenticate clients and servers. It offers a dependable third-party authentication service, making network resources accessible securely and limiting unauthorised access.

OAuth and OpenID Connect:

For secure authentication and authorisation in online and mobile apps, OAuth and OpenID Connect are used as protocols. They let users to securely access resources from different services service providers after authenticating with one service identity provider without disclosing their login information.

The protocols used in security engineering are only a few examples. The protocols chosen and put into use rely on the particular security needs, the make-up of the systems or networks, and industry best practices. It

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

is crucial to choose protocols that provide the required security features and guarantee interoperability with the operating systems and applications. To resolve vulnerabilities and maintain a secure environment, periodic protocol upgrades and patching are also necessary.

DISCUSSION

Password Eavesdropping Risks

Since they remain the primary method for establishing user authentication with computers, passwords and PINs continue to serve as the cornerstone around which most of computer security is built. In the last chapter, I spoke about the usability and 'human interface' issues with passwords. Let's now have a look at some more sophisticated assaults of the kind we must take into account while creating more generic protocols that work across machines. Simple embedded systems, like the remote control you use to access your garage or unlock the doors of automobiles made up until the mid-1990s, provide for an excellent case study [5]–[7]. The password for these archaic remote controllers is just their serial number, which is broadcast.

Using a "grabber," a device that records a code broadcast locally and replays it later, was a typical kind of attack. The signal used to lock a car door could be recorded by these devices, which seemed to be from Taiwan, and then replayed by criminals hiding in parking lots to open the vehicle after the owner had left. Using different codes for lock and unlock was one defence. But even so, this is not ideal. Before you leave for work in the morning, the burglar may first wait outside your home and note the unlock combination; he can then return at night and assist himself. Furthermore, sixteen-bit passwords are inadequate.

On rare occasions, users discovered they may accidentally unlock the incorrect vehicle or even activate the alarm on a vehicle whose owner was unaware it was equipped with one. And by the middle of the 1990s, gadgets that could attempt every potential code one at a time started to arrive. After around 215 attempts or under an hour and 10 attempts per second a code will be discovered. A car flashing its lights in response to a burglar would happen in less than a minute in a parking lot with 100 cars nearby. So an additional defence was to increase the password's length from 16 to 32 bits. Over 4 billion codes were proudly publicised by the producers. But this merely demonstrated that they had not fully grasped the issue. Grabbers continued to function as intended, and there was still only one code or two codes for each automobile. Guessing was no longer an option. A second weakness of using a serial number as a password is that numerous individuals can have access to it. For an automobile, this might imply that all the The workers at the dealership and maybe the state's automobile registration office. Serial numbers have also been utilised as master passwords by certain burglar alarms, and in this case it's worse since they may be found on the order, the delivery note, the invoice, and all the other common business documents. Sometimes the best technology is a simple password, even if it also serves as a serial number. For instance, my monthly season pass to the pool just contains a barcode. With our photocopier and laminating machine, I'm confident I could create a reliable fake, but because the turnstile is manned and the attendants learn to know the "regulars," there is no need for anything more costly. My card keys for entering the lab where I work are a little more difficult to counterfeit since the one for student areas utilises an infrared barcode, while the one for staff areas contains an RFID chip that can be scanned over short-range radio to reveal its serial number. Once again, they are probably pretty appropriate considering that our more costly equipment is located in spaces with decent mechanical door locks. However, more technology is required for items like vehicles that are often stolen. This takes us to procedures for cryptographic authentication.

Simple Authentication

The question "Who Goes There?" is often asked in the context of authentication to confirm the legitimacy of people or organisations before allowing them access to a system, place, or piece of information. It highlights how crucial it is to establish identify and guard against

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

unauthorised access. There are a variety of technologies and techniques for authentication that range from basic to complicated. I'll describe a simple authentication procedure that may be used to confirm a person's identity.

Password and user name:

The most popular and simple way of authenticating is this one. The user enters a special username and a matching password. The computer verifies that the entered username and password correspond to the user's previously saved information. Access is allowed if there is a successful match.

Two-factor authentication (2FA):

2FA adds an additional degree of protection by requiring the user to provide information in addition to their login and password. This usually entails creating a one-time code or getting it from a different gadget or communication channel, such a text message or an authentication app. To obtain access, the user must input this code in addition to their login and password.

Biometric authentication:

Utilising distinctive physical or behavioural characteristics to identify people is called biometrics. This can include speech recognition, iris scanning, or voice and fingerprint recognition. By relying on distinctive biological traits, biometric identification offers a high degree of security [8]–[10].

Security questions:

When creating an account for the first time, you may add security questions as an additional straightforward way. The user chooses or generates predetermined questions with answers that are simple for them to remember but challenging for others to guess. The user must answer the security questions truthfully in order to log in.

Token-based authentication:

In this procedure, the user's identity is verified via a tangible or digital token. It might be a software-based token produced by a mobile app, a smart card, or a USB key. To prove their identification, the user must insert the token or input the generated code. It's crucial to remember that although these techniques provide a fundamental degree of authentication, a system's total security also rely on elements like password strength, encryption, and system layout. To provide tighter security measures, many times a mix of these techniques or more sophisticated authentication procedures may be utilised.

Challenge and Response

Nowadays, the majority of automobiles have remote-controlled doors that can be unlocked, but most also have a metal key as a backup, ensuring that you can still enter your car even in an unfavourable RF environment. To actually approve engine start, many additionally use the challenge-response variant of the twopass protocol. The engine controller uses short-range radio to transmit a challenge containing a random n-bit number to the key as it is put into the steering lock. The automobile key uses encryption to calculate the answer to the challenge. The protocol may thus be written as E for the engine controller, T for the transponder found in the vehicle key, K for the cryptographic key shared by the transponder and the engine controller, and N for the random challenge.

$$E \longrightarrow T : N$$

$$T \longrightarrow E: \{T, N\}K$$

In one arrangement, it was easy for a burglar to interrogate the key in the automobile owner's pocket as he went by with the expected next challenge since the random numbers the engine management unit produced were predictable. In reality, a lot of encryption-enabled devices have been cracked at some point because their random number generators weren't sufficiently random. From one application to another, the fix is different. Radioactive decay may be used to create hardware random number generators, however this is uncommon due to safety and health issues. In big systems like PCs, there are many sources of exploitable randomness. One example is the minor fluctuations in the hard disk's rotation speed brought on by air turbulence.

The manner these sources are mixed is often crucial, since PC software packages frequently integrate randomness from a variety of external sources, including network traffic and keystroke timing, as well

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

as from internal system sources. However, in a typical embedded system, like a vehicle lock, the random challenge is created by encrypting a counter with a unique key that is stored within the device and isn't utilised for anything else.

Challenge-response protocols are not exclusively used in locks. In HTTP Digest Authentication, a web server sends a nonce to a client or proxy that it shares a password with in order to challenge them. The password, the nonce, and the requested URI are hashed together to form the answer. This offers a system that is impervious to password spying. For instance, it's used in SIP, the protocol for Voice-Over-IP (VOIP) telephony, to authenticate clients and servers. Although it is significantly better than transmitting a password in the open, it has a number of flaws, the most important of which are middleperson attacks, which I'll cover in a moment. The two-factor authentication process employs challenge-response in a much more noticeable way. Many businesses provide password generators to their employees so they may access the company's computer systems. These could resemble calculators. Their primary use is as follows, while they may also be used as calculators.

When you call up a login screen to log in to a computer on the network, you are given a random challenge, sometimes seven digits long. Along with a PIN of maybe four numbers, you enter this into your password generator. The first seven digits of the result are shown after the device encrypts these eleven digits using a secret key that is shared with the corporate security server. As your password, you type these seven numbers. Figure 1 provides an illustration of this approach. The corporate computer system will allow you access if you have a password generator with the proper secret key, input the PIN accurately, and typed in the correct output. However, your chances of logging in are slim if you don't have a reliable password generator for which you know the PIN. Formally, with S for the server, P for the password generator, PIN for the user's Personal Identification Number that bootstraps the password generator, U for the user and N for the random nonce:

$S \longrightarrow U : N$

$U \longrightarrow P : N, PIN$

$P \longrightarrow U : \{N, PIN\}K$

$U \longrightarrow S : \{N, PIN\}K$

Figure 1: Illustrate the Password generator use.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

These gadgets started to become popular in the early 1980s with phone companies, then in the 1990s with banks for usage by employees. There are more straightforward variants available that don't have a keyboard and instead just produce a new access code every few minutes by encrypting a counter; the most well-known of these is the RSA SecurID. A variety of industries have begun using authentication tokens in place of or in addition to passwords. The US Defence Department reported in 2007 that the implementation of an authentication system based on the DoD Common Access Card had reduced network intrusions by 46% in the prior year.

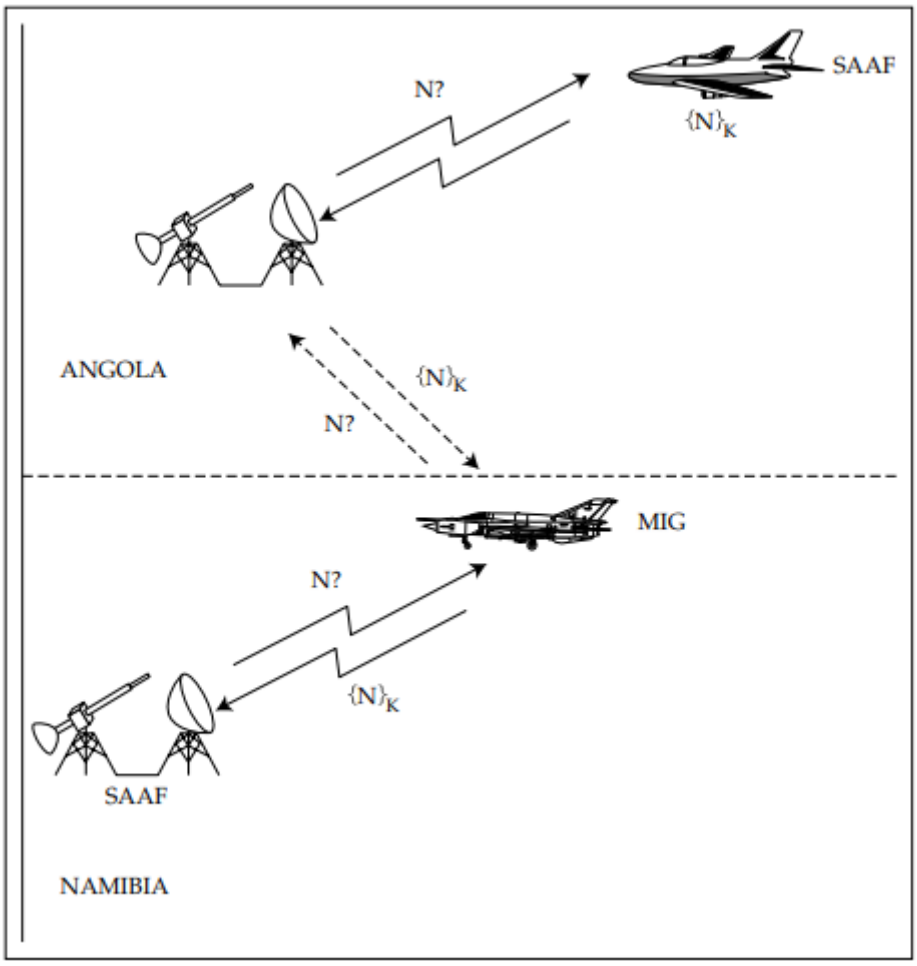

Figure 2: Illustrate the MIG-in-the middle attack.

The customer side of things is now beginning to benefit from the technology. By 2001, a few elite private banks, including Coutts, were using password generators to verify their internet clients. These banks never fell victim to phishing scams. A few banks in the Netherlands and Scandinavia began using the technology for all of their millions of clients by the year 2006; this is when the scams began. Once the victim has verified herself to the bank, the phishermen often utilise real-time man-in-the-middle assaults to gain control of a session which I'll explain in the next section. The Chip Authentication Program (CAP), which is accomplished by providing bank clients a calculator that utilises their bank card to perform crypto2, has been deployed by various banks in the UK and other parts of Europe as of late 2007. When a bank

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

card is loaded into this calculator, it will prompt the user for their PIN. If this information is provided accurately, the calculator will compute a response code based on either a counter for one-time authentication codes for card transactions or one-step logons to banking websites or a challenge (for two-step logons). There is a third mode of operation as well: the CAP calculator may also be used to verify transaction data if session takeover starts to be an issue. In this instance, it is intended to have the customer input the amount and the payee account number's final eight digits into her CAP calculator.

However, the outcome in banking could not be as favourable as it has been in the military. First, if your wallet is taken, the burglar may be able to read your PIN from the calculator since those numbers will be on the grimy, worn-out calculator keys. If you only use one bank card, the likelihood of a burglar guessing your PIN in three attempts has now decreased from around 1 in 3000 to approximately 1 in 10. Second, the bad guys have all the tools they need to empty your account when you use your card at a Mafia-run business or in a business where the terminals have been covertly reprogramd without the owner's knowledge. Additionally, they have the ability to generate a series of CAP codes that will let them access in the future and exploit your account for evil deeds like money laundering. In Figure 2 shown the MIG-in-the middle attack.

CONCLUSION

One (basic) illustration of the security protocol, a broader idea, is passwords. The procedures that principals take to build confidence in a system, such as verifying a claim to identity, proving ownership of a credential, or approving a claim on a resource, are specified by protocols. One-pass using random nonces, for example and two-pass challenge-response cryptographic authentication protocols are used for a variety of these purposes, from basic entity authentication to provide infrastructure for distributed systems that allows trust to be taken from where it exists to where it is needed. Security protocols are implemented in a variety of systems, including distributed computer systems for authentication and remote automobile door locks for the military. Designing efficient security mechanisms is challenging. Middleperson assaults, modification attacks, reflection attacks, and replay attacks are some of the possible issues they face. These dangers may interplay with design flaws like inadequate random number generators. Although it may be helpful, using mathematical approaches to check if protocols are proper won't detect every error. The environment for which a protocol was developed gradually changing to the point that the protection it provides is no longer sufficient is one of the most destructive failures.

REFERENCES

[1] R. P. Jover and V. Marojevic, “Security and protocol exploit analysis of the 5G specifications,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2899254.

[2] H. Yang and Z. Liu, “An optimization routing protocol for FANETs,” *Eurasip J. Wirel. Commun. Netw.*, 2019, doi: 10.1186/s13638-019-1442-0.

[3] Y. Liu, Q. Wu, T. Zhao, Y. Tie, F. Bai, and M. Jin, “An improved energy-efficient routing protocol for wireless sensor networks,” *Sensors (Switzerland)*, 2019, doi: 10.3390/s19204579.

[4] R. Elhabyan, W. Shi, and M. St-Hilaire, “Coverage protocols for wireless sensor networks: Review and future directions,” *J. Commun. Networks*, 2019, doi: 10.1109/JCN.2019.000005.

[5] X. Luo, D. Chen, Y. Wang, and P. Xie, “A type-aware approach to message clustering for protocol reverse engineering,” *Sensors (Switzerland)*, 2019, doi: 10.3390/s19030716.

[6] Y. H. Goo, K. S. Shim, M. S. Lee, and M. S. Kim, “Protocol Specification Extraction Based on Contiguous Sequential Pattern Algorithm,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2905353.

[7] H. Tschofenig and E. Baccelli, “Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security,” *IEEE Secur. Priv.*, 2019, doi: 10.1109/MSEC.2019.2923973.

[8] I. Chinwe C, P. Seth, and A. Obiageli J, “Biometric Authentication System Using Face Geometry,” *Int. J. Eng. Comput. Sci.*, 2019, doi: 10.18535/ijecs/v8i08.4332.

[9] B. Abazi, B. Qeliaja, and E. Hajrizi, “Application of biometric models of authentication in mobile equipment,” in *IFAC-PapersOnLine*, 2019. doi: 10.1016/j.ifacol.2019.12.602.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

[10] G. R. Sinha and P. Sone Oo, "Introduction to biometrics and special emphasis on myanmar sign language recognition," in *Advances in Biometrics: Modern Methods and Implementation Strategies*, 2019. doi: 10.1007/978-3-030-30436-2_1.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Brief Discussion on Evaluation of Access Control

Mr. Dileep Balaga
Assistant Professor, Department of Petroleum Engineering, Presidency University, Bangalore, India,
Email Id-balagadileepkumar@presidencyuniversity.in

ABSTRACT: ***By ensuring that only authorised persons or organisations are given access to systems, resources, or information, access control plays a crucial role in security engineering. Effective access control systems are crucial for preserving the integrity and confidentiality of resources, protecting sensitive data, and preventing unauthorised activity. This abstract gives a general overview of access control within the framework of security engineering by examining its core ideas, guiding principles, and available methods. Access control and its importance in the larger subject of security engineering are first defined in the abstract. The main goals of access control are emphasised, including secrecy, integrity, and availability. In order to express permissions and access privileges inside a system, the idea of an access control matrix is proposed. Following that, the abstract explores several access control models, including role-based access control (RBAC), mandatory access control (MAC), and discretionary access control (DAC). Each model is briefly explained, highlighting its special traits, benefits, and possible drawbacks. It also examines the function of access control rules, such as security labels and access control lists (ACLs). The abstract then looks at several technologies and access control methods used in security engineering. These might include smart cards, access tokens, biometric authentication, two-factor authentication, and password-based authentication. Their advantages, disadvantages, and contribution to creating reliable access control are highlighted in the abstract.***

KEYWORDS: ***Access Control, Authentication, Biometric, Virtualization.***

INTRODUCTION

The conventional focal point of computer security is access control [1]–[4]. It is the intersection of computer science and security engineering. Its role is to manage which principals (people, processes, machines, etc.) have access to which system resources – which files they can read, which programs they can run, how they communicate data with other principals, etc. Access control works at a number of levels (Figure 1).

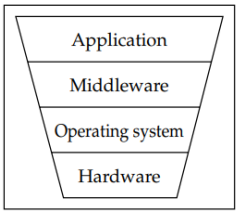

Figure 1: Illustrate the Access controls at different levels in a system.

1. The user may be presented with access control methods that, at the application level, reflect a highly detailed and intricate security policy. A contemporary online company may allocate employees to one of dozens of distinct positions, each of which could start a small fraction of the system's several hundred potential interactions. Some of them (like refunds) could need dual control or supervisor approval. And even that is simple compared to the complexity of access restrictions on a contemporary social networking site, which would have a maze of guidelines and choices about who may see, copy, and search what material from whom.
2. Applications may be built on top of middleware that enforces various security features, such as a database management system or accounting software. Database software typically has access controls that specify which dictionaries a given user can select and which procedures they can run, while bookkeeping software, for instance, may ensure that a transaction that debits one

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

ledger for a certain amount must credit another ledger for the same amount.

3. The underlying operating system's capabilities will be used by the middleware. This assumes the duty for providing means to regulate access to them since it creates resources like files and communications ports from lower level components.
4. Finally, the hardware capabilities offered by the CPU or by related memory management hardware will often be used by the operating system access controls. These regulate which memory addresses a certain process is allowed to access.

The controls become more sophisticated and unreliable as we go from the hardware via the operating system and middleware to the application layer. The majority of true computer frauds involve employees either misusing elements of the program that they were supposed to be using responsibly or accidently finding features of the application code that they may exploit in an opportunistic manner. However, flaws in access-control techniques, such as those in database software used by several web servers, might simultaneously expose multiple systems and force many businesses to fix or rebuild their products. The principles of access control at the hardware, operating system, and database levels will thus be the emphasis of this chapter. To create functional application-level controls, you must also be aware of the fundamental concepts (I provide several examples of how to integrate access controls with the requirements of particular applications in Part II).

Access control, like the other building blocks covered so far, is only useful when used in conjunction with a protection objective, which is often defined as a security policy. Many apps need administrator privileges to execute since the outdated single-user operating systems on PCs, such as DOS and Win95/98, allowed any process to edit any data. Granted access to the whole system and privileges. Additionally, it is more convenient for the programr to require that your product execute as administrator. Individuals do, however, have implicit protective aims, thus you wouldn't anticipate a shrinkwrap program to wipe out your hard drive. Therefore, having a clear security policy is a smart idea. Preventing program interference is now one of the top computer security issues. You don't want a virus to be able to hack a banking application to steal your money or to be able to grab the credentials from your browser. Additionally, a lot of common reliability issues are caused by how apps interact with one another or with the setup of the system.

When a client wants to exchange data, it is challenging to segregate apps. Simply preventing individuals from pasting URLs from emails into browsers would make phishing considerably more difficult, but it would also make daily living much more difficult. People are used to a variety of working methods that are not actually consistent with effectively isolating apps and their data due to the single-user history of personal computing. In fact, a top official at Microsoft expressed the opinion in 2000 that operating-system access restrictions weren't actually needed since client PCs and server PCs only ran a single program and had a single user.

Right now, the pendulum is returning. Virtualization is being used more often by hosting facilities; purchasing computers for your personal usage will cost you multiple times as much as purchasing the same resource on shared machines. Even if you don't care about security, keeping your programs from overwriting one other's configuration files should make your PC far more dependable, according to the Trusted Computing project and Microsoft Vista. You don't want your brokerage account to be compromised by a computer game you downloaded that turns out to be vulnerable; while operating systems get more secure, there are an increasing number of technical assaults on software other than the operating system. It makes sense to have a partition (or virtual machine) for business and another for recreation since companies would prefer measures to ensure that workers' computers don't pick up viruses at home. It will be difficult to undo the harm caused by years of information-sharing promiscuity, but in the near term, it is reasonable to expect for a framework that limits interactions between apps to manageable interfaces.

The operating system's built-in mechanisms provide the foundation for many access control solutions. I'll begin by talking about the operating-system security features that facilitate the isolation of various processes. These were historically created with the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

first time-sharing systems in the 1960s, and they continue to serve as the basis for numerous higher-layer techniques. The discussion of database systems, which provide roughly comparable access control techniques that may or may not be connected to operating-systems processes, will follow. Finally, I'll talk about sandboxing, virtualization, and "Trusted Computing," three advanced protection strategies. Virtualization runs beneath the operating system, creating two or more independent virtual machines between which information flows can be controlled or prevented. Trusted Computing is a project to create two virtual machines side-by-side, one being the 'old, insecure' version of an operating system and the second being a more restricted environment. Sandboxing is an application-level control, run for example in a browser to restrict what mobile code can do.

The goal of the three contemporary techniques is to put us back where we would be if all applications had to run with user privileges rather than as the administrator. The newest Microsoft operating system, Vista, is attempting to move away from running all code with administrator privilege. When users used time-shared minicomputers and mainframes to run their programs as unauthorised processes in the 1970s, that was essentially where computing was at the time. Only time will tell whether we can restore the Eden of order and control that Roger Needham alludes to at the beginning of this chapter and escape the chaotic present that Rick Maybury alludes to, but it is surely worthwhile to try.

DISCUSSION

The access controls included with an operating system often offer primary authentication using a system like passwords or Kerberos, after which they mediate their access to files, communications ports, and other system resources. Their impact may often be predicted using an access rights matrix with rows for people and columns for files. As shown in Figure 2, we'll write r for read access, w for write access, x for program execution access, and - for no access at all.

	Operating System	Accounts Program	Accounting Data	Audit Trail
Sam	rwx	rwx	rw	r
Alice	x	x	rw	–
Bob	rx	r	r	r

Figure 2: Naive access control matrix.

Sam is the system administrator in this simplified scenario, and he has complete access to everything (except from the audit trail, which even he should only be able to view). The manager, Alice, must run the operating system and the application. She must not be able to tamper with them; access must be restricted to the allowed interfaces. She must read and write the data as well. Bob, the auditor, is a master reader. This is sufficient in most cases, but it falls short in the particular instance of a bookkeeping system. We wouldn't want Alice to have unrestricted write access to the account file because we want to make sure that all transactions are wellformed, meaning that each debit must be matched by a credit someplace else. We also rather Sam didn't have access to this information. Therefore, we would like that only the accounting program be able to write to the accounting data file.

Now, the access permissions may resemble Figure 3:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

User	Operating System	Accounts Program	Accounting Data	Audit Trail
Sam	rwx	rwx	r	r
Alice	rx	x	–	–
Accounts program	rx	r	rw	w
Bob	rx	r	r	r

Figure 3: Access control matrix for bookkeeping.

A policy of this kind might also be expressed using access triples user, program, file) The protection domain, which is a collection of processes or threads that have access to the same resources but may sometimes have different files open or different scheduling priorities, is what we are generally concerned with rather than a specific program in the general situation. Access control matrices whether in two or three dimensions may be used to both model and put into practise security measures. But they struggle to scale. For instance, a bank with 50,000 employees and 300 apps would have a 15,000,000 entry access control matrix. This is a really big inconvenience. It could not only cause a performance issue, but it might also be susceptible to errors made by administrators. Typically, we'll need a more efficient method of storing and handling this data. Compressing the users and the rights are the two basic methods for doing this. For the first of these, it is easiest to utilise groups or roles to handle permissions for several people at once, but for the second, we can store the access control matrix using either columns for access control lists or rows for capabilities, often referred to as "tickets". There are more intricate methods incorporating policy engines, but let's start by learning to walk.

Groups and Roles

When we examine huge businesses, the majority of the employees often falls into one or both of a select few groups. A bank may have 40 or 50 employees, including branch managers, accountants, and chief tellers. Only a small number of individuals security manager, chief foreign currency trader, etc. will need having their access permissions specifically established. Therefore, we need a limited number of pre-established groups or functional responsibilities that staff members may be allocated to. A group is a list of principals, whereas a role is a fixed set of access permissions that one or more principals may assume for a period of time using a defined procedure. Although some people interchange the terms group and role, and they do so in many systems, the more accurate definition is that a group is a list of principals. The officer of the watch aboard a ship is the archetypal illustration of a role. There is always precisely one watchkeeper on duty, and when the watch changes, one officer officially relieves another. In reality, the role rather than the individual is what counts in the majority of corporate and government applications.

Roles and groups may be mixed together. All ships that are at sea right now have officers of the watch who have a variety of responsibilities. In the banking industry, the manager of the Cambridge branch may have rights that are reflected by becoming a group manager and taking on the position of acting manager of the Cambridge branch. when the function of acting manager may involve an assistant accountant filling in when the manager, deputy manager, and branch accountant are all absent due to illness, the group manager may indicate a rank within the business and maybe even a pay band. The application will determine whether or not we need to be cautious while making this difference. If everyone more senior has been slain aboard a battleship, we want even an average sailor to be permitted to keep watch. In a bank, we may establish a rule that transactions exceeding $10 million need to be authorised by two employees, at least one of whom must be a manager and one of whom must be an assistant accountant. If the branch

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

manager is ill, the assistant accountant serving in that capacity may need to ask the regional head office to sign off on a significant transfer twice.

For groups and roles, operating-system level support is available, but its adoption is still sluggish and its emergence is quite new. This kind of capability used to be implemented by programrs as special middleware or in application code (during the 1980s, I worked on two bank projects where group support was manually built as mainframe operating system extensions). While academic academics have been working hard on role-based access control (RBAC), which I'll cover in more detail in Part II, and which is beginning to be implemented in some major systems, since the mid-1990s, Windows 2000 offered substantial support for groups.

Access Control Lists

The access control matrix and the resource that each column refers to may be stored one column at a time, which further simplifies the administration of access rights [4]–[7]. An access control list, or ACL (pronounced "ackle"), is what this is. The ACL for file 3 (the account file) in the first of our instances above would resemble what is seen in Figure 4. As a tool for maintaining security status, ACLs offer both benefits and drawbacks. These may be separated into two categories: universal ACL attributes and implementation-specific properties.

ACLs are a logical option in settings where users are responsible for managing their own file security, and they gained popularity in the 1970s with the rise of Unix systems in colleges and research laboratories. The access controls in Windows are similarly based on ACLs, but have evolved through time to become more complicated. They are the fundamental access control mechanism in Unix-based systems like GNU/Linux and Apple's OS/X. ACLs, where access control policy is set centrally, are best suited for environments where data protection is a priority; they are less suitable for environments with a large and dynamic user population or where users want to be able to grant another user temporary access to run a specific program. ACLs are easy to set up, but they are ineffective as a way to do security checks at runtime since an operating system often knows which user is executing a certain program rather than what files it has been granted access to since it was started.

Every time a file is accessed, the operating system must either verify the ACL or find another mechanism to maintain track of the current access privileges. Last but not least, the distribution of access rules into ACLs makes it difficult to identify all the files to which a user has access. It is often necessary to deactivate a dismissed employee's password or another form of authentication in order to deny them access. Running system-wide checks could also be laborious; for instance, ensuring that no files have been left world-writable would require checking ACLs on millions of user files. Let's examine Windows and Unix implementations of ACLs, which are two crucial instances.

User	Accounting Data
Sam	rw
Alice	rw
Bob	r

Figure 4: Illustrate the Access control list (ACL).

Unix Operating System Security

In Unix, the operating system kernel the program that takes over when the computer boots runs as the supervisor and has complete access to the whole system. The users who operate the other programs have access to them. The manager acts as a mediator. The userid connected to the program is used to make access choices. However, if this is 0 (root), the choice to allow access is "yes." Therefore, root is free to view any file, change into any user, or do whatever else it wants. Additionally, there are certain actions that can only be performed by root, such initiating specific communication procedures. The system administrator usually has access to the root userid. This implies that the system administrator can alter anything under most Unix flavours, hence it is challenging to establish an audit trail as a file that he cannot change. This not only implies that Sam, in our hypothetical scenario, might tamper with the accounts and find it difficult to defend himself if he were wrongly accused of doing so, but it also implies that a hacker who was able to get access

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

to the system administrator could erase all traces of his incursion.

The Berkeley distributions, which include OS/X and FreeBSD, help to partially resolve the issue. For the user, system, or both, files may be made to be append-only, immutable, or undeletable. They cannot be changed or withdrawn later, not even by root, when they are set by a user at a high enough security level during the startup process. Different military configurations go to considerably more pains to provide separation of duty. However, keeping logs separate is the most straightforward and popular method of safeguarding them from root attack. Previously, this meant sending the system log to a locked-room printer; now, given the amount of data, it involves sending it to a different workstation that is managed by a different person. Second, there is no easy method to construct access triples of (user, program, file) since ACLs only store the names of people, not programs.

Apple's OS/X

Based on the FreeBSD variant of Unix, which runs on top of the Mach kernel, is Apple's OS/X operating system. Applications cannot access system memory (or each other's) unless they are operating with advanced permissions thanks to the BSD layer's memory protection. This implies, for instance, that you Stuck program using the 'Force Quit' command; in most cases, you do not need to restart the computer. Numerous graphical components, like as OpenGL, Quartz, Quicktime, and Carbon, are built on top of the Unix core while, at the user's level, the Aqua user interface presents an attractive and well-organized perspective.

In terms of file systems, OS/X resembles a conventional Unix. Users who may manage the system are in a group called "wheel," which gives them the ability to su to root even if the root account is disabled by default. The most obvious effect is that you can install programs if you are such a user (you are prompted for the root password when you do this). This might be a marginally better strategy than Windows (up to XP) or Linux, which, in practise, only allow administrators to install software but do not require an authentication step when they do so. The many Windows users who run as administrator for convenience do terrible things by accident (and malware they download does terrible things on purpose). Apple's edge may be boosted by OS/X version 10.5 (Leopard), which is based on TrustedBSD, a BSD variation created for government systems that contains required access control, despite Microsoft's struggles to catch up with Vista, as I'll detail below.

Windows Basic Architecture

Windows is the most popular PC operating system, and since Windows NT, its security has been mostly dependent on access control lists. Because Windows Vista is rather complicated, it might be useful to look back at earlier versions of the operating system. The security of Windows NT (Windows v4) was modelled after Unix and has subsequently adhered to the Microsoft principle of "embrace and extend." First, take ownership, modify permissions, and delete are all independent properties rather than simply read, write, and execute, allowing for more flexible delegation to be handled. These characteristics apply to both users and groups, and with group permissions, you may get a similar result to sued programs under Unix. As opposed to Unix, attributes have numerous values that may be specified, such as AccessDenied, AccessAllowed, or SystemAudit. It parses them in that sequence. No access is allowed regardless of any conflicting AccessAllowed flags if an AccessDenied is found in an ACL for the appropriate user or group. The richer syntax has the advantage of allowing you to set up things such that routine setup operations, like installing printers, don't need full administrator capabilities. This isn't done very often, however. Second, people and assets may be divided up into domains with unique administrators, and trust can be passed down from one domain to the next or both. In a typical big firm, all users may be placed in a personnel domain run by Human Resources, while resources like servers and printers would be in resource domains under departmental administration; individual workstations might even be run by their users [8]–[11].

CONCLUSION

In a system, access control techniques may be used at several levels, from applications via middleware to the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

operating system and hardware. Higher level mechanisms have the potential to be more expressive but also have a tendency to be more attackable for a range of causes, from inherent complexity to implementer skill levels. The majority of attacks involve the opportunistic use of faults, and highly big, very extensively used, or both software items (such as operating systems and databases) are more prone to have security flaws discovered and made public. Systems at all levels are susceptible to environmental changes that call into question the underlying presumptions that guided their design.

Access control's primary purpose is to reduce the potential harm that may be caused by certain groups, users, and programs, whether unintentionally or on purpose. The two most significant real-world examples are Unix and Windows, both of which have many characteristics but Windows is more expressive. Database products are often significantly more expressive (and hence even more challenging to deploy safely). Access control is a crucial component of the design of hardware intended for a specific purpose, such as smartcards and other encryption tools. In order to reduce the frequency of implementation flaws, such as stack overflow assaults, new strategies are being developed. However, new attacks are constantly being discovered, and the general dependability of big software systems only slowly increases. The fundamental principles of access control, such as read, write, and execute permissions as well as groups and roles, will recur often. They may not be readily apparent in certain distributed systems since the underlying mechanics could be completely different. An example comes from public key infrastructures, which are a new application of the capacity, an antiquated access control idea. The fundamental processes (and their issues) are widespread, however.

REFERENCES

[1] M. Uddin, S. Islam, And A. Al-Nemrat, "A Dynamic Access Control Model Using Authorising Workflow And Task-Role-Based Access Control," *Ieee Access*, 2019, Doi: 10.1109/Access.2019.2947377.

[2] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, And J. Wan, "Smart Contract-Based Access Control For The Internet Of Things," *Ieee Internet Things J.*, 2019, Doi: 10.1109/Jiot.2018.2847705.

[3] S. Ravidas, A. Lekidis, F. Paci, And N. Zannone, "Access Control In Internet-Of-Things: A Survey," *J. Netw. Comput. Appl.*, 2019, Doi: 10.1016/J.Jnca.2019.06.017.

[4] S. Wang, X. Wang, And Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based On Blockchain," *Ieee Access*, 2019, Doi: 10.1109/Access.2019.2929205.

[5] P. Colombo And E. Ferrari, "Access Control Technologies For Big Data Management Systems: Literature Review And Future Trends," *Cybersecurity*, 2019, Doi: 10.1186/S42400-018-0020-9.

[6] K. Riad, R. Hamza, And H. Yan, "Sensitive And Energetic Iot Access Control For Managing Cloud Electronic Health Records," *Ieee Access*, 2019, Doi: 10.1109/Access.2019.2926354.

[7] J. S. Shi And R. Li, "Survey Of Blockchain Access Control In Internet Of Things," *Ruan Jian Xue Bao/Journal Of Software*. 2019. Doi: 10.13328/J.Cnki.Jos.005740.

[8] N. Paladi And C. Gehrmann, "Sdn Access Control For The Masses," *Comput. Secur.*, 2019, Doi: 10.1016/J.Cose.2018.10.003.

[9] Y. Wang, L. Tian, And Z. Chen, "Game Analysis Of Access Control Based On User Behavior Trust," *Inf.*, 2019, Doi: 10.3390/Info10040132.

[10] A. Di Liu, X. H. Du, N. Wang, And S. Z. Li, "Blockchain-Based Access Control Mechanism For Big Data," *Ruan Jian Xue Bao/Journal Softw.*, 2019, Doi: 10.13328/J.Cnki.Jos.005771.

[11] S. Figueroa, J. Añorga, And S. Arrizabalaga, "An Attribute-Based Access Control Model In Rfid Systems Based On Blockchain Decentralized Applications For Healthcare Environments," *Computers*, 2019, Doi: 10.3390/Computers8030057.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Analysis of Cryptography

Mr. Gangaraju
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-gangaraju@presidencyuniversity.in

ABSTRACT: ***In order to safeguard sensitive data, enable secure communication, and preserve information's secrecy, integrity, and authenticity, cryptography plays a crucial role in security engineering. This abstract gives a general introduction of cryptography within the framework of security engineering and examines its fundamental ideas, algorithms, and protocols as well as how they are used to protect digital systems and communications. The abstract opens with a definition of cryptography and its role in contemporary security procedures. It draws attention to the fundamental goals of cryptography, including non-repudiation, secrecy, and integrity. The contrast between symmetric and asymmetric (public-key) cryptography, as well as its unique advantages and applications, is covered in the abstract. The introduction then looks at a variety of cryptographic methods that are often used in security engineering. It includes symmetric encryption methods like Triple DES (3DES), Data Encryption Standard (DES), and Advanced Encryption Standard (AES). Additionally covered are asymmetric encryption techniques like Diffie-Hellman key exchange, Rivest-Shamir-Adleman, and RSA. Their mathematical roots, security characteristics, and key management issues are all mentioned in the abstract.***

KEYWORDS: ***Algorithms, Cryptography, Oracle Model, Protocols.***

INTRODUCTION

The intersection between security engineering and mathematics is cryptography. It gives us the resources needed to support the majority of contemporary security standards. It is surprisingly hard to get correctly, while being the most important enabling technology for safeguarding dispersed systems [1]–[3]. Cryptography has often been used to protect the wrong things or to protect them in the wrong ways, as we previously saw, "Protocols." When we begin examining actual applications in depth, we'll see a tonne more instances. Sadly, for the last 25 years, there has been a growing gap between the worlds of computer security and cryptology. Both security experts and crypto experts often lack a thorough understanding of the issues that exist in the actual world. This is due to a variety of factors, including disparate

professional backgrounds mathematics vs computer science and financing sources governments have attempted to support computer security research while stifling cryptography. It makes me think of a tale a physician buddy once told me. When she was young, she spent a few years working in a nation where the length of medical degrees had been cut for economic reasons in favour of generating experts as rapidly as feasible. One day, a woman who was waiting for a kidney transplant and had had both of her kidneys removed wanted to have her dialysis shunt replaced. The doctor discharged the patient back to the lack of a recorded urinalysis, theatre. He just had no idea that a person without kidneys could not excrete pee. A security engineer must be knowledgeable in cryptology as well as computer security among other things, just as a doctor must be conversant in physiology and surgery. The target audience for this chapter is non-cryptographers; experienced cryptologists won't learn anything new from it. I won't go into much of the mathematics since I only have a few hundred pages and a full presentation of current cryptography would take thousands see the conclusion of the chapter for more reading. I'll simply go through the fundamental notions and constructs that appear to be confusing the most. I highly advise reading a tonne more about cryptography and consulting some actual professionals if you have to utilise it in anything like a new method. In a keynote address at Crypto 2007, the security engineer Paul Kocher said that any cryptocurrency product created by "any company that doesn't employ someone in this room" might be expected to be broken. That has a decent amount of validity.

People who work in computer security often want non-mathematical descriptions of cryptographic jargon. According to standard nomenclature, cryptography and cryptanalysis are the science and art of creating cyphers, respectively, while cryptology often abbreviated as simply crypto is the study of both. The result of an encryption

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

process is known as ciphertext, whereas the input is often referred to as plaintext. After then, things start to become a little trickier. Numerous cryptographic primitives exist. These fundamental building blocks include hash functions, block cyphers, and stream cyphers. Block cyphers may either have different keys for encryption and decryption, in which case they are known as public-key or asymmetric block cyphers, or they can have a single key for both encryption and decryption, in which case they are known as shared-key (also known as secret-key or symmetric). A specific kind of asymmetric crypto primitive is a digital signature system. I'll first provide some straightforward historical examples in the next sections of this chapter to help clarify the fundamental ideas. I'll next introduce the random oracle model, which many cryptologists utilise, in an effort to clarify concepts. Finally, I'll demonstrate some of the most significant cryptographic algorithms in action and how they might be applied to data security.

DISCUSSION

The Random Oracle Model

I want to spend a few pages clarifying the concepts of the many kinds of cypher before getting into the specific design of contemporary cyphers. Readers who have a fear of theoretical computer science should avoid this part at first [4]–[7]. I included it since many new research publications on cryptography need a basic understanding of the nomenclature of random oracles.

The random oracle model aims to formalise the notion that a cypher is "good" if, when seen in the right manner, it is identical to a certain kind of random function. If a cryptographic primitive satisfies all the statistical and other criteria that a random function of the right kind would pass, regardless of the computing model we are employing, I will refer to it as pseudorandom. The cryptographic primitive will actually be an algorithm, implemented as a hardware or software program or array of gates, but given the type and number of tests that our computation model supports, the outputs should 'look random' in that they are identical to a suitable random oracle.

By doing this, we may attempt to distinguish between the challenge of creating cyphers and the challenge of employing them effectively. The pseudorandomness of the cyphers created by mathematicians may be shown. Separately, a computer scientist may attempt to demonstrate the security of a cryptographic protocol on the premise that the crypto primitives used to create it are pseudorandom. As shown by the demonstrations of the validity of the protocol, the procedure is not perfect. Theorems may include errors, much like programs, and the issue may have been idealised incorrectly. Additionally, mathematicians and computer scientists may have differing models for how computing works. In fact, the value of formal models and proofs is now up for dispute among cryptologists. But the study of cryptography may help us better grasp how cyphers operate and how to utilise them securely.

A random oracle might be seen as an elf sitting within a black box that contains a source of physical randomness and some kind of storage, which in our illustration are the dice and the scroll. A certain form of input will be accepted by the elf, who will then check the scroll to determine whether the question has already been addressed. If so, it will provide the solution it discovers there; if not, it will roll the dice to provide a solution at random. We'll further suppose that there is some kind of bandwidth restriction and that the elf can only respond to a certain number of requests per second. This ideal will be helpful in improving our understanding of digital signature algorithms, block cyphers, hash functions, stream cyphers, and hash functions.

Finally, by highlighting that encryption may be used to safeguard data both locally and remotely, we can simplify our conceptual model in a helpful way. A nice illustration is when we encrypt data before putting it in a third-party backup service and then have the option of decrypting it afterwards in the event of a disc disaster. Instead of requiring an encryption/decryption device at each end of a communications channel, we just need one in this scenario. Let's suppose for the sake of simplicity that this kind of application is what we are replicating here. The user inserts a diskette into the cypher machine, enters a key, gives a command, and the contents are appropriately altered. She returns a year later to have the data validated and encrypted. We'll now take a closer look at this paradigm for various cryptographic primitives.

1. **Random Functions —**

Hash Functions: The random function is the first category of random oracle. An input string of any length may be sent into a random function, which returns a random string of a predetermined length, such as n bits. The elf therefore has a straightforward set of inputs and outputs that continuously expands as it operates. (We'll assume that all requests are answered in a consistent amount of time and disregard any scroll size impacts.)

We model one-way functions, often known as cryptographic hash functions, which have a wide range of applications. As I indicated in the chapter on security protocols, they were originally employed in computer systems for the one-way

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

encryption of passwords in the 1960s and are still used in a variety of authentication systems today. In forensic applications, they are used to calculate checksums on files. Given a computer seized from a suspect, you may compute the hash values of the files to determine which files are well-known (like system files) and which are new (like user data). Since hash values vary if a file is damaged, they may also be used to verify the integrity of files. Hashes are often referred to as message digests in messaging applications; given a message M, we may put it through a pseudorandom function to get a digest, say h(M), which can substitute for the message in several applications. Digital signatures are one example. Since signature algorithms are often sluggish for big messages, it is generally more convenient to sign a message digest rather than the message itself.

The timestamping function has another use. We may submit an electronic document to an online time-stamping service if we need proof that we had it on hand on a certain day. However, if the document is still secret, such as a patentable innovation for which we just need to establish a priority date, we may only submit the message digest to the timestamping service instead of the whole document.

2. Properties:

One-wayness is a random function's primary characteristic. If we know the input x, we can quickly calculate the hash value h(x), but if we don't already know the preimage x, it is highly challenging to locate it given the hash value h(x). (The elf will only choose outputs for specified inputs; not vice versa.) The best an attacker who wishes to invert a random function can accomplish given that the output is random is to keep adding additional inputs until he strikes it fortunate. Contrary to our definition, a pseudorandom function will have the same features or they may be utilised to separate it from a random function. If there are enough potential outputs, it follows that a pseudorandom function will also be a one-way function if the opponent cannot randomly locate the target output, they want. This entails selecting an n-bit value as the output such that the adversary cannot do anything close to 2n calculations.

A second characteristic of pseudorandom functions is that even a small portion of the output will not reveal any information about the input. As a result, the value x may be encrypted in one direction by calculating h(x, k) after concatenating it with a secret key k. However, utilising the hash function in this way for one-way encryption is asking for problems if the hash function isn't sufficiently random. A current example is the authentication process used by GSM mobile phones, which combines a 16-byte base station challenge with a 16-byte secret key known only to the phone to create a 32-byte number, which is then sent through a hash function to get an 11-byte output. The notion is that although someone listening in on the radio connection may get a number of values of the random challenge x and related output from h(x, k), the phone company also knows k and can verify this calculation. Therefore, the eavesdropper can't calculate h(y, k) for a fresh input y or get any information about k. However, the one-way function used by many phone companies is insufficiently one-way, making it possible for the key to be calculated by an eavesdropper who can pose as a base station and send a phone around 150,000 acceptable challenges in exchange for the phone's replies. A third characteristic of pseudorandom functions with suitably lengthy outputs is that collisions—that is, separate messages M1 = M2 with h(M1) = h(M2)—are difficult to locate. The optimal method of determining a collision is to assemble a large collection of messages Mi and their accompanying hashes h(Mi), sort the hashes, and then search for a match, unless the adversary can discover a shortcut approach (which would indicate that the function wasn't really pseudorandom). The number of hashes the adversary will need to calculate before he can reasonably expect to discover a match will be around the square root of this, or 2n/2 hashes, if the output of the hash function is an n-bit integer, meaning that there are 2n potential hash values. Let's take a closer look at this fact as security engineering relies heavily on it.

3. Random Generators

Stream Ciphers: The random generator, commonly referred to as a keystream generator or stream cypher, is the second fundamental cryptographic primitive. Similar to the hash function, this random function likewise has a small input and a lengthy output. (If we had a good pseudorandom function with input and output that were each one billion bits long and we never wanted to handle any objects larger than this, we could turn it into a hash function by erasing all but a small portion of the output and into a stream cypher by padding all but a small portion of the input with a constant.) On a conceptual level, though, it's typical to imagine a stream cypher as a random oracle with a set input length and an extremely long stream of bits that is known as the keystream as the output.

To use it, just go to the keystream generator, insert a key, and obtain a large file of random bits. Combine those random bits with your plaintext data to create ciphertext, which you can then send to your backup contractor. When the elf is given a new key as input, we may imagine that he creates a random tape of the necessary length, produces it, gives it to us, and keeps a duplicate of it on his scroll for reference in case he receives the same key again. If we need

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

to retrieve the data, we simply return to the generator, input the same key, and get the same lengthy file of random data. We then exclusive-or this data with our ciphertext to recover the plaintext data. Without the key, other users of the keystream generator won't be able to produce the same keystream. I previously stated the one-time pad and Shannon's conclusion that a cypher achieves perfect secrecy if and only if there are as many alternative plaintexts as feasible and every key is equally probable. Such security is referred to as unconditional (or statistical) security since it is independent of both the opponent's computational capability and any potential future developments in mathematics that may lead to a cypher attack shortcut. One-time pad systems closely match our theoretical model, with the exception that they are often employed to encrypt interstellar communications than time: a copy of the randomly generated keystream has been exchanged in advance by the two communication parties. A contemporary diplomatic system may employ DVDs, sent in a tamper-evident container in a diplomatic bag, as opposed to Vernam's original telegraph cypher machine, which used punched paper tape. The random generation has been done using a variety of approaches. Marks recalls how tiny elderly women shuffled counters in Oxford to create the silken keys used by SOE agents.

4. Random Permutations

Block Ciphers: The block cypher, which we describe as a random permutation, is the third category of primitives and is the most significant in contemporary commercial cryptography. The input plaintext and the output ciphertext are both of a fixed size, and the function is invertible in this case. Input and output for Playfair are both two characters, however for DES they are both bit strings made up of 64 bits. No matter how many symbols are used or what alphabet is used as a foundation, encryption operates on a block of a certain length. (Therefore, if you wish to encrypt a shorter input, you must pad it, like in our Playfair example with the last 'z'.)

Block encryption may be pictured like follows. The same elf in a box with dice and a scroll is present. This has a column of plaintexts on the left and a column of ciphertexts on the right. The elf examines the left-hand column to see whether it has a record of the message when we want it to be encrypted. If not, it rolls the dice to create an appropriate-sized random ciphertext (which isn't yet visible in the right-hand column of the scroll), and then it enters the plaintext and ciphertext pair in the scroll. If a record is discovered, the right-hand column's associated ciphertext is sent to us.

The elf follows the same procedure when requested to decrypt, but with the columns' functions reversed: he takes the input ciphertext, verifies it (this time on the right-hand scroll), and if he finds it, he provides the message it was previously connected with. If not, he randomly selects a message (that is not already present in the left column) and writes it down [8]–[11]. A keyed family of pseudorandom permutations makes up a block cypher. We have a single permutation for each key that stands alone from all the others. Each key may be considered to correlate to a separate scroll. It seems sense that a cypher machine would produce the ciphertext if given the plaintext and the key, and the plaintext if given the ciphertext and the key, but it wouldn't output anything if given only the plaintext and the ciphertext.

CONCLUSION

We need a precise description of what a cypher accomplishes since many cyphers fail because they are applied incorrectly. The random oracle model offers a helpful intuition: we presumptively assume that each new value supplied by the encryption engine is random in the sense of being statistically independent of all the other outputs observed before. Block cyphers for symmetric key applications may be built by carefully combining replacements and permutations, whereas number theory is used for asymmetric applications like public key encryption and digital signatures. There is a sizable amount of mathematics that applies to both situations. Block cyphers may be used to create stream cyphers and hash functions if they are used in the right operational modes. These have various qualities for integrity protection, pattern concealment, and error propagation. Although there are many subtle things that might go wrong, it is not too difficult to comprehend the fundamental qualities that the security engineer has to be aware of surprisingly difficult to design systems with robustness against component failure (or encouragement of failure) and where the cryptographic processes are seamlessly linked with other security measures like physical security and access control. Later chapters will make frequent references to this.

REFERENCES

[1] M. Raikwar, D. Gligoroski, and K. Kralevska, “SoK of Used Cryptography in Blockchain,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2946983.

[2] M. T. Gençoğlu and M. T. Gençoğlu, “Importance of Cryptography in Information Security,” *ISOR J. Comput. Eng.*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

[3] Z. Khalid, M. Rizwan, A. Shabbir, M. Shabbir, F. Ahmad, and J. Manzoor, "Cloud server security using Bio-cryptography," *Int. J. Adv. Comput. Sci. Appl.*, 2019, doi: 10.14569/IJACSA.2019.0100321.

[4] S. A. Alsuhibany, "Developing a Visual Cryptography Tool for Arabic Text," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2920858.

[5] P. K. Pradhan, S. Rakshit, and S. Datta, "Lattice based cryptography," in *Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019*, 2019. doi: 10.1109/ICCMC.2019.8819706.

[6] A. P. Bhatt and A. Sharma, "Quantum cryptography for internet of things security," *J. Electron. Sci. Technol.*, 2019, doi: 10.11989/JEST.1674-862X.90523016.

[7] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in *IOP Conference Series: Materials Science and Engineering*, 2019. doi: 10.1088/1757-899X/518/5/052003.

[8] A. M. Qadir and N. Varol, "A review paper on cryptography," in *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 2019. doi: 10.1109/ISDFS.2019.8757514.

[9] C. Watt, J. Renner, N. Popescu, S. Cauligi, and D. Stefan, "CT-WASM: Type-driven secure cryptography for the web ecosystem," *Proc. ACM Program. Lang.*, 2019, doi: 10.1145/3290390.

[10] P. Siva Sankaran and V. B. Kirubanand, "Hybrid cryptography security in public cloud using TwoFish and ECC algorithm," *Int. J. Electr. Comput. Eng.*, 2019, doi: 10.11591/ijece.v9i4.pp2578-2584.

[11] A. Di Falco, V. Mazzone, A. Cruz, and A. Fratalocchi, "Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips," *Nat. Commun.*, 2019, doi: 10.1038/s41467-019-13740-y.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Discussion on Distributed Systems

Mr. Aravinda Telagu
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-aravinda@presidencyuniversity.in

ABSTRACT: ***In many fields, distributed systems are essential because they make it possible to handle, store, and transmit enormous volumes of data effectively. To maintain the integrity, confidentiality, and availability of resources, specific security concerns presented by these systems' distributed architecture must be addressed. An overview of the relationship between distributed systems and security engineering is given in this abstract, with an emphasis on essential ideas, difficulties, and methods for reducing security risks. Distributed systems are defined at the outset of the abstract, along with some of its key features, such as decentralized control, many linked nodes, and data dissemination. It highlights the need of strong security controls in distributed contexts where bad actors could take advantage of flaws in network connectivity, data replication, and resource allocation. The abstract then looks at the underlying security issues that distributed systems encounter. These difficulties include distributed denial-of-service (DDoS) attack prevention, secure communication and data transmission, fault tolerance and resilience, privacy protection, and authentication and access management. The abstract addresses how these difficulties affect system scalability, performance, and overall security posture.***

KEYWORDS: ***Concurrency, Deadlock, Distributed Systems, Thread Management.***

INTRODUCTION

In the recent chapters, we've seen how security protocols can be used to authenticate users to systems (and systems to each other); access controls can be used to control which principals can perform which operations in a system; and some of the mechanics of how crypto can be used to support access control in distributed systems. However, establishing access restrictions, protocols, and cryptography is just one part of creating a secure distributed system. There is often a qualitative shift in complexity when systems scale up, and certain issues that are straightforward to handle in a network of just a few computers and principals (such as naming) suddenly become significant [1]–[3].

Researchers in computer science have developed several distributed systems over the last 40 years and investigated topics including concurrency, failure recovery, and naming. A rising corpus of knowledge from business, government, and industry supports the hypothesis. Despite being fundamental to the design of efficient secure systems, these concerns are often addressed poorly. Attacks on security protocols that may be seen as concurrency failures have previously been covered by me. We run a higher risk of a confidentiality breach if we repeat data to make a system fault-tolerant. And naming is a particularly challenging issue. Many governments and organisations are attempting to create bigger, flatter namespaces by employing RFID to identify items and identification cards to identify persons, but in the 1990s, efforts to create viable public key infrastructures were hampered by naming issues.

DISCUSSION

Concurrency

When many processes are active at once, they are said to be concurrent, and this leads to a variety of well-known issues. Processes might use outdated data, make inconsistent updates, or update in the wrong order. The system might also get stuck, and the data in various systems might never converge to a single value. As a result, it can be more difficult than you might think to get things done in the right order or even to know the precise time.

Systems are now quickly increasing their concurrency. First, the scope of internet commerce has expanded quickly; although Google may have begun with four computers, its server farms today number in the hundreds of thousands. Second, technology is growing more sophisticated; nowadays, a premium automobile

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

might have over forty separate processors [4]–[7]. Third, the parts are becoming more intricate. For example, your computer's microprocessor may already have two, four, or even more CPU cores, and it will likely have even more in the future. Likewise, your graphics card, disc controller, and other peripherals all have their own processors. Additionally, a few actual CPUs may be converted into hundreds or even thousands of virtual CPUs using virtualization technologies like VMware and Xen.

Concurrent system programming is challenging, and sadly, the majority of textbook examples come from the relatively specialised fields of operating system internals and thread management. Concurrency control, however, also raises security concerns. It exists to stop users from interfering with one another, whether unintentionally or on purpose, similar to access control. Concurrency issues may also arise at several system levels, from the hardware all the way up to the business environment. I provide some specific instances of how concurrency affects security in what follows. These are in no way all-inclusive.

1. Using Old Data Versus Paying to Propagate State:

Two kind of concurrency problems have previously been discussed. The first kind of attack involves replaying protocols in order to pass off outdated credentials. Then there are racial conditions. I spoke about the'mkdir' vulnerability from Unix, which allowed for a midway attack on a privileged instruction that is performed in two parts by renaming an object on which it operates. There have long been issues like this.

In one of the earliest multiuser operating systems, IBM's OS/360, when a file was attempted to be opened, its permissions were verified, and if the user was permitted access, the file was read once more. A time-of-check-to-time-of-use (TOCTTOU) attack uses instances like these. There Systematic methods of detecting such assaults in file systems exist, but as our infrastructure gets more concurrent, attacks appear at other levels, such as system calls in virtualized settings, which may call for other methods. At the level of business logic, they are also present. It's not always cost-effective to prevent them since it might be costly to propagate changes in security status.

For instance, the banking sector maintains a list of all hot credit cards (whether they have been stolen or used fraudulently), but due to the millions of them in circulation worldwide, it is not feasible to keep a complete list of hot cards in every merchant terminal, and it would be too costly to verify every transaction with the bank that issued the card. There are several stages of stand-in processing instead. Terminals are permitted to process transactions up to a predetermined limit (the floor limit) offline; larger transactions require online verification with a local bank, which will be aware of all the local hot cards as well as foreign cards that are actively being abused; above another limit, there may be a reference to an organisation such as VISA with a larger international list; and the largest transactions may require a reference to the card issuer. Effectively, only local or significant transactions are validated before being used.

The main systems that control the spread of security state globally are credit card systems, and they are intriguing because they operate on the assumption that most occurrences are local, of low importance, or both. We learned from them that it was costly to swiftly and globally revoke compromised credentials. When building infrastructures of public key certificates in the 1990s to support everything from web commerce to corporate networks, there was concern that the biggest cost would be revoking the credentials of principals who moved, changed jobs, had their private keys compromised, or were fired. In general, this turned out to be untrue1. Large online services are another example of the expenses associated with revocation. It would be costly to verify a user's credentials against a database each time she visited one of the service's thousands of computers. Using cookies to provide the user with an encrypted credential that her browser automatically displays on each visit is a frequent technique. In this manner, just the key has to be distributed across the several computers making up the server farm. A different way must be discovered to achieve this, however, if promptly revoking users is crucial to the program.

2. Locking to Prevent Inconsistent Updates:

When many individuals are working on a document at once, a version control system may be used to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

guarantee that only one person has written access to any particular section of the document at any one moment. This demonstrates the value of locking as a means of controlling congestion for resources like filesystems and lowering the possibility of conflicting changes. A server may store a list of all clients who depend on it for security status and alert them when the state changes. Callback is another approach.

Additionally important in secure distributed systems are locking and callback. Another example is provided by credit cards. If a guest checks in at my hotel using a credit card, I approach the card company for a pre-authorization, which notifies them that I may wish to make a debit transaction in the near future. I may then make a claim on "up to $500" of the guest's available credit. Her bank may contact me and ask that I notify the police if the card is revoked the next day or urge her to pay with cash. Depending on the kind of contract I was able to negotiate with my bank, I may or may not have been given a money guarantee. This is an example of how to do resilient authorisation in distributed systems using the publish-register-notify approach (of which there is a more detailed discussion in). However, callback systems are not a perfect solution. The issuer of the credentials may not wish to operate a callback service, and the client could object out of respect for her privacy to the issuer being informed of all her comings and goings. Take passports as an example. Government ID is needed in many nations for a variety of transactions, yet governments seldom provide any assurances, and the majority of people would protest if the government kept track of each time an ID paper was shown. In fact, one of the common criticisms of the British government's plan for biometric ID cards is that verifying a person's fingerprints against a database each time they present their ID would leave a trail of every location the card was used. In general, there is a difference between identification documents like credit cards that, upon use, impose some responsibility on the issuer and other documents like passports. The significance of the updates' chronological sequence is one of the variances.

3. The Order of Updates:

The sequence in which two transactions are applied may not be important if they arrive in the government's bank account as a credit of $500,000 and a debit of $400,000, for example. However, the order will significantly influence the result if they are delivered to my bank account. In actuality, there is no simple answer to the issue of choosing the order in which transactions are implemented. It is strongly tied to the issue of how to parallelize a computation, and a large portion of the art of creating effective distributed systems consists in structuring things such that operations are either simply sequential or entirely parallel.

Retail checking account systems often batch transactions throughout the course of the night and apply all credits to each account before applying all debits. Before the nighttime reconciliation, inputs from machines like ATMs and check sorters are first bulked up into journals. Payments that bounce must then be reversed out as an unavoidable side effect, and in the case of ATM and other transactions where cash has already been disbursed, clients may wind up borrowing money without consent. In reality, chains of unsuccessful payments end, even if this isn't always the case in principle. Real-time gross settlement, in which transactions are recorded in order of arrival, is being used by several interbank payment methods. The drawback of this is that network whimsy may affect the conclusion.

There isn't much consensus on which practice is preferable, but some individuals believed this would reduce the systemic danger that a nonterminating payment chain may bring down the global financial system. Credit limits are managed by credit cards using a hybrid of the two systems, with each authorisation reducing the available credit limit while settlement is managed similarly to a bank account. The drawback of this is that a store may lock up your card by requesting a hefty pre-authorization. The community of parallel systems has lately conducted research on the checking-account technique. Disconnected apps are supposed to provide hesitant update transactions that are afterwards applied to a master copy. Instability may be avoided via a variety of strategies; methods for tentative updating, such those found in bank journals, are crucial.

Application-level sanity checks are crucial; banks are aware of the daily net payment settlement amounts they should anticipate to pay one other, and big cash

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

flows are validated. The sequence in which transactions arrive is substantially less significant in other systems. An illustration would be passports. The sequence in which visas are stamped on passports is unimportant; only their creation and expiry dates are taken into consideration. (There are few outliers, like the Arab nations who won't allow you in if your passport has an Israeli stamp, but the majority of pure identification systems are stateless.)

4. Deadlock:

The issue of deadlock is another. Due to the fact that two systems are waiting for each other to move first, anything might go wrong. The dining philosophers' dilemma, in which many philosophers are sitting around a table, is a well-known example of a stalemate. Each philosopher has a chopstick in between them, and he can only eat when he can take the two chopsticks on each side. If they all attempt to eat at once and each takes up (let's say) the chopstick on his right, a deadlock may result. In a famous study by Dijkstra, this issue and the strategies that may be employed to prevent it are discussed. When you have several lock hierarchies spread across various systems, some of which fail particularly when failures might indicate that the locks are unreliable, things can become quite complicated. The subject has been extensively discussed in the literature on distributed systems.

However, it is not merely a technological issue; business operations often include Catch-22 circumstances. There may be a workaround for the catch as long as the procedure remains manual, however once it is put into software, this alternative may not be accessible anymore. The fudge can sometimes not be removed. The battle of the forms is a well-known business issue when one firm issues an order with its own conditions attached, another company accepts it according to its own requirements, and trade continues without any understanding of whose conditions control the contract. Only if anything goes wrong and the two firms wind up in court will the dispute be settled; even then, one company's conditions may specify an American court while the other's may specify an English court. As trade grows increasingly computerised, it seems that problems like this will only become worse.

5. Non-Convergent State:

The "motherhood and apple pie" of building protocols to update the state of a distributed system is ACID, which states that transactions should be atomic, consistent, isolated, and durable. If you "do it all or not at all," then a transaction is atomic, which makes it simpler to restore the system after a failure. If some invariant is maintained, such as the requirement that the books remain balance, it is consistent. This is a standard practice in banking systems, and it is accomplished by mandating that every credit to one account be matched by an equal and opposite debit to another (I'll go into more detail about this in Chapter 10, "Banking and Bookkeeping"). Transactions are isolated if they seem the same to each other, or if they can be serialised. They are also durable if they cannot be undone after they have been completed.

These qualities may be both insufficient and excessive. On the one hand, each of these has the potential to fail or be attacked in a variety of sneaky ways; on the other hand, designing the system to be convergent is often sufficient. This indicates that ultimately there would be a constant condition across if the transaction volume were to decline. In order to ensure convergence, semantic methods like timestamps and version numbers are often used; in cases where transactions are added to files rather than rewritten, this is frequently sufficient.

In reality, however, you also need to know how to deal with things that go wrong and aren't entirely fixable. A security or audit manager's job might include a never-ending struggle with entropy since there are often apparent deficiencies (and surpluses) that are difficult to explain. Payment gateways often have to make educated guesses about data in order to make things work, for instance, since various national systems have different assumptions about whether fields in bank transaction records are necessary or optional. Sometimes they make the erroneous assumptions, and other times, individuals identify and take advantage of flaws that aren't fully recognised for a very long time, if ever. By adding a corrective factor, referred to as something like "branch differences," and establishing a goal for maintaining it below a certain yearly level, things are ultimately fudged [7]–[10].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Fault Tolerance and Failure Recovery

Even while failure recovery is often the most crucial component of security engineering, it is also one of the most ignored. Since many years ago, authenticity and integrity and secrecy have dominated research articles on computer security, with availability receiving less attention. However, a typical bank's real expenses are the opposite. A third or so of total IT expenses may be spent on availability and recovery techniques, such as hot standby processing sites and multiple redundant networks; a small percentage is spent on integrity techniques, like internal audit; and a negligible sum is spent on confidentiality techniques, like encryption boxes. You'll discover as you read this book that many additional applications, including as burglar alarms, electronic warfare, and safeguarding a business from service denial assaults on the Internet, are basically about availability.

A significant portion of the security engineer's duties include fault tolerance and failure recovery. Traditional fault tolerance is often built on locking and logging techniques, and it becomes far more difficult to implement when it must survive malicious assaults on these mechanisms. The failure model, the kind of resilience, the location of redundancy utilised to supply it, and defence against service denial assaults are just a few of the ways fault tolerance interacts with security. I'll use the definitions below: A failure is a departure from the system's intended behaviour and may result from a defect, which can result in an error, which is an inaccurate condition. Several elements, such as fault detection, error recovery, and failure recovery if required, will be included in the resilience we design into a system to tolerate flaws and recover from failures. It should be clear what mean-time-before-failure (MTBF) and mean-time-to-repair (MTTR) imply.

CONCLUSION

Because their creators disregarded the fundamental principles of how to construct and how not to build distributed systems, many secure distributed systems have incurred significant expenses or acquired critical flaws. The majority of these lessons remain true, and there are yet more to be learned. Concurrency failures of one sort or another cause a significant portion of security lapses; systems utilise outdated data, perform changes inconsistently or in the incorrect sequence, or presume that data is consistent when it isn't possible or possible for it to be.

It's more difficult than it seems to know when to act. It's crucial to have fault tolerance and failure recovery. For many businesses, the major goal of the protection budget is to provide the capacity to recover from security failures and sporadic physical calamities. Technically speaking, resilience and protective measures interact in important ways. Byzantine failure, when flawed systems cooperate instead than failing randomly, is a problem that affects the cryptographic technologies we use. Redundancy comes in a variety of flavors, and we must utilise the proper blend. We need to safeguard against purposeful efforts to disrupt service, which often form a component of bigger attack strategies, in addition to protecting against errors and attempted manipulation.

A name may also cause a lot of issues when it is overused or when assumptions are made about it that are untrue outside of a certain system, culture, or legal area. For instance, it should be allowed to cancel a user's user name and withdraw their access to a system without fear of being sued since other functions were also cancelled. Often, the easiest answer is to provide each principle a special identification number that is only used for that purpose, like a bank account number or a system login name. But when two systems that utilise naming methods that are incompatible for any reason are combined, various issues occur. When two systems employ a same combination, such "name plus date of birth," to monitor people but do so in separate ways, this merger may sometimes even occur accidentally.

REFERENCES

[1] Q. Jia, L. Guo, Y. Fang, And G. Wang, “Efficient Privacy-Preserving Machine Learning In Hierarchical Distributed System,” *Ieee Trans. Netw. Sci. Eng.*, 2019, Doi: 10.1109/Tnse.2018.2859420.

[2] S. A. Hamid, R. A. Abdalrahman, I. A. Lafta, And I. Al Barazanchi, “Web Services Architecture Model To Support Distributed Systems,” *Xinan Jiaotong Daxue Xuebao/Journal Southwest Jiaotong Univ.*, 2019, Doi: 10.35741/Issn.0258-2724.54.6.4.

[3] E. Michael, D. Woos, T. Anderson, M. D. Ernst, And Z. Tatlock, “Teaching Rigorous Distributed

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Systems With Efficient Model Checking," In *Proceedings Of The 14th Eurosys Conference 2019*, 2019. Doi: 10.1145/3302424.3303947.

[4] F. N. Al-Wesabi, H. G. Iskandar, And M. M. Ghilan, "Improving Performance In Component Based Distributed Systems," *Eai Endorsed Trans. Scalable Inf. Syst.*, 2019, Doi: 10.4108/Eai.13-7-2018.159357.

[5] M. Ali And S. Bagchi, "Probabilistic Normed Load Monitoring In Large Scale Distributed Systems Using Mobile Agents," *Futur. Gener. Comput. Syst.*, 2019, Doi: 10.1016/J.Future.2019.01.053.

[6] K. Chaitanya, K. R. Rao, And J. K. R. Sastry, "A Framework For Testing Distributed Embedded Systems," *Int. J. Adv. Trends Comput. Sci. Eng.*, 2019, Doi: 10.30534/Ijatcse/2019/30842019.

[7] C. F. Cheng And K. T. Tsai, "A Flexible Consensus Protocol For Distributed Systems," *Ieee Access*, 2019, Doi: 10.1109/Access.2019.2926888.

[8] W. S. Ocaña, A. M. Abata, E. S. Jácome, And V. M. Mora, "Distributed Systems And Industrial Communication Networks With The Internet Of Things, Aimed At Industry 4.0," *Int. Rev. Autom. Control*, 2019, Doi: 10.15866/Ireaco.V12i5.17687.

[9] C. Muriana, G. Gilia, V. Mistretta, T. Piazza, And G. B. Vizzini, "A Distributed Integration System Enabling Electronic Health Records: An Italian Experience," *Int. J. Med. Eng. Inform.*, 2019, Doi: 10.1504/Ijmei.2019.096889.

[10] F. Myter, C. Scholliers, And W. De Meuter, "Distributed Reactive Programming For Reactive Distributed Systems," *Art, Sci. Eng. Program.*, 2019, Doi: 10.22152/Programming-Journal.Org/2019/3/5.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Discussion on the Aspects of Economics

Mr. B Muralidhar
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-muralidhar@presidencyuniversity.in

ABSTRACT: ***The cost-benefit analysis, incentives, and decision-making processes that affect the design, deployment, and maintenance of secure systems are influenced by economics, which is a significant component of security engineering. The main ideas, difficulties, and uses of economic thinking in the subject of security are highlighted in this abstract, which examines the junction of economics and security engineering. The necessity of economics in comprehending security-related issues is emphasized in the abstract's first paragraph. It emphasizes the significance of risk management and the trade-offs between the costs of security measures and their benefits. In the security context, it also highlights the financial incentives and motives that drive both attackers and defenders. The abstract continues by exploring the idea of cost-benefit analysis and how it relates to security engineering. It looks at how economic analysis may calculate possible damages from security breaches, assess the efficacy of security solutions, and direct choices about how to allocate resources. The notion of the security ROI (Return on Investment) and its significance in helping investors make well-informed judgments regarding security investments are covered in the abstract.***

KEYWORDS: ***Classical Economics, Incentives, Security Engineer, System Designer.***

INTRODUCTION

Recently, the study of information security economics has flourished and advanced quickly. Around 2000, we began to discover that many security system failures weren't caused by technological flaws as much as they were because of improper incentives. The classic example is when the individuals who maintain a system are not the ones who suffer when it malfunctions. Security features are often purposefully created to transfer responsibility, which frequently causes problems [1]–[3].

At the most basic level of cost accounting, economics has always been significant to engineering. A successful engineer was one who could construct a bridge securely with 1,000 tonnes of concrete while everyone else needed 2,000 tonnes. However, the perverse incentives that develop in large systems with various owners make economic concerns for the security engineer both more significant and complicated. We expect that selfish local activities will lead to acceptable global results because really global systems, like the Internet, are the product of the actions of millions of autonomous principals with different interests.

In general, individuals need an incentive to act, else they won't. Markets are often the greatest indicator of what kinds of processes succeed or fail that we have. Markets may sometimes fail; monopolies have plagued the computer industry from the beginning. The causes of this are now known, and they are beginning to interact with security. Now that we have a principled response to provide in place of merely criticising Redmond as a result of poor weather when someone asks "Why is Microsoft software insecure?" The emerging discipline of security economics offers insightful information not just on 'security' issues like privacy, bugs, spam, and phishing but also on more general concerns like system reliability. What is, for instance, the ideal split between programrs' and testers' efforts? also allows us to assess the policy challenges raised by security technologies, such as those relating to digital rights management. Questions of competition law and consumer rights arise when protective measures are employed by the system designer to control the owner of a machine rather than to defend her against external opponents. Economics

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

offers the framework for these discussions. The harmony between public and private activity is also under doubt. Similar to air pollution or traffic congestion, users who connect unsecured gadgets to the Internet do not always face the full costs of their activities. What proportion of the protection effort may or should be carried by people, and what proportion by businesses, authorities, or law enforcement?

DISCUSSION

Classical Economics

The study of modern economics spans a wide range of behavioural features of people. It is heavily influenced by microeconomics and game theory, and portions of it so far have found use in security [3]–[5]. In this part, I'll briefly review the most important concepts from microeconomics before moving on to talk about game theory. Instead of serving as an introduction to economics or even information economics, as I would recommend you do by reading Carl Shapiro and Hal Varian's book "Information Rules", the exercise's goal is to acquaint you with the key concepts and terminology so that we can discuss security economics.

When the industrial revolution and expanding commerce altered the globe in the 18th century, people sought to understand why. This is when the modern topic emerged. The famous work "The Wealth of Nations" by Adam Smith, published in 1776, served as a first draught, outlining how rational self-interest in a free-market system produces economic prosperity. Every degree of specialisation increases productivity, from a tiny factory to global commerce, and development is driven by the self-interested striving of many people and businesses because people need to make goods that others value in order to live in a cutthroat market. He said in his well-known quote that "It is not from the goodness of the butcher, the brewer, or the baker, that we can expect our dinner, but from their regard to their own interest."

These concepts were developed by economists of the nineteenth century. David Ricardo strengthened and clarified Adam Smith's pro-free trade arguments, Stanley Jevons, Leon Walras, and Carl Menger built intricate supply and demand models, and by the end of the century Alfred Marshall had combined supply and demand models in markets for goods, labour, and capital into a comprehensive "classical" model in which, at equilibrium, all the excess profits would be competed away. By demonstrating that markets provide efficient results under specific circumstances in 1948, Kenneth Arrow and Gerard Debreu had established this on a solid mathematical basis. The situations in which these prerequisites aren't satisfied, leading to monopolies and other issues, are a big part of what makes economics interesting, particularly to those in the computer industry and security experts in particular.

Monopoly: To get a quick introduction to the topic, think of a classic example of monopoly. Imagine there is a demand for flats in a university town where the students come from various socioeconomic backgrounds. We could have one wealthy student who can afford to pay $4000 per month, 300 individuals who are willing to pay $2000 per month, and (to round things out) 1000 others who are ready to spend $1000 per month. That gives us the demand curve shown in Figure 1 below.

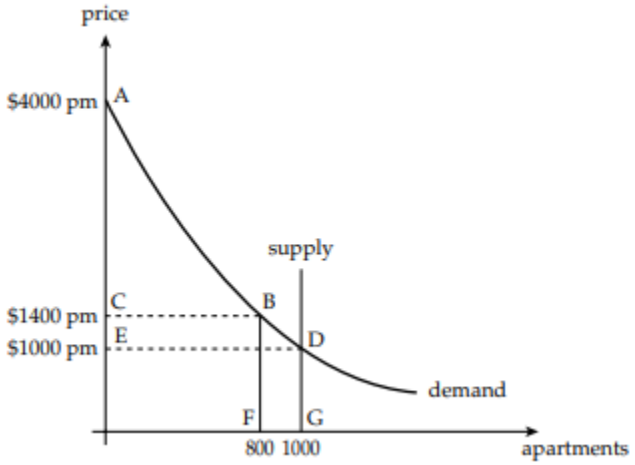

Figure 1: Illustrate the market for apartments.

As a result, if there are 1000 flats being rented out by several rival landlords, the market-clearing price will be $1000, which is where the demand curve and the vertical supply curve connect. Imagine, though, that

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

the market is rigged. Perhaps the landlords have formed a cartel, or perhaps the institution requires its students to rent via a connected agency. Let's suppose a single monopolist landlord for the sake of simplicity. When he looks at the demand curve, he realises that he can earn $1400 per month for each of the 800 flats he rents out.

800 times $1400 now is $1,120,000 per month, which is more than the $1 million per month he would earn at the market price of $1,000. (Economists claim that CBFO, not EDGO, is his "revenue box.") He thus sets an inflated price, and 200 flats are left vacant. The Italian economist Vilfredo Pareto created a clever approach to formalise this inefficiency. Any adjustment that might benefit some individuals without harming anybody else is known as a Pareto improvement, and an allocation is Pareto efficient if no Pareto improvements are possible. The allocation in this case is inefficient since the monopolist might rent out one unoccupied flat to anybody for less money, benefiting both him and them. Now, Pareto efficiency is a somewhat flimsy standard; both the ideal forms of communism in which everyone receives the equal income and dictatorships in which the President receives all money are Pareto-efficient. You cannot improve anyone's situation without also impairing someone else in either scenario. Even in this extremely weak sense, the basic monopoly presented here is inefficient [6]–[8].

So, what is the monopolist's option? One option is that he could set each student's rent at the precise amount they are willing to pay if he could charge various prices to different people. Such a landlord is referred to be a discriminating monopolist; he exacts $4000 from the wealthy student and $1000 from the 1000th student. The same students get flats as previously, but practically everyone is in worse financial shape. The wealthy student loses $3,000, which is money that he was prepared to pay but previously didn't have to; economists refer to this excess as money that was saved. In actuality, the discriminating monopolist is successful in capturing the whole consumer surplus.

Since ancient times, merchants have attempted to price discriminate. This game is being played by the carpet merchant in Damascus who promises to "make a very special price, just for you," by Microsoft when it provides seven distinct versions of Vista at various price points, and by airlines when they sell first, business, and cattle class tickets. The degree to which businesses are able to accomplish this is influenced by a variety of variables, but mostly by their market strength and the quantity of information they possess. A merchant's market power indicates how near he or she is to having a monopoly; in a situation of perfect competition, a merchant merely needs to accept the price that the market decides upon he or she is a price taker. One of the primary elements undermining privacy in the contemporary world is technology's tendency to strengthen market power while simultaneously lowering the cost of consumer information.

Public Goods: When everyone receives the same amount of a product, whether or not they desire it, this is a second sort of market failure. Examples from the past include scientific research, national defence, and air quality. These are what economists refer to as public goods, and the technical definition is that they are products that are non-rivalrous using them doesn't mean there's less available for you and non-excludable there isn't a workable means to prevent others from eating them. In general, uncoordinated markets are unable to provide enough public goods to meet societal needs. Governments may directly provide public goods like national defence or they can use covert means like market coordination to do so. The classic example is how copyright and patent laws provide creators of inventions, literary works, and musical compositions a temporary monopoly, rendering the products in issue excludable for a certain amount of time. Public goods are frequently provided through a combination of public and private action; scientific research is carried out in universities that receive some public funding, some revenue from student fees, and some research contracts from business where business may receive patents on the useful inventions while the underlying scientific research is made publicly available for use. The mix can be contentious; the debate on global warming pits

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

those who support direct government action in the form of a "carbon tax" which would be simple and easy to enforce against those who support a "cap and trade" system where firms and countries can trade licences to emit carbon which, in a perfect world, would cause emission reductions by the firms who could do so most cheaply, but which may well be more open to abuse and evasion.

Since many components of security are considered to be public goods, this is significant to us. I don't have an anti-aircraft gun on my roof because government intervention is the most effective way to deal with air defence threats, which originate from a limited number of people. So, what about online safety? There are undoubtedly significant externalities at play, and just as with those who burn polluting coal fires, those who connect unsecure computers to the Internet end up shifting costs to others. What should we do in response, then? One might see a tax on vulnerabilities being imposed by the government, with awards going to researchers who find them and heftier penalties going to the companies whose software they were found in. Once again, one of the first publications on security economics proposed a vulnerability cap-and-trade system, wherein software suppliers who could not be bothered to make their software safe could purchase permits from other software manufacturers who were making the effort to tighten up their goods. The proponents of free software would oppose both configurations. Is air defence or air pollution the better analogue, though? A lot of tiny actors used to be the source of threats like viruses and spam, but starting about 2004, as malware authors and users have become commercial, we've seen a lot more consolidation. By 2007, there were so few malicious spammers that ISPs no longer saw substantial variations in

There is no longer a rule of huge numbers that governs spam levels since the major spammers undertake specific campaigns [. This proposes an alternative maybe a more concentrated method. State action may be required today, as it was then, if our air defence danger in 1987 came mostly from the Russian air force, and our cyber defence threat in 2007 comes primarily from a small number of Russian gangs, who are inflicting significant costs on US and European Internet users and businesses. Our governments might exert pressure on the Russians to apprehend and imprison their cyber-gangsters instead of asking us to purchase antivirus software. I'll go into more depth about this in Part III, but for now it should be evident that ideas like "monopoly" and "public goods" are crucial to the security engineer and really to everyone who works in IT. Just consider the top two desktop and server operating systems in use today: Linux and OpenBSD are widespread Unix systems that are maintained by volunteers, while Windows is a monopoly. Why should this be the case? Why are information products and services marketplaces such an oddity?

Information Economics

One of the discoveries made by the economists Jevons and Menger in the nineteenth century is that the marginal cost of production is the price of a thing at equilibrium. When coal cost nine shillings a tonne in 1870, it wasn't necessarily true that all mines mined coal at that price; rather, it meant that the marginal producers those who were barely making ends meet could sell at that price. These mines would shut down if the price decreased, and they would open if the price increased. That was the way supply changed to meet shifting demand.

a) The Price of Information:

The price of knowledge should thus equal its marginal cost of production in a competitive equilibrium. But that is practically nothing! This explains why there is so much material on the Internet that is offered for free; the appropriate price for it is zero. The temptation will be for them to keep lowering their rates without end if two or more providers compete to provide an operating system, map, or encyclopedia that they can reproduce for free. The Britannica used to cost $1,600 for 32 volumes; when Microsoft released Encarta for $49.95, Britannica was forced to provide a low-priced CD version; and now we have Wikipedia for free. One company after another has been forced to switch to a business model where the products are given away for

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

free and the revenue is derived from advertising or a secondary market. Many Linux developers volunteer their time for free to the project while they are still in college since their involvement improves their resume and increases their chances of landing a decent job after graduation. Linux firms offer freely an operating system and earn their money through support. Consider terrestrial TV as an example of an industry that transitioned to an advertising or service model due to its high fixed costs and low marginal costs. Others have followed suit. Since most newspapers rely heavily on advertising for revenue, the transition between free online versions and paid print editions, which all put the lucrative advertisements in front of readers, was not straightforward. Other businesses, like travel and lodging, on the other hand, have a tendency to develop into monopolies that seek to control certain routes or regions and impose varying fees on various clientele.

b) The Value of Lock-In:

An intriguing finding is attributed to Shapiro and Varian: the value of a software firm is the complete lock-in of all of its clients (owing to both technical and network effects). Consider a company that uses Office and has paid $500 a copy for each of its 100 employees to use it to show how this would work. It could save $50,000 by switching to OpenOffice, thus it would switch if the overall switching costs, which include installing the new software, retraining workers, converting data, and other expenses, were less than $50,000. However, Microsoft would raise its charges if the expenses of switching exceeded $50,000.

Technical lock-in always existed, but the transition to the digital economy has greatly increased its significance. You must use only Volvo parts and accessories if you own a Volvo vehicle, but you can always swap it in for a Mercedes if you become tired of it. But if you possess an Apple Mac, you'll also likely have hundreds of audio songs that you've ripped to iTunes, as well as Mac software and a Mac printer. Additionally, you would need to learn how to utilise various interfaces and instructions. Spending $700 on a new laptop would be considerably more unpleasant than switching to Windows. You would have to retrain yourself and purchase Office for Windows instead of Office for Mac. And if you had purchased several songs from the iTunes store, it may have been much more traumatic (because though the iPod functions better with the Mac, you would probably chose to retain your iPod with your new Windows computer rather than switching to a Windows music player). This demonstrates why lock-in can last for so long despite the fact that each piece of equipment, whether it be a Mac laptop, an iPod, or a printer, degrades with time due to their complimentary nature. This also holds true for Internet service providers (ISPs), commercial software systems like databases, hardware like telephone exchanges, and a variety of online services.

This explains why standards disputes and antitrust lawsuits are so labor-intensive. It's also the reason why so many security measures currently focus on restricting compatibility. In these situations, the most probable hackers are the equipment's owners or new businesses looking to upend the status quo by producing suitable items, not malevolent outsiders. The problems are complicated by the fact that innovation is often incremental and that technologies prosper when new businesses identify game-changing uses for them [607]. For instance, IBM built the PC to run spreadsheets; if they had restricted it to just this one use, they would have missed out on a huge potential. In fact, one of the reasons the IBM PC overtook the Apple Mac as the preferred desktop platform was because it was more open.

c) Asymmetric Information:

Beyond monopolies and public goods, one further way that markets may go wrong is when some principals have more knowledge than others. In 1970, George Akerlof published a well-known work on the "market for lemons" [19] for which he received the Nobel Prize, which served as the catalyst for the study of asymmetric information. It offers the following simple yet deep insight: Imagine that a town has 100 used automobiles for sale, 50 of which are well-kept and cost $2000 each, and 50 of which are "lemons" and cost $1,000 each. The purchasers don't know which is which; the sellers do. What is the used automobile

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

market price? You would think $1500, but no excellent automobiles will be put up for sale at that price. Therefore, the market price will be around $1,000.

One explanation for the prevalence of subpar security solutions is this. When consumers are unable to distinguish between excellent and terrible products, they may choose to spend $10 on a subpar antiviral program as opposed to $20 on a superior one, and a price war may result. Between concealed information and hidden action, another difference may be made. For instance, Volvo is recognised for making safe vehicles that recover well from collisions, yet it is commonly known that Volvo drivers are involved in more collisions. Is this due to the fact that individuals in Volvos drive more quickly or because people who are lousy drivers choose Volvos to reduce their risk of being killed? The first is the hidden-information scenario, which is also referred to as adverse selection, and the second is the hidden-action example, which is also referred to as moral hazard. Security depends on both impacts, which may mix in certain circumstances. (In the case of drivers, it seems that a growing body of evidence supports the idea that individuals should modify their driving habits to maintain their risk exposure at a level with which they are comfortable.

Additionally, this explains why legislation requiring the use of seatbelts only serve to shift the deaths from car passengers to pedestrians and bicycles [10]. Many market failures in the real world are explained by asymmetric knowledge, from low pricing in used vehicle markets to the difficulties elderly people have in obtaining insurance on fair terms those who are unwell would likely to purchase more of it, making it unprofitable for the healthy. It often results in rationing or monitoring.

CONCLUSION

Instead of due to a flaw in the technological design, many systems fail because the incentives are flawed. As a consequence, in addition to knowing the fundamentals of cryptography, protocols, access controls, and psychology, a security engineer also has to grasp basic economics. A rapidly expanding field of study called security economics explains many of the phenomena that we previously dismissed as being caused by "bad weather," including Windows' vulnerability. It often offers exciting new insights on a variety of issues, including how to optimise the patching cycle, whether users truly care about privacy, and potential legislative responses to DRM.

REFERENCES

[1] A. Schulan, “Behavioural Economics of Security,” *Eur. J. Secur. Res.*, 2019, doi: 10.1007/s41125-019-00045-w.

[2] S. Ekelund and Z. Iskoujina, “Cybersecurity economics – balancing operational security spending,” *Inf. Technol. People*, 2019, doi: 10.1108/ITP-05-2018-0252.

[3] M. DiGiuseppe and K. B. Kleinberg, “Economics, security, and individual-level preferences for trade agreements,” *Int. Interact.*, 2019, doi: 10.1080/03050629.2019.1551007.

[4] K. Malinova, “Economics of Technology, Securities and Capital Markets,” *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3461760.

[5] R. Beck, P. Eklund, and J. Spasovski, “How blockchain impacts cloud-based system performance : a case study for a groupware communication application,” *Australas. Conf. Inf. Syst.*, 2019.

[6] A. Sukhorukov, “International economics: security of economic system and transboundary crisis,” *Confront. Coop. 1000 Years Polish-German-Russian Relations*, 2019, doi: 10.2478/conc-2019-0005.

[7] P. E. Harrell, E. Rosenberg, W. D. S. Cohen, G. M. Shiffman, D. Singh, and A. Szubin, “Economic Dominance, Financial Technology, and the Future of U.S. Economic Coercion,” *Cent. a New Am. Secur.*, 2019.

[8] S. Panda, D. W. Woods, A. Laszka, A. Fielder, and E. Panaousis, “Post-incident audits on cyber insurance discounts,” *Comput. Secur.*, 2019, doi: 10.1016/j.cose.2019.101593.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Concepts of Multilevel Security

Mr. Yarlagadda Kumar
Assistant Professor, Department of Petroleum Engineering, Presidency University, Bangalore, India,
Email Id-dheerajkumar@presidencyuniversity.in

ABSTRACT: ***By offering efficient protection and access control for information systems that handle sensitive and classified data, multilevel security plays a significant role in security engineering. In the context of security engineering, this abstract presents an overview of multilevel security by examining its core ideas, guiding principles, and useful applications. Beginning with a definition of multilevel security and its importance in handling the complicated security needs of organisations that deal with data of various sensitivity levels, the abstract explains the purpose of multilevel security. It draws attention to the core goals of multilayer security, such as preserving information's confidentiality, integrity, and accessibility across different security levels. The abstract talks about compartments and security levels as the basic components of multilevel security. It looks at the Biba and Bell-LaPadula models' guiding principles, which serve as the foundation for multilevel security systems' enforcement of secrecy and integrity, respectively. The abstract also emphasizes the need of having a clear security strategy that establishes the guidelines and limitations regulating user access and data flow.***

KEYWORDS: ***Accessibility, Multilevel Security, Threat Model, Trusted Computing Base.***

INTRODUCTION

Multilevel secure systems are important because:

1. Due to military support for computer science in the USA, a significant amount of research has been done on them [1]–[3]. As a result, the military model of protection has been developed in more depth than any other and provides us with several instances of the second-order and even third-order impacts of strictly enforcing security policies;
2. Numerous commercial systems today incorporate multilayer integrity rules, despite the fact that multilevel principles were first created to promote secrecy in military systems. For instance, telecom operators want their billing system to be able to observe but not influence what is occurring in their switching system;
3. Mandatory access control techniques have lately begun to be included into products like Microsoft Vista and Red Hat Linux. They have also been disguising themselves as DRM systems. Red Hat, for instance, employs SELinux methods created by the NSA to separate several servers operating on a platform, ensuring that even if your web server is compromised, your DNS server won't necessarily follow. Internet Explorer runs by default at "Low" under Vista's multilevel integrity policy, which means that even if it is taken over, the attacker shouldn't be able to edit system files or anything else with a higher integrity level. Although their usage in the workplace is growing, these techniques are still mostly opaque to the average household computer user;
4. Due to the significant vested interests and momentum behind multilayer confidentiality concepts, they are often used in situations where they are useless or even destructive. Large system initiatives may fail as a result of this, particularly in the public sector.

According to Sir Isiah Berlin, a thinker is either a fox or a hedgehog: a fox knows many little things, whereas a hedgehog only knows one large thing. The hedgehog method of security engineering involves multidimensional thinking.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

DISCUSSION

When top-down security engineering is feasible, it usually takes the shape of a threat model, security policy, and security mechanisms. The security policy is an important but sometimes overlooked step in this process.

What Is a Security Policy Model?

A security policy is a document that communicates concisely and concisely briefly describing the goals of the protective measures. It is influenced by how we perceive dangers, which in turn influences how we designed our systems. It often takes the form of declarations regarding which users are permitted to access certain data. It serves the same purpose as the system specification for general functionality in defining the system's protection needs and determining if they have been satisfied. A security policy may, in fact, be included in a system specification, and like the specification, its main purpose is communication [4]–[7]. The term "security policy," as used by many organisations, refers to a set of meaningless assertions.

Despite being fairly prevalent, this waffle is worthless to a security engineer. Its first flaw is that it sidesteps the crucial question, "Who determines "need to-know" and how?" Second, it combines assertions made at several levels logically, organisational approval of a policy shouldn't be included in the policy itself. Third, a system exists, but it's suggested rather than stated explicitly: "staff shall obey," but what does this truly entail? Users are "on their honour," therefore does the system need to impose obedience? Fourth, who is specifically responsible for reporting breaches and how are they to be found?

Better must be done than this. In reality, three more explicit phrases have emerged to express the definition of protection needs since the term "security policy" is often misused to denote a collection of managerialist clichés. A system's or a particular kind of system protection attributes are briefly stated in a security policy model. Its main ideas may usually be condensed into one page or less. It is the document in which the protection objectives of the system are agreed upon with the top management of a client or with the whole community. It may even serve as the foundation for formal mathematical analysis.

The protective mechanisms that a certain implementation offers are described in further depth in a security target, together with how they relate to a set of control goals some of which, but not all of which, are often obtained from the policy model. The security goal serves as the foundation for a product's testing and assessment. Similar to a security target, a protection profile is described in a fashion that is implementation-independent to allow for comparative assessments across products and versions. This may include using a semi-formal language or at the very least, appropriate security lingo. Products that are to be assessed using the Common Criteria must have a protection profile.

When I don't need to be as specific, I may use the term "security policy" to refer to a security objective or a security policy model. I'll never refer to it as a compilation of cliches. Sometimes we are forced to create a security policy model from start since we are dealing with a brand-new application. Most often, a model already exists; we only need to choose the best one and turn it into a security target. Both of these actions are difficult. Providing a variety of security policy models, describing them in the context of actual systems, and looking at the engineering processes and related limitations that a security target might utilise to achieve them are, in fact, some of the goals of this chapter of the book. The word "security policy" may also be used in a third context to refer to a collection of particular configuration options for a security product. In the paragraphs that follow, we'll refer to this as configuration management or, on rare occasions, trustworthy configuration management.

The Bell-LaPadula Security Policy Model

Bell and LaPadula's 1973 proposal of a security policy model was in response to US Air Force worries about the security of time-sharing mainframe systems. People began to discover that the security provided by many commercial operating systems was inadequate and was not getting any better by the early 1970s. Every time an operating system issue was repaired, a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

new vulnerability was found. Modern dependability growth models, which I go into more detail about in section 26.2.4, can quantify this and show that the pessimism was right. There was a persistent concern that even inexperienced users would find vulnerabilities and exploit them, and there was also a sharp and rising understanding of the harm posed by malicious code. Viruses weren't created until the decade after; in the 1970s, Trojans were the main threat. When it was revealed that the Pentagon's World Wide Military Command and Control System was susceptible to Trojan Horse assaults, there was a significant concern; unfortunately, this resulted in its usage being limited to those with a "Top Secret" clearance. Finally, innovative new concepts for protection were being developed by university and corporate researchers, which I will address below.

The US government came to the conclusion from research by James Anderson that a secure system should only accomplish one or two things effectively, and that these protective features should be enforced by processes that were easy to verify and that would only sometimes change. It presented the idea of a reference monitor, an operating system component that would mediate access control decisions and be small enough to be susceptible to testing and analysis with the ability to guarantee completeness. These parts along with the corresponding operating systems are referred to as the Trusted Computing Base (TCB) in current terminology. The term "TCB" refers more specifically to a group of elements (hardware, software, human, etc.) whose proper operation is sufficient to guarantee that the security policy is upheld, or, more viscerally, whose failure might result in a violation of the security policy. The Anderson study sought to simplify the security policy so that rigorous verification could be conducted by the TCB.

Classifications and Clearances: Following the Second World War and the Cold War, NATO states adopted a uniform protective marking system to indicate the level of document sensitivity. According to Figure 1, classifications are designations that go from Unclassified through Confidential, Secret, and Top Secret. The specifics are always changing. The initial concept was that information designated "Top Secret" might potentially save many lives, whereas information marked "Secret" could potentially lose many lives. Employees of the government are given clearances based on how thoroughly they have been vetted; in the USA, for instance, a "Secret" clearance entails verifying FBI fingerprint data, while a "Top Secret" clearance additionally entails background checks for the five to fifteen years prior to employment.

An official could only view a document if his clearance level was at least as high as the classification of the document. An official with access to "Top Secret" information could read "Secret" information, but not the other way around. Information may only go upward from private to secret to top secret as a result; it can never move lower unless a designated individual makes a conscious choice to declassify it.

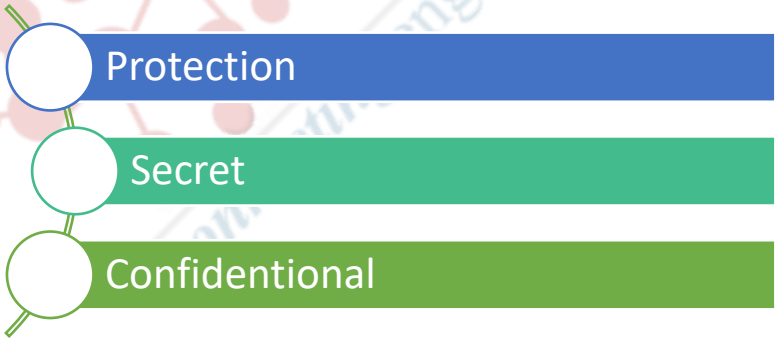

Figure 1: Illustrate the Multilevel Security.

A "Confidential" document may be maintained in a closed file cabinet in a regular government office, but higher levels may call for licenced safes, guarded rooms with control over photocopiers, and other

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

restrictions. A overview of the methods employed with "top secret" intelligence material is provided in the NSA security handbook. The system quickly became increasingly intricate. The criterion for classifying papers was widened to include economic hardship, political disgrace, and even potential military repercussions. Between "Unclassified" and "Confidential," the UK has a level called "Restricted"; the USA formerly had a similar level but got rid of it when the Freedom of Information Act was passed. America currently has two more distinct markings: "Unclassified but Sensitive" covers both FOUO and material that could be disclosed in response to a FOIA request, and "For Official Use Only" (FOUO) designates unclassified information that cannot be disclosed under FOIA. In the UK, 'Restricted' material is really freely available, but by designating anything as 'Restricted,' leakers like journalists may be held accountable under the Official Secrets Act. Its other significant practical impact is that a US document that is transferred over the Atlantic without being classified automatically becomes 'Restricted' in the UK and 'Confidential' when delivered back to the US. American manufacturers of military systems claim that British legislation violates US classification guidelines.

Additionally, information, particularly at the Secret level and higher, may be further limited via a system of codewords. For instance, information that could reveal intelligence sources or methods, such as agent identities or decryptions of foreign government traffic, is typically classified as "Top Secret Special Compartmented Intelligence" or TS/SCI, which imposes additional restrictions based on the so-called "need to know" principle and requires the use of one or more codewords. Some of the codewords are only known to a certain set of identifiable users and pertain to a specific military activity or intelligence source. A user has to know all of the codewords connected to a documein order to read it. A security category, or compartment if there is at least one codeword, is a collection of records with the same access control policy that is made up of a classification label and a set of codewords. I go into further depth on compartmentation in the multilateral security chapter. Descriptors, warnings, and IDO markers are also included. Words like "Management," "Budget," and "Appointments" are examples of descriptors. Since they do not indicate any particular handling requirements, we may treat a file marked "Confidential Management" in the same way that we would treat one that is just marked "Confidential." Warnings like "UK Eyes Only" or its American counterpart, "NOFORN," are examples of caveats. There are also marks from the International Defence Organisation, such NATO. One of the things that may make the system unclear is the absence of apparent distinctions between codewords, descriptors, cautions, and IDO marking. [1051] provides a more thorough justification. The last general observation regarding access control concept is that permitting information to go upward exclusively also simulates eavesdropping.

When someone's phone was tapped in the past, it included installing a physical wire at the exchange; nowadays, everything is handled via the telephone exchange software, which has the effect of turning the target conversations into conference calls with an additional party. The typical security criterion is that the person being investigated should not be aware that he is being wiretapped, therefore the third party should be quiet and its existence should be hidden from the person being investigated. For instance, because wiretaps are increasingly used as quiet conference calls, it is important to make sure that the wiretapper is charged for the conference call service rather than the target. A data flow policy that allows the 'High' principal to access the 'Low' data while preventing the 'Low' principal from knowing if the 'High' principle is reading any data at all, much alone what data, is necessary for wiretapping.

Information Flow Control: The BellLaPadula or BLP model of computer security was created in 1973 in the context of the categorization of government data. It is also known as multilevel security, and the systems that use it are sometimes referred to as MLS systems, or multilevel secure. Information cannot flow

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

downhill, which is their fundamental property [8]–[10].

The Bell-LaPadula model explicitly imposes two properties:

1. **The simple security property:** No process is allowed to read data over a certain level. Another name for this is no read up (NRU);
2. **The *-property:** A lower level may not be written to by any procedure. No write down (NWD) is another name for this.

Bell and LaPadula were instrumental in developing the *- property. It was motivated by concern about assaults using malicious code. An uncleared user may create a Trojan and leave it lying about for a system administrator cleared to 'Secret' to run; it might then copy itself into the 'Secret' area of the system, read the data there, and attempt to signal it down in some way. It's also conceivable that an enemy agent would get a position at a for-profit software company and insert some code into a program that searches for classified information to duplicate. The security policy would have been broken if it had been able to copy them and leave them somewhere where its author could view them. If programs have the ability to write down, information may potentially be exposed as a consequence of a bug.

It is expected that there exist vulnerabilities, such as malicious and flawed code. Extensive operational security procedures have long been utilised, particularly in military organisations, to prevent workers from leaking paper documents. It is also thought that most employees are sloppy and some are dishonest. (All copies of circuit schematics, drawings, etc. were numbered and had to be accounted for when I worked in defence avionics as a young person.) The use of computers didn't alter the pre-existing culture in which security policy was implemented without regard to user behaviour. It has to be made clear, and BellLaPadula does that: the security policy needs to be upheld not simply independently of users' direct actions, but of their indirect actions.

The Biba Model and Vista: The inclusion of a multilevel integrity model in Windows Vista has rekindled attention in a security model developed in 1975 by Ken Biba [168], sometimes known as "Bell-LaPadula upside down" in textbooks. The Biba paradigm focuses only on honesty and disregards secrecy. The crucial finding is that

In some ways, confidentiality and integrity are two different ideas. While integrity places restrictions on who may create or change a message, confidentiality places restrictions on who can read it. An electronic medical instrument, like an ECG, may have two distinct modes: calibration and usage, to provide one example. Normal users must be prevented from corrupting calibration data, thus they will only be allowed to read it and not write to it. When a normal user resets the device, the user state (i.e., any patient data in memory) will be lost, but the calibration will not be affected.

We can use a multilevel integrity policy to model such a system, with the rules that we can read data at higher levels for example, a user process can read the calibration data and write to lower levels for example, a calibration process can write to a user process' buffer however, we must never read down or write up because either could cause High integrity objects to become contaminated with Low that is potentially unreliable data. The integrity of an item is the lowest level of all the objects that contributed to its production, according to the low water mark concept, which is the dual of the high water mark principle explained above.

This was the first official integrity model. Surprisingly many actual systems operate in a Biba-like fashion. For instance, a railroad's passenger information system may get information from the signalling system, but it shouldn't be allowed to modify it other than through a trusted interface, like a member of the control crew. Few designers of these systems, nevertheless, are familiar with the Biba paradigm or the lessons it may provide.

Vista applies a default policy of NoWriteUp and assigns file objects an integrity level, which might be Low, Medium, High, or System. With the exception of Internet Explorer, which is set at Low by default, critical Vista files are at System and other items are at Medium. As a result, programs downloaded using

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Internet Explorer can read most files on a Vista machine but not write them. The goal is to reduce the harm that viruses and other malware might do. I'll go into more depth on Vista's workings below.

LOMAC, a Linux module that introduced a low water mark policy, was an intriguing forerunner to Vista. With system files at high integrity and the network at poor integrity, it offered two layers of protection. A program (like a daemon) was immediately demoted to Low as soon as it received network traffic. This means that even if the traffic includes an attack that forks a root shell, the forked shell would not be able to write to the password file in the same way as a regular root shell. As one would anticipate, a few system functions (like logging) proved challenging and needed trustworthy code.

CONCLUSION

Military applications drove the development of mandatory access control, most notably for specialised firewalls (guards and pumps). They are being added to widely used operating systems like Vista and Linux. They are even more significant since they have been the focus of computer security research since the middle of the 1970s and because many of the systems used for security assessment are based on their presumptions. It is crucial for the practitioner to be aware of both their strengths and weaknesses so they may draw on the extensive study literature when necessary and avoid making mistakes when they shouldn't.

REFERENCES

[1] H. Wei, C. Zhang, T. Wu, H. Huang, And K. Qiu, "Chaotic Multilevel Separated Encryption For Security Enhancement Of Ofdm-Pon," *Ieee Access*, 2019, Doi: 10.1109/Access.2019.2938910.

[2] P. Oberoi, S. Mittal, And R. K. Gujral, "Multilevel Cloud Security Policy (Mcsp) For Cloud-Based Environments," *Int. J. Innov. Technol. Explor. Eng.*, 2019.

[3] A. Al-Haj And B. Aziz, "Enforcing Multilevel Security Policies In Database-Defined Networks Using Row-Level Security," In *Proceedings Of The 2019 International Conference On Networked Systems, Netsys 2019*, 2019. Doi: 10.1109/Netsys.2019.8854491.

[4] A. Y. Mahmoud And M. N. A. Alqumboz, "Encryption Based On Multilevel Security For Relational Database Ebmsr," In *Proceedings - 2019 International Conference On Promising Electronic Technologies, Icpet 2019*, 2019. Doi: 10.1109/Icpet.2019.00031.

[5] S. C. V. Bhaskar, J. V. Gopal, And S. Anitha, "A Constructive Multilevel Security System With Cryptographic Techniques By Using Cyber-Physical System In The Space/Defense Applications," In *Acm International Conference Proceeding Series*, 2019. Doi: 10.1145/3372422.3372427.

[6] G. Muneeswari And A. Puthussery, "Multilevel Security And Dual Otp System For Online Transaction Against Attacks," In *Proceedings Of The 3rd International Conference On I-Smac Iot In Social, Mobile, Analytics And Cloud, I-Smac 2019*, 2019. Doi: 10.1109/I-Smac47947.2019.9032466.

[7] R. J. Rasras, Z. Alqadi, M. R. A. Sara, And B. Zahran, "Developing New Multilevel Security Algorithm For Data Encryption-Decryption (Mls_Ed)," *Int. J. Adv. Trends Comput. Sci. Eng.*, 2019, Doi: 10.30534/Ijatcse/2019/90862019.

[8] D. A. Gayan Nayanajith And K. A. Damunupola, "Effects Of Subjective Norms And Security On Online Banking Adoption : Multilevel Linear Model Analysis," *Asian J. Multidiscip. Stud.*, 2019.

[9] A. K. Soni And N. Khare, "A Review On Multilevel Approaches For Security In Cloud By Using Abe," *Int. J. Innov. Res. Comput. Sci. Technol.*, 2019, Doi: 10.21276/Ijircst.2019.7.2.3.

[10] N. Ganesh And R. C. Narayanan, "Multilevel Secured Finger Print Payment System Simulation Using Android," *Int. J. Recent Technol. Eng.*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Discussion on Multilateral Security

Dr. Udaya Ravi Mannar
Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-udayaravim@presidencyuniversity.in

ABSTRACT: ***In the context of security engineering, the term "multilateral security" refers to the idea of using a holistic and linked strategy to solve various security concerns. An overview of multilateral security in security engineering is given in this abstract, together with an examination of its core values and important factors to take into account while putting multilateral security measures into practise. Multilateral security and its importance in the area of security engineering are defined at the outset of the abstract. It highlights the necessity for a comprehensive and integrated approach to security that takes into consideration a number of factors, including operational security, human security, information security, and physical security. The interconnection of these dimensions is emphasised since they all work together to affect an organization's or system's overall security posture. The paper then explores the essential tenets of multilateral security. The significance of risk assessment and risk management is discussed, focusing on the need to identify and rank possible risks and vulnerabilities. The abstract also examines the idea of defence in depth, which is adding more security measures on top of each other to build a strong security architecture. The advantages of multilateral security are then highlighted in the abstract. It highlights how a thorough strategy aids in reducing single points of failure and offers a more durable security framework. By taking into account possible risks and threats holistically, multilateral security offers a proactive attitude, supporting efficient prevention, detection, and response techniques.***

KEYWORDS: ***Compartmentation, Multilateral Security, Risk Assessment, Orthopaedic Technician.***

INTRODUCTION

Our aim is often to stop information from moving "across" departments rather than "down" a hierarchy. Relevant applications include the majority of those where the privacy of specific clients', citizens', or patients' data is in jeopardy. These applications span from healthcare to national intelligence [1]. They make up a major percentage of information processing systems, but their security is often badly planned and executed. This has resulted in a number of costly failures. The fundamental issue is that by centralising systems that hold sensitive data, you run the danger of making them a more valuable asset while simultaneously granting more individuals access to it. The accumulation of petabytes of users' private information by online apps has made this a critical issue in the "Web 2.0" era. Additionally, a lot of agencies want to store your medical data online; it's not only Google Docs. Microsoft has unveiled HealthVault, which will provide your physicians the ability to keep your medical information online in a data centre and allow you some control over access; other IT companies have ideas that are largely comparable to Microsoft's. Although this may be useful in an emergency, privacy campaigners point out that it also grants access to insurance firms, governmental organisations, and anybody else who shows up with a court order. What are the true problems with such systems, should they be developed, if so, how can we safeguard them, and are there any examples we can study?

A private investigator used to have to bribe someone at the branch where your account was stored in order to get copies of your bank statements. However, as banks connected all of their locations to the internet in the 1980s, they usually allowed any teller to inquire about any customer's account. This made it possible to pay checks while you are out of town, but it also meant that private investigators could purchase and resell your bank statements for a few hundred dollars. Instead of one at each branch, they only need to corrupt one employee at each bank. Another example comes from the UK Inland Revenue, which is

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

responsible for collecting taxes; employees there were exposed for improperly accessing the records of famous people, selling their information to other parties, and disclosing financial information in alimony cases. In Figure 1 shown the Multilevel security.

Figure 1: Illustrate the Multilevel security.

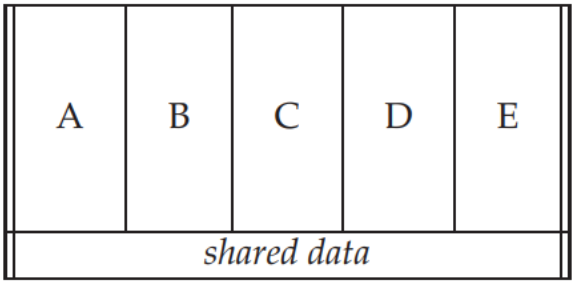

Figure 2: Illustrate The Multilateral Security.

Users shouldn't be allowed to access data that belong to a different branch, area, or partner in the company unless there are stringent restrictions in place, according to usual requirements for such systems. Therefore, we need the information flow control borders to be mostly vertical, as indicated in Figure 2, rather than horizontal as we saw in the Bell-LaPadula model.

These organisational constraints on lateral information flow may apply to an intelligence organisation that wishes to keep the identities of its agents operating abroad hidden from the department in charge of spying on another. They may be founded on privilege, like in a legal practice where the affairs of various clients and the clients of various partners must be kept separate. They could even be a combination of the two, as in medicine, where patient confidentiality is based on the law and the patient's rights but is often enforced by restricting access to medical records to a certain hospital department.

The regulation of lateral information flows is a very widespread issue, and we'll use the clear and well researched example of medicine to illustrate it. The issues with medical systems are significant from an economic and social standpoint and are easily understood by non-specialists. Many of our observations about them apply with little to no modification to the practice of other professions as well as to government applications where access to certain types of classified material is limited to specific teams or departments.

Terminology is one little issue we have. There are several names for the kind of information flow restrictions we're interested in; in the U.S. intelligence community, for instance, they're known as compartmented security or compartmentation. Since the application of healthcare is more extensive than that of intelligence, we shall use the word "multilateral security" in Europe. This term also refers to the employment of methods like anonymity, with deidentified research databases of medical information serving as a typical example. This contributes significantly to international security. In addition to avoiding overt information leaks, we also need to stop information leakage via things like disclosed statistics and billing data. De-identified data may be used in many contexts. Another example is the handling of census data. Inference control is the generic term used to describe the pertinent protection methods. The challenges faced by the administrators of census databases and medical research databases are largely the same, despite occasional terminological discrepancies.

DISCUSSION

Compartmentation, the Chinese wall and the

In a multilateral security paradigm, there are at least three alternative ways to implement access controls and information flow restrictions. The Chinese Wall and compartmentation are examples of tools employed by the intelligence sector [2]–[6]. The BMA model, created by the British Medical Association to define

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

the information flows authorised by medical ethics, outlines the procedures employed to avoid conflicts of interest in professional practice. Outside of their original fields, each of these has potential uses.

Compartmentation and the Lattice Model: For many years, it has been common procedure in the administrations of the United States and its allies to limit access to information by using codewords and classifications. The codename Ultra in World is the most well-documented instance. For many years, it has been common procedure in the administrations of the United States and its allies to limit access to information by using codewords and classifications. The codeword Ultra from World War 2 is the best known instance of this. It refers to British and American decryptions of German transmissions encrypted using the Enigma cypher machine. The discovery that the Enigma had been cracked was so crucial that it warranted safeguarding at all costs.

Thus, Ultra clearances were only granted to a select group of individuals, including the cryptanalysts and their support personnel, top Allied generals, and hand-picked analysts. No one who had ever had an Ultra clearance could ever be in danger of being captured, and the information could never be utilised in a manner that would lead Hitler to believe that his main cypher had been cracked. Therefore, the Allies would send an aircraft over to'spot' a target when Ultra informed them of it, such as an Italian convoy to North Africa, and report its location by radio an hour or so before the assault. separate handling guidelines were used to enforce this strategy; for instance, Churchill received his Ultra summaries in a separate dispatch box to which he had a key but not his staff. Access to a codeword is frequently referred to as an indoctrination rather than just a clearance since such particular requirements can be applicable.

Today, same security measures are used to safeguard data including agent identities, cryptanalytic accomplishments, the capabilities of electronic eavesdropping equipment, and satellite performance that may be compromised and reveal intelligence sources or techniques. There are many compartments due to the overuse of codewords, particularly at classification levels above Top Secret. Because derivative work inherits classifications, a report based on sources from "Secret Desert Storm" and "Top Secret Umbra" may theoretically only be viewed by those having a clearance of "Top Secret" and membership in the organisations "Umbra" and "Desert Storm." Some intelligence services have over a million active compartments, and each combination of codewords creates a compartment. The management of them is a serious issue. People with high level clearances are permitted to access more resources at other organisations. However, the outcome might be devastating if the control systems fail. Almost the entire U.S. agent network in Russia was exposed by Aldritch Ames, a CIA official who had gained access to several compartments due to his lengthy service, rank, and counterintelligence operations.

Codewords are essentially a pre-computer method of representing access control groups, and they may be handled using a Bell-LaPadula version known as the lattice model. Classifications and codewords combine to generate a lattice, a mathematical framework in which any two items, A and B, may have either an A > B or B > A dominance relationship. They don't have to be; A and B might simply be uncomparable (albeit in this case, the structure would still have a least upper limit and largest lower bound in order for it to be a lattice). As an example, let's pretend we have the codeword "Crypto." Consequently, a person with a clearance of "Top Secret" would be able to view documents classified as "Top Secret" and "Secret," but he would not have access to documents marked "Secret Crypto" unless he also possessed a cryptographic clearance. We must condense the core of classifications, clearances, and labels into a security policy that we can use to guide security aims, implementation, and assessment in order for information systems to support this. As it turns out, the Bell-LaPadula model remains largely intact. As previously, information continues to flow between High and Low, with High acting as Low's dominant compartment. There should be no information flow between two nodes in a lattice that are incompatible,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

such as "Top Secret" and "Secret Crypto" in the picture above.

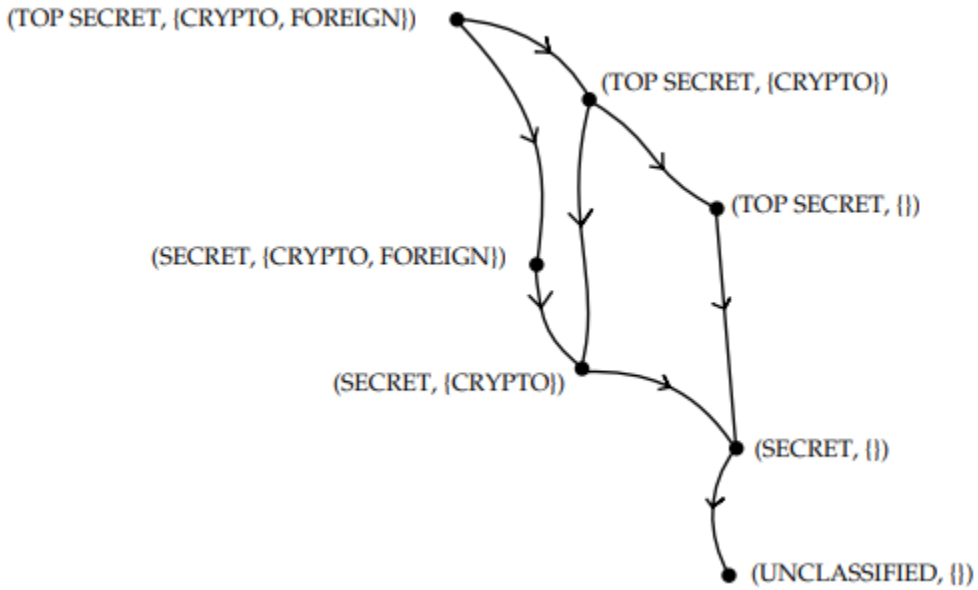

Figure 3: Illustrate the A lattice of security labels.

Most goods created for the market of multilayer safe items may be utilised again in compartmented mode. But in reality, these items don't work as well as one would want. Giving them incompatible titles (such as "Secret Tulip," "Secret Daffodil," or "Secret Crocus") makes it simple to employ a multilayer operating system to keep data in various compartments separate. The fundamental issue is how to regulate information exchange since the operating system has evolved into an isolating mechanism rather than a sharing mechanism. One way is to use an algorithm to put least upper boundaries on the lattice. The mechanism the Saudi Arabian government uses to oversee the Haj, the yearly pilgrimage to Mecca, serves as an example. The mixture of data from several compartments, whereas most compartments are by nature Confidential, is Secret. Therefore, although "Haj-visas" and "Gov-guest" are private, their combination is secret.

Data owners don't want a higher classification level where everything is accessible in intelligence systems where users already have the greatest degree of clearance. The lattice model essentially builds a third compartment utilising data from two compartments. It is difficult to control the growth of millions of compartments, which may be connected with applications. In order to make sure that "untrustworthy" email gets sent to filters, a more popular method is to employ a typical multilayer product, such a mail guard. However, filters, not guards, now make up the heart of the trusted computing platform. Even worse, the guard can lose some of the underlying operating system's most crucial features. For instance, the Standard Mail Guard was constructed on top of the LOCK operating system, whose fundamental feature is type enforcement, as discussed in the chapter before. Role-based access control, which would be a more suitable approach to manage the connections between compartments directly, is supported by later versions of LOCK. It could have been pointless to use it just as a means of promoting BLP.

The Chinese Wall

The Chinese Wall model of international security was created by Brewer and Nash. Its name is derived from

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

the fact that financial services companies, like accountants and investment banks, have internal regulations referred to as "Chinese Walls" that are intended to avoid conflicts of interest. The model's application is not limited to finance. There are numerous professional and service businesses, including software suppliers and advertising agencies, whose customers may be in direct rivalry with one another. Typically, a partner who recently worked for one firm in a certain industry is not permitted to see the documents of any other company operating in that industry. Therefore, for a certain amount of time after working on, let's say, the Shell account, an advertising copywriter will be prohibited from working on any other oil company's account.

A partner may pick which oil business to work for, but once that choice is made, his options are fully confined in that industry. As a result, the Chinese Wall model combines freedom of choice with required access restriction. It also integrates the division of duties idea into access control.

The BMA Model

Medical information systems are perhaps the most significant, engaging, and instructional example of international security. In wealthy nations, the healthcare industry spends a higher percentage of GDP than the armed forces, and while hospitals still lag behind in automation, they are catching up quickly. Health information technology (HIT) expenditures may pay for themselves in three to thirteen years, according to a 2006 study for the U.S. Department of Health and Human Services (DHHS). HIT also has the potential to improve patient safety.

In many nations, concerns about healthcare safety and particularly privacy have gained traction. After many privacy gaffes, Congress in the USA approved the Health Insurance Portability and Accountability Act (HIPAA) in 1996. In a well-known instance, Mark Farley, a convicted child rapist who was employed as an orthopaedic technician at Newton-Wellesley Hospital in Newton, Massachusetts, was discovered using a former employee's password to access the records of 954 patients, the majority of whom were young females, in order to obtain the phone numbers of girls to whom he then made lewd phone calls. Senator Edward Kennedy of Massachusetts, one of HIPAA's supporters, ended up sending him to prison. There are a lot more less spectacular events as well. The UK government made an effort to centralise all medical records in 1995–1996 as well, which sparked a dispute with the British Medical Association (BMA). I was engaged by the BMA to create a policy for the security and privacy of clinical data, which I'll go into below. The argument persisted. A controversial initiative in Iceland in the late 1990s sought to create a national medical database that would include not just medical records but also genetic and genealogical information in order to monitor hereditary disorders through generations. When 11% of the population opted out, the Icelandic Supreme Court finally ruled that the database had to be opt-in rather than opt-out, and now, around 50% of the population participates.

The "Privacy Rule," rewritten and loosened by President Bush in 2002, was followed by more "administrative simplification" in 2006. The current state of affairs in the United States is that, although medical information must still be safeguarded in hospitals, clinics, and insurance companies, its usage outside of the immediate treatment environment (for instance, by researchers, employers, and welfare agencies) is outside of the restrictions and therefore considerably less restricted. Nobody is wholly satisfied with the system; health privacy activists find it to be woefully insufficient; hospitals say that it raises their expenses needlessly; and patient advocates point out that hospital workers often exploit HIPAA as an excuse to be unhelpful.

At the time this article was written (2007), Atlanta's Piedmont Hospital had just been the first US institution to undergo an audit for adherence to the security and privacy laws that had just taken effect in 2005. This audit, which examined everything from staff security policy breaches to physical and logical access to systems and data over the Internet, influenced the decision of many other healthcare institutions to spend money on encryption and other security measures. Additionally, the Government Accountability Office (GAO) recently stated that the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

DHHS needs to do much more to protect patient privacy, particularly by developing a comprehensive privacy strategy and adopting milestones for handling national health data exchange (which is complicated by both inconsistent state laws and insufficient technical protection).

There have been discussions concerning the safety and privacy tradeoffs related to emergency medical information in a number of European nations. Other nations have refrained from doing this, reasoning that if information currently held on a human-readable MedAlert bracelet, such as allergies, is moved to a machine-readable device such as a smartcard, then there is a risk to patients who fall ill in locations where there is no reader available, like on an aeroplane or a foreign vacation. The Germans have put data such as current prescriptions and allergies on the medical insurance card that residents carry. The UK government is developing a "summary care record" of prescriptions and allergies that will be stored on a single database and accessible to many health-care providers, including emergency department physicians, paramedics, and the operators of after-hours medical helplines [7]–[11].

CONCLUSION

We examined the issue of ensuring the confidentiality of medical records in this chapter. This is representative of many information security issues, from the protection of census data to the protection of national intelligence data via ordinary professional practice. It turns out that there is a simple issue, a tougher problem, and a very hard problem with medical records. Setting up access control mechanisms to ensure that only a reasonable number of staff members have access to a certain record is the simple issue. Role-based access controls are now the preferred technology for such systems and may be used to create them primarily by automating current working procedures. The more challenging issue is statistical security, or how to create census returns or medical record databases so that researchers may do statistical analyses without jeopardising the privacy of specific people. How to govern their interaction and, in the case of medication specifically, how to stop the distribution of payment information, is the trickiest issue. Regulation is the only practical answer to this problem.

Additionally, we may learn from medical systems about the limitations of various privacy-enhancing technologies like de-identification. Making medical records anonymous may assist to lessen the effects of unauthorised access and stop mission creep, but it is by no means foolproof. Re-identification of rich data on genuine individuals is often possible. It is important to investigate the techniques used in healthcare to address this issue.

REFERENCES

[1] S. Wohlgemuth, K. Umezawa, Y. Mishina, and K. Takaragi, “Competitive Compliance with Blockchain,” in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019*, 2019. doi: 10.1109/PERCOMW.2019.8730684.

[2] P. M. Beach, L. O. Mailloux, B. T. Langhals, and R. F. Mills, “Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2930718.

[3] G. McGraw, R. Bonett, H. Figueroa, and V. Shepardson, “Security engineering for machine learning,” *Computer (Long. Beach. Calif).*, 2019, doi: 10.1109/MC.2019.2909955.

[4] S. Spiekermann, J. Korunovska, and M. Langheinrich, “Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers,” *Proc. IEEE*, 2019, doi: 10.1109/JPROC.2018.2866769.

[5] H. Aldawood and G. Skinner, “Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues,” *Future Internet*. 2019. doi: 10.3390/fi11030073.

[6] S. Marksteiner, H. Vallant, and K. Nahrgang, “Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling,” *J. Inf. Secur. Appl.*, 2019, doi: 10.1016/j.jisa.2019.102389.

[7] S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, *Security and Quality in Cyber-Physical Systems Engineering*. 2019. doi: 10.1007/978-3-030-25312-7.

[8] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, “Security Chaos Engineering for Cloud Services: Work in Progress,” in *2019 IEEE 18th*

International Symposium on Network Computing and Applications, NCA 2019, 2019. doi: 10.1109/NCA.2019.8935046.

[9] R. M. Beswick, "Computer security as an engineering practice: A system engineering discussion," *Adv. Sci. Technol. Eng. Syst.*, 2019, doi: 10.25046/aj040245.

[10] M. Kreitz, "Security by Design in Software Engineering," *ACM SIGSOFT Softw. Eng. Notes*, 2019, doi: 10.1145/3356773.3356798.

[11] R. Bramberger, H. Martin, B. Gallina, and C. Schmittner, "Co-engineering of safety and security life cycles for engineering of automotive systems," *Ada User J.*, 2019, doi: 10.1145/3394514.3394519.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Brief Discussion on Banking and Bookkeeping

Mr. Sagar Gorad
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-goradsagarramachandra@presidencyuniversity.in

ABSTRACT: ***In the financial industry, banking and accounting systems are essential for handling transactions, keeping track of finances, and guaranteeing the reliability of financial data. Establishing strong security measures is crucial in the field of security engineering to safeguard sensitive financial and accounting data from unauthorized access, manipulation, and fraud. The main factors and methods for safeguarding banking and accounting systems within the framework of security engineering are summarized in this abstract. The abstract opens by emphasizing the importance of security in the world of finance and accountancy. Given the sensitivity of client information and the need of correct financial records, it emphasizes the significance of the confidentiality, integrity, and availability of financial data. The possible dangers and difficulties are also discussed, including data breaches, identity theft, insider threats, and regulatory compliance. The paper also takes into consideration how banking and bookkeeping are changing as a result of the emergence of digital banking, mobile commerce, and cloud-based accounting systems. It talks about the security issues that come with it and the need for safe software development procedures, secure communication protocols, and frequent security audits. The abstract also discusses the significance of regulatory compliance in the banking and financial sector, highlighting adherence to industry standards and laws including the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).***

KEYWORDS: ***Accounting Systems, Banking Systems, Cryptology Transactions, Ledger System.***

INTRODUCTION

Banking systems include anything from networks for cash registers and offline and online credit card processing to high-value interbank money transfer systems and the back-end accounting systems that keep track of it all and pay the bills afterwards. There are specialist systems for everything, including stock trading and bills of lading, and big businesses have internal accounting and cash management systems that mimic many bank operations [1].

These systems are crucial for a variety of reasons. To begin with, knowing transaction processing is necessary in order to address the bigger issues with electronic commerce and fraud. Many dotcom companies made serious mistakes with basic accounting; established business practises were disregarded in the haste to attract capital and develop websites. A significant portion of the investment in information security is now driven by legislation like Sarbanes-Oxley and Gramm-Leach-Bliley, which were passed in response to the Enron disaster and tightened board-level responsibility for internal control. When you suggest security measures to a customer,

The degree to which they'll aid directors in fulfilling their fiduciary duties to the firm is likely to be one of the first questions you'll be asked. Second, with banking being its most extensive application field, accounting was for a long time the backbone of the computer industry. Although more computers are capable of running personal apps like web browsers and Office, accounting is still the most important application for the majority of businesses. Therefore, the security of accounting systems is crucial from a practical standpoint. It also provides us with a clear paradigm of protection whereby the value of records' integrity (and their immutability once created) takes precedence above secrecy.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Third, the application that gave commercial cryptology its start was transaction processing systems, whether for large wire transfers worth millions of dollars or little debits like $50 cash machine withdrawals. Not only were encryption algorithms and protocols developed in response to banking applications, but also related supporting technologies, such tamper-resistant cryptographic processors. The trusted computing foundation exemplified by these processors is significant and compelling in comparison to the hardened operating systems mentioned in the context of multilayer security. Commercial cryptography is where many instructional errors were originally made or at least publicly published. Before anybody else in the open research community, financial cryptographers explored the issue of how to integrate crypto with access control. Another example of multilateral security that focuses on authenticity rather than secrecy is seen in financial systems. A banking system should prevent customers from defrauding one another or the bank; it should prevent bank employees from defrauding the bank or its customers; and it should provide evidence that is convincing enough to prevent any one of these principals from defrauding another principal.

In this chapter, I'll first go through the accounting procedures used to maintain track of assets despite sometimes dishonest employees; these procedures are quite typical of accounting procedures used by other businesses as well. The main international funds-transfer systems used by banks will subsequently be discussed. Similar systems are also used to settle securities transactions and maintain trade papers like bills of lading. I'll next go into detail about ATM systems, which are becoming the public face of banking and whose technology has been used in products like utility meters. Finally, I'll tell you about credit cards, which have evolved into the primary method of online payment. Then, I'll discuss more recent technological developments, such as the smartcards that were just launched in Europe, RFID credit cards, and nonbank payment systems like PayPal. I'll sum up with some remarks on money laundering and whether fraud prevention measures are really effective.

DISCUSSION

The Origins of Bookkeeping

Just after the development of agriculture in the Neolithic Middle East about 8500 BC, bookkeeping seems to have begun. When humans began to produce excess food, they began to trade and preserve it. They urgently need a system for keeping track of which villager had contributed how much to the common storage. The first step was to symbolise each unit of food (sheep, wheat, oil, etc.) with a clay token, or bulla, which was then enclosed in a clay envelope and sealed using the pattern of the storekeeper [2]–[4].

The seal was broken by the keeper in front of a witness when the farmer requested his food back. The first known security protocol might be this one. This eventually led to the development of writing about 3000 BC, and another thousand years later, we discover precursors to promissory notes, bills of shipping, and other documents. Around the same period, assayers began to encase metal ingots inside of bullas, which were employed as intermediary commodities. King Croesus of Lydia began directly stamping the metal about 700 BC, which led to the invention of coins. By the Athens of Pericles, a lot of rich people were engaged in banking. Figure 1 shown the Clay envelope and its content of tokens representing 7 jars of oil, from Uruk, present day Iraq, ca. 3300 BC.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Figure 1: Clay envelope and its content of tokens representing 7 jars of oil, from Uruk, present day Iraq, ca. 3300 BC.

The following important development was created in the late mediaeval period. Some enterprises grew to be too big for a single family to run when the dark ages ended and commerce began to expand. The first clearly modern banks emerged at this time, allowing them to effectively finance commerce by establishing branches in several cities. However, as the economy expanded, it became essential to recruit managers from outside, and the owner's family was unable to constantly monitor them. Due to the heightened danger of fraud brought on by this, double-entry bookkeeping emerged as a way to manage it. Despite the fact that the first book on it did not emerge until 1494, following the invention of the printing press, people used to believe that this was created in Italy somewhere in the 1300s. However, historians have recently discovered double-entry records made by Jewish traders in Cairo around the twelfth century, and it is now thought that the Italians acquired the practice from them.

Double-Entry Bookkeeping

Like most very significant concepts, the fundamental principle underlying double-entry bookkeeping is rather straightforward. Each transaction is recorded as a credit in one book and as a debit in the other. For instance, when a business sells. When a consumer purchases $100 worth of products on credit, a credit of $100 is posted to the Sales account and a debit of $100 is sent to the Receivables account. The customer's payment will debit the Cash account and credit the Receivables account, lowering the asset of money receivable. (The accounting school's motto is "debit the receiver, credit the giver.") The books should balance, or add up to zero, at the end of the day; the assets and liabilities should be equal. (If the company has earned a profit, then the shareholders are liable.) The books must balance at the end of each month (or day in banks) and are maintained by various clerks in all but the smallest businesses.

The ledger system may be designed effectively to ensure that each store or branch can be balanced independently. Thus, before putting her cash tray in the vault for the night, each cashier will balance it; the debits in the cash legder should precisely equal the actual banknotes she has collected. Therefore, most frauds need the cooperation of two or more

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

employees; this split responsibility idea, also known as dual control, is reinforced by audit. Not only are the books audited at year's end, but there are also sporadic audits; an inspection team may show up at a branch without warning and demand that all the books be balanced before the staff leaves for the day.

How Bank Computer Systems Work

One of the first significant businesses to adopt computers for accounting was the banking industry. The majority of the rest of their back-office operations were automated during the 1960s and 1970s after they began in the late 1950s and early 1960s with applications like cheque processing and realised that even those slow and expensive computers of the time were much less expensive than armies of clerks. Banks began providing automated payroll services to their corporate clients in the 1960s, and by the 1970s, they were facilitating business-to-business electronic commerce based on electronic data interchange (EDI), whereby companies could transact electronically [5]–[7].

Systems were developed by companies from General Motors to Marks & Spencer that allowed them to connect their computers to their suppliers' computers so that products could be ordered automatically. Similar methods were established by travel agencies to purchase plane tickets instantly. In the 1970s, a large number of ATMs were introduced, followed by online banking systems in the 1980s and web-based banking in the 1990s. However, the sophisticated front-end systems continue to depend on conventional back-office automation to manage account data and carry out settlement.

The double-entry motif is often claimed to be implemented by accounting computers. The level of control, however, varies greatly. The user interface's double-entry features could only be a cosmetic addition, but the underlying file formats lack integrity checks. A person with root access, physical access, and a debugging tool may be able to edit the records to circumvent the balance restrictions even if all the ledgers are maintained on the same system. Additionally, there may be other methods to get around the balance measures; for example, staff members may find software defects and exploit them. Despite all of these issues, most industrialised nations' laws mandate that businesses have strong internal controls and hold managers accountable for them. These rules serve as the primary impetus for investment in information security tools, but they also contribute to a significant amount of wasted capital. Therefore, we must examine the workings of electronic accounting in more depth.

There are several data structures in a typical financial system. There are several journals that hold transactions that have been received from teller stations, cash machines, cheque sorters and other sources but have not yet been entered in the ledgers, an account master file that contains each customer's current balance as well as previous transactions for a period of perhaps ninety days, a number of ledgers that track cash and other assets moving through the system and an audit trail that documents which employee did what and when.

A collection of nightly batch processing programs that apply the transactions from the journals to the different ledgers and the account master file are part of the processing software that operates on these data structures. A variety of modules that publish transactions to the appropriate combinations of ledgers will be part of the online processing. So, when a client deposits $100 into his savings account, the teller will record a transaction that credits $100 to the customer's savings account ledger and debits the same amount from the cash ledger, which shows how much money is in the drawer. A crucial check is provided by the fact that all ledgers should always equal zero; if the bank or one of its branches ever goes out of balance, an alert will sound, and investigations will begin to determine the reason. The ledger system's invariant is checked each day during the overnight batch run, so a programr who wants to increase his own account balance will need to withdraw funds from another account rather than just making them appear out of thin air by modifying the account master file.

Similar to how different ledgers are controlled by different clerks in a typical corporation, several programrs are in charge of various subsystems in a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

financial data processing facility. All code is also examined by an internal auditor and tested by a different test department. Once it has been authorised, it will be used on a production computer that only runs approved object code and data and lacks a development environment [8]–[12].

Wholesale Payment Systems

People often picture a Hollywood scenario in which cunning Russian hackers crack a bank's security codes and move millions of dollars' worth of wire transfers to tax havens when they think of electronic bank fraud. Electronic money transfer systems are sometimes the subject of sophisticated criminality. Beginning in the early 1970s, bankers began to see the need for an update to this venerable old Victorian system. First off, most test-key systems were theoretically susceptible to cryptanalysis; by carefully observing several transactions, one might eventually deduce the key information.

Second, even though the test key tables were maintained in the safe, nothing truly prevented staff employees from developing tests for illegal communications concurrently with tests for approved messages. Theoretically, you may demand that two employees get the tables out of the safe, sit across from one another at a table, and conduct the computation. A bent employee may subconsciously calculate the test on an unauthorised message while blatantly calculating the test on an authorised one. In practice, workers would work sequentially in a corner (the tables were secret, after all). In actuality, dual control was not supported by test key schemes. Having one staff member calculate the results and another verify them increased rather than decreased the danger.

Third, cost and efficiency were major issues. It didn't seem like much of a benefit to have the bank's computer printout a transaction in the telex room, calculate a test manually, write a telex to the other bank, verify the test and then input it into the computer of the other bank. Since the telex operators added typing mistakes, typos became a far bigger concern than frauds. Customers who unintentionally received large sums into their accounts occasionally merely spent the money, and in one instance, an unintended receiver spent part of his windfall on astute solicitors who assisted him in keeping it. The sector was surprised by this. There must be a way for the payments to transfer instantly from one bank's computer to another.

Automatic Teller Machines

Studying the security of automated teller machines (ATMs) teaches us yet another set of lessons regarding the challenges and limitations of dual control. One of the most important technical advancements of the 20th century was the introduction of ATMs, commonly referred to as cash machines. The first systems for processing retail transactions on a broad scale were ATMs. They were created in 1938 by the same person who came up with the teleprompter and the self-focusing camera, Luther Simjian. In New York in 1939, he convinced Citicorp to install his "Bankamat" machine; they removed it after six months, claiming that "the only people using the machines were a small number of prostitutes and gamblers who didn't want to deal with tellers face to face" [1168]. Its commercial debut occurred in 1967 when Barclays Bank installed a De La Rue machine in Enfield, London. Currently, it is estimated that there are 1,500,000 units installed worldwide. Currently, card payment terminals in stores also employ the technology that was created for them.

As PINs are generated and verified in secure hardware devices found within ATMs and at bank computer centres, modern block cyphers were first widely utilised in ATM networks. Block cyphers, tamper-resistant hardware, and accompanying protocols were employed in this technology, which was ultimately utilised in several other applications, such as postal franking machines and ticket machines for the lottery. In other words, the 'killer app' that launched contemporary business cryptography and retail payment technologies was ATMs.

CONCLUSION

Many things make banking systems intriguing. Applications for bookkeeping provide a mature example of systems where security is focused on accountability and authenticity rather than secrecy.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Their protective objective is to stop and catch insider scams before they are perpetrated. They may be modelled after the Clark-Wilson security strategy. It can be summed up as follows: "All transactions must preserve a system invariant, namely that the books must balance (so a negative entry in one ledger must be balanced by a positive entry in another one); some transactions must be carried out by two or more staff members; and records of transactions cannot be destroyed after they have been committed." This was based on established accounting practices, which encouraged the research community to think about alternative systems outside Bell-LaPadula versions.

However, dual control is not the only method used by manual accounting systems. Although certain systems do require that transactions be permitted in parallel by two or more employees, a separation of duties policy often operates in sequence, meaning that different individuals handle each transaction differently as it moves through the system. Creating accounting systems that are effective at doing this is a challenging and often disregarded topic that requires participation from many disciplines. Non-repudiation is another typical need, which states that principals must be able to create, store, and utilise evidence concerning the relevant activities of other principals.

Remote payment, the second main banking application, is becoming more and more important for all types of trade. In actuality, money transfers through wire date all the way back to the middle of the Victorian period. Payment systems are a useful way to learn about what goes wrong since there is a clear reason to attack them and criminals who steal a lot and are found are usually penalised. Their loss history shows us how critical it is to reduce background error rates, guard against procedural assaults that circumvent technological restrictions (such stealing ATM cards from the mail), and maintain sufficient controls to prevent and identify internal fraud.

REFERENCES

[1] T. Walker and L. Morris, *The Handbook of Banking Technology*. 2019. doi: 10.1002/9781119328094.

[2] T. Baskar, “Application of book-keeping in small medium enterprises,” *Seuiars*, 2019.

[3] L. Antoney and T. J. Augusthy, “Block Chain Accounting-The Face Of Accounting & Auditing In Industry 4.0,” *Int. Multiling. J. Sci. Technol.*, 2019.

[4] S. O. James, “Farm Records, Bookkeeping and Agricultural Data: A Case Study of Small-Scale Farmers in Nasarawa state, Nigeria,” *Prod. Agric. Technol.*, 2019.

[5] N. Yildirim and A. Varol, “A research on security vulnerabilities in online and mobile banking systems,” in *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 2019. doi: 10.1109/ISDFS.2019.8757495.

[6] N. Priya, P. Nandhini, D. J. Priya, and N. Sharma, “Applying cryptography in e-banking security,” *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.I3252.0789S319.

[7] N. Sundaram, C. Thomas, and L. Agilandeeswari, “A review: Customers online security on usage of banking technologies in smartphones and computers,” *Pertanika Journal of Science and Technology*. 2019.

[8] M. A. Ali, N. Hussin, and I. A. Abed, “E-banking fraud detection: A short review,” *Int. J. Innov. Creat. Chang.*, 2019.

[9] Y. Ivanov, “Correlation between Ensuring Information Security in the Banking System of Ukraine and National Critical Infrastructure Security,” *Inf. Secur. Pers. Soc. State*, 2019, doi: 10.51369/2707-7276-2019-2-6.

[10] S. Sri Hari, C. Kavinkumar, G. K. Niketh, and N. Harini, “Enhancing security of one time passwords in online banking systems,” *Int. J. Recent Technol. Eng.*, 2019.

[11] A. E. Kelly and S. Palaniappan, “Information Technology & Software Engineering Survey on Customer Satisfaction , Adoption , Perception , Behaviour , and Security on Mobile Banking,” *J Inf. Tech Softw Eng*, 2019.

[12] G. Kumar, A. R. Chaudhary, and K. Kumar, “Internet banking security enhancement using naïve bayes algorithm,” *Int. J. Innov. Technol. Explor. Eng.*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Evaluation of Physical Protection

Mr. Bhairab Gogoi
Assistant Professor, Department of Petroleum Engineering, Presidency University, Bangalore, India,
Email Id-bhairabjyoti@presidencyuniversity.in

ABSTRACT: ***A crucial part of security engineering is physical protection, which focuses on defending physical resources, facilities, and assets from theft, vandalism, unauthorized entry, and other physical threats. This abstract explores the essential ideas, principles, and methods of physical protection within the framework of security engineering. The definition of physical protection and its importance in the larger subject of security engineering are presented at the beginning of the abstract. It draws attention to the main goals of physical protection, such as asset preservation, worker safety, and business continuity. An essential boundary that creates the restricted access region is the idea of the physical security perimeter. The abstract then explores various components and defense strategies. These include surveillance systems, electronic card readers, physical barriers, locks, and access control systems that use biometric authentication. In order to preserve physical security, it examines the significance of security professionals as well as their jobs, duties, and training.***

KEYWORDS: Deterrence, Logical Protection, Mechanical Locks, Physical Security.

INTRODUCTION

Nowadays, the majority of security engineers are primarily focused on electronic systems, but physical protection cannot be completely disregarded for a number of reasons. Walls and locks are a consideration if you are giving advice on a company's overall risk management approach. Second, as it is simpler to educate someone with a background in electrical engineering or computer science the fundamentals of physical security than the reverse, it will be up to the systems person to handle interactions between physical and logical protection. Third, you'll often be asked for your opinion on the installations your customer has made. These installations were likely made by reputable local contractors who have a limited understanding of system difficulties but are well-known to your client. You'll need to be able to respond with knowledge and tact [1], [2].

Fourth, if a bad guy obtains physical access to security systems, whether at the manufacturer, during shipping, or before installation, many security systems may be overpowered. Fifth, a simple covert entry method called "bumping" has recently been used to fully compromise a number of locks; the producers of these locks (including those who sold "high-security" devices) seemed to be oblivious of the flaws that allow their products to be easily circumvented. Finally, the systems managers who most often seek your guidance will be in charge of your client's hosting centres, which are typically its most secure facilities.

Physical security is mostly simply common sense, but there are a few unexpected twists and there have been substantial recent technological advancements, particularly in lock-picking and other covert access methods. There are suggestions for lowering the occurrence of crime around your facilities from both criminology and architecture. The most significant kind of alarm, and possibly the one with the most fascinating system features, is a burglar alarm.

For instance, it suffices to stop a burglar alarm from operating, or in many circumstances to convince its operators that it is no longer dependable. This brings up the possibility of denial of service assaults, which are crucial but sometimes difficult to handle. Monitoring programs provide us with the archetypal example of systems meant to be consistently accessible, much as we have seen military communications systems built to ensure secrecy and accounting systems whose aim is to preserve record authenticity. If there is a burglar in my bank vault, I

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

don't really care who finds out so secrecy is unimportant to me or who informed me so authenticity is unimportant to me nevertheless, I do care that an effort to notify me is not blocked. Historically, just 9% of computer security research focused on authenticity, 90% on confidentiality, and 1% on availability. However, real assaults and company spending usually go in the other direction: more money is spent on availability than on authenticity and confidentiality put together. Alarm systems are also the best source of availability-related information.

DISCUSSION

Threats and Barriers

Physical security is fundamentally the same as computer security in that you do a threat analysis, create a system that includes tools and protocols, test it, and so on. A facility may use strong tactics, like guards and razorwire fences, to dissuade intruders, or gentler approaches, such becoming unnoticeable [1], [3]–[6]. Then, it will contain one or more levels of obstacles and sensors whose purpose it is to deter accidental invaders, spot intentional attackers, and make it impossible for them to swiftly circumvent your protection. An alert system that will prompt a timely reaction will be added to this defense-in-depth strategy. Doors will be built within the barriers to allow authorised workers to enter and exit; this calls for some kind of access control system, which might range from metal keys to biometric scanners. Finally, operational controls will be used to support these efforts. How would you react, for instance, if the bad guys kidnapped the family of your facility manager?

As I said earlier, one of the ways to encourage your people to embrace dual controls and incorporate them into their work culture is by emphasising the fact that these controls safeguard both the employees and the assets. Physical security is just as important as computer security in that neither can function effectively until operational security is ingrained in the culture of the company. Additionally, it's critical to obtain unified operational security across the physical, business, and information domains: protecting a vault containing $100 million worth of diamonds with $10 million is pointless if a bad guy can infiltrate your system, create a false delivery order, and dispatch a DHL van to retrieve the diamonds from reception. Another reason you, as the information security expert, must pay attention to the physical aspect is that without it, you won't get comprehensive security.

Deterrence: The first thing to think about is whether you can stop evil individuals from even attempting to break in. If you can, try to make your asset invisible and unnoticeable. It may be a plain suburban structure; in a city with sky-high real estate costs like Hong Kong, it might be the bottom level of a bland skyscraper.

It affects where you live since some areas have considerably lower crime rates than others. This depends in part on how well-protected neighbouring homes are, as well as how simple it is for thieves to identify those that are. Some property owners may transfer crime to their neighbours if they just install visible alarms, but invisible alarms that catch criminals rather than merely send them next door may have significant positive externalities. For instance, Ian Ayres and Steven Levitt investigated the impact of Lojack, a radio tag that is hidden within automobiles and helps the police track down stolen vehicles. Car thieves are swiftly apprehended in places where many vehicles have Lojack, and "chop-shops" that disassemble stolen vehicles for components are shut down. According to Ayres and Levitt, even though installing Lojack costs a driver roughly $100 per year, the decreased automobile crime experienced by others results in a $1500 societal benefit. As many individuals would free-ride off their neighbours, one conclusion is that the free market may undersupply effective alarm services. Only wealthy people, those with newer automobiles, or those who are very loss-averse will install alarms. The same rule holds true for real estate; a wealthy area where a good proportion of homes have high-end alarm systems that discreetly contact the authorities is a risky location for a thief to operate.

But by no means is it everything. A sizable body of scholarship on employing environmental design to deflect and repel threats has emerged since the 1960s.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Much of this developed when criminologists and architects discovered which architectural features increased or decreased the likelihood of crime in low-income homes. Elizabeth Wood recommended architects to make apartment units more visible to inhabitants and to designate gathering places where people might congregate and maintain apartment doors in view in order to promote social supervision since regions that are hidden from view are more susceptible. Buildings have to be made to "release the latent sense of territoriality and community" that people have, according to Oscar Newman, who extended this idea into the notion of "Defensible Space" in 1972.

Small courtyards are preferable to big parks because trespassers are more likely to be seen and challenged there. The four "model" villains in our collection are representative of Ray Jeffery's model, which was created at the same time and is based on psychology rather than sociology to account for the vast variances between individual offenders. Not all intruders are the same and are reasonable. Numerous antiquated notions regarding deterrence are called into question by Jeffery's renowned book, "Crime Prevention Through Environmental Design." Old timers preferred bright security lights, but they produce glare and shadowy areas where criminals may hide. It is preferable to have a refined façade with windows facing out into walkways and parking lots. Cyclone fences with barbed wire were formerly believed to be beneficial, but they now convey a lack of human control. A common space with picnic tables and regular activity has a stronger deterrent impact. Trees are also beneficial because they provide the impression that shared spaces are safer (perhaps as a nod to our ancestors' grasslands, when the presence of some trees allowed us to spot approaching predators and flee to safety). Access is important as well, and defendable areas should have just one exit so that would-be burglars fear being trapped. For instance, it has been shown that CCTV cameras only serve to discourage crime in locations like parking lots where there is only one exit. There are also various techniques that have been developed over the years, such as placing low thorn bushes behind windows and employing passing cars to increase site visibility. The more recent standards like provide guidance on these.

Walls and Barriers: Anyway, after deciding which environmental aspects to use to discourage Derek or Charlie from attempting to get into your site and how to make it more difficult for Bruno to choose which of your sites he should break into, you then have the challenge of constructing the physical barriers.

Determine what it is that you are really seeking to defend as your first duty. Banks used to take tremendous measures to make life very difficult for thieves, but this had its limitations since a thief could always threaten to kill a client. Thus, the mentality had changed to "give him all the money he can see" by a generation ago. The remainder of retail now adheres to this paradigm. After a botched heist that resulted in the deaths of three workers, Starbucks evaluated physical security in 1997. They took the decision to relocate the safes from the manager's office to the front of the shop, where they were clearly visible to both the control room through CCTV as well as to employees, customers, and onlookers. Customer service was enhanced as a bonus. A number of U.S. sites tried the new design, and the increased sales and decreased losses resulted in a positive return on investment. In fact, I've seen that more and more young people are leaving their vehicle keys at the front door at home. If someone were to get into your home and take your automobile, would you really want to fight them with your hands?

After deciding on your protection objectives, the second step is to determine what security boundaries will be used for what reasons and where they will be placed. The supply of vehicle traps to stop car bombs from being carried near to recognisable terrorist targets has lately seen expansion. A typical mistake, meanwhile, is to ignore regular risks in favour of uncommon but 'interesting' ones. A terrorist might blow himself up at your main gate without any ill effects, but an environmental protester could cripple your factory and cost you hundreds of millions of dollars in lost production by climbing on the roof, cutting a hole, and dropping some burning newspaper.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Mechanical Locks: A few events in the past few years that revealed the weakness of numerous inexpensive mechanical locks have substantially disrupted the locksmithing sector. Bumping is the first of them. By employing equipment that are now easily accessible, this approach allows many locks to be unlocked quickly and without harm by untrained individuals. Its primary target is the pin-tumbler lock, which Linus Yale first developed in 1860 (see Figure 1). Although several companies now create variations, this was first used in ancient Egypt. Yale rediscovered it, and today it is sometimes referred to as a "Yale lock."

Figure 1: A cutaway pin-tumbler lock (Courtesy of Marc Weber Tobias).

These locks have a cylindrical plug that is enclosed in a shell and restrained from turning by a number of pin stacks. Usually, there are two or three pins in each stack, stacked one on top of the other. A top pin or driver pin, which is spring-loaded, pushes the bottom pin as far down into the keyway as feasible. The bottom pin, also known as the key pin, makes direct contact with the key. When the right key is used, the gaps between the top and bottom pins line up with the plug's edge and form a shear line, allowing the plug to be twisted. A common home or office lock may contain five or six pins, and each pin's gap may be in ten distinct locations, resulting in a theoretical key variety of 105 or 106 potential key variations. Because of mechanical tolerances and key-cutting limitations, the real number will be smaller.

For years, it had been known that, with the right tools, such locks could be picked. Details may be found in the MIT Lock Picking Manual or in books by authors like Marc Weber Tobias. The fundamental concept is to use a tension wrench to gently twist the plug, then a lockpick to manipulate the pins until they all line up along the shear line. Such methods are used by intelligence agencies, locksmiths, and high-level criminals; nevertheless, they need a lot of practice, and in many countries, it is illegal to own the necessary instruments for information on the regulations in the USA. Lockpicking was formerly regarded to pose a danger mainly to high-value targets like investment banks and embassies where stealthy entrance was valuable to an attacker.

It has recently been discovered that an attacker may insert a bump key that has been carefully produced, with each tooth positioned at the lowest pin position and a slightly rounded shoulder. These keys are often referred to as "999" keys since the lowest set of teeth, which is number 9, is bitting. Then, using his fingers to slightly twist the key, he may tap the key's head with a rubber mallet. When the pins are shocked, they bounce upward; when the spring forces them back down, but with a gap at the cylinder edge, they stick due to the applied torsion. The result is that the lock may be unlocked with only a few strokes of the mallet. This approach has been around for a while, but lately improved tools and methods made it considerably more efficient. A 2005 white paper by Barry Wels and Rop Gonggrijp of the Open Organisation of Lockpickers (TOOOL), a Dutch 'lock sports' organisation as the hobby of amateur locksmithing is becoming to be termed, made the information public. The message was widely disseminated through television coverage. Following that, lock specialist Marc Weber Tobias provided a technical study; in his opinion, the greatest danger from bumping is that it de-skills lockpicking. The repercussions might be disastrous. For instance, it has been shown that locks on American mailboxes and pin-tumbler locks, which account for 70% of the domestic market, are both simple to open. An arms race has begun as a result of the Dutch paper and the attention that followed it, with suppliers creating more intricate designs and amateur

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

locksmiths reporting bumping assaults on many of them.

Electronic Locks: One reason why electronic locks are beginning to acquire market dominance is the difficulty of revocation. Hotels have been utilising card locks since the 1970s, so they have been around for a while. There is a huge variety of product options that use a variety of methods, including contactless smartcards, PIN pads, and biometrics. Most of the topics in this book may be applied in one way or another to the design, assessment, and assurance of many of these, and many of them can be avoided in different ways. Additionally, certain electromechanical locks, which combine mechanical and electrical (or magnetic) components, are difficult to break without resorting to physical force. However, from the perspective of a business utilising locks to secure critical locations, the main issue is not so much the locks themselves as it is how to connect dozens or even hundreds of locks across a structure. Consider a research facility where some of the rooms contain priceless innovations that haven't yet been granted a patent, or a legal company where the offices may hold highly confidential information about impending acquisitions. Both insiders and outsiders are a concern here [2], [7].

Alarms

Alarms are utilised for much more than just preventing break-ins. Their uses vary from keeping tabs on freezer temps in grocery stores (so employees don't "accidentally" turn off freezer cabinets in the expectation of receiving food to take home) to monitoring improvised explosive devices in Iraq and other places that are sometimes booby-trapped. It is more practical to talk about them in relation to burglary and the security of storage areas for assets like computers. Alarms also provide a solid foundation for understanding the broader issue of service denial assaults, which dominate the field of electronic warfare and are a concern globally.

Alarm standards and specifications range across nations and between various danger levels. For this kind of job, you will often hire a nearby specialized company, but as a security engineer, you must be aware of the problems. Alarms frequently have an impact on larger system designs. In my own professional experience, this has included everything from the alarms built into automated teller machines to the assessment of the security of the communications used by an alarm system for significant risks like wholesale jewellers to continuously staffed systems used to protect bank computer rooms.

A bank vault alarm is a relatively straightforward situation since it is extremely well shielded against manipulation at least by outsiders. I'll take into account the challenge of creating an alarm system for an art museum in order to approach the issue more broadly. Because attackers may enter as regular people throughout the day and create trouble, this is more intriguing. We'll pretend Bruno, the skilled professional art thief, is the assailant. Bruno is often portrayed as organizing sophisticated assaults on alarm systems after spending days studying the construction drawings in the nearby town hall. This sort of incident is probably covered in the news multiple times a year [8]–[10].

CONCLUSION

Whether they like it or not, security engineers must work with physical security in addition to computers and cypher systems. In fact, just as the convergence of computers and telecommunications led to the displacement of traditional phone company methods of operation by computer-industry standards and working procedures, so too will the rising automation of physical security systems bring the world of barriers, locks, and alarms into our sphere of influence. Buildings of the future are probably going to have a lot more integrated entrance controls, alarms, and system security. Instead of retired police officers, system administrators will be in charge of managing them. I highlighted a few important points in this chapter. First, environmental conservation is important. There is a lot of knowledge about how lighting, gardening, and design may affect the environment. Second, despite what you may believe, physical locks are not always secure. Recent advancements in covert entry

technologies have resulted in the widespread release of techniques that weaken even the most commonly used high-security locks and popular mechanical locks. The tools required for such assaults on several locks, including bump keys, are readily accessible online. Third, alarms the one part of physical security that is currently largely automated offer a wealth of lessons. Alarms serve as an excellent illustration of a system whose security strategy prioritises availability above secrecy or integrity. When dealing with service-denial assaults in different situations, they might provide us with some insightful information.

REFERENCES

[1] A. Ahmed *et al.*, "Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems," *IEEE Trans. Ind. Appl.*, 2019, doi: 10.1109/TIA.2019.2928500.

[2] F. Frattini, U. Giordano, and V. Conti, "Facing cyber-physical security threats by PSIM-SIEM integration," in *Proceedings - 2019 15th European Dependable Computing Conference, EDCC 2019*, 2019. doi: 10.1109/EDCC.2019.00026.

[3] Z. Min, G. Yang, A. K. Sangaiah, S. Bai, and G. Liu, "A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems," *Eurasip J. Wirel. Commun. Netw.*, 2019, doi: 10.1186/s13638-018-1317-9.

[4] I. Elgendi, M. F. Hossain, A. Jamalipour, and K. S. Munasinghe, "Protecting Cyber Physical Systems Using a Learned MAPE-K Model," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2927037.

[5] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," *IEEE Trans. Ind. Informatics*, 2019, doi: 10.1109/TII.2018.2884728.

[6] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, 2019, doi: 10.1109/TSG.2017.2776279.

[7] Y. Tang, M. Li, Q. Wang, and M. Ni, "A Review on Research of Cyber-attacks and Defense in Cyber Physical Power Systems Part Two Detection and Protection," *Dianli Xitong Zidonghua/Automation of Electric Power Systems*. 2019. doi: 10.7500/AEPS20180906007.

[8] X. Li, C. Zhou, Y. C. Tian, and Y. Qin, "A Dynamic Decision-Making Approach for Intrusion Response in Industrial Control Systems," *IEEE Trans. Ind. Informatics*, 2019, doi: 10.1109/TII.2018.2866445.

[9] K. Bou Chaaya, M. Barhamgi, R. Chbeir, P. Arnould, and D. Benslimane, "Context-aware System for Dynamic Privacy Risk Inference: Application to smart IoT environments," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2019.07.011.

[10] M. Wu, "Intrusion Detection for Cyber-physical Attacks in Cyber-manufacturing System," *ProQuest Diss. Theses*, 2019.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Discussion on Monitoring and Metering

Dr. Sivasankara Reddy Nanja Reddy
Assistant Professor, Department of Engineering Physics, Presidency University, Bangalore, India,
Email Id-sivasankarareddy@presidencyuniversity.in

ABSTRACT: ***The identification, analysis, and prevention of security events depend on monitoring and metering, which are fundamental elements of security engineering. In order to secure the integrity, availability, and confidentiality of systems and resources, this abstract focuses on the function of monitoring and metering in security engineering and examines their relevance, approaches, and technologies. In the context of security engineering, the abstract opens by describing monitoring and metering. In order to spot any security flaws or abnormalities, monitoring entails the ongoing observation and analysis of system activity, network traffic, and user behavior. For efficient resource management and capacity planning, metering, on the other hand, focuses on measuring and monitoring resource utilization, such as bandwidth, CPU consumption, or storage capacity. The importance of automation and machine learning in monitoring and metering is also covered in the abstract. It examines how to increase the effectiveness and accuracy of security monitoring by using sophisticated analytics, anomaly detection algorithms, and behavioral analysis methodologies. It highlights the need for adaptive and intelligent systems that can take lessons from past data and dynamically modify security precautions to fend off new attacks. The abstract also covers the legal ramifications of monitoring and metering practices as well as privacy issues. It emphasizes the need of abiding by relevant laws and moral standards in order to safeguard people's right to privacy while maintaining proper security precautions.***

KEYWORDS: ***Prepayment Meters, Postal Meters Resource Management, Tachographs.***

INTRODUCTION

Monitoring and measuring the environment is a major problem for many security systems. They have a lengthy history. The steam engine's creator, James Watt, issued licences for his inventions using a sealed counter that counted the number of engine rotations. His inspectors periodically scanned this counter and invoiced the licensee for fees [1]–[5]. Older mechanical systems are being quickly replaced by electronic systems that utilise encryption and tamper-resistance while also offering up a wide range of new uses. There are many applications for ticketing, ranging from transportation to sports to theatre; my case study for ticketing is the meters used for utilities like gas and electricity. The most well-known of these could be taxi metres, but I'll focus on tachographs devices used in Europe to track the speed and working hours of truck and bus drivers and in the USA to track the arrivals and departures of bank trucks. The electronic postage meter used to frank mail is the subject of my third case study.

You may remember that all it takes to discredit a burglar alarm is for it to look unreliable. The handling of such service-denial assaults may be challenging enough; meters provide another nuance. Although sensor defeats obviously important, when we spoke about an alert in a bank vault, we were more worried about assaults on communications. However, many metering systems are physically far more exposed. If a taxi driver (or owner) wants the meter to show more miles or minutes than were really put in, he may alter the inputs or attempt to interfere with it in order for it to overmeasure. When it comes to tachographs, the situation is the opposite: truck drivers often want to exceed the speed limit or put in dangerously lengthy shifts, thus they want to use them to disregard portions of their driving. Utility customers also have an incentive to get their metres to stop recording part of the passing power. These allow the attacker to either fail the device outright or produce misleading readings. There are also marketplaces for dishonest individuals who can offer exploits, such as phone power meter tickets or gadgets that can be fitted in a car to trick a taxi meter or tachograph.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

We are also concerned with evidence in numerous metering and vehicle monitoring systems (as well as with nuclear verification. By tampering with communications (such as replaying previous messages, an adversary may gain an edge, or they could make up evidence that someone else did it. The threat model for postal franking systems has some interesting twists; the post office is mostly concerned with stopping wholesale fraud, like dishonest direct marketers who pay off postal workers to smuggle a truckload of mail into the system. It is not enough for the attacker to cause a failure in these systems because then he cannot post his letters. As a result, it is focused more inwardly than outwardly.

DISCUSSION

Prepayment Meters

Prepayment meters are the subject of our first case study. There are several systems where the user purchases a token such as a smartcard, a magic number, or a cardboard ticket with a magnetic strip in one location and utilises the stored value in another. Examples include the stored-value cards used to operate photocopiers in libraries, ski resort lift tickets, and university residence halls' washing machine tokens. Many transit tickets are comparable, particularly when the ticket validation terminals are installed on buses or trains and are not often available online. The primary protection objective in these systems is to stop bulk duplication or mass forging of the stored-value tokens. It's not difficult to duplicate a single tube ticket, and it's simple to use the same magic number again [2], [6], [7].

If we make each token unique and keep track of how they are used on both sides, this won't matter. However, things get more challenging when the token-accepting device lacks a communication path back to the ticket issuer, necessitating offline replay and forgery detection on a terminal that is often open to physical assault. So, if we just use a single universal master key to encrypt all of our tokens, a bad guy might steal it from a terminal and set up shop at token-selling establishments.

On the server end of things, there are also assaults. One clever assault took advantage of the fact that when a card was recharged, the vending machine first read the previous amount, then requested for money, and finally wrote the updated amount. This technique was employed in the employee cafeteria of one of our neighbourhood supermarkets. The trick was to place a card with money on it say, £49 on top of a card that was otherwise blank. After removing the top card and inserting a £1 coin, the machine would properly write £50 to the empty card. The criminal was left with two cards for a combined total of £99 as a result. Two levers that extended to grasp the card in the machine were intended to stop this sort of assault. This safety measure, however, might be readily circumvented by cutting the corners off the top card (see Figure 1). This attack is intriguing since no amount of card content encryption will prevent it from happening. Theoretically, it could be halted by maintaining records at both ends, but they would need to be made with a little more care than normal.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

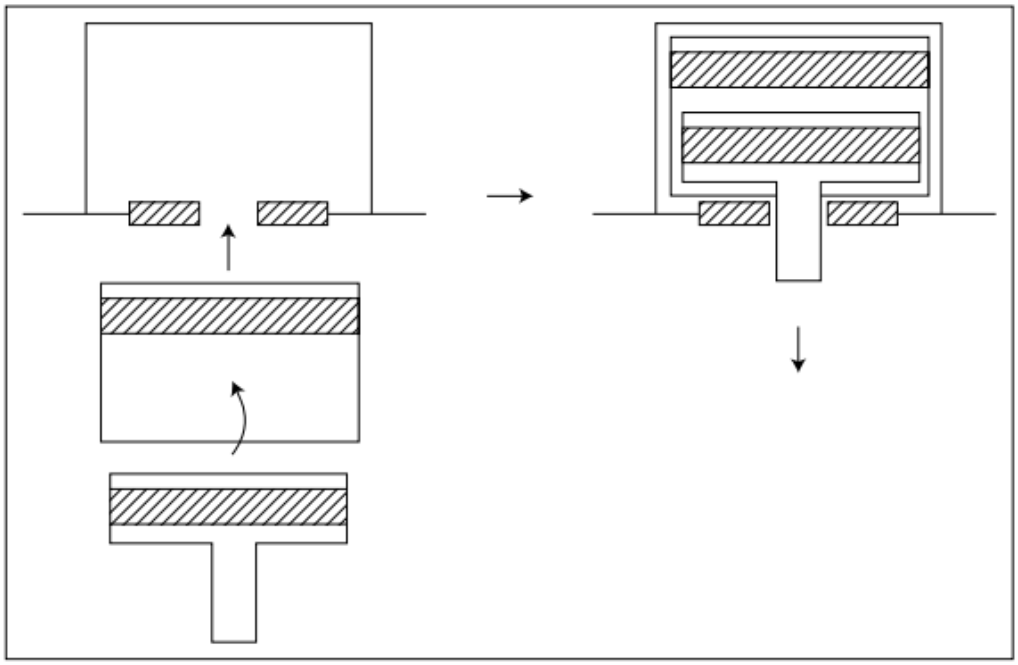

Figure 1: Superposing two payment cards.

However, we must be careful not to get carried away with such ingenious methods or we run the danger of being so engrossed with even more deft countermeasures that we once again succumb to the Titanic Effect by disregarding the system level problems. Petty fraud is simple in the majority of ticketing systems. An electricity meter can have a bypass switch connected across it, a free rider can skip the barrier at a subway station, and a scanner and printer can be used to counterfeit barcoded parking lot tickets and ski lift tickets. The aim is to stop fraud from being institutionalised. Therefore, there should be more significant controls in place to prevent someone from forging tickets on a big enough scale to create a black market that may harm your client's company. Petty fraud should be at least somewhat uncomfortable.

Utility Metering

Householders in a number of European nations who are unable to get credit (due to being on assistance, having a court order against them, or for other reasons) purchase gas and electricity services using prepayment metres (Figure 2). They used to be coin-operated, but due to the expense of coin collecting, merchants instead developed token-based metres. 3.6 million electricity metres and 2 million gas metres are now in use in the UK. Due to a national priority initiative to electrify the townships, growth in South Africa moved exceptionally quickly. Prepayment was the only option since many of the homes were improvised and the owners lacked even addresses (much alone credit scores). There are now 5.5 million of these metres in use in South Africa, and 1.5 million have been exported to other African, Latin American, and international nations. The consumer enters a store and purchases a token, which might be a magic number, a smartcard, or even simply a disposable cardboard ticket with a magnetic strip. 1.2 million power metres in the UK use magnetic tickets, whereas 2.4 million use smartcards1. The majority of metres in South Africa use a magic number. This option may be the most practical for customers since no specific vending machine is needed; a ticket may be issued at a grocery store checkout, an ATM, or even over the phone.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Figure 2: A prepayment electricity meter (Courtesy of Schlumberger).

The token is essentially simply a series of bits that contain one or more instructions and are encrypted with a meter-specific key, which the meter then decodes and executes. The majority of tokens include text that reads, "meter 12345 dispense 50KWh of electricity!" The meter is supposed to distribute the bought quantity before cutting off the flow. Some tokens also serve engineering purposes. The meter may need to know the relative costs and the periods at which the tariffs vary, for instance, if the electricity supplier has different rates for the day and the evening. These and keys may both be changed using unique tokens. Smartcard-enabled metres feature a back channel that allows them to communicate use trends, attempted tampering, and other information to the power provider; magnetic-ticket and magic-number metres do not.

The production of these metres has grown significantly. Prepayment metres were the only way the South African government could keep its election promise to fast electrify millions of households. Growth in the third world is robust. Prepayment metres are mostly used in affluent countries to save administrative expenses. When the costs of meter reading, billing, credit management, bad debts and other expenses are added together, electric utilities discover that billing systems may eat nearly 20% of retail customer income. Prepayment systems often cost less than 10% of the whole cost; the store that sells the tokens receives 5% of the sale, while the infrastructure, metres, and other costs are almost equal.

How the System Works

Prepayment meter security requirements seem to be simple. Tokens shouldn't be simple to counterfeit, and real ones shouldn't function twice in the same meter or in the incorrect one. One method is to utilise smartcard chips of some kind to make the tokens tamper-resistant; an option is to link each token to a certain meter in order to prevent someone from using the same magic number in two distinct metres. Tokens must be individually identifiable using serial numbers or random numbers to prevent double usage in the same meter. But a surprising amount of field work has been required experience to transform the concept into a reliable system.

For the meter to be able to trust the vending station's instructions, it requires a cryptographic key. Each community in the original system featured a single vending machine, often housed in a nearby shop. The device contains a vend key KV that serves as the neighborhood's master key and, when required, generates the device key by encrypting the meter ID under the vend key:

$$KID = ID + KV$$

The primary diversification strategy for parking lot access devices was discussed in Chapter 3 and is the same here. extending the vend key KV to a collection of meter keys KID offers a fairly simple approach in which all the tokens are purchased locally. After the system went live, we discovered that actual life was less simple. Due to deregulation of the electricity sector in Britain, there are now many distinct electricity firms that purchase energy from generators

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

and sell it to homes over a shared infrastructure. As a result, metering systems must handle several power providers with various pricing structures. Since many South Africans drive considerable distances from their hometowns or townships to their workplaces, they are seldom at home during regular business hours and prefer to purchase tickets where they work. As a result, we had to serve various merchants by allowing consumers to register at a vending machine located elsewhere. In a manner similar to ATM networks, this entailed protocols for sending a customer meter key from the vending station that 'owns' the meter to another station and for passing sales data in the reverse way for balancing and settlement. Online vending, which was introduced in 2007, allows a client to purchase a magic number from a central token server via the Internet or through their mobile device.

Four million consumers may be served directly by this server, together with 10,000 online vending machines like ATMs. The term "nontechnical losses" is used to describe power theft caused by tampering with metres or unauthorized direct connections to mains cables. Statistical balancing is used to identify these types of losses. The method compares token sales to those homes with readings on a feeder meter that may service 30 residences.

What Goes Wrong

Service denial is still a significant problem. The sole source of information on how much power has been sold in cases where there is no return path from the meter to the vending station is the vending machine itself. The vending machine operators are often small-time business owners or other local entrepreneurs who have little money and are thus permitted to sell power on credit. Some agents simply ditched their equipment and reported it stolen when they were unable to pay the operating company's power bill at the end of the month. When a company, such a local government, is permitted to sell significant quantities of power via several outlets, there is unquestionably a vulnerability, but it is manageable with tiny agents. Dealing with untrustworthy (and reciprocally untrustworthy) principals required a significant amount of intricacy.

Environmental robustness is essential, just as it is with burglar alarms. The meter is really a microprocessor with a 3-kilometer lightning conductor connected, and many locations experience violent thunderstorms in addition to the wide range of temperatures (which are as changeable in South Africa as they are in the continental United States). Customers who complained after metres were struck by lightning received reimbursement for the amount they said was still in use. In order to mimic the impact of the lightning, they proceeded to put live mains cables into the meter. It was discovered that if a certain component of the circuitry (located beneath the token slot) was broken, one brand of meter would provide limitless credit. Service denial attacks were successful enough to gain popularity.

To make matters worse. The costliest security blunder in the programr occurred when children in Soweto noticed that a certain brand of meter would reach maximum credit during a brown-out, which is a drop in electricity from 220 to 180 volts. Soon, youngsters started tossing steel chains over the 11KV feeders and counting every meter in the area. This was due to a straightforward defect in the meter ROM that went undetected since brown-out testing wasn't stated. The fundamental issue was that environmental standards from wealthy nations couldn't be used in Africa and needed to be revised. 100,000 metres had to be taken out and re-ROMmed, which had an impact on the business and almost caused the responsible firm to fail. There were a lot more bugs. One particular kind of meter sold power worth so much at such-and-such a rate rather than a specific amount. It found out that vending personnel could reduce the fee to a very little amount, making it almost perpetually operational. Another permitted refunds, but a duplicate of the returned token might still be utilised (it is difficult to blacklist the serial numbers of refunded tokens in follow-up token requests since tokens are hoarded and used improperly). By alternating inputting copies of two tokens, another might be charged forever since it only remembers the latest token serial number submitted. Similar to cash machines, the genuine security breaches were caused by errors and defects

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

that were often difficult to find, but were still opportunistically exploited. Sometimes these flaws were severe and required millions of dollars to correct.

Taxi Meters, Tachographs and Truck Speed Limiters

A variety of techniques are used to keep an eye on and manage cars. The odometer in your automobile is most likely the most well-known. When purchasing a secondhand automobile, you'll be worried that the vehicle has been "clocked," or that its stated mileage has been lowered. Clocking is evolving into a kind of computer fraud as odometers become digital; a conviction has already been documented. Chipping, or changing or reprogramming the engine controller, is a related issue. There are two main rationales for doing this. The engine controller is the obvious target if you want to steal a car without taking the key (you might replace the controller in the street, or else tow the car and replace or reprogram the controller later). First of all, the engine controller serves as the server for the remote key-entry systems that prevent most modern cars from theft, as described in Chapter 3. Second, individuals modify the engine controllers in their vehicles to raise their speed, which is not preferred by the makers due to the rise in warranty claims for burned-out engines. In order to increase the controllers' tamper resistance or at the very least, tamper evidentiality details this intriguing arms competition. Some modern automobiles store records that are sent to the manufacturer during maintenance. In 1990, General Motors began installing black boxes in some of its cars to capture collision information. About six million automobiles had been instrumented by the time the logging was made public in 1999, and the revelation sparked objections from privacy campaigners. In fact, ESCAR, a conference entirely focused on electronic security in automobiles, has just been held. The taxi meter may be the most well-known of the several monitoring devices that are available in addition to those supplied by the engine manufacturer. If he can get away with it, a cab driver will adjust the meter to reflect more miles driven (or minutes waited). From aeroplanes to fishing boats to armoured bank trucks, several additional types of "black box" are utilised to record the movements of vehicles, and their operators have varying degrees of motivation to tamper with them. The black boxes provided by insurers who sell "pay-as-you-drive" insurance to young and high-risk drivers are a recent development. These boxes contain satellite navigation systems that allow the insurer to charge a few pennies per mile for afternoon driving along a country road but a few dollars per mile for evening driving in an inner city. This may be the only insurance option for many young people in a few years; if hazardous drivers swarm to any flat-rate contracts that are still available, they may become expensive.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

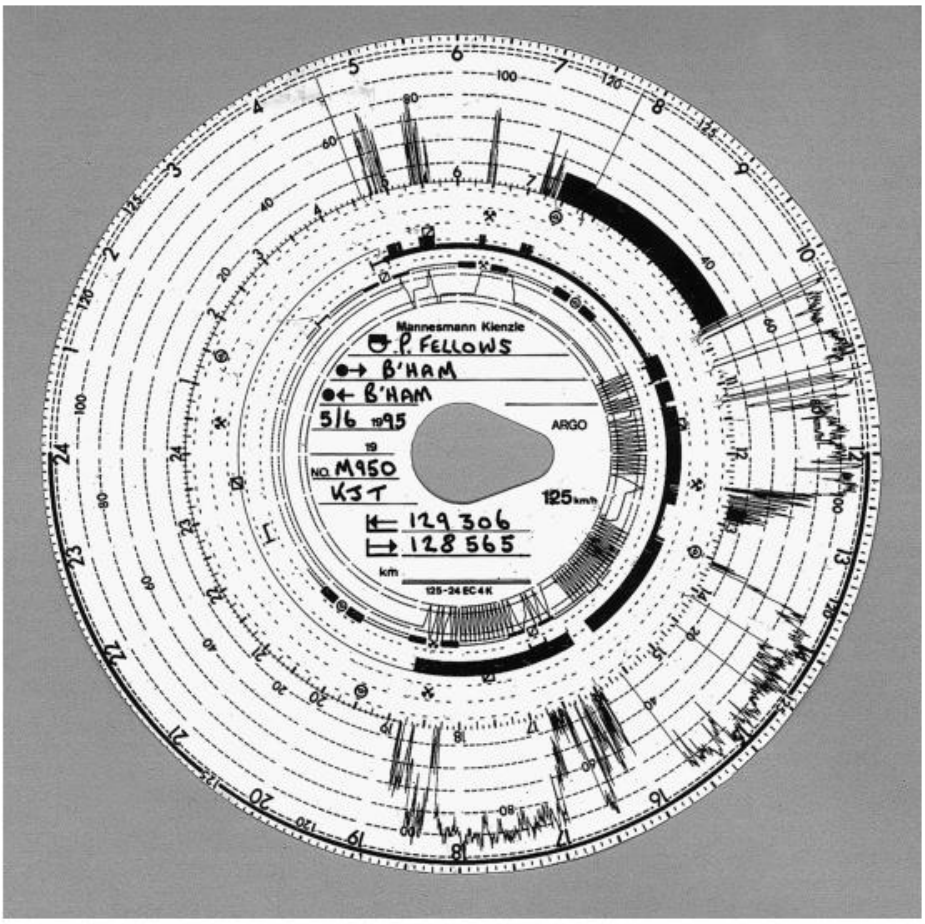

Figure 3: A tachograph chart

.

Therefore, there will be a tremendous incentive for any young guy who wants to impress females by driving about town on a Saturday night to defeat the black box [8], [9].

CONCLUSION

Monitoring or measuring any component of the environment is a common problem for security systems. They include utility metres, taxi metres, postal metres, and tachographs. Later chapters will cover additional metering and payment methods, including those that stop printer cartridges from printing after a set number of pages and prepay scratch cards for mobile phones, which may be the biggest application-specific payment method in the world.

As the globe transitions from analogue to digital technology, many monitoring, metering, and payment systems are being updated. Redesigns may be successful or unsuccessful in different situations. The new digital prepayment energy metres have been used successfully across the developing world as a technology that enables utilities to sell electricity to customers who don't even have addresses, much alone credit histories. Digital tachographs have been far less spectacular; they just perform the same functions as the previous analogue devices, although less effectively. Postage metres, our third example, seem to be a success.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Similar to burglar alarms, the security of these systems depends on their reliability; while developing one, one must carefully consider the types of service denial attacks that might be launched against system components. Key management may be problematic, particularly in low-cost, widely dispersed systems when the need for a centralised key management facility or a sufficient pool of dependable employees is not there. Systems often need to be built on the least expensive microcontrollers feasible and may have to deal with a large number of parties that are sceptical of one another. They often end up in the hands of the opposition. Additionally, there are other application-level nuances that must be addressed if you want your design to be successful.

REFERENCES

[1] H. Zhu, S. Wang, Z. Li, X. Yan, Z. Song, and P. Gong, "A new high-precision timely monitoring and metering system for early kick and loss," *Nat. Gas Ind. B*, 2019, doi: 10.1016/j.ngib.2019.01.015.

[2] S. G. Priyadharshini, C. Subramani, and J. Preetha Roselyn, "An IOT based smart metering development for energy management system," *Int. J. Electr. Comput. Eng.*, 2019, doi: 10.11591/ijece.v9i4.pp3041-3050.

[3] B. Wu, N. Tan, and X. P. Yu, "An Energy Metering Chip with a Flexible Computing Engine," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2909435.

[4] O. Florencias-Oliveros, J. J. González-De-La-Rosa, A. Agüera-Pérez, and J. C. Palomares-Salas, "Reliability monitoring based on higher-order statistics: A scalable proposal for the smart grid," *Energies*, 2019, doi: 10.3390/en12010055.

[5] F. Fortes and V. Fialho, "Smart energy meter for iot applications," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.K2168.0981119.

[6] P. Van Aubel and E. Poll, "Smart metering in the Netherlands: What, how, and why," *International Journal of Electrical Power and Energy Systems*. 2019. doi: 10.1016/j.ijepes.2019.01.001.

[7] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," *IEEE Commun. Surv. Tutorials*, 2019, doi: 10.1109/COMST.2019.2899354.

[8] G. Xu, Y. Shi, X. Sun, and W. Shen, "Internet of things in marine environment monitoring: A review," *Sensors (Switzerland)*. 2019. doi: 10.3390/s19071711.

[9] S. Schuch, D. Dignath, M. Steinhauser, and M. Janczyk, "Monitoring and control in multitasking," *Psychonomic Bulletin and Review*. 2019. doi: 10.3758/s13423-018-1512-z.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Brief Discussion on Nuclear Demand and Control

Mr. Madhusudhan Mariswamy
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-madhusudhan@presidencyuniversity.in

ABSTRACT: ***In terms of security engineering, nuclear plants and the materials they are involved with present particular difficulties. It is crucial to protect nuclear resources and ensure that they are used in a regulated manner in order to stop bad actors from gaining access, stealing, sabotaging, or acquiring nuclear weapons. This abstract examines security engineering's relationship to the complex dynamics of nuclear demand and control. The abstract opens with a description of the global nuclear environment, emphasizing the spread of nuclear technology, materials, and facilities on a global scale. It emphasizes the dangers that might arise from nuclear activity, such as the possibility of nuclear terrorism and the catastrophic effects of nuclear catastrophes or accidents. The abstract then explores the idea of demand and control in the context of nuclear power. The need for nuclear materials, technology, and capabilities is examined, including both legal and illegal uses, such as the generation of electricity and medical research, as well as legitimate civilian applications, such as the creation of nuclear weapons. The abstract goes into further detail on how security engineering may be used to build reliable control systems and manage nuclear demand. The need of comprehensive security frameworks that take into account human dependability, physical security, access restrictions, intrusion detection systems, and surveillance technologies is discussed. In order to handle the worldwide difficulties of nuclear demand and control, it also emphasizes the significance of international collaboration, information exchange, and regulatory frameworks.***

KEYWORDS: ***Cryptomathematics, Intrusion Detection Systems, Nonproliferation, Surveillance Technologies.***

INTRODUCTION

The United States and other nuclear powers have spent enormous sums of money safeguarding not only nuclear warheads but also the supporting infrastructure, industry, and materials due to the catastrophic harm that could be caused by the unauthorised use of a nuclear weapon or by the proliferation of nuclear technology to unsuitable states or substate groups. Nuclear security is more important than ever because of the rising worry about global warming. How can we construct new nuclear power plants without significantly raising the possibility that malicious individuals get weapons or fissile materials? There has been a startling quantity of disclosed nuclear security knowledge. In reality, even if it were deemed desirable, there are strict restrictions on how much may be kept hidden. Although several nations (including Japan, Australia, Switzerland, etc.) have the technology to make nuclear weapons, they have chosen not to (leading to the maintenance of restrictions on nuclear materials in a civilian context). The true strength of nonproliferation is mostly cultural; it has been developed over time via diplomacy and the restraint of nuclear countries, who since 1945 have refrained from using these weapons even when they were being defeated by non-nuclear nations [1]–[3].

International nonproliferation treaties, such the Convention on the Physical Protection of Nuclear Material, which is upheld by the International Atomic Energy Agency (IAEA), support the culture. Civil reactors generate 11 tonnes of plutonium year, and if humanity is to depend on nuclear energy in the long run, we will be producing plutonium both directly and as a byproduct of uranium burning. Therefore, methods for protecting the material must be developed, and these methods must inspire trust on a global scale, not only among governments but also among an increasingly dubious public1.

As a result, the nuclear program has given rise to a wide spectrum of security technologies. With almost

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

limitless resources, the three U.S. Department of Energy weapons laboratories Sandia, Lawrence Livermore, and Los Alamos have toiled for two generations to make nuclear weapons and materials as safe as possible. Some of their less interesting offspring, such as high-end burglar alarm systems and the realisation that passwords longer than twelve digits were useless in combat situations, have previously been discussed. One of their tricks is to thread an optical fibre around the warheads in an armoury and use interference effects to detect changes in length of less than a micron. This method will always sound an alert if any of the warheads are relocated.

We'll see much more nuclear-derived technologies in coming chapters. For instance, the U.S. Department of Energy funded the development of iris recognition, the most precise system for biometric identification of individuals, to control access to the plutonium store. Likewise, a large portion of the knowledge in tamper-resistance and tamper-sensing technology originally developed to prevent the abuse of stolen weapons or control devices. Since 9/11, there has been a rise in tension, which has resulted in the expansion of regulations, particularly when it was established that obtaining fissile materials like plutonium or uranium-235 is not essential for terrorist activities. A "dirty bomb," a weapon that would spread radioactive material across a whole city block, is another genuine danger that Islamists have discussed. Even if it doesn't result in deaths, it might generate panic and inflict significant economic harm in a financial hub. For instance, in March 2007, GAO investigators created a fictitious business and obtained a licence from the Nuclear Regulatory Commission allowing them to purchase the isotopes needed to construct such a radiological dispersion system. Americium-241 and cesium-137-containing moisture density gauges were ordered using the licence, which was printed on regular paper and changed by the investigators to vary the amount of material they could purchase. This episode raises the possibility that economic material control may become fairly pervasive, and it also raises the possibility that many of the technologies covered in this book may become more frequently used.

We are always learning about the boundaries of assurance from the field of nuclear safety. For instance, it's tempting to think that if a certain action has a chance of 1 in 10 of occurring due to human error, you can lower the likelihood to 1 in 100,000 by having five separate individuals check. The American Air Force concurred. However, in October 2007, six American hydrogen bombs were missing for 36 hours after being inadvertently placed onto an aircraft carrying cruise missiles from Minot Air Force Base in North Dakota to Barksdale in Louisiana. This was supposed to be prevented by the handlers inspecting every missile in the storage area and comparing it to a schedule (which was outdated), by the ground crew waiting for the inspection to finish before moving any missiles (they didn't), by the ground crew inspecting the missiles (they didn't look in little glass portholes to see whether the warheads were real or dummy), by the driver calling in the identification numbers to a control centre (nobody did that), and by the ground crew Before the ground personnel in Louisiana came to unload the missiles and found out they were live, the jet had taken off, flown to Louisiana, landed, and remained unattended on the runway for nine hours. This serves as an example of one of shared control's limitations. People will depend on others and procrastinate; this is a lesson also learned in the field of medical security. In the USAF instance, it really found out that the pilots had substituted their own "informal" timetable for the official ones. So how can you create systems that don't malfunction in this manner?

DISCUSSION

The Kennedy Memorandum

All of it was altered by the Cuban missile crisis. Policymakers in the US (as well as many others) all of a sudden started to worry a lot that a global war may break out accidentally. Allied nations like Greece and Turkey, which weren't especially stable and periodically engaged in war with one another, were home to hundreds of American nuclear weapons. There was no physical reason why these weapons couldn't be taken in a crisis as they were simply

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

guarded by minimal U.S. custodial personnel. The possibility of American commanders using nuclear weapons without authorization also caused considerable concern. For instance, a local commander under pressure could believe that if Washington realised how terrible things were there, they would authorize the use of the bomb. Three urgent investigations conducted by presidential scientific advisor Jerome Wiesner validated these concerns [4]–[7].

National Security Action Memo No. 160 was President Kennedy's reaction. This mandated that all 7,000 American nuclear weapons whether they were in the possession of American or ally forces be brought under positive U.S. control by technological methods before being disseminated to NATO headquarters. Though the concerns of a lunatic "Dr. Strangelove" were at the top of Wiesner's list, they were obviously ignored politically even though this strategy was presented to Congress as defending American nuclear weapons from outsiders.

Nuclear weapon safety mechanisms were already being developed by the Department of Energy. The fundamental idea was that for the weapon to arm, it had to detect a certain characteristic of the surroundings.

For instance, although certain free-fall bombs and missile warheads had to encounter zero gravity, artillery rounds had to accelerate by thousands of G. Atomic demolition weapons were the one exception. These are designed to be transported to their intended locations by ground forces and then exploded using time fuses. There doesn't seem to be any need for a special environmental sensor to stop purposeful or unintentional explosion. The answer at the time was a covert arming code that opened a solenoid safe lock concealed deep under the weapon's plutonium pit. Maintenance was the primary engineering challenge. The code may be discovered if the lock was disclosed, for instance, to change the power supply. Thus, using the same code in all weapons was unacceptable. One alternative was group codes, or firing codes that only a limited number of warheads shared.

In response to the Kennedy memo, it was recommended that all nuclear weapons should be secured by code locks and that there should be a "universal unlock" command that could only be issued by the president or his legal heirs. Finding a secure mechanism to transform this code to a vast number of unique firing codes, each of which permitted a limited group of weapons, was the challenge. The issue became worse when the policy switched from huge reprisal to "measured response" in the 1960s and 1970s. The President now needed to be able to equip specific batches (such as "all nuclear artillery in Germany") rather than all nuclear weapons or none. When we discover that we also require disarming codes for maintenance purposes and that we need a way to balance the trade-offs between weapon safety and effective command, it becomes evident that this is beginning to lead to a system of considerable complexity.

Authorization, Environment, Intent

The key issue was thus what security guidelines nuclear safety and command systems should follow. The principle of "authorization, environment, and intent" came to be. A warhead must fulfil three requirements in order to explode.

1. **Authorization:** The President and his legitimate successors in office, who serve as the national command authority, must have given their approval before the weapon in issue was used.
2. **Environment:** The weapon must have detected the right environmental feature. (With atomic demolition weapons, the use of a unique container is required in lieu of this requirement.)
3. **Intent:** The officer in charge of the aircraft, ship, or other unit must clearly order the employment of the weapon.

In early systems, "authorization" entailed entering a four-digit authorisation number into the device.

The way that "intent" was signalled varied on the platform. 'Use control' or the arming code for aircraft is normally six digits long. Two officers control the command consoles for the intercontinental ballistic

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

missiles; to fire the missile, each officer must input and turn a key. Whichever method is used,

The commonly held belief is that each signal must be distinct, and the approximately 22 bits obtained from a six-digit code is seen to be a suitable compromise between a number of factors. Many elements, ranging from usability to reducing the chance of unintentional arming.

Unconditionally Secure Authentication

One-time authentication codes were developed as a result of nuclear command and control. In that a keyed transformation is made to the message to produce a brief authentication code, also known as an authenticator or tag, they are conceptually comparable to the test keys, which were developed to safeguard telegraphic money transactions. Authentication codes may be made unconditionally safe since the keys are only used once. The one-time pad serves the same purpose for secrecy as they do for authentication. The perfect security offered by the one-time pad is independent of the computing resources available to the attacker. A computationally secure system might be defeated by some known calculation and relies on this being too hard.

However, there are several distinctions between the one-time pad and authentication codes. Since the authentication code is finite in length, it is always possible for the adversary to guess it. The likelihood that the adversary will be successful in doing so will vary depending on whether the adversary attempted to guess a valid message entirely from scratch (impersonation) or modified an already existing valid message in order to obtain a different one (substitution).

This should be made explicit using an example. Consider a scenario in which a commander and a subordinate have agreed on an authentication technique in which a directive is to be encoded as a three-digit number between 000 and 999. 'Attack Russia' and 'Attack China' are two possible values for the directive. Which of these will be encoded with an even number and which with an odd number will be determined by the secret key. By ensuring that the message's residue, when divided by 337, equals a secret number, which is the second component of the key, the message's veracity will be attested to.

Shared Control Schemes

Since the late 1970s, there has been worry that a Soviet decapitation strike on the U.S. national command authority may leave the arsenal intact but worthless, further complicating the nuclear command and control business. The harm that an electromagnetic pulse (and other potential assaults on communications) may inflict made it unwise to presume that communications between the authority and field commanders could be maintained over a certain level of preparedness.

The answer was discovered in a different area of cryptomathematics called secret sharing, whose advancement it assisted with. A backup control mechanism that enables various combinations of office holders or field commanders to consent to the arming of a weapon will be triggered in times of strain, according to the plan. Otherwise, it would probably be impossible to retain precise central control of that many weapons. In the case of ballistic missiles fired from submarines, there was some precedence. These exist in part to provide a second-strike capability, or the capacity to exact revenge on a nation that has attacked your country first and destroyed it. The submarine captain cannot be prevented from arming his weapons in such a situation without receiving a code from the President. As a result, ammunition is stored in safes under the supervision of the boat's officers, along with directives from the command authority over when to employ weapons [8]–[11].

Giving each of the two persons their own half of the authentication key is now an apparent approach to implement shared control. The disadvantage is that you need a key that is twice as long if you want the initial security parameter to be true even if one of them is compromised. Giving them each a number and having them add the two to the key is an alternate strategy. Automatic teller machine keys are controlled in this manner2. However, this may not be sufficient in command applications since one cannot be certain that the people using the device would agree to unleash Armageddon without being asked or questioned. Therefore, Blakley and Shamir separately developed a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

more comprehensive strategy in 1979. Their main concept is shown in the graphic that follows (Figure 1).

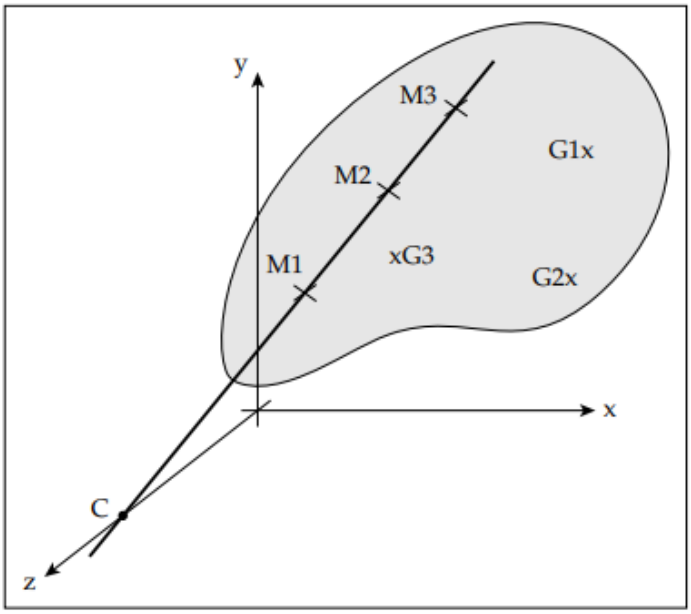

Figure 1: Shared control using geometry.

Assume that if the Prime Minister is killed, Britain will impose the rule that any two cabinet ministers, any three generals, or any cabinet minister and two generals may arm a weapon. To put this into practice, make the unlock code for the weapon point C on the z-axis. We now assign each cabinet minister a random position on the line that passes through C. Now, any two of them may figure out the line's coordinates and determine point C, which marks the line's intersection with the z axis. In a similar manner, we assign each general a random position on the plane and embed the line in the plane. The aircraft may now be rebuilt by any three generals, or by two generals and a minister, leading to the firing code C. This approach permits the linking of weapons, commanders, and choices with a complexity limited only by the bandwidth available by generalising this basic design to geometries of n dimensions or to extending algebraic structures instead of lines and planes.

CONCLUSION

Security technology has greatly benefited from the management of nuclear weapons and related tasks, such as safeguarding the integrity of the national command system, physically securing nuclear installations, and keeping track of international arms control treaties. A great deal of mathematics and science that has found use elsewhere was developed as a result of the sensible determination that weapons and fissile material had to be safeguarded nearly regardless of the cost. Authentication codes, shared control protocols, and subliminal channels are the specific examples that we have focused on in this chapter. Other examples may be found throughout the remainder of the book, including seals, iris biometrics, tamper-resistant electronics, and alarms.

REFERENCES

[1] N. Rastogi and A. Kumar Srivastava, “Control system design for tokamak remote maintenance

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

operations using assisted virtual reality and haptic feedback," *Fusion Eng. Des.*, 2019, doi: 10.1016/j.fusengdes.2018.12.094.

[2] T. Tsuboi *et al.*, "Mitochondrial volume fraction controls translation of nuclear-encoded mitochondrial proteins," *bioRxiv*, 2019.

[3] P. Morilhat, S. Feutry, C. Le Maitre, and J. M. Favennec, "Nuclear Power Plant Flexibility at EDF," *VGB PowerTech*, 2019.

[4] P. E. Edem *et al.*, "Evaluation of the inverse electron demand Diels-Alder reaction in rats using a scandium-44-labelled tetrazine for pretargeted PET imaging," *EJNMMI Res.*, 2019, doi: 10.1186/s13550-019-0520-y.

[5] T. Greenwood and A. Streeter, "Uranium," in *Natural Resources in U.S.-canadian Relations, Volume 2: Patterns and Trends in Resource Supplies and Policies*, 2019. doi: 10.4324/9780429051340-10.

[6] Z. Liu, J. Wang, S. Tan, S. Qiao, and H. Ding, "Multi-objective optimal design of the nuclear reactor pressurizer," *Int. J. Adv. Nucl. React. Des. Technol.*, 2019, doi: 10.1016/j.jandt.2019.09.001.

[7] K. J. Chalvatzis, H. Malekpoor, N. Mishra, F. Lettice, and S. Choudhary, "Sustainable resource allocation for power generation: The role of big data in enabling interindustry architectural innovation," *Technol. Forecast. Soc. Change*, 2019, doi: 10.1016/j.techfore.2018.04.031.

[8] X. Ji, K. Yang, X. Na, C. Lv, Y. Liu, and Y. Liu, "Feedback Game-Based Shared Control Scheme Design for Emergency Collision Avoidance: A Fuzzy-Linear Quadratic Regulator Approach," *J. Dyn. Syst. Meas. Control. Trans. ASME*, 2019, doi: 10.1115/1.4042880.

[9] Y. Xu, C. Yang, X. Liu, and Z. Li, "A Teleoperated Shared Control Scheme for Mobile Robot Based sEMG," in *ICARM 2018 - 2018 3rd International Conference on Advanced Robotics and Mechatronics*, 2019. doi: 10.1109/ICARM.2018.8610753.

[10] W. Zhang, Y. Zhao, X. Zhang, and F. Lin, "Shared control for lane keeping assistance system based on multiple-phase handling inverse dynamics," *Control Eng. Pract.*, 2019, doi: 10.1016/j.conengprac.2019.104182.

[11] M. Kimmel, J. Pfort, J. Wöhlke, and S. Hirche, "Shared invariance control for constraint satisfaction in multi-robot systems," *Int. J. Rob. Res.*, 2019, doi: 10.1177/0278364919867133.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Discussion on Biometrics

Mr. Sandeep Ganesh Mukunda
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-sandeepgm@presidencyuniversity.in

ABSTRACT: ***In the realm of security engineering, biometrics the measurement and analysis of distinctive physical or behavioral characteristics has become a dominant tool. These traits such as fingerprints, facial features, iris patterns, voice, or gait are used by biometric systems to establish and confirm a person's identification. An overview of biometrics in the context of security engineering is given in this abstract, along with an examination of its core ideas, uses, advantages, and drawbacks. The abstract opens with a definition of biometrics and its importance in security engineering, emphasizing the need for trustworthy and precise identity verification techniques. It examines the primary goals of biometric systems, such as non-repudiation, identification, and authentication. A basic idea in biometric systems is the idea of biometric templates, which stand for distinctive traits taken from biometric samples. The abstract goes on to discuss other biometric modalities that are often used in security engineering. It analyses each modality's advantages and disadvantages, including gait recognition, voice recognition, iris recognition, face recognition, and fingerprint recognition. It also discusses how crucial it is to choose the best biometric modality based on the unique security needs and environmental considerations.***

KEYWORDS: Bertillonage, Face Recognition, Fingerprint Recognition, Handwritten Signatures.

INTRODUCTION

The aforementioned quote could be the first known military use of a security system that depends on a human being's characteristic in this example, his accent for verification. (There were less formal instances prior to this, such as when Isaac attempted to identify Esau by his body hair but was tricked by Jacob or when individuals recognised one another by their faces which I'll address later.) People are identified using biometrics by measuring some component of their unique anatomy or physiology (such as their voice or hand geometry), a deeply established skill or behaviour (such as their handwriting), or a mix of both [1]–[4].

People have created a lot of biometric gadgets in the past twenty-five years or so. The market has grown significantly since 9/11, thanks to a number of large-scale initiatives, such as the international standards for biometric travel documents, the US-VISIT program, which collects visitor fingerprints, the Schengen visa for Europe, various ID card initiatives, and various registered traveller programs. The FBI's fingerprint database, which is now being extended to include a variety of biometric data for both identification and forensic reasons, is one of the many major systems that previously existed. According to reports, the market for biometric systems was valued over $1.5 billion in 2005, a significant rise from $50 million in 1998. I have reported how personnel at a nuclear plant in the late 1970s used hand geometry to identify them. The most trusted biometric methods, however, such as the use of handwritten signatures, facial characteristics, and fingerprints, stretch back to a time when computers ever existed. I'll examine them first before moving on to the more elaborate, "high-tech" approaches.

DISCUSSION

Handwritten Signatures

In traditional China, handwritten signatures were utilised, but carved personal seals grew to be seen as having more importance; they are still used for important transactions in China, Japan, and Korea. In contrast, seals were used in Europe throughout the Middle Ages, but when writing became more widespread following the Renaissance, individuals began signing papers simply with their names. The signature was eventually adopted as the norm. Handwritten signatures on papers are used every day

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

to seal deals worth billions of dollars; how they will be replaced by electronic procedures is still a hot topic in politics and technology.

Despite being a fairly flimsy identification method in and of themselves easy to forge handwritten signatures have served their purpose well for generations. Liability for forgery is a significant consideration. A faked handwritten signature is absolutely invalid according to UK law, and this has been preserved in the legal systems of many nations that were a part of the British Empire at the time. It implies that the person who depends on the signature bears the risk of a forgery, and that a bank cannot shift the risk to the consumer using its regular terms and conditions. Therefore, although the PINs and electronic tokens that are increasingly replacing them may be better for the bank, handwriting autographs are better for the consumer. This is not always true; some Swiss banks hold clients accountable for fake checks. The use of electronics doesn't significantly alter the rules of the game in the USA since Regulation E holds banks accountable for the electronic systems they use. The likelihood that a faked signature would be considered as genuine now mostly relies on the degree of attention used while studying it. Needless to say, European banks have pushed clients away from handwritten signatures far further than U.S. banks.

Since many bank card transactions in retailers are approved without even giving the card's sample signature a second thought, many Americans forego signing their credit cards altogether1. However, even thorough signature verification cannot completely eliminate the possibility of forgery. An experiment revealed that 6.5% of the documents were incorrectly assigned by the 105 expert document examiners who performed 144 pairwise comparisons each. A control group of 34 untrained individuals with the same degree of education made mistakes 38.3% of the time, and performance of the nonprofessionals could not be enhanced by providing them with financial incentives. Professional mistakes are a topic of ongoing debate in the field, however they are believed to be a reflection of the examiner's beliefs and context. It appears reasonable to infer that the outcomes for authenticating signatures on checks or credit card vouchers would be even worse given that the participants in these tests were provided with acceptable handwriting samples rather than simply a signature [5]–[8].

Therefore, there are a variety of customs and unique laws that apply to handwritten signatures and that differ from nation to country. These laws go well beyond banking. For instance, in order to purchase a home in England with money borrowed from a bank with whom you have no prior business relationship, you would visit a lawyer's office with a document like a passport, sign the property transfer and loan contract, and then have the lawyer countersign the paperwork. The necessity that a real estate acquisition be in writing was established by the government several centuries ago in order to collect tax on property transactions, while the mortgage lender imposes the demand for government-issued picture ID in order to maintain the satisfaction of its insurers. There may be specific requirements for the notarization of other sorts of documents, such expert testimony. The development of the typewriter in the nineteenth century is credited with several puzzling abnormalities. Some nations demand that each page of machine-written contracts be initialled, while others do not, and these variations have sometimes lasted for more than a century. Conventional conflicts continue to be a major concern. In one instance, a UK firm went bankrupt as a consequence of a real estate transaction in Spain being declared unlawful because it was finalised via fax.

However, the majority of papers in the English-speaking world do not need further authentication. An illiterate's 'X' on a document is just as genuine as an educated man's flourish because the purpose of the signer is the substance of a signature. A plaintext name at the bottom of an email message really has the same amount of weight in legal terms, unless there are explicit restrictions that state the opposite. Each nation's laws may have a variety of cryptic signature rules. Since the context usually makes it plain who did what, it is really exceedingly uncommon for signatures to be challenged in legal proceedings. We therefore

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

have a very feeble biometric system that performs well in practice, except for the fact that it is stymied by country- and application-specific procedural constraints and liability traps.

There is a lot of worldwide action going on about the organisation of this mess and the imposition of somewhat standard regulations for electronic documents has an overview of the concerns, and analyses them by nation. I'll go into more detail on a few of the topics in Part III. Meanwhile, keep in mind that a signature's appearance, forgery risk, and legal legitimacy in a particular situation are mainly unrelated issues. Better automated handwritten signature recognition might be useful in one particular application. Check clearance is done here. A bank's check processing centre will often only confirm signatures on checks that are above a specific amount, such as $1,000, $10,000, or a percentage of the account's activity over the previous three months. An operator who is concurrently shown the cheque picture and the customer's reference signature on the screen does the signature verification. Small-amount cheque verification is not cost-effective unless it can be automated.

Consequently, some academics have developed tools that compare handwritten signatures automatically. Due to the variation between each real signature, this turns out to be an extremely challenging image processing problem. The usage of a signature tablet is a much simpler choice. This is a sensor surface that the user signs on; it captures not only the curve's form but also its dynamics (the hand's speed, the location where the pen was taken off the paper, etc.). Delivery drivers utilise tablets to collect receipts for deliveries; since the early 1990s, there have been devices that match collected signatures to sample enrolled earlier.

Similar to alarm systems, most biometric systems trade off between false accept and false reject rates, often known as type 1 and type 2 mistakes in the biometric literature and the fraud and insult rates in the banking sector. It is possible to tweak several systems to favour one over the other. When you put up the gain on your radar set too much, you can't see the target for clutter, but if you bring it down too far, you can't see it at all. This trade-off is known as the receiver operating characteristic, a phrase originally used by radar operators. The operator must decide which point on this curve is appropriate. When the system is calibrated such that the probability of false accept and false reject are equal, the error rate is equal. The equal error rate for tablet-based signature recognition systems is at most 1%; for purely optical comparison, it is several percent. This is not deadly in a check processing centre operation since suspicious checks are already selected for inspection by a human operator using the automated comparison as a filter. In a customer-facing application, like a retail shop, it is a deal-breaker. The frustration to clients would be intolerable if one out of every hundred transactions failed. Therefore, UK banks set an objective for biometrics that is beyond the present state of the art in signature verification and even fingerprint scanning: a fraud rate of 1% and an insult rate of 0.01%.

Face Recognition

The oldest kind of identification, dating at least as far back as our earliest monkey ancestors, is the recognition of individuals based on their facial characteristics. According to biologists, a significant portion of our cognitive ability developed to provide us effective means of recognising the facial emotions and traits of others. We are quite adept at recognising when someone is staring at us, for instance. Humans tend to be significantly more adept at recognising individuals by their looks in everyday social situations than any automated facial-recognition system created to date. Because picture ID is so widely used, the security engineer places a premium on the human capacity to recognise faces. Driver's licences, passports, and other forms of identification are used to boot up the majority of other systems in addition to controlling access to computer rooms directly while someone presents a picture ID while applying for a job, establishing a bank account, or doing anything else that requires a photo ID, the procedure that leads to the issuance of a password, smartcard, or the registration of a user for a biometric system using another method, such iris recognition, often ends with those actions.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Even if we are adept at knowing friends in person, how skilled are we at detecting strangers from their picture ID? We are not, to put it simply. A unique study was carried out by psychologists at the University of Westminster with the assistance of a bank and a large grocery chain. They recruited 44 students and issued each of them with four credit cards each with a different photograph on it:

1. One of the pictures was very nice. It was recent and true;
2. The second one was "bad, good." The student now wore new clothes and had a different hairdo, so it was authentic but a little dated. In other words, it was a normal image seen on most people's picture IDs;
3. It was a "good, bad one" for the third. Investigators selected the image that most closely resembled the subject from a collection of around 100 random images of other individuals. In other words, it was a typical match that thieves might get if they possessed a collection of cards that had been taken;
4. The fourth was 'terrible, awful'. Except for the fact that it had the same sex and race as the subject, it was picked at random. In other words, it was a classic match for particularly irresponsible and lazy thieves.

After regular business hours, the experiment was carried out at a grocery store with knowledgeable cashiers who were aware of its aim. Each kid used a different card to pass the checkout many times. It turned out that no checkout employee could detect the difference between "good, bad" and "bad, good" photographs. Some of them, in fact, had trouble distinguishing between "good, good" and "bad, bad." Now, this experiment was carried out in ideal circumstances with skilled personnel, lots of time, and no chance of humiliation or physical harm if a card was refused. Performance in real-world situations is likely to be poorer. In reality, a lot of retailers fail to give their checkout personnel the compensation that credit card issuers provide for finding stolen cards. Therefore, even the most fundamental motive is lacking [1], [8]–[10].

The financial sector had a mixed reaction to this trial. With the use of photographs on credit cards, at least two banks saw a significant decrease in fraud to less than 1% of what was anticipated in the case of one Scottish bank. The general opinion was that the main advantage of having a picture ID is its deterrence impact. Therefore, it's possible that individuals won't utilise their facial recognition abilities in identification circumstances efficiently, or that the knowledge we use to recognise people in social settings is stored in our brains in a different way than the knowledge we get from looking at a single image. (It's far tougher to recognise passing strangers than it is to recognise someone you know. According to estimates, 20% of witnesses err in identity parades, which is still terrible but not as bad as the results of matching faces with images. Misidentifications are thought to be the major factor in wrongful incarceration.

Bertillonage

The nineteenth century saw a lot of effort put into attempts to identify persons based on their physical characteristics. Alphonse Bertillon, the most well-known of them, began his career as a clerk in the police records division in Paris.

The challenge of identifying repeat offenders was crucial. He established a technique in 1882 that was based on physical characteristics such height while standing and sitting, face length and breadth, and ear size and angle. These were primarily used to organise a set of record cards that included mugshots and thumbprints that could be used to verify an individual's identity. In commemoration of its inventor, Bertillon, this method was known as "anthropometry" and also "Bertillonage." Once police forces learned how to index and search for fingerprints, it eventually lost popularity. In the guise of hand-geometry readers, this method has reemerged.

The U.S. Immigration and Naturalisation Service currently uses hand geometry at airports to provide regular fliers a "fast track" in addition to its usage at nuclear sites entrance control since the 1970s. It is straightforward to use and somewhat reliable, and the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

NPL experiments discovered a single-attempt equal error rate of roughly 1%. (Passport inspection is a less important use than one would originally believe since airline workers also cross-reference passports with passenger records and provide these lists to homeland security personnel.) The biometric market share for hand geometry is now 8.8%.

Verifying Positive or Negative Identity Claims

Like in nineteenth-century England, many criminals today in America change their identities and relocate after being released from jail. This is okay when criminals turn their lives around, but what about runaways and repeat offenders? In the past, American law enforcement has utilised fingerprints to identify individuals who have been apprehended in order to ascertain if they are now sought by other agencies, whether they have criminal histories, and whether they have previously been identified by another name. For this aim, the FBI operates a sizable internet system that locates roughly 8,000 fugitives each month. Additionally, it is used to screen job candidates. For instance, FBI fingerprint checks are required for anybody seeking a clearance level of Secret or higher from the U.S. government, and certain persons applying for jobs working with children or the elderly may also be subject to them. There are 900,000 federal, local, and state law enforcement officials that have access, and up to 100,000 fingerprint checks are performed daily.

There is now a scheme to extend this to include more biometrics, to store data on foreign nationals, and to provide a 'rap-back' service that would notify the employer of anybody with a clearance who encounters legal issues. All of this alarms civil rights organisations. Since 9/11, immigration has also employed fingerprints. All foreign nationals entering U.S. ports are fingerprinted as part of the US-VISIT program, and their fingerprints are compared to a global watch list of criminals and terrorists.

Iris Codes

We are now switching from conventional to cutting-edge methods of identifying individuals. When assessed under controlled laboratory circumstances, facial recognition software consistently has the lowest mistake rates of any automated system. The Department of Energy financed the research because it sought the most secure method of regulating access to locations like plutonium stockpiles. The technology is being employed in areas like immigration. The most recent international standards for travel papers that can be read by machines include the use of pictures and allow for the inclusion of fingerprints and iris scans.

Every human iris is, as far as is known, measurable unique. It is pretty simple to see in a video image, it doesn't deteriorate, and the cornea which also has a cleaning mechanism isolates it from the outside world. The iris pattern looks to have several times as many degrees of freedom as a fingerprint and includes a significant level of unpredictability. It develops between the third and eighth month of gestation and is phenotypic, similar to the fingerprint pattern in that there seems to be little genetic effect and that the processes forming it are chaotic. Therefore, the patterns are varied even in identical twins and for a person's two eyes, and they seem to remain constant throughout life.

Other Systems

There have been several different biometric methods suggested. Typing patterns, also known as keystroke dynamics, were utilised in goods in the 1980s, although they don't seem to have been very effective. Typing patterns had a notable predecessor in the wartime tactic of identifying wireless telegraphy operators by their fist, the way they manipulated a Morse key. Vein patterns have been employed in a few systems, but they don't seem to have been extensively adopted (in the NPL experiments, the vein identification ROC curve was the poorest of the bunch; it was nearly entirely outside the other curves). Recently, there has been an increase in interest in identifying unknown writers by their writing styles. Of course, literary analysis has a long history; when William Friedman was a young man, a strange billionaire commissioned him to investigate if Shakespeare was written by Bacon. (He ultimately refuted this theory but developed an interest in cryptography in the process.) With the use of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

computers, it is now feasible to do ever-so-subtle statistical checks; examples include attempting to identify individuals who post on extremist online forums and more routine tasks like plagiarism detection. Such software may transition from forensic to real-time surveillance, in which case it would turn into a biometric identification technique.

CONCLUSION

Since the beginning of time, various biometric measurements have been used to identify persons, with handwritten signatures, facial traits, and fingerprints being the most common ones. These techniques, along with more recent ones like voiceprints and iris patterns, have been used to create systems that automate the work of recognition. These systems' advantages and disadvantages vary. Although iris recognition is better, hand geometry is marginally better, and face recognition is much worse, most automated operations have error rates on the order of 1%. The false accept rate also known as the fraud rate and the false reject rate also known as the insult rate are always a trade-off. Error rate numbers are surprisingly hard to understand.

The danger of fraud in unattended operation increases if any biometric is utilised extensively. System designers should take into account voice synthesisers, iris pictures, fingerprint moulds, and even plain old falsified signatures. These do not exclude the use of biometrics, since conventional techniques like handwritten signatures are nonetheless effective in the real world while having extremely high mistake rates. That specific instance shows us that context is important; even a poor biometric may be useful if its usage is well ingrained in the social and legal framework.

In attended operations, when proper system design allows the respective strengths and limitations of the human guard and the machine recognition system to complement one another, biometrics are often more effective. Courts now far less naively believe even fingerprint evidence than they did five years ago, and forensic uses are troublesome. Finally, rather than actually detecting criminals, many biometric technologies accomplish most or all of their results by discouraging them.

REFERENCES

[1] M. G. Galterio, S. A. Shavit, and T. Hayajneh, “A review of facial biometrics security for smart devices,” *Computers*. 2018. doi: 10.3390/computers7030037.

[2] G. M. Weiss, K. Yoneda, and T. Hayajneh, “Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2940729.

[3] B. Hassan, E. Izquierdo, and T. Piatrik, “Soft biometrics: a survey: Benchmark analysis, open challenges and recommendations,” *Multimed. Tools Appl.*, 2021, doi: 10.1007/s11042-021-10622-8.

[4] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, “Biometrics for internet-of-things security: A review,” *Sensors*. 2021. doi: 10.3390/s21186163.

[5] J. W. Crampton, “Platform biometrics,” *Surveill. Soc.*, 2019, doi: 10.24908/ss.v17i1/2.13111.

[6] V. Arulalan, V. Premanand, and G. Balamurugan, “An overview on multimodal biometrics,” *Int. J. Appl. Eng. Res.*, 2015, doi: 10.5121/sipij.2013.4105.

[7] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *Eurasip Journal on Information Security*. 2011. doi: 10.1186/1687-417X-2011-3.

[8] B. Meden *et al.*, “Privacy-Enhancing Face Biometrics: A Comprehensive Survey,” *IEEE Trans. Inf. Forensics Secur.*, 2021, doi: 10.1109/TIFS.2021.3096024.

[9] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and accuracy of fingerprint-based biometrics: A review,” *Symmetry*. 2019. doi: 10.3390/sym11020141.

[10] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, “Behavioral biometrics & continuous user authentication on mobile devices: A survey,” *Inf. Fusion*, 2021, doi: 10.1016/j.inffus.2020.08.021.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Physical Tamper Resistance

Dr. Krishnappa Venkatesharaju,
Assistant Professor, Department of Environmental Science and Engineering, Presidency University, Bangalore, India,
Email Id-venkateshraju.k@presidencyuniversity.in

ABSTRACT: ***A key component of security engineering is physical tamper resistance, which aims to defend sensitive data and cryptographic systems against physical assaults. The idea of physical tamper resistance, its importance in security engineering, and the numerous strategies and countermeasures used to prevent physical tampering are all explored in this abstract. In the introduction, the abstract defines physical tamper resistance and discusses how it protects the availability, confidentiality, and integrity of sensitive assets. It highlights how crucial it is to safeguard hardware security modules (HSMs), smart cards, and other physical components that store or process sensitive data. The goes on to discuss many types of physical tampering attacks, including intrusive ones (like probing, microprobing, and reverse engineering) and non-invasive ones (like side-channel assaults and fault injection). It also discusses combination attacks that make use of a variety of different methods. It draws attention to the possible negative effects of physical tampering assaults, such as unauthorized access, key extraction, data alteration, and device compromise. Following that, the explores a variety of physical tamper resistance strategies used in security engineering. These methods include the use of tamper-resistant materials and coatings, as well as physical security features including tamper-evident seals, shields, and enclosures. Also included are tamper-responsive designs, such those that self-destruct or erase secure keys in the event of tampering. The also discusses the function of sensors, intrusion detection systems, and secure boot procedures as active and passive tamper detection measures. With a focus on hardware-based security modules and secure components, it also examines the idea of secure key management and storage.***

KEYWORDS: ***Cryptography, Infringements, Replication, Tamper Resistance.***

INTRODUCTION

Cheap tamper-resistant technology is virtually often used now. I've already mentioned several examples, like:

1. Smartcards used as bank cards and SIMs in mobile phones in Europe; auxiliary control chips used in printer toner, mobile phone batteries, and memory chips for gaming consoles;
2. The TPM chips used in PCs and Macs, which provide software registration, DRM, and hard-disk encryption;
3. POS terminals and ATMs as well as server farms for banks utilise security modules to maintain bank PINs;
4. Security components hidden in vending machines that sell anything from postal stamps to the magic digits that turn on your power meter to train tickets.

Many products on the market are just pitiful, such as banking terminals, which, although being assessed by VISA and employing the Common Criteria framework, may be trivially compromised in under a minute using basic tools [1]–[3].

However, certain tamper-proof processors are improving. For instance, I am aware of one company that attempted but failed to reverse-engineer the protocol used by a games console maker to prevent rivals from creating memory modules compatible with their equipment. However, this was not the situation a few years ago. A competition between businesses that sought to lock down their goods and others who wanted to unlock them resulted in serious tamper resistance. Reverse engineering for compatibility was being done by some of the attackers, which included legitimate businesses acting within their legal rights. Others were solicitors who used product reverse engineering to demonstrate patent infringements. The legal reverse engineers and a half-dozen specialised

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

businesses work for the attorneys. Some academics break into systems for fame and to advance the state of the art. There are nefarious individuals, such as pay-TV pirates who copy subscriber cards. Finally, there are a lot of ambiguities. Is it illegal to discover a technique to unlock a certain brand of mobile phone so that it may be used on any network? The response is, it depends on whatever nation you're in.

Nowadays, a wide range of devices, from affordable microcontrollers to pricey cryptoprocessors, are available on the market that make the claim to be tamper-resistant. Some of them are excellent, many are passable, and a few are just plain bad. The security engineer must progressively be aware of what tamper resistance is and what it can and cannot do. I'm going to walk you over the last fifteen years or so in this chapter as more cunning assaults have been met with ever more advanced defences. Making computers resistant to physical manipulation has always been vital because, in theory, an attacker who gains access may modify the software and make the system perform anything he wants. Even though computers were large things, the strategies covered in the earlier chapters physical barriers, sensors, and alarms were still applicable. In some applications, a computer is still built as a large, heavy object. For example, an ATM is essentially a PC in a safe with cash dispensers and alarm sensors, while sensor packages for illegal nuclear tests may be placed at the bottom of a borehole that is backfilled with concrete and several hundred feet deep.

Replication may sometimes be used to achieve tamper resistance in places where it is just necessary for integrity and availability as opposed to physical security. A service that executes transactions concurrently and allows users to vote on the outcome may be deployed on several servers across various websites. However, tamper-proof systems may also guarantee data confidentiality. The idea that many things may be accomplished using either metal or mathematics fails in this regard.

DISCUSSION

Tamper resistance in cryptography has been used for millennia. Naval codebooks were weighted so they could be tossed overboard in the event of capture; today, the British government still uses dispatch boxes. State documents are transported by ministers' assistants in lead-lined boats that sink. Russian one-time pads were printed on cellulose nitrate, so that they would burn fiercely if lit, and one American wartime cypher machine came with self-destruct thermite charges so that it could be quickly destroyed. Codes and, more recently, the keys for wartime cypher machines have also been printed in water soluble ink. Key information was often taken in surprise assaults, therefore such methods relied on the operator's alertness. Therefore, efforts were undertaken to automate the procedure. Early electrical gadgets and certain mechanical cyphers were designed with the key settings being lost upon opening the casing [4]–[8]. Engineers paid more attention to the issue of how to protect keys in transit after a number of incidents in which key material was sold to the opposing side by cypher staff, such as the infamous Walker family in the USA who sold U.S. Navy key material to the Russians for more than 20 years.The objective was to "reduce the street value of key material to zero," and this may be done using either tamper-resistant or tamper-evident devices, from which it would be easy to extract the key.

Paper keys used to be transported in "tattle-tale containers," which were intended to reveal signs of manipulation. When electronic key distribution emerged, the "fill gun," a portable device that releases crypto keys in a controlled manner, was a common option. Today, a tiny security processor, such a smartcard, is often used to accomplish this role; similarly to electricity metres, it may be packaged as a "crypto ignition key." Control methods vary from procedures employing public key cryptography to guarantee that keys are only loaded into authorised equipment to a limit on the number of times a key may be distributed. Additionally, the control over important information was expanded. It was centralised and used to compel the use of duly

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

authorised computer and communications goods in both the USA and the UK. Live key material wouldn't be sent to a system until after it had received the required accreditation. After the first keys have been loaded, further keys may be transferred using other key agreement and authentication procedures. Many of the fundamental techniques, including key diversification, were covered in the chapter on protocols in Part I; I'll have more to say about protocols in the chapter on API assaults. I'm going to start by examining the physical safeguards against manipulation here.

High-End Physically Secure Processors

The IBM 4758 (Figures 1 and 2) is a case worth looking into. There are three reasons why this is crucial. It was the first commercially available processor to successfully pass the highest degree of tamper testing, to start with. The American government then erected resistance (FIPS 140-1 level 4). Second, there is a wealth of information available to the general public about it, including the development of its design history, its security features, and the transaction set it supports. Third, it was the most high-profile target in the field of tamper resistance since it was the first level-4-evaluated product, and from 2000 to 2005, my students and I made an effort to attack it.

Figure 1: The IBM 4758 cryptoprocessor (courtesy of Steve Weingart).

Figure 2: The 4758 partially opened showing (from top left downward) the circuitry, aluminium electromagnetic shielding, tamper sensing mesh and potting material (courtesy of Frank Stajano).

The progression that resulted in this product may be summed up as follows. Due to the proliferation of multi-user operating systems and the frequency with which security flaws were discovered, many persons might potentially get access to the data being processed. The Anderson report and multilayer security were the responses from the military computer community. The banking industry's response was to concentrate on especially sensitive data, notably long-term cryptographic keys and the personal identification numbers (PINs) that bank clients use to sign in at ATMs. Early in the 1980s, it became apparent that the degree of security offered by commercial operating systems would probably always be inadequate for these "crown jewels."

The IBM 3848 and the VISA security module were among the first independent security modules to achieve commercial success as a result of this. Both of them had static RAM that was intended to be zeroed out when the enclosure was opened, unique key memory, and encryption circuitry. They were housed in sturdy metal enclosures. To do this, many lid switches were used to connect the power supply to the key memory. As a result, whenever the maintenance team arrived to change the batteries, they would open the lid and steal the keys. The device operators would then replenish the key material after they were done. This allowed the device's owner to rejoice in the fact

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

that only its own employees had access to the device's keys.

Medium Security Processors

The iButton and 5002 security processors from Dallas Semiconductor and the Capstone chip used to secure U.S. military communications up to "Secret" are also excellent examples of "level 3.5" devices. These goods cost between $10 and $20, compared to the $2000 cost of the 4758. But launching an assault on them would be far from simple [4], [5], [9].

i. The iButton:

Dallas Semiconductor's first iButton was intended to be a simple, standalone cryptographic processor for use in things like postal metres. It is housed in a steel container with a lithium battery that can keep keys in the RAM for a design life of 10 years, a microcontroller, static RAM for keys and software, a clock, and tamper sensors (see Figure 3). It is compact enough to be carried as a key fob or worn as a signet ring. One early usage was as an access token for the "Electronic Red Box," a safe laptop system created for ministers of the UK government. The minister had to insert his signet ring into a reader on the side of the laptop to get access to classified papers. (A requirement for design was that "Ministers shall not be required to use passwords.") Other uses for tokens include ticketing for the public transport system in Istanbul, parking metres in Argentina and quick logons for bar personnel at tills.

When I created the initial iteration of the iButton in 2000, it was a purely security device, and certain models even had a cryptoprocessor to do actions using public keys. The first iButton was broken in December 1999. Lexmark, the printer manufacturer, had begun putting iButtons in some of its printer cartridges in 1998 to prevent aftermarket sellers from selling ones that were compatible, but Static Control Components eventually cracked the code and created a compatible chip for the aftermarket in December 1999. Since then, the iButton has developed into a wider line of products, and Dallas has become a subsidiary of Maxim. Existing versions include basic ones that are essentially simply RFID tokens, versions with temperature sensors that offer a reliable temperature history of perishable products in transit, and versions with a JVM that are more complicated. Therefore, it is no longer true that all iButtons are "secure" since a specific device may not have been intended to be safe or may have had its security features intentionally or unintentionally disabled. The range still includes tamper-proof gadgets that allow cryptographic authentication using SHA-1, and security applications still often utilise it.

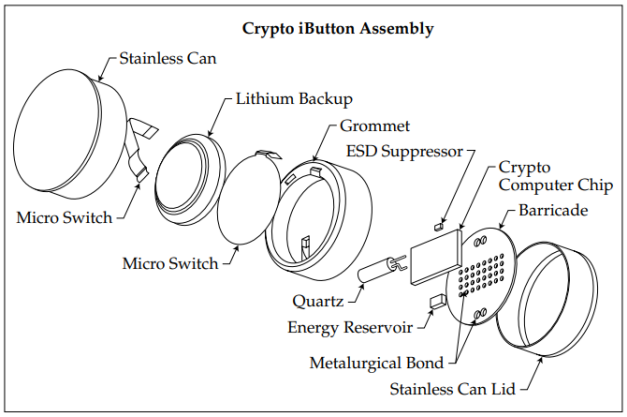

Figure 3: iButton internals (courtesy of Dallas Semiconductor Inc.)

ii. The Dallas 5000 Series:

The 5000 series secure microcontroller from Maxim / Dallas is another medium-grade security device that is commonly used in devices like as point-of-sale terminals, where it maintains the keys necessary to encrypt customer PINs. Bus encryption is the clever concept behind this gadget. The chip now includes technology that encrypts memory locations and contents as data is loaded and saved. This implies that the gadget may use external memory rather than the minimal amount of RAM that can be packed within a low-cost tamper-sensing package. When a gadget is switched on, it generates a unique master key at random. The program is then loaded via serial port, encrypted, and stored in external memory. The gadget is now ready to use. Power must be maintained continuously or the internal register that carries the master key will lose it; this also occurs if a physical tampering event is detected (the DS5002 includes a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

tamper-sensing mesh built into the top metal layer of the chip, similar to the iButton).

An early version of the 5002 (1995) succumbed to Markus Kuhn's innovative protocol attack, the cypher instruction search attack. The notion is that certain of the processor's instructions, such as I/O, have a visible external consequence. There is one instruction in particular that causes the next byte in memory to be output to the device's parallel port. So the secret is to use a test clip to intercept the bus between the processor and memory and feed in all possible 8-bit instruction bytes at some point in the instruction stream. One of these should decode and output the plaintext version of the next'encrypted memory' byte. By altering this byte, a table of equivalent plaintext and ciphertext might be constructed. After learning the encryption function for a seven or eight-byte sequence, the attacker might encrypt and run a small program to dump the full memory contents[7], [10]. The exact specifics are a little more complicated. The issue has subsequently been resolved, and Dallas is now marketing replacement items such as the 5250. The assault on bus encryption, on the other hand, is a fantastic illustration of the entirely unforeseen things that go wrong when attempting to apply a sophisticated new security idea for the first time.

CONCLUSION

Systems and devices that are tamper-resistant have a long history that goes back to electronic computing. There are several techniques to protect computers against physical tampering, including locking them up in a secured room. A number of more affordable and portable options are also available, ranging from thousands of dollars in hardware security modules that are certified to withstand all known attacks, to smartcards whose hardware is now quite difficult to penetrate, to low-cost security microcontrollers that are frequently defeated with a few hours to days of work. I have presented various examples of implementations and detailed how hardware tamper-resistance developed during the 1990s via a number of cycles of attack and improved defence. Security processors are often useful in applications where we need to connect processing to physical objects and keep track of value in the absence of a stable online service. However, they are virtually always susceptible to assaults on interfaces (human, sensor, or system).

REFERENCES

[1] H. Abarua, “Relationship Of Parenting To Temper Tantrum Behavior Of Children 3-5 Years Old In Paud Mawar Fkip Unpatti,” *Edu Sci. J.*, 2020, Doi: 10.30598/Edusciencesvol1iss1pp44-51.

[2] M. Shingala, C. Patel, And N. Doshi, “An Improve Three Factor Remote User Authentication Scheme Using Smart Card,” *Wirel. Pers. Commun.*, 2018, Doi: 10.1007/S11277-017-5055-9.

[3] Y. Birol, “Thermal Fatigue Testing Of Inconel 617 And Stellite 6 Alloys As Potential Tooling Materials For Thixoforming Of Steels,” *Mater. Sci. Eng. A*, 2010, Doi: 10.1016/J.Msea.2009.11.021.

[4] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, And R. Mcquaid, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” *Natl. Inst. Stand. Technol.*, 2021.

[5] K. Rindell, J. Ruohonen, J. Holvitie, S. Hyrynsalmi, And V. Leppänen, “Security In Agile Software Development: A Practitioner Survey,” *Inf. Softw. Technol.*, 2021, Doi: 10.1016/J.Infsof.2020.106488.

[6] D. Mellado, C. Blanco, L. E. Sánchez, And E. Fernández-Medina, “A Systematic Review Of Security Requirements Engineering,” *Computer Standards And Interfaces*. 2010. Doi: 10.1016/J.Csi.2010.01.006.

[7] D. Mažeika And R. Butleris, “Integrating Security Requirements Engineering Into Mbse: Profile And Guidelines,” *Secur. Commun. Networks*, 2020, Doi: 10.1155/2020/5137625.

[8] Á. Török And Z. Pethő, “Introducing Safety And Security Co-Engineering Related Research Orientations In The Field Of Automotive Security,” *Period. Polytech. Transp. Eng.*, 2020, Doi: 10.3311/Pptr.15850.

[9] P. H. Nguyen, S. Ali, And T. Yue, “Model-Based Security Engineering For Cyber-Physical Systems: A Systematic Mapping Study,” *Information And Software Technology*. 2017. Doi: 10.1016/J.Infsof.2016.11.004.

[10] H. Aldawood And G. Skinner, “Reviewing Cyber Security Social Engineering Training And Awareness Programs-Pitfalls And Ongoing Issues,” *Future Internet*. 2019. Doi: 10.3390/Fi11030073.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Application Programming Interface Security

Mr. Vijaykumar Lingaiah
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-vijaykumarsl@presidencyuniversity.in

ABSTRACT: ***In security engineering, API (Application Programming Interface) security is crucial for assuring the safety and integrity of data and services transferred between software programs. Understanding the foundational ideas and recommended practices for securing APIs is crucial given the expanding use of APIs in contemporary systems and the relevance of interconnectivity. This abstract gives a general review of API security within the framework of security engineering, examining its importance, difficulties, and important factors. The abstract opens with a definition of APIs and a discussion of their crucial function in facilitating data exchange and communication across apps. It emphasizes the need for strong security measures to thwart unauthorized access, data breaches, and malicious actions that can jeopardise the confidentiality, integrity, and accessibility of API resources. The abstract then goes through the primary dangers and difficulties related to API security. These difficulties include user input security, API endpoint security, data protection and encryption, authentication and access management, and secure communication protocols. The abstract focuses on how crucial it is to deal with these difficulties before they arise in order to build a solid security posture for APIs. The abstract also emphasizes the need of thorough API security plans that cover the full software development lifecycle. The need of safe API design, implementation, testing, and continuous maintenance is emphasized in order to reduce security risks and guarantee a strong security posture.***

KEYWORDS: ***API Design, Application, Operating Systems, Programming Interface.***

INTRODUCTION

Many ostensibly secure devices contain some type of application programming interface, or API, that untrustworthy persons and processes may use to execute a job [1]–[4].

1. The server of a bank will query an associated hardware security module. 'Here is a client account number and PIN, with the PIN encrypted using the key we share with VISA. 'Does the PIN work?'
2. When you activate javascript, your browser exposes an application programming interface javascript that website owners may use to accomplish a variety of things.
3. A secure operating system may restrict the calls that an application program may make by enforcing a policy such as limiting information transfer from High to Low using a reference monitor or other wrapper.

The obvious issue is whether it is safe to divide jobs into trusted and less trusted components, and it has recently been shown that the answer is often negative.

Designing security APIs is a difficult task. API security is linked to several of the issues I've previously mentioned. For example, multilayer secure systems impose flow limits on static data, while a security API often attempts to prohibit certain information flow in the presence of a security API.

A considerably more difficult challenge is one of tight and dynamic interaction. It's also connected to protocol security: as I'll explain momentarily, bank security modules are often unsafe due to interactions between the many protocols that they support. It raises concerns regarding software security: the javascript implementation in Firefox allows calling programs to check all variables defined by current plugins, which may jeopardise your privacy by exposing information about your browsing habits and web mail use. The javascript developers simply did not consider creating a distinct sandbox for each visited page. Indeed, the most prevalent API failure pattern is that safe transactions become insecure when combined, whether due to application syntax, feature interaction, sluggish information leaking, or concurrency issues.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

There are plenty such instances. I described prepaid electricity metres in the context of embedded systems, and token vending machines utilise tamper-resistant security modules to secure keys and value counters. An assault there was to reduce the energy rate to the lowest feasible value and distribute tokens entitling recipients to power for considerably less than its market worth. The design flaw was failing to include tariff reporting into the end-to-end protocol architecture.

'Trusted Computing' is an important example. This program has placed a TPM chip for secure crypto key storage on the majority of PC and Mac motherboards on the market today. According to Microsoft, future applications will have both a traditional 'insecure' part running on top of Windows as before, and a'secure' part or NCA running on top of a new security kernel known as the Nexus, which will be formally verified and thus much more resistant to software attacks. The Nexus and the NCA will protect crypto keys and other application-critical variables. The difficulty that this creates is how to safeguard the interface between the application and the NCA. The language used by a trustworthy computer while communicating with a less trusted machine is crucial. Expect the less trusted device to try out all kinds of surprising command combinations in attempt to fool the more trusted one. How can we approach this methodically?

DISCUSSION

Failures of the hardware security modules used by banks to safeguard PINs and cryptographic keys for ATM networks have taught us a lot about API security. While working with security module provider Eracom in 1988, Longley and Rigby saw the value of differentiating key types. We disclosed a security issue in a security module that resulted from a bespoke transaction back in 1993. Nevertheless, the topic truly took off around 2000 when I began to consider if one could possibly call a sequence of transactions from a security module that would compromise its safety. How can you be certain that a series of 17 transactions won't accidentally reveal a clear key, I queried. I found the following weakness when reading the instructions [5]–[7].

The XOR-To-Null-Key Attack

The "XOR-to-Null-Key" attack, sometimes called the "XOR-based encryption attack," is a cryptographic flaw that may happen when the symmetric encryption technique XOR (exclusive OR) is applied with a null (zero) key. This assault brings to light the flaws in XOR encryption that result from employing a zero key, as well as the significance of sound key management in cryptographic systems. In XOR encryption, the ciphertext is created by combining the plaintext with a key and performing an XOR operation. The same key is XORed with the ciphertext to decode it and reveal the original plaintext. Being reversible, XOR will produce the original plaintext if the ciphertext and key are combined once again.

The ciphertext, however, is unaltered when an XOR null key (all zeroes) is employed. XORing any value with zero results in the same value, which explains why. As a consequence, by XORing the ciphertext with a null key, an attacker who is aware of this flaw may quickly get the plaintext. The XOR-to-Null-Key exploit is a serious flaw since it entirely discredits the protection that encryption offers. It enables an attacker to retrieve the plaintext without having access to the original key by completely sidestepping the encryption process. When used against systems that only use XOR encryption with a null key for secrecy, this attack may be quite destructive.

It is essential to adhere to established practices for key management in order to prevent the XOR-to-Null-Key attack and guarantee the security of cryptographic systems. This entails creating secure, random keys that are kept private and guarded against unauthorized access. The security of the system may also be increased by using a strong encryption technique with the right key sizes, adding more layers of encryption, and including authentication. In real-world cryptographic applications, XOR encryption with a null key should not be employed since it is a crude and unsafe encryption technique. To protect the confidentiality and integrity of sensitive data, it is crucial to use strong encryption algorithms and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

properly manage encryption keys. The XOR-to-Null-Key attack serves as a sobering illustration for this.

The Attack on the 4758

The phrase "Attack on the 4758" refers to a particular piece of cryptographic hardware, the IBM 4758 Cryptographic Coprocessor, which was successfully attacked in the late 1990s. Because it revealed flaws in a widely used and very secure cryptographic device, the assault on the 4758 is noteworthy because it casts doubt on the efficacy of hardware-based security methods. A tamper-proof hardware component called the IBM 4758 Cryptographic Coprocessor was created to provide safe cryptographic functions including encryption, decryption, key management, and digital signatures. It was extensively used across several sectors and regarded as one of the safest technology at the time [8].

Researchers at Cambridge University initially demonstrated the assault on the 4758, often known as the "Wire Attack" or "Timing Attack," in 1997. During the assault, electrical signals generated by the device were intercepted and examined in order to learn more about the cryptographic methods and keys being utilised.

The researchers were eventually able to extract the cryptographic keys from the 4758 by deducing key information from the timing and power consumption characteristics of the device. This assault showed how side-channel attacks, which take advantage of information leakage via unanticipated channels like power consumption, timing, or electromagnetic emissions, might weaken even strong hardware security systems.

The assault on the 4758 had important ramifications since it called into question the notion that tamper-resistant hardware was impervious to attacks. It brought attention to the need of effective side-channel attack defences and the significance of carefully assessing the security of cryptographic hardware.

Multiparty Computation, and Differential Protocol Attacks

Jolyon Clulow started the subsequent wave of attacks against security module APIs in 2003, and they rely on altering the specifics of the application logic in order to leak data. His first assault made use of error messages. However, it turned out that using exclusive-or was a poor method for doing this (much as when combining keys). The device would decrypt the PIN block, xor in the account number, find (with acceptable probability) that the result was not a decimal number, and provide an error message if the incorrect account number had been received along with the PIN block. The ultimate result was that you could rapidly figure out the PIN by submitting a series of transactions to the security module that included the incorrect account number. Mike Bond and Piotr Zielinski later discovered an even more straightforward approach. In Figure 1 shown the IBM method for generating bank card PINs.

Account number *PAN*:	8807012345691715
PIN key *KP*:	FEFEFEFEFEFEFEFE
Result of DES $\{PAN\}_{KP}$:	A2CE126C69AEC82D
$\{N\}_{KP}$ decimalized:	0224126269042823
Natural PIN:	0224
Offset:	6565
Customer PIN:	6789

Figure 1: IBM method for generating bank card PINs.

The PIN verification key is used to encrypt the customer account number, creating a string of 16 hexadecimal digits. Using a user-supplied function called the decimalization table, the first four are changed to decimal digits and used as the PIN. This supplies the natural PIN; a subsequent offset, whose purpose is to allow the client to choose a memorable PIN, is added. The offset is added to the natural PIN to create the customer PIN. The most popular decimalization table, 012345689012345, simply multiplies the result of the DES by 10.

The decimalization table may be changed, which is an issue. The PIN '0000' will be produced and returned in encrypted form if the table is set to all zeroes (i.e., 0000000000000000). The call is then repeated using table 1000000000000000. We can tell if the DES output includes a 0 in its first four digits if the encrypted result changes. The PIN value may be discovered with a few hundred well designed

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

inquiries. We dubbed this attack differential protocol analysis since the approach contrasts several executions of the same protocol that have undergone minor modifications. Initial industry action consisted on establishing guidelines for acceptable decimalization tables. For instance, one vendor mandated that a table must include at least eight distinct entries, with no value appearing more than four times. Try 0123456789012345, then 1123456789012345, and so on if this isn't good enough. You can pay your security module manufacturer additional money to offer you a computer that has your own bank's decimalization table hard-coded, but that is really the only genuine fix.

Philosophically, this nicely demonstrates the difficulty of designing a device that will perform a secure multiparty computation, where a computation must be performed using secret information from one party, and some inputs that can be modified by a hostile party [64]1. Even in this very simple case, it's so difficult that you end up having to abandon the IBM method of PIN generation, or at least nail down its parameters so hard that you might as well just use a different method entirely. It serves as a concrete example of one of the major problems with APIs. To meet the demands of an increasing variety of consumers, they get more and more complicated until an assault occurs out of the blue.

The EMV Attack

You'd have expected that security module authors would have begun more cautious while introducing new transactions after the original set of API exploits were exposed in 2001. Not so! The banking sector has repeatedly pushed for the inclusion of new transactions that heighten security. A recent transaction mandated by the EMV consortium to facilitate secure transmission between a smartcard and a bank security module is an intriguing example. The intention is for the bank to be able to request that a parameter, such as a new key, be changed when a bank card is used in an online transaction. Thus far, so good. The specification, however, had a severe flaw that has been picked up by several implementations [9]–[12].

The Secure Messaging for Keys transaction enables the server to instruct the security module to encrypt a text message using a key that is of the kind that can be shared with bank smartcards. The text message may have a configurable length and be encrypted in either CBC or ECB mode. This gives the attacker the option to choose a message length such that just one byte of the target key actually crosses an encryption block's border. Then, by sending a sequence of messages that are each one byte longer, the key byte may be located by cycling through all other potential values with the additional bytes. The other key bytes may then be attacked one at a time by the attacker. This allows for the extraction of any exportable key from the module. (There is also a transaction called Secure Messaging for PINs, but why bother if you can just steal all the master keys instead of extracting PINs one at a time?) In conclusion, since the APIs were so poorly constructed, the security modules offered to the banking sector over the last 25 years were almost wholly unsecure. We discovered an attack on at least one version of every security module available at some point. The vendors eventually prevented or reduced the majority of these assaults by distributing software updates. However, the customers the banking sector kept coming up with inventive new uses for payment networks, and these keep breaking the APIs again. The common attacks require repeated transactions, with feature interaction (with program features that are especially carelessly constructed) or sluggish information leaking as the technical reason. Feturitis is the underlying reason, as it is in many other aspects of our specialty. APIs are often too complicated, and the breaks aren't always evident.

API Attacks on Operating Systems

A second category of API attacks involves concurrency, and Robert Watson's discovery of flaws in system call wrappers is a good example of this. The reference monitors detailed in Chapter 8 are one example of how system call wrappers are used to strengthen operating system security, and antivirus software is another. Applications' requests to the operating system are intercepted by wrappers, which then parse, audit, and maybe modify them before

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

passing them on. For instance, a Low process trying to access High data can be redirected to fake data or get an error message. You may create wrappers for popular operating systems using a variety of frameworks, such as Systrace, the Generic Software Wrapper Toolkit (GSWTK), and CerbNG. They normally just encapsulate security logic, examine the entrance and exit states of all system calls, and run in the kernel's address space.

John Anderson specified that the reference monitor should be tamper-proof, non-bypassable, and small enough to verify when he first suggested the idea in 1972. On the surface, today's wrappers seem to be perfect until you consider the passage of time. System calls are not atomic; instead, contemporary operating system kernels are very concurrent. Wrappers often presume this. System calls are not atomic in their relationships to wrappers or to one another.

A classic attack involves racing on user-process memory by inducing an unfavorable kernel sleep, such as via a page failure. In a GSWTK attack, Watson calls a route whose name crosses a page boundary by one byte, putting the kernel to sleep while fetching the page. He then replaces the path in memory. It seems that the race windows are substantial and trustworthy. Operating systems are tuned to take use of processors as they become more concurrent and more processors are deployed in each CPU chip throughout time. Race conditions may start to replace stack overflows as the preferred assault when this kind of attack becomes more and more prevalent as code analysis technologies reduce the frequency of stack overflows.

How can they be restricted? The API must be rewritten as the only effective fix. Operating systems would switch to a message-passing architecture in an ideal world, which would remove (or at least significantly minimise) concurrency problems. For operating system manufacturers, whose business models rely on backwards compatibility, it is scarcely realistic. Building capabilities into the operating system particularly to cope with concurrent threats is a practical compromise; Linux Security Modules and Mac OS/X 10.5 (based on TrustedBSD, on which Watson worked) both achieve this.

In summary, there are a number of documented flaws in the APIs provided by conventional operating systems, but the wrapper solution, which involves placing another API in front of the vulnerable API, seems to be particularly brittle in a situation with many of concurrent users. For the wrapper to be truly functional, it would need to have a good understanding of the memory layout, which would make it just as sophisticated (and susceptible) as the operating system it was meant to defend.

CONCLUSION

Over time, user interfaces get more complex, grubbier, and nastier. Many embedded systems, including antivirus software and the operating system, as well as the realm of cryptoprocessors and other diverse embedded systems, have interface design faults. The interface is likely to leak more information than the trusted program's creator intended wherever that software with higher levels of trust interacts. Complexity usually causes failures. I've covered two key case histories: system call wrappers, which attempt to audit and filter calls to an operating system's API, and cryptoprocessors, which collected transactions beyond the designers' comprehension of their interactions.

In terms of pure computer science, the former may be seen as examples of the composition issue or the secure multiparty computing problem, while the later could be viewed as concurrency failures. But instead of being blackboard systems, they are industrial-scale systems. Hundreds of transactions may be present in a security module, and each update would add a new batch. Many of the errors may be categorised as feature interactions at the application level. There are also particular failures like the gradual information leaking from poorly built cryptosystems, which would not be important in the event of a single transaction but becomes lethal when an adversary can take over a server and inject hundreds of transactions per second.

REFERENCES

[1] A. Munsch and P. Munsch, “The Future of API (Application Programming Interface) Security: The Adoption of APIs for Digital Communications and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

the Implications for Cyber Security Vulnerabilities," *J. Int. Technol. Inf. Manag.*, 2021, doi: 10.58729/1941-6679.1454.

[2] M. Mehrtak *et al.*, "Security challenges and solutions using healthcare cloud computing," *Journal of Medicine and Life*. 2021. doi: 10.25122/jml-2021-0100.

[3] H. C. Chen, W. J. Yang, and C. L. Chou, "An online cognitive authentication and trust evaluation application programming interface for cognitive security gateway based on distributed massive Internet of Things network," in *Concurrency and Computation: Practice and Experience*, 2021. doi: 10.1002/cpe.6128.

[4] A. N. Aqil, B. Dirgantara, Istikmal, U. A. Ahmad, and R. R. Septiawan, "Robot Chat System (Chatbot) To Help Users 'Homelab' Based In Deep Learning," *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120870.

[5] P. Karthika and P. Vidhya Saraswathi, "IoT using machine learning security enhancement in video steganography allocation for Raspberry Pi," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02126-4.

[6] M. H. Saudi, M. Mohd Saudi, A. Rahmana, and M. A. Husainiamer, "Gaming Mobile Applications: Proof of Concept for Security Exploitation," *Turkish J. Comput. Math. Educ.*, 2021.

[7] C. Wijayarathna and N. A. G. Arachchilage, "Using cognitive dimensions to evaluate the usability of security APIs: An empirical investigation," *Inf. Softw. Technol.*, 2019, doi: 10.1016/j.infsof.2019.07.007.

[8] M. Bond, "Attacks on cryptoprocessor transaction sets," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2001. doi: 10.1007/3-540-44709-1_19.

[9] M. Bond, M. O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, "Be Prepared: The EMV Preplay Attack," in *IEEE Security and Privacy*, 2015. doi: 10.1109/MSP.2015.24.

[10] M. Alqahtani and A. van Moorsel, "Risk Assessment Methodology For EMV Financial Transaction Systems," *Electron. Notes Theor. Comput. Sci.*, 2018, doi: 10.1016/j.entcs.2018.09.010.

[11] O. Al-Maliki and H. Al-Assam, "Challenge-response mutual authentication protocol for EMV contactless cards," *Comput. Secur.*, 2021, doi: 10.1016/j.cose.2021.102186.

[12] N. El Madhoun, E. Bertin, M. Badra, and G. Pujolle, "Towards more secure EMV purchase transactions: A new security protocol formally analyzed by the Scyther tool," *Ann. des Telecommun. Telecommun.*, 2021, doi: 10.1007/s12243-020-00784-1.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Study on Security Printing and Seals

Dr. Suman Paul
Associate Professor, Department of Petroleum Engineering, Presidency University, Bangalore, India,
Email Id-sumanpaul@presidencyuniversity.in

ABSTRACT: ***In order to prevent forgery, tampering, and unauthorized reproduction of confidential documents, goods, or assets, security printing and seals are essential elements of security engineering. This abstract examines the foundational ideas, developments, and uses of security printing and seals in the context of security engineering. The abstract opens by discussing security printing, security seals, and the role they play in protecting valuable data and assets. It outlines the main goals of security printing, such as tamper evidence, authenticity verification, and traceability. In numerous industries, including cash, identification papers, product packaging, and private documents, the abstract highlights the function of security printing and sealing.***

KEYWORDS: Holography, Microprinting, Secure Printing, Reproduction.

INTRODUCTION

The paper then explores several security printing methods and tools used in security engineering. Holography, microprinting, guilloche designs, security inks, UV/IR inks, serial numbering, watermarking, and unique substrates are a few examples of these. Each method is briefly explained, with an emphasis on its characteristics, potency, and connection with security measures. The relevance of tamper-evident seals and their uses in guaranteeing the integrity of goods, containers, and documents are further explored in the abstract. It goes through several seal types, their characteristics, and workings, including mechanical seals, security tapes, and adhesive seals. The abstract also emphasizes new technologies for improved security and tracking, such as RFID (Radio Frequency Identification) and NFC (Near Field Communication) [1]–[3].

The paper also discusses the difficulties and weaknesses of security printing and seals. It examines various defenses used by forgers and tamperers, including sophisticated printing procedures, forging tactics, and seal tampering methods. It highlights how security printing technology must constantly innovate and evolve in order to keep up with emerging dangers. The paper emphasizes the value of incorporating security printing and seals into a complete security framework as a last point of emphasis. It emphasizes the need of careful implementation, quality control, and regular evaluations to guarantee the efficacy of security measures. The abstract also emphasizes the multidisciplinary approach used by printing specialists, material scientists, and security experts in the development of secure printing and seals.

Secure printing, packaging, and sealing play a role in many computer systems to some level in ensuring crucial components of their security.

a) The majority of security devices can be overcome if a bad guy can access them. Before you install them, whether to repair them, harm them, or replace them. To ensure the user that the product hasn't been tampered with since leaving the plant, trustworthy distribution may be aided by seals and typically tamper-evident packaging.
b) Seals and packaging are used to protect many software items against counterfeiting. They can at least somewhat increase the expense of large-scale counterfeiting.
c) We observed that seals are often used by monitoring systems, like taxi metres, to make it more difficult for users to tamper with input. A seals failure may constitute a system defeat, regardless of how advanced the cryptography.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

d) I also spoke about how man-in-the-middle attacks may be employed against contactless systems, such as those found in passport and identification card chips. Before allowing an engineer from one of your suppliers inside your hosting facility, it might be a good idea to check his identification.

e) Both viewing the ID visually and electronically is a good idea. If you just do the latter, he could be telling someone else about the transaction. Therefore, security printing may still be important even with electronic ID cards.

Smartcards are one kind of security token that is challenging to produce totally tamper-proof. The adversary may be able to take the gadget apart and examine the contents. A more achievable objective would be tamper evidence rather than tamper proofness: if someone takes apart their smartcard and extracts the keys, they shouldn't be able to put it back together in a way that will pass careful scrutiny. Here, security printing might be useful. If a bank's smartcard is really tamper-evident, the bank may inform its clients that any complaints will only be considered if they can show the card to be untampered with. (Banks may not get away with this however, since consumer protection attorneys would require that banks act honestly with honest clients who lose their cards or have them stolen).

A new front has been opened up by the ease with which contemporary colour scanners and printers may be utilised to create acceptable forgeries, apart from these direct uses of printing and sealing technologies. Printers of banknotes are now advocating digital security measures. These include indistinct copyright markings that may assist vending machines identify real cash, enabling forgeries to be discovered, and trigger alerts in image processing software if you attempt to scan or duplicate them. Vendors of colour copiers and printers also include forensic tracking codes into printouts that include the serial number, date, and time of the machine. As a result, the worlds of digital technology and "funny inks" are increasingly merging.

DISCUSSION

A lengthy and fascinating history surrounds seals. I explained how accounting systems originated from the clay tablets, or bullae, employed by Mesopotamian neolithic warehouse keepers as produce receipts in the chapter on banking systems. The bulla method was modified over 5000 years ago to settle conflicts by having the warehouse keeper bake the bulla in a clay envelope with his mark on it.

Authenticating documents using seals was a widespread practice in classical and early Chinese civilizations. Prior to the invention of paper, they were used as a form of social control in mediaeval Europe. For example, a carter would receive a lead seal at one toll booth and turn it in at the next, and pilgrims would receive lead tokens from shrines to prove that they had made a pilgrimage. In fact, the young Gutenberg got his start in business by developing a method of inserting slivers of mirror into lead seals to prevent forgery and safeguard church revenues [559]. Even after digital signatures had replaced handwritten signatures as the primary method of letter authentication, handwritten signatures persisted as a backup method. Before the eighteenth century, letters weren't put in envelopes; instead, they were folded numerous times and sealed with a signet ring and hot wax.

For essential documents, seals continue to be the favored authentication method in China, Japan, and Korea. The corporate seals, notary seals, and national seals that certain heads of state attach to archive copies of laws are some examples of how their historic significance is still evident elsewhere [4]–[6]. However, by the middle of the 20th century, their usage for authenticating packaging had surpassed their use for papers in the West. Moving from loose commodities to packaged goods and the increasing prominence of brands not only increased the possibility of better quality control but also exposed products to possible product tampering by dishonest individuals. A high of 235 documented occurrences of product tampering in the USA in 1993 resulted from an outbreak of tampering events, notably involving soft drinks and pharmaceuticals. This encouraged

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

numerous manufacturers to include tamper-evident features in their goods.

Software businesses have relied more and more on packaging to thwart counterfeiters as a result of the ease with which software may be duplicated and customer hostility to technological copy-protection systems starting in the middle of the 1980s. That was but a small portion of a much bigger sector in which counterfeiting of expensive branded goods from cigarettes and perfume to aeroplane parts and pharmaceuticals was being prevented. On conclusion, a lot of money has been invested on sealing and other safe packaging methods. Unfortunately, the majority of seals are still pretty simple to kill. The standard seal now involves glueing or tying a substrate with security printing to the item being sealed. Therefore, we must first examine security printing. No amount of glue or string will assist if the whole seal can be readily forged.

Security Printing

Napoleon's introduction of paper money to Europe in the early 1800s, along with the introduction of other valuable papers like bearer securities and passports, sparked a conflict between security printers and counterfeiters that exhibited many traits of a coevolution of predators and prey. The defenders were supported by photography (1839), followed by colour printing and steel etching (1850s). Holograms and other optically changeable technologies have recently been developed to compete with the colour copier and the low-cost scanner. When a government's intelligence services attempt to counterfeit another government's passports or even its cash, as both sides did during World War Two, it is sometimes the same individuals who are active on both sides.

There are times when banknote designers fall victim to the Titanic Effect, which is when they put too much stock in cutting-edge technology or a specific gimmick. The 1990s British currency counterfeit serves as one example. These notes contain a window thread, which is an 8-mm-long, 1 mm-wide metal strip that passes through the paper. Therefore, the note seems to have a dotted metallic line running across it when seen via reflected light, but when it is held up and viewed by transmitted light, the metal strip is black and solid. This was supposed to be difficult to replicate. However, a band of criminals developed a stunning hack. They applied a metal strip to the paper's surface using a low-cost hot stamping technique, and then they printed over it with white ink a pattern of solid bars so that the anticipated metal pattern would still be visible. They were found guilty of forging tens of millions of pounds' worth of notes during their trial. There was also a complacency problem; European bankers thought that because the US dollar only had three colours at the time, forgers would target it.

Packaging and Seals

This brings up the additional issues with sealing and packing. A seal is a "tamperindicating device designed to leave non-erasable, unambiguous evidence of unauthorised entry or tampering," according to the Los Alamos vulnerability assessment team. Not all seals adhere a substrate with security printing to the item being sealed in order to function. I described the lead and wire seals used to guard against tampering with truck speed sensors. However, there are numerous items utilising other materials that adhere to the same basic idea, such as plastic straps that are simple to tighten but difficult to remove without cutting. Additionally, we discussed the use of minuscule bar codes, specific chemical coatings, and other techniques to make items or product batches traceable [7]–[9].

However, the majority of seals now in use function by first creating a tag on a substrate using some kind of security printing, which is then fixed to the item that needs to be secured. Though it's good to keep in mind other uses as well, such as nuclear nonproliferation, shipping containers, and voting machines, the security of pharmaceutical items from both counterfeiting and tampering may be the most significant in terms of money.

Systemic Vulnerabilities

From the specific risks against certain printing techniques and adhesives, we are now moving on to the many system-level concerns.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Figure 1 provides an example that could be helpful. At the swimming pool nearby, In order to reduce congestion, wristbands are given to swimmers during peak hours. Every twenty minutes or so, a new colour is provided, and sometimes, all wearers of a certain colour are ordered to leave. Waxed paper was used to make the band. It contains adhesive on one side and a printed pattern and serial number on the other side at one end. The paper is cross-cut, so if you carelessly peel it off, it will be entirely ruined. It resembles the baggage seals used at certain airports very well.

Figure 1: A wristband seal from our local swimming pool.

Calling the supplier is the easiest strategy; boxes of 100 wristbands cost roughly $8. If you don't want to spend any money, you may use each band just once before gently easing it off by tugging it alternately from various directions to produce the appearance shown in the picture. The printing is creased but still in tact; the damage isn't obvious to a poolside staff and may have really been the result of sloppy application. The problem is that the harm done to the seal by meticulously repairing it twice cannot be clearly distinguished from the results of a careless operator repairing it only once. An even more potent assault is to use something else to repair the seal, such a safety pin or your own adhesive, instead of removing the backing tape off it at all.

Despite this, the wristband seal serves its duty just fine. Because Olympic aspirants utilise the pool when it is not crowded and swim for two hours at a time, there is no motivation to deceive. Additionally, they get a season ticket so they can go out whenever they want and buy a band in the trending colour. But it demonstrates a lot of the potential pitfalls. Customers are the adversary because they apply the seals, the consequences of seal reuse are indistinguishable from those of random failure, unused seals can be purchased on the open market, fake seals can be produced for very little money, and thorough inspection is impractical. However, compared to many sealing systems used for high-value industrial applications, this pool seal is still more difficult to breach.

In certain systems, such as those used in banking, the consumer is the adversary. In military systems, the opponent might be a lone rebellious soldier or the other side's Special Forces attempting to disrupt your machinery. The host government may be attempting to remove fissile materials from a legally operating civilian reactor, according to nuclear monitoring systems. However, the most challenging sealing challenges sometimes appear in business. Once again, the opponent will often put the seal on. An example of this is when a business subcontracts the production of part of its items because it is concerned that the contractor will create more of the goods than anticipated. By value, overproduction is the primary cause of counterfeit products globally; offenders have access to legal manufacturing facilities and raw materials, and grey markets provide convenient distribution networks. It might be challenging to even identify such scams, much alone establish them in court.

For high-value products like cosmetics, a common strategy may be to get packaging components from many separate businesses while keeping their identities hidden from the company running the final assembly facility. Serial numbers may be incorporated into some of these materials in a variety of ways for example, by laser carving serial numbers into bottle

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

glass or printing serial numbers with UV-only inks on cellophane. The manufacturer's field representatives may have access to an internet service that allows them to check the serial numbers of samples they randomly buy from retailers, or there may be a digital signature on the package that connects all the serial numbers for offline verification.

Seals can only do so much on their own. When a vineyard deceptively labels as vintage a thousand more cases of wine that were really created from blended grapes that were purchased, the brand owner is sometimes the villain. Therefore, each bottle of South African wine has a government-mandated seal with a specific serial number; although this does not prove fraud, it does make it more difficult for a dishonest winemaker to get around additional controls like inspection and audit. Therefore, it is frequently necessary to design sealing mechanisms with the audit, testing, and inspection process in mind.

Inspection may be more difficult than one would imagine. The distributor may intentionally mislead the inspectors without having any criminal intent if they purchased counterfeit items on the black market and believed them to be genuine. When grey markets are a problem, the goods purchased from "Fred" will be distributed quickly to the clients, making sure that the inspectors only see authorised goods in his stockroom. Additionally, the distributor may be totally ignorant of the situation; his employees might be selling the fake goods. A well-known fraud involves airline employees purchasing fake jewellery, watches, and other items in the Far East, selling them to passengers on board, and pocketing the money. All of the stocks in the airline's warehouses (as well as those on the duty-free carts when the flights arrive) will be 100 percent real. Therefore, sample purchases made by agents are often necessary, and the sealing systems must accommodate this.

Evaluation Methodology

This discussion offers a methodical approach to assessing a seal product for a specific application. We need to track the seal from its design and field test through production, application, usage, checking, destruction, and eventually retirement from service rather than merely asking, "Can you remove the seal in ways other than the obvious one?" These are some of the inquiries that need to be made:

a) Who is meant to recognise a fake seal if one exists? How often will they encounter real seals if it's the general public? Has the vendor conducted studies to determine the probabilities of false accept and false reject rates that meet the requirements of applied psychology? How much will the tools and training for your inspectors on the field cost? And how motivated are these inspectors, whether they work for the government or are professionals, to spot and disclose flaws?

b) Has anybody who is really skilled at what they do made valiant attempts to undermine the system? And what exactly constitutes a loss—tampering, falsification, change, erosion of the weight of the evidence, or a "PR" assault on your reputation in the marketplace?

c) How well-known is the design team behind it? Have they a track record of outperforming rivals' products?

d) How long has it been in play, and how probable is it that advancement will make a loss much simpler?

e) What other people may purchase, feign, or steal supplies? How broadly accessible are the sealing materials?

f) How will you handle it if the individual applying the seal is irresponsible or dishonest?

g) Does the intended usage of the seal provide enough or the proper protection for the product?

h) What defects are there? What about noise, vibration, cleaning agents, grease, dirt, and manufacturing flaws? Will the product need to withstand exposure to the elements, fuel spills, being carried close to the skin, or being put into a beer glass? Or is it expected to react in a visible way if anything like that occurs? What consequences would random seal

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

failures have and how often will they occur? Exist any evidentiary problems? Are there any other experts than you (or the vendor's) whom the opposing party may depend on if you wind up in court? Is it a good thing or a negative thing if the response is no?

i) Why should the jury trust the system's creator, you, as opposed to the kind-hearted elderly woman in the dock? Will the court absolve her on the basis of a fair trial even though it would be difficult for her to satisfy the burden of evidence to refute your technical claims? (This is precisely what occurred in Judd v. Citibank, the case that resulted in a change to the law regarding 'phantom withdrawals' from cash machines in the US.)

j) How will the seals be disposed of once the product has been used? Would it disturb you if any old seals were found in the garbage?

CONCLUSION

When seal examination is done carelessly by unskilled workers, it is very simple to overcome the majority of commercially available sealing products. Hostile testing is strongly recommended in important applications; sealing must be examined across the whole lifespan of the seal, from production through materials control, application, verification, and ultimately destruction. Security printing, about which generally identical remarks may be made, is often used in seals.

REFERENCES

[1] R. Anderson, “Security Printing and Seals,” in *Security Engineering*, 2020. doi: 10.1002/9781119644682.ch16.

[2] H. A. Hanžuraŭ, “Graphics of units of the state document of turnover of the Republic of Belarus (1991–2019),” *Proc. Natl. Acad. Sci. Belarus, Humanit. Ser.*, 2021, doi: 10.29235/2524-2369-2021-66-2-200-206.

[3] R. Anderson, “Chapter 12 - Security Printing and Seals,” *Secur. Eng. a Guid. to Build. dependable Distrib. Syst.*, 2008.

[4] R. Anderson, “Chapter 11: Physical Protection,” in *Security engineering : a guide to building dependable distributed systems*, 2008.

[5] K. Shirai, “New Thermal Dye Transfer Printing Applications by Using an Intermediate Transfer Printing Method,” in *International Conference on Digital Printing Technologies*, 1999.

[6] J. Zhang and G. He, “Research on anti-printing & scanning watermark algorithm based on spread spectrum coding,” in *Proceedings - 2009 International Conference on Information Technology and Computer Science, ITCS 2009*, 2009. doi: 10.1109/ITCS.2009.267.

[7] Y. Suzuki, V. Dupuit, T. Kojima, Y. Kanamori, and S. Tanaka, “Silicon migration seal wafer-level vacuum encapsulation,” *Electron. Commun. Japan*, 2021, doi: 10.1002/ecj.12283.

[8] B. Bamps, B. De Ketelaere, J. Wolf, and R. Peeters, “Evaluation and optimization of the peel performance of a heat sealed topfilm and bottomweb undergoing cool processing,” *Packag. Technol. Sci.*, 2021, doi: 10.1002/pts.2562.

[9] M. R. Safizadeh, “The Effect of Various Film Packaging, Wax Coating and Storage Conditions on the Shelf Life and Quality of Pomegranate Fruits,” *J. Hortic. Res.*, 2020, doi: 10.2478/johr-2019-0008.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Electronic and Information Warfare

Mr. Manjunath Narayan Rao
Assistant Professor, Department Of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-manjunath.n@presidencyuniversity.in

ABSTRACT: ***A variety of tactics and methods are utilised in electronic and information warfare (EIW) to obtain an edge on the contemporary cyberspace battlefield. This abstract examines the function of EIW in the context of security engineering, emphasizing its significance, difficulties, and potential solutions. EIW is introduced in the abstract as the use of electronic and information-based capabilities to interfere with, trick, deny, or take advantage of an adversary's information systems. It draws attention to the importance of EIW in modern wars, where its dependence on digital infrastructure and linked networks makes it a crucial area for both offensive and defensive operations. The paper then explores the various elements of EIW, such as information warfare (IW), which includes operations aimed at influencing, manipulating, or undermining information systems and processes, and electronic warfare (EW), which involves the use of electromagnetic energy to attack or defend against adversaries. It examines how EW and IW work together and how to incorporate them into current fighting tactics. The issues presented by EIW in security engineering are then discussed in the abstract. It talks about how sophisticated and always changing EIW techniques like malware, phishing, social engineering, and network assaults are. Additionally, it discusses the challenge of linking EIW operations to particular individuals and the danger of unintended repercussions or collateral harm.***

KEYWORDS: ***Echelon System, Information Warfare, Malware, Social Engineering.***

INTRODUCTION

Despite the fact that they both utilise certain similar technology (like encryption), computer security and electronic warfare have existed as independent topics for many years. As components of the two disciplines combine to create the new field of information warfare, this is beginning to alter. Even if the principles, philosophy, and strategy of information warfare are still in their infancy, the Pentagon's use of the phrase as a slogan in the closing years of the twentieth century confirmed its significance. Even if it's not certain that the Russian government was behind the Estonian denial-of-service attacks in 2007, it's evident that they were. As far as we know, it may have simply been a group of Russian hackers [1]–[4].

A security engineer should be familiar with electronic warfare for additional reasons. There are several examples of technology that were once created for the warrior and have now been transformed for commercial usage. We discover deception schemes and tactics of a special depth and sophistication in the fight to dominate the electromagnetic spectrum, which has occupied so many smart people and tens of billions of dollars. It is the only domain of electronic security to have gone through a prolonged phase of attack and defence coevolution with proficient motivated adversaries.

When it comes to service-denial assaults, a subject that computer security professionals disregarded for years, electronic warfare is also our primary instructor. Due to denial-of-service assaults on for-profit websites a few years ago, it suddenly gained attention. Things grew serious when blackmailers began bringing down Internet gambling sites and demanding payment. I'll attempt to highlight the similarities between electronic warfare and other information security issues as I build this debate. Electronic warfare generally has these concepts backwards and inverted whereas computer security is often said to be about confidentiality, integrity, and availability. The precedences are:

1. Denial of service, which includes physical assault, mimicking, and jamming;
2. Deceit, which may be directed towards individuals or automated systems; and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

3. Exploiting the enemy's use of his electronic systems, which involves not just listening in on conversations but also gaining any operationally useful information.

DISCUSSION

Controlling the electromagnetic spectrum is the aim of electronic warfare. It is often thought to include:

1. electronic assault, such as the use of high-powered microwaves to destroy enemy equipment and jam radar or communications;
2. electronic defence, which includes jamming-resistant system design, equipment hardening to withstand high-power microwave assault, and anti-radiation missile jammer destruction; and
3. electronic assistance, which provides the essential threat detection and information to enable efficient assault and defence. It enables commanders to look for, identify, and pinpoint the origins of malicious and electromagnetic energy that isn't intended.

Schleher is where these definitions were pulled from. The traditional area of cryptography, known as communications security (Comsec), makes up a very minor portion of electronic security, just as it is becoming to do with information security in more comprehensive systems. Signals intelligence, or Sigint, is a component of electronic support and is made up of both communications intelligence (Comint) and electronic intelligence (Elint). The former gathers messages from the adversary, including both message content. The latter, meanwhile, is concerned with identifying enemy radars and other non-communicating sources of electromagnetic radiation. It also collects traffic data about which units are communicating.

The core of an electronic assault is deception. To deceive the adversary is the aim by tampering with his senses to reduce the precision of his intelligence and target identification. Clarity about who (or what) is to be fooled, about what, and for how long, as well as the exploitation of pride, greed, sloth, and other vices where the targets of deceit are human are necessary for its successful application. Deception is becoming more and more important to business systems and may be very cost-effective [5]–[9]. A significant component of the mix is physical destruction; although certain enemy sensors and communications lines may be neutralized by jamming referred to as a "soft kill", others will often be destroyed a "hard kill". The use of the various instruments in a coordinated manner is essential for effective electronic warfare. Similar to conventional weapons, electronic warfare systems include input devices like jammers, lasers, missiles, and explosives as well as output devices like communications lines that transmit sensor data to the command and control center. Since communications systems are the most self-contained, I'll talk about them first, followed by sensors and related jammers, and then additional gadgets like electromagnetic pulse generators.

ComPhysical dispatch dominated military communications until about 1860, followed by the telegraph until 1915 and the telephone until recently. Nowadays, a typical command and control system is composed of multiple tactical and strategic radio networks that may transmit and receive speech, data, and picture signals and can operate through point-to-point connections. The commander's effectiveness is likely to be limited in the absence of situational awareness and the ability to lead troops. However, the requirement for communication security is considerably more widespread than one may first think, and the dangers are far more varied.

a) For communications with covert assets, such as agents in the field, there are stricter standards. In this case, location security is crucial in addition to cypher security concerns. The agent will need to take precautions to reduce the possibility of being discovered due to communications monitoring. If he uses a communication channel that the adversary can listen to, like the public telephone network or radio, then a lot of his effort can go into trying to navigate confusing traffic patterns and radio direction finding.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

b) Similarly stricter (though somewhat different) requirements apply to tactical communications, such as those between headquarters and a platoon in the field. Radio direction finding remains a challenge, but jamming may be just as problematic. Intentionally misleading communications may also be a problem. For instance, there is technology that makes it possible to record the vocal instructions of an enemy air controller, separate the spoken commands into phonemes, and then piece the phonemes back together to create false commands. The likelihood of spoofing attacks on unprotected communications may rise as speech morphing methods are developed for commercial usage. As a result, cypher security may also incorporate authenticity in addition to secrecy and stealth.

c) It is necessary to safeguard control and telemetry communications from jamming and manipulation, such as signals transferred from an aeroplane to a missile it has just fired. Additionally, it would be ideal if they could operate covertly (in order to avoid setting off a target's warning receiver), but this would conflict with the power levels required to disarm defensive jamming devices. Making the communications adaptable is one way to do this; for example, starting in a low-probability-of-interception mode and increasing the power as necessary to counter jamming.

Therefore, depending on the situation, a combination of content secrecy, authenticity, resistance to traffic analysis and radio direction finding, and resistance to different types of jamming will be needed to safeguard communications. These interact in a few rather subtle ways. For instance, a radio created for use by opposition groups in Eastern Europe in the early 1980s broadcast on the same radio frequencies as Voice of America and BBC World Service, which the Russians often jammed. The theory was that the Russians would struggle with navigation unless they were willing to switch off their jammers.

Even when the goal is only denial of service rather than analysis or direction finding, attacks often involve a variety of tactics. According to Soviet doctrine, a thorough and effective attack on a military communications infrastructure would entail physically destroying one third of it, effectively denying use of a second third through the use of jamming, trojans, or deception, and then allowing the enemy to disable the remaining third by attempting to pass all of his traffic over a third of his installed capacity. Owen Lewis summarizes it succinctly. This holds true even in guerrilla conflicts; in Malaya, Kenya, and Cyprus, the rebels managed to deteriorate the telephone network to the point that the police were compelled to establish radio nets.

In the 1980s, NATO created a similar doctrine known as Counter-Command, Control and Communications operations (C-C3, pronounced C-C cubed). In the Gulf War, it first began to bloom. Attacking an army's command structures is, of course, a far older tactic; it is also fundamental to fire first at an officer before his soldiers.

Signals Intelligence Techniques

The enemy's network has to be mapped before communications can be targeted. The most costly and important challenge in signals intelligence is locating and separating the valuable information from the cacophony of radio signals and the enormous volume of data being sent across systems like the Internet and the telephone network. Although many of the technologies in use are secret, some of them are available to the general public [10].

Communications intelligence organisations keep vast databases of radio signals, including which stations or services utilise which frequencies, using receiving equipment that can identify a wide range of signal kinds. Signal analysis often makes it easy to identify certain pieces of equipment. Any unintended frequency modulation, the form of the transmitter turn-on transient, the exact center frequency, and the harmonics of the final-stage amplifier are examples of possible components. In the middle of the 1990s, this

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

RF fingerprinting, or RFID, technology was declassified for use in locating cloned mobile phones, where its creators claim a 95% success rate. It is a direct descendent of the method employed during World War 2 to identify a wireless operator by the manner he utilised Morse Code.

RDF, or radio direction finding, is also essential. In the past, this entailed utilising directional antennas at two monitoring sites to triangulate the signal of interest. Therefore, before needing to relocate, spies may have a few minutes to send a message home. By comparing the phase of the signals received at two places, modern monitoring stations employ time difference of arrival (TDOA) to find a suspicious signal quickly, precisely, and automatically; anything more than a few seconds of transmission may be a dead giveaway.

Traffic analysis, which counts the number of messages by source and destination, can also provide very useful information, not just about impending attacks (which, in World War 1, were indicated by a significantly increased volume of radio messages), but also about unit movements and other less important issues. It is impossible to exaggerate the relevance of traffic analysis (both for national intelligence and police reasons) when it comes to filtering through traffic on public networks. Traffic analysis used to be the purview of intelligence organisations until a few years ago; in fact, most of the "hunting" that NSA agents described themselves as doing was traffic analysis. But in recent years, traffic analysis has emerged from the background and grown into a significant academic field.

The snowball search is one of the fundamental methods. If you think Alice is engaging in espionage (or drug selling, or anything else), you should keep track of everyone she calls and everyone who calls her. You now have a list of several suspects.

You delete numbers like banks and physicians because they get too many calls to analyse (your whitelist), and then you repeat the process for each other number. You end up with a pile of thousands of contacts after repeating this process multiple times; they build up like a snowball sliding downhill. You now go through the information you've gathered, checking it for things like persons who are already on one of your blacklists and phone numbers that pop up more than once. Therefore, if Bob, Camilla, and Donald are Alice's connections, and Bob, Camilla, and Eve are in communication with Farquhar as well as Donald and Eve, all of these individuals may be suspects. You now create a friendship tree that approximates Alice's network to some extent and then improve it by combining it with more intelligence. Since 9/11, covert community identification has gained a lot of attention, and academics have explored a variety of hierarchical clustering and graph partitioning techniques to solve the issue.

In order to optimize modularity, Mark Newman's leading algorithm employs spectral approaches to divide a network into its natural communities. However, reality is messier, even with sophisticated mathematical tools for studying abstract networks. People share numbers and may possess many numbers. It becomes much more difficult when the conspirators use active defences; for example, Bob may get a call from Alice at his work number and then dial Eve from a pay phone. If you're operating a terrorist cell, your signals officer should get employment in a dentist's office, a doctor's office, or another establishment that is likely to be whitelisted.

Additionally, you'll need a way to link names and phone numbers. Prepaid mobile phones, as well as duplicate phones and compromised PBXs, may cause major problems, even if you have access to the phone company's database of unlisted numbers. Since ISPs don't typically preserve the Radius data for long, tying IP addresses to specific individuals is much more difficult. Later chapters will go into greater depth on each of these topics, but for now I'll simply say that anonymous interactions are nothing new. Public phone booths and mail boxes have been around for many years.

However, as most criminals lack the discipline to utilise anonymous communications correctly, they are not a universal solution for the thief. For instance, it has been stated that the 9/11 planner Khalid Sheikh Mohammed was apprehended after using a prepaid SIM card purchased in Switzerland in the same batch

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

as a SIM card used in another Al-Qaida operation in Pakistan.

Signals gathering is not limited to obtaining access to call logs and itemised billing details from phone carriers. Additionally, it calls for a broad variety of specialised facilities, from pricey permanent installations that replicate global satellite linkages to quick tactical solutions. The primary fixed collecting network run by the United States, Canada, the United Kingdom, Australia, and New Zealand is described in a book by Nicky Hagar.

The Echelon system, which consists of a number of fixed collection stations and dictionaries that search passing traffic for intriguing phone numbers, network addresses, and machine-readable content, monitors international phone, fax, and data traffic. This is done using search strings entered by intelligence analysts. This may be compared to Google for phone networks, albeit with the current data levels, material is often chosen in real time since even the NSA cannot afford to retain all the data on the Internet and phone networks.

When necessary, tactical collecting facilities are added to this permanent network; for instance, Hagar tells how Australian and New Zealand naval frigates were sent to Fiji during military coups in the 1980s to monitor domestic communications. Fulghum recounts the gathering of aerial signals in, Koch and Sperber address American and German sites in Germany, and there are also clandestine collecting facilities that are not known to the host nation.

However, despite all of this significant capital expenditure, traffic selection—rather than collection—remains the operation's most challenging and costly component [770]. Therefore, despite what one may first believe, encryption can actually increase the vulnerability of communications when utilised improperly, which is the majority of the time. If you just encrypt all of the communication you believe to be significant, the opponent will be able to gather it. Additionally, if your cryptosecurity were flawless, you would have simply given the adversary the ability to map your network and gather all of the unencrypted communications that you exchange with other parties. Now, if everyone encrypted all of their data, it may be much simpler to conceal traffic, which is why signals intelligence organisations are trying to stop people from using cryptography even if it is freely accessible to individuals. This comes up the subject of assaults.

Interaction between Civil and Military Uses

The overlap between civil and military applications of communications is growing. The civilian infrastructure of the Gulf States was heavily utilised during Operation Desert Storm (the First Gulf War against Iraq): a sizable tactical communications network was quickly built using satellites, radio links, and leased lines, and experts from various U.S. armed services claim that the impact of communications capability on the war was utterly decisive. Both military and substate organisations are likely to target civilian infrastructure in order to deny it to their rivals. Satellite connections are already susceptible to uplink jamming, as I said.

The Global Positioning System, or GPS, is just another illustration of our increasing interdependence. This was originally a navigation system for the U.S. military, and it included a selective availability function that reduced accuracy to around 100 yards unless the user possessed the necessary cryptographic key. Due to a shortage of military GPS units during Desert Storm, civilian equipment had to be utilised in its place, forcing this to be switched off. As time passed, GPS proved to be so helpful, especially in civil aircraft that the FAA assisted in developing techniques to circumvent selective availability, which provides an accuracy of roughly 3 yards as opposed to a reported 8 yards for the basic military receiver [431]. President Clinton finally proclaimed the end of limited access in May 2000. It turns out that jamming GPS is not all that difficult, and there has been considerable discussion of the systemic vulnerabilities that arise from relying too much on it [490]. Various individuals have tried with it.

Even yet, the U.S. government has the authority to disable GPS or insert flaws into it, for instance if terrorists were suspected of using it. But a variety of systems now rely on GPS, and many of them have vocal critics. For example, several nations are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

beginning to utilise GPS to implement road pricing or to deploy electronic ankle bands to enforce parole requirements on convicts who have been released from custody. Due to truck drivers' attempts to evade road toll systems and motorists' efforts to circumvent pay-as-you-drive insurance programs, GPS jammers first appeared in automobile magazines in 2007 for $700. However, the price is sure to drop. For other GPS users, the results might be shocking once their usage becomes commonplace. Russia has its own navigation satellite system, and Europe is considering developing its own. Diversity may hold the key to finding a solution. Regardless, research on the security of navigational signals is beginning.

Government organisations, particularly those in the intelligence sector, may also access various defensive systems via the civilian infrastructure. Secure web servers provide some options, and another example is the anonymous remailer, a device that accepts encrypted email, decrypts it, and then sends it on to a destination contained within the outer encrypted envelope. I mentioned the prepaid mobile phone, which offers a fair amount of anonymity. The U.S. Navy-initiated Tor network achieves a similar result for web pages by offering a low-latency method of browsing the internet via a network of proxies. Indeed, many military applications in the future are likely to use the Internet, which will bring up a number of intriguing issues, from the morality of attacking the information infrastructure of adversarial or neutral nations to the specifics of how different types of military traffic can be masked among civilian packets and bistreams.

There might be some convergence after all. Although message secrecy and authentication have traditionally been used to describe communications security on the internet, in the future jamming, service denial, anonymity, and deception may become much more prevalent, similar to military communications. Later, I'll come back to this subject. Let's now examine parts of electronic warfare related to target acquisition and weapon guidance as these are the areas where jamming and deception techniques have advanced the most. Even though there is a lot more available literature on the use of electronic assault and defence against radar than against communications, much of the same information is applicable to both.

CONCLUSION

Compared to the majority of other information security domains, electronic warfare is far more advanced. From the technical level up to the tactical level to issues with planning and strategy, there are numerous lessons to be learnt. These lessons will likely be crucial for engineers if information warfare succeeds and transforms from a cutting-edge idea into a well-established doctrine and practice.

REFERENCES

[1] R. Anderson, “Electronic and Information Warfare,” in *Security Engineering*, 2020. doi: 10.1002/9781119644682.ch23.

[2] L. Gherman, “Electronic Warfare in the Information Age,” *Rev. Air Force Acad.*, 2014.

[3] D. McCrory, “Russian Electronic Warfare, Cyber and Information Operations in Ukraine,” *RUSI J.*, 2020, doi: 10.1080/03071847.2021.1888654.

[4] B. Van Niekerk and C. Cloete, “Management Information Systems for Electronic Warfare Command and Decision Support,” *J. Inf. Warf.*, 2015.

[5] P. Sharma, K. K. Sarma, and N. E. Mastorakis, “Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3044453.

[6] K. Parlin *et al.*, “Full-Duplex Tactical Information and Electronic Warfare Systems,” *IEEE Commun. Mag.*, 2021, doi: 10.1109/MCOM.001.2001139.

[7] M. Ajir and B. Vailliant, “Russian Information Warfare: Implications for Deterrence Theory,” *Strateg. Stud. Q. SSQ*, 2018.

[8] D. Sharma, “Integrated Network Electronic Warfare: China’s New Concept of Information Warfare,” *J. Def. Stud.*, 2010.

[9] A. Al-Khawaja and S. B. Sadkhan, “Intelligence and Electronic Warfare: Challenges and Future Trends,” in *7th International Conference on Contemporary Information Technology and Mathematics, ICCITM 2021*, 2021. doi: 10.1109/ICCITM53167.2021.9677877.

[10] V. B. Niekerk and M. Maharaj, “The Future Roles of Electronic Warfare in the Information Warfare Spectrum,” *J. Inf. Warf.*, 2009.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Brief Discussion on Emission Security

Dr. Chinnakurli S Ramesh
Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-rameshcs@presidencyuniversity.in

ABSTRACT: ***The protection of sensitive information against leakage via unintended emissions, such as electromagnetic radiation or auditory signals, is a crucial component of security engineering. An overview of emission security, its importance in the area of security engineering, and several methods to reduce the dangers related to information leakage are provided in this paper. The paper opens with a definition of emission security and how important it is for protecting private data. It highlights the risks that might be created by accidental emissions and how enemies can use them to collect sensitive information. In a variety of applications, including those involving governmental bodies, military activities, financial institutions, and business settings, the paper emphasises the significance of emission security. The paper then looks at the various emissions that attackers may use, such as electromagnetic radiation, acoustic emanations, and optical emissions.***

KEYWORDS: ***Cryptographic Algorithms, Electromagnetic Compatibility, Emission Security, Technical Surveillance.***

INTRODUCTION

It talks about how these emissions are susceptible to side-channel assaults that might collect data from them. The paper goes on to cover further emission security strategies and countermeasures. The employment of Faraday cages, electromagnetic compatibility testing, electromagnetic shielding methods, secure design principles, and the use of cryptographic algorithms resistant to side-channel assaults are a few examples of these precautions. The paper also discusses the need of physical security measures for emission security, including monitoring systems, access control, and secure facility design. Additionally, it emphasizes the need of regular security audits, vulnerability analyses, and testing to find and address possible gaps in emission security [1], [2]. The paper also looks at new technologies and research projects that attempt to improve emission security. Improvements in signal processing, safe hardware construction, and the creation of new encryption algorithms resistant to side-channel assaults are a few examples. The paper ends by highlighting the need of an all-encompassing strategy for emission security that takes both technological and physical security precautions. It emphasizes how crucial it is to include emission security into a larger security architecture and to regularly review and update security procedures in order to handle new threats and weaknesses. An overview of emission security in security engineering is given in this paper, emphasizing its importance, possible dangers, and mitigation techniques. It provides as a starting point for researchers, professionals, and organisations looking to comprehend and put into practice efficient emission security methods to guard against unintentional information leakage [3], [4].

Emsec, or emission security, tries to prevent attacks that exploit compromising emanations, such as electromagnetic impulses transferred or released. It has several aspects. Tempest barriers, which prevent an opponent from picking up stray RF emitted by computers and other electronic equipment and using it to reconstruct the data being processed, are critical to military groups. After a Dutch group realised they could tell which party a voter had chosen on a voting machine from a distance, temper has recently become an issue for electronic voting as well. Power analysis, which entails seeing a smartcard do a computation (such as a digital signature) by measuring the current consumed by the CPU and the measurements required to reconstruct the key), has severely strained the smartcard industry. These dangers are intertwined, and there are several responses against them. Researchers have also discovered attacks that make advantage of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

stray optical, thermal, and acoustic emanations from many kinds of equipment [5], [6].

Because the information is being leaked via a channel other than those intended for communication, such approaches are also known as side channel assaults. People often underestimate the importance of Emsec. However, it seems that it got the same amount of support from worldwide military agencies as cryptography during the final twenty-four months of the twentieth century. The realisation that all smartcards on the market at the time were extremely vulnerable to simple attacks, which required the attacker to only successfully trick the customer into using a specially modified terminal that would analyse the current it drew during a small number of transactions, significantly slowed the commercial uptake of smartcards in the last few years of that century. Because they did not breach the card, these attacks may have left no trace. They were significantly less costly to deploy than probing attacks and would have allowed for massive card cloning operations against a population of naïve cardholders.

Electromagnetic eavesdropping attacks on various commercial systems, such as automated teller machines, have been demonstrated. Rogue software may cause a machine to emit a louder signal than usual in order to smuggle stolen data past a business firewall. It may also influence the signal. Concerns have also been raised about disruptive electromagnetic attacks, in which a terrorist outfit may use a high-energy microwave source to destroy the computers of a target company without harming people. Electromagnetic compatibility (EMC) and radio frequency interference (RFI), which have the ability to degrade systems accidentally, are inextricably linked to both active and passive Emsec safeguards. If you fly often, you're undoubtedly accustomed to the captain telling everyone to switch off their gadgets and not turn them back on until the seatbelt indication goes off. This problem is worsening as more and more objects become electronic and clock frequencies rise. And how can you obey the captain's instructions when more and more devices are "always on" and the "off" option just turns off the green warning light? All of these vulnerabilities, including RFI/EMC, Emsec, and various electronic warfare threats, will only worsen as more and more devices connect to wireless networks and processor speeds reach gigahertz levels [7], [8].

DISCUSSION

The pioneers of telephony in the nineteenth century, whose two-wire networks were placed on tiers of crosstrees on supporting poles, were fully aware of crosstalk between telephone wires. One solution was to employ 'transpositions,' which included crossing the wires across at regular intervals to create a twisted pair circuit. This issue seems to have been raised for the first time by the military during the British Army campaign to the Nile and Suakin in 1884-85. It was 1914 that compromising emanations were first used in battle. To link the men trapped in the mud of Flanders with their headquarters, field telephone lines were built; these cables often ran parallel to German trenches that were only a few hundred yards distant and often extended for kilometres. A single-core insulated cable used for a phone circuit included an earth return to reduce the cable's weight and overall size by halving it.

It was quickly found that earth leakage produced a great deal of crosstalk, including communications from the other side. It didn't take long to set up listening sites and implement safety precautions including the usage of twisted pair wire. By 1915, valve amplifiers had increased the earth leakage listening range for telephony and Morse code to 100 yards and 300 yards, respectively. It was discovered that the maze of abandoned telegraph wire in no-man's land served as such an effective communications conduit and spilled so much traffic to the Germans that removing it became a mission that required the sacrifice of life. Earth return circuits were no longer used within 3000 yards of the front by 1916. The skills were given to the USA when they entered the conflict [9], [10].

Radar, passive direction finding, and low-probability-of-interception approaches all saw advancements during the Second World War, which I'll cover in more detail in the chapter on electronic warfare. By the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

1960s, 'TV detector vans' were being used in Britain, where TV owners must pay an annual licence fee to support public broadcast services, to target stray RF escaping from the local oscillator signals in household television sets. Information leakage via cross-coupling and stray RF was something that some individuals in the computer security field were also aware of. The first known publication seems to be a Willis Ware-authored Rand Corporation paper from 1970.

Additionally, the intelligence community began to make use of side channel assaults. The Hagelin cypher machine settings for the Egyptian embassy were discovered by the British via a phone bug during the 1956 Suez crisis. The scientists of the British government's security service noticed that the enciphered traffic from the French embassy carried a faint secondary signal in 1960, after the Prime Minister ordered surveillance of the embassy during talks to join the European Economic Community, and they built equipment to recover it. It was the plaintext, which had somehow gotten past the cypher system.

There have been many instances of cypher machines broadcasting in clear over radio frequencies, which is more common than one would think though often there is cause to believe that the vendor's government was aware of this. Emission security was heavily classified throughout the 1970s, and it was no longer discussed in the literature. It was brought back to the public's notice in 1985 when Wim van Eck, a Dutch researcher, wrote an essay outlining how he had used a modified TV set to remotely rebuild the image on a VDU. The computer security industry trembled at the news that Tempest assaults were not only possible but could also be carried out using cheap, home-made tools.

In the second part of the 1990s, published research on linked and emission security-related themes really took off. A lot of smartcards may be compromised by introducing transients, or glitches, into their power or clock lines, Markus Kuhn and I discovered in 1996. Paul Kocher also demonstrated how many popular cryptosystem implementations may be compromised by taking accurate time measurements. In 1998, Kuhn and I demonstrated how the use of the right software controls might improve or exacerbate several of the compromising emanations from a PC. Kocher demonstrated in 1998–1999 that smartcard cryptographic keys may be retrieved with the right processing of exact measurements of the current drawn by the card. Kocher's differential power analysis offered a straightforward and potent signal processing technique for recovering data that completely overcame the somewhat rudimentary defences that the industry had seen fit to provide, even though smartcard vendors had been aware of a potential issue since the late 1980s.

Results have consistently followed in subsequent years. Results on optical leakage were published in 2002. Markus Kuhn demonstrated that the contents of a VDU screen can be recovered optically, even from diffuse light reflected off the operator's face or the walls of the room. Joe Loughry and David Umphress also discovered serial port data in many of the LED status indicators on data serial lines. Li Zhuang, Feng Zhou, and Doug Tygar improved this in 2005 by using keyboard characteristics and text statistics to decipher a recording text typed for ten minutes on a random keyboard, to which there had been no prior access to train the recognition software. In 2004, Dmitri Asonov and Rakesh Agrawal demonstrated that the different keys on a keyboard made sufficiently different sounds that someone's typing could be picked up from acoustic emanations. Steven Murdoch demonstrated in 2006 that many computers betray their CPU load via thermal leakage; clock skew depends on the surrounding temperature and may be remotely detected. He further proposed that it may be used to determine the longitude and latitude of a target machine. These outcomes simply seem to keep piling up.

Technical Surveillance and Countermeasures

We should pause and consider bugs before getting carried away with high-tech toys like Tempest surveillance receivers. The simplest and most common electromagnetic spectrum assaults involve the introduction of a specially constructed device by the attacker rather than an accidental characteristic of unimportant equipment.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Most highly sensitive information is first created either as speech or as keystrokes on a PC, regardless of how effectively it is secured by encryption and access restrictions when in transit or storage. At this point, if it can be taken by the adversary, no further defences are likely to be particularly effective.

So an extraordinary range of bugs is available on the market:

1. A basic radio microphone may be purchased for a few tens of dollars and placed under a table when you visit the target, on the low end. The fundamental limitation of these gadgets is their battery life. They normally have a lifespan of a few days to a few weeks and a range of just a few hundred yards.
2. The gadgets that receive their power from the mains, a phone wire, or some other external electrical source are the next step up and can endure forever once installed. Some of them are simple mics that a foe with a few minutes of privacy in a room may place simply in cable ducting. Others are introduced by drilling almost all the way through a wall or floor of a neighbouring structure or flat. Yet other devices, which seem to be electrical adaptors but are really TV cameras, radio transmitters, and microphones. Others keep track of data, like a Trojan computer keyboard with bugging technology built into the cable connection.
3. Modern bugs often make advantage of generic mobile phone technologies. They may be thought of as slightly altered cellphones that discreetly disconnect when called. This gives them a global range; whether they can be attached to a power source when installed will determine if they can operate for more than a week or so.
4. Laser microphones function by aiming a laser beam towards a reflecting or semi reflected surface in the room where the target conversation is taking place, such as a window pane. Sound waves alter reflected light, which may be detected and interpreted from a distance.
5. Today's high-end government gadgets, which may cost upwards of $10,000, use low-probability-of-intercept radio methods such as frequency hopping and burst transmission. They can also be remotely switched on and off. These characteristics might make them considerably more difficult to locate.
6. People are continuously coming up with innovative new ideas. The jitterbug, which you plug into a keyboard cord, is a modern example. It transforms keyboard data, such as passwords, into imperceptible keystroke delays. This implies that even if your connection is encrypted, a password you input may be readily guessed by an attacker who wiretaps it.

Passive Attacks

We'll start with passive attacks, in which the opponent uses whatever electromagnetic signals are supplied to him without making any attempt to produce them. Although light is electromagnetic, I'll ignore optical signals for the time being; I'll cover them together with acoustic assaults later. Electromagnetic attacks are broadly classified into two types. The signal may be sent through a circuit (such as a power line or phone line), or it can be emitted as radio frequency radiation. The military refers to these two categories of threats as 'Hijack' and 'Tempest', respectively.

They are not mutually exclusive; conducted RF threats are common.

Radio signals generated by a computer, for example, may be picked up by mains power circuits and carried into neighbouring buildings. However, most of the time it is an acceptable functioning categorisation.

Active Attacks

However, it’s not enough to simply encrypt a keyboard scan pattern to protect it, as the attacker can use active as well as passive techniques. Against a keyboard, the technique is to irradiate the cable with a radio wave at its resonant frequency. Thanks to the nonlinear junction effect, the keypress codes are modulated into

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

the return signal which is reradiated by the cable. This can be picked up at a distance of 50–100 yards. To prevent it, one must also encrypt the signal from the keyboard to the PC.

Optical, Acoustic and Thermal Side Channels

There has been a steady trickle of intriguing new discoveries on unique side-channel assaults in recent years. Have you ever seen someone working late in their workplace at night, their face and shirt lit up by the diffuse reflected illumination from their computer monitor? Have you ever considered if any information may be gleaned from the glow? Markus Kuhn demonstrated in 2002 that the answer is 'everything': he connected a high-performance photomultiplier tube to an oscilloscope and discovered that the light from the blue and green phosphors used in conventional VDU tubes decays after a few microseconds. As a consequence, most of the screen information is contained in the temporal domain in the diffuse reflected light. With a telescope, a photomultiplier tube, and appropriate image-processing software, it was feasible to decode the light dispersed off a banker's face or shirt to read the computer screen at which he was staring. The following headline was written by Joe Loughry and David Umphress, who looked at the LED status indicators seen on the data serial lines of PCs, modems, routers, and other communication equipment. Several of them were optically sending serial data: 11 of 12 modems, 2 of 7 routers, and 1 data storage device were tested. The designers were just driving the tell-tale light off the serial data line, not realising that the LED had enough bandwidth to relay the data to a waiting telescope.

There had long been a 'folk tale' that spooks could discern what someone was typing on the ancient IBM Selectric typewriter by just recording the sound they produced, and that data could be extracted from the noise created by dot matrix printers. Dmitri Asonov and Rakesh Agrawal demonstrated in 2004 that the various keys on a keyboard produced enough distinct sounds. They trained a neural network to distinguish key press clicks on a target keyboard and found that typing may be detected from acoustic emanations with a few percent error rate. Now Dawn Song, David Wagner, and XuQing Tian demonstrated that SSH encrypted sessions leak a significant amount of information because keystrokes are sent in individual packets, the time-delays between which are visible to an attacker; they calculated that this would give an attacker a factor of 50 advantage in guessing a password whose encrypted value he had observed.

Li Zhuang, Feng Zhou, and Doug Tygar merged these threads in 2005 to create an even more devastating assault. They distinguished individual keys in a recording of someone typing text in English for around ten minutes on an unfamiliar keyboard, then utilised inter-keypress timings and English statistics to figure out which key was whose. As a result, they were able to decipher text from a recording of a keyboard to which they had never had access.

How Serious are Emsec Attacks?

In both government and business, technical surveillance and its countermeasures bugs are the most essential aspects of Emsec. They are likely to stay that way. The variety of bugs and other surveillance devices available for purchase is extensive and expanding. People will continue to be motivated to spy on their competitors, coworkers, and lovers. If anything, the transition to a connected society will increase the need of electronic monitoring, and countermeasures will consume more of security expenditures. Tempest, Teapot, Hijack, Nonstop, and the various types of power and glitch attack aspects of Emsec that concern equipment not designed for surveillance are set to become another of the many technologies that began in the government sector but have become important in the design of commercial products.

CONCLUSION

Emission security encompasses a wide spectrum of risks in which system security may be compromised by compromising emanations, whether from implanted bugs, inadvertent radio frequency or conducted electromagnetic leakage, or emanations that are produced in some manner. Although Emsec was once a worry in the national intelligence community, it is now a serious problem for enterprises

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

who manufacture security goods such as smartcards and payment machines. By monitoring stray RF or transmitted signals, many of these items may be defeated. Protecting against such risks is not as simple as it may seem.

REFERENCES

[1] E. Papadis And G. Tsatsaronis, 'Challenges In The Decarbonization Of The Energy Sector', *Energy*. 2020. Doi: 10.1016/J.Energy.2020.118025.

[2] A. Sharma, G. Singh, And S. K. Arya, 'Biofuel From Rice Straw', *Journal Of Cleaner Production*. 2020. Doi: 10.1016/J.Jclepro.2020.124101.

[3] O. K. Bishoge, G. G. Kombe, And B. N. Mvile, 'Renewable Energy For Sustainable Development In Sub-Saharan African Countries: Challenges And Way Forward', *Journal Of Renewable And Sustainable Energy*. 2020. Doi: 10.1063/5.0009297.

[4] T. Krikser, A. Profeta, S. Grimm, And H. Huther, 'Willingness-To-Pay For District Heating From Renewables Of Private Households In Germany', *Sustain.*, 2020, Doi: 10.3390/Su12104129.

[5] Yusuf A.S, Adeyemi T.O, Adeleye A.S, Bakpolor V.R, Adegboyega D.A, And Adetola O.O, 'Impacts Of Agriculture And Forestry In The Control Of Climate Change: The Role Of Extension Services', *Int. J. Integr. Educ.*, 2020, Doi: 10.31149/Ijie.V3i10.681.

[6] M. F. Kotb And A. A. El-Fergany, 'Optimal Power Flow Solution Using Moth Swarm Optimizer Considering Generating Units Prohibited Zones And Valve Ripples', *J. Electr. Eng. Technol.*, 2020, Doi: 10.1007/S42835-019-00144-7.

[7] S. P. Mishra, 'Tax And Pandemic; Curbing Carbon Burden Of India's Blue Sky', *Curr. J. Appl. Sci. Technol.*, 2020, Doi: 10.9734/Cjast/2020/V39i3531053.

[8] N. K. Mazitov, R. L. Sakhapov, S. G. Mudarisov, R. S. Rakhimov, And N. E. Garipov, 'The Impact Of Heavy Machine-Tractor Units On The Efficiency Of Agricultural Production', *Tekhnicheskiy Serv. Mashin*, 2020, Doi: 10.22314/2618-8287-2020-58-2-58-66.

[9] A. K. Alnaim, 'Towards A Security Reference Architecture For Network Function Virtualization', *Fau Diss.*, 2020.

[10] T. M. Chaloner, S. J. Gurr, And D. P. Bebber, 'The Global Burden Of Plant Disease Tracks Crop Yields Under Climate Change', *J. Chem. Inf. Model.*, 2020.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Network Attack and Defence

Dr. Devendra Dandotiya
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-devendradandotiya@presidencyuniversity.in

ABSTRACT: ***Modern computer systems rely on networks to enable communication, data transport, and resource sharing. Networks are widely used, but this also makes them a perfect target for illicit activity and online assaults. In the context of security engineering, this abstract presents an overview of network attack and defence while examining the many methods, plans, and defences used to safeguard network infrastructures. The abstract opens by emphasising the value of network security in protecting sensitive information, preserving privacy, and preserving the integrity and accessibility of network resources. It highlights the changing threat environment, which is characterised by complex assaults, advanced persistent threats (APTs), and the rising incidence of insider threats. The paper then looks at many kinds of network assaults. Typical attacks are covered, including Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), Phishing, SQL Injection, Cross-Site Scripting (XSS), and Network Eavesdropping. Each attack's goals, tactics, and possible effects on network security are briefly outlined.***

KEYWORDS: ***DNS Server, Deperimiterization, Network Protocols, Topology.***

INTRODUCTION

We have seen several assaults on certain PCs and other devices up to this point. Attacks, however, rely on connection more and more [1]–[4]. Take a look at the following instances.

1. An email attachment is clicked by a worker at an office. As a result, her PC becomes infected with malware that compromises other computers in her workplace by spying on passwords sent over the LAN.
2. She opened the attachment since her mother sent the email, which is why she did. Her mother's computer had been infected by malware, which transmitted itself and a copy of a recent email to everyone in her address book.
3. By using a generic password for his ISP account, an old acquaintance of her mother's spread the infection. The bad guys don't have to be picky when there are numerous computers on a network; instead of attempting to guess the password for a specific account, they merely try one password repeatedly for millions of accounts. If they have access to a webmail account, they can send spam to everyone on their contact list. Google hacking is another attack method that only makes sense in a network setting. Here, malicious actors employ search engines to locate web servers hosting apps that are vulnerable.
4. Using a series of techniques similar to these, the malware authors infect a large number of PCs in an almost random manner. They then search for prime targets, such as corporate computers that can be used to steal a huge number of credit card details or web servers that can also be used to host phishing web pages. These might be put up for sale and used by experts. Finally, they rent out the remaining hacked machines to spammers, phishermen, and extortionists for less than a dollar each. The botnet herder runs a vast network of compromised computers that he leases out to these criminals.
5. Fast-flux is one of the applications. This makes a website's IP address change, sometimes once every 20 minutes, making it much harder to take down. With each change of IP address, a separate botnet computer serves as the host (or as a proxy to the actual host), therefore banning such an address has at best a momentary impact. The most sophisticated phishing groups put their fake bank websites on fast-flux servers.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Once we have a big number of devices networked together, a variety of assaults and defences appear. The most crucial of them rely on the protocols the network use, among other variables. A second set of variables is related to the network topology: can every computer communicate with every other machine, or does it only have direct access to a small number of them? Like the flu virus, the virus in our previous scenario travels from one buddy to another via a social network.

Before, especially in the chapters on telecomms and electronic warfare, I briefly discussed network elements of attack and defence. However, I'm going to attempt to assemble the network security features into a unified architecture in this chapter. Networking protocols will be covered first, followed by malware; finally, defensive technologies, such as filtering and intrusion detection as well as the popular crypto protocols TLS, SSH, IPsec, and wireless LAN encryption, will be covered.

I'll talk about network topology last. This collection of technologies is most immediately used to protect PC networks from malware, but as more devices become online, the lessons will also be applicable to others. Additionally, a lot of network security approaches have numerous uses. Whether you like it or not, if you create a stronger firewall, you've also created a better tool for internet censorship and a better wiretap tool for the police.

On the other hand, if mobility and virtual private networks make life difficult for the firewall builder, they may also make life difficult for the censor and the police wiretap unit.

DISCUSSION

Vulnerabilities in Network Protocols

Basic network protocols shouldn't be explained in this book. Following is a telegraphic summary. A stateless protocol called the Internet Protocol (IP) is used to transmit packet data from one system to another; Version 4 of IP use 32-bit IP addresses, which are often represented by four decimal integers in the range 0-255, such as 172.16.8.93. Since IPv6 utilizes 128-bit addresses and the 4 billion IPv4 addresses that may have been assigned somewhere between 2010 and 2015, people have begun to move to this version of the Internet protocol. The majority of contemporary equipment is IPv6 ready, but the transition, which businesses will likely do one LAN at a time, will undoubtedly provide some intriguing challenges. The Domain Name System (DNS) enables the mapping of IP addresses of any type to mnemonic names like www.ross-anderson.com. There is a hierarchy of DNS servers that performs this, starting with thirteen top-level servers and moving down through ISP and local network machines that cache DNS records for performance and reliability [5]–[8].

The Border Gateway Protocol (BGP) is the primary routing protocol used on the Internet. The Autonomous Systems (ASs) that make up the Internet include several ISPs, telcos, and huge corporations, each of which is in charge of a variety of IP addresses. The routers, which are specialized computers that send packets across the Internet, utilise BGP to maintain routing tables and share information about the routes that are available to reach certain blocks of IP addresses. A protocol called transmission control protocol (TCP), which is placed on top of IP and offers virtual circuits, is used by the majority of Internet services. To do this, the data stream is divided into IP packets, which are then reassembled at the other end. Any packets whose reception is not acknowledged are automatically retransmitted.

The domain name system (DNS), a globally distributed service in which higherlevel name servers refer to local name servers for specific domains, converts IP addresses into the well-known Internet host addresses. Most local networks utilise Ethernet, in which each device has a distinct Ethernet address (also known as a MAC address), which is then translated into an IP address via the address resolution protocol (ARP). The majority of businesses and ISPs currently utilise the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to machines as required and to guarantee that each IP address is unique due to the rising IP address scarcity. Therefore,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

you often need to get the logs that map MAC addresses to IP addresses if you want to find a computer that has done something bad.

The protocol suite includes a large number of additional parts for controlling communications and offering higher-level services. The majority of them were created back when the internet only had trusted hosts and security wasn't an issue. Therefore, there is not much built-in authentication. This is a specific issue with DNS and BGP. For instance, if a small ISP inadvertently informs a big neighbor that it has excellent access to a significant portion of the Internet, the small ISP may get overloaded with traffic. Since ISPs either swap or pay for routes with their neighbors, there are at least sound economic incentives in this case; BGP security is really compromised by human interference. DNS is more difficult since errors are more often intentional than accidental.

A DNS server could receive false information to direct users to a malicious website. This may be done in bulk, locally, or via an assault on a major ISP's DNS servers. For instance, a lot of households have a wireless router connected to a broadband connection, and the router has the DNS server address that the user uses. Drive-By Pharming is an attack where the bad guy entices you to read a web page with JavaScript code that changes your router's DNS server to one under his control. As a result, the next time you attempt to access www.citibank.com, you can be sent to a phishing website that looks just like it. This makes changing the router at your house's default password a particularly excellent idea.

Attacks on Local Networks

Therefore, the degree to which you have the network secured will determine how easily a bad computer on your network may take control of other machines, and the amount of harm that a bad machine can do will depend on the size of the local network. There are restrictions on how far a system administrator may go; for example, your company may need to manage a complicated mix of old systems for which Kerberos just cannot be made to operate. A system administrator who is concerned with security may also impose significant expenses. Since our academic network shouldn't be made accessible to commercial customers, our lab's sysadmins have fought our attempts to provide access to the Internet for visiting visitors on both technical protection and policy grounds. In the end, we established a distinct guest network that is linked to a commercial ISP rather than the University's backbone to resolve the issue.

Where is the network border, which is a bigger issue? Many businesses formerly had a single internal network that was linked to the Internet via a firewall of some kind. However, compartmentalization often makes sense, as I covered in Chapter 9: distinct networks for each department may reduce the harm that a hacked system can do. If some departments in your organisation have strict protection needs while others require a lot of flexibility, there may be especially compelling reasons in favor of this. In our institution, for instance, we separate the student, staff, and administrative networks, with the first two of these also being divided by college and department. This is because we don't want the students using the same LAN as the payroll employees. The establishment of distinct network borders has become more difficult recently due to mobility and virtual networks.

Deperimiterization is the buzzword used in this discussion, and I'll come back to it. Under the category of assaults on local networks, one more attack the rogue access point deserves to be mentioned. On occasion, maliciously installed Wi-Fi connection points may be found in public places like airports.

If you use it, the operator, who may be sitting in the airport lounge, will be able to sniff any plaintext passwords you enter, such as those for your webmail or Amazon accounts. If you tried to conduct online banking, he might theoretically direct you to a malicious website. The results may thus resemble drive-by pharming, but more consistently and with a less impact. Rogue access points may also be legitimate nodes that have been misconfigured so that they don't encrypt communications or even devices that staff have placed for their own convenience in violation of company regulations. Depending on the situation, unencrypted Wi-Fi communication may or

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

may not be a huge concern; I'll go into more depth on this when we get to encryption later.

Trojans, Viruses, Worms and Rootkits

Experts in computer security have long been aware of the danger posed by rogue code. The first of these programs was called Trojan Horses, after the horse the Greeks left for the Trojans that really housed troops who opened Troy's gates for the Greek invasion. The phrase "malicious code" has been used for many years. There are also worms and viruses, which are malevolent programs that spread on their own. There is disagreement over their exact definitions, but according to common usage, a Trojan is a program that performs malicious actions (like stealing passwords) when it is launched by an unaware user, a worm is something that reproduces, and a virus is a worm that multiplies by attaching itself to other programs.

The rootkit, a piece of software that after being placed on a system secretly gives it remote control, is the last and most quickly spreading issue. Rootkits are useful for both targeted assaults (law enforcement agencies employ them to convert suspects' computers into listening posts) and financial theft (they may include key loggers that record passwords). Stealth is one of the most prominent characteristics of rootkits nowadays; they attempt to conceal themselves from the operating system so that they cannot be found and eliminated using common techniques. But eventually rootkits are discovered, and removal programs are developed. Another way to frame the issue is how botnets are set up, managed, and utilised since most infected PCs acquired in this manner join them. In order to provide their clients, the botnet operators, with the means to update their rootkits for which removal tools are becoming accessible, the rootkit sellers are now providing after-sales support [5], [7], [9].

Countermeasures

As soon as the first PC viruses started to circulate in the wild in 1987, businesses began to offer antivirus software. As a result, both sides engaged in an arms race to outsmart one another. Early software mostly came in two flavors: check summers and scanners. Programs called scanners look for a string of bytes in executable files that are known to come from a particular infection. Virus authors replied in a variety of ways, including with targeted counterattacks against well-known antivirus software; the most common method is polymorphism. The goal is to make it more difficult to create efficient scanners by changing the code each time the virus or worm multiplies.

The standard method is to encrypt the code using a simple cypher and provide a brief header with decryption instructions. With each replication, the virus changes the key used to re-encrypt itself and modifies the decryption code by inserting similar sets of instructions. All permitted executables on the system are listed by checksummers together with the checksums of the original versions, which are commonly calculated using a hash algorithm. Stealth is the principal defence, which in this case implies that the virus keeps an eye out for operating system calls similar to those made by the checksummer and hides whenever a check is conducted.

Researchers have also studied the replication hypothesis of malware. When a viral infection reaches the epidemic threshold, which is the point at which it replicates more quickly than it is eliminated, it becomes self-sustaining. This relies not just on how contagious the virus is, but also on how many susceptible linked devices there are. Although the distinct topology of software interaction (sharing of software is very localized) limits them, epidemic models from medicine may be used to a certain degree and anticipate greater infection rates than are actually seen. (Topology will be covered again later.) Immune system models have also been used in the development of distributed malware detection systems.

Topology

The way a network's nodes are linked is known as its topology. Every computer is effectively (possibly) in touch with every other machine since the Internet is traditionally conceived of as a cloud to which all machines are connected. Therefore, the network may be seen as a fully linked graph from the perspective of a flash worm that spreads from one system to another

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

immediately, without human interaction, and by selecting the next machine to attack at random. But in many networks, each node converses with a relatively small number of other nodes. This may be the consequence of logical connection or physical connectivity, such as between PCs on a separate LAN or a camera and laptop via Bluetooth. The network that a virus is infecting, for instance, is one whose nodes are users of the susceptible email client and whose edges are their presence in one another's address books. This is the case when a virus spreads by emailing itself to everyone in an infected machine's address book.

When the network really functions as a social network in this way, we may use additional concepts and resources. The emerging field of network analysis is reviewed in [965], and has been applied to disciplines ranging from criminology to the study of how new technologies diffuse. Recently, physicists and sociologists have worked together to apply thermodynamic models to the analysis of complex networks of social interactions. Service denial attacks turn out to be dependent on network layout. When suppressing dissenters, rulers have long recognized that it is preferable to concentrate on the ringleaders; similarly, when music industry enforcers attempt to shut down peer-to-peer file-sharing networks, they target the most prominent nodes. Now, this has a strong scientific foundation. It turns out that a sort of graph with a power-law distribution of vertex order, or one in which a high number of edges terminate at a small number of nodes, may be used to simulate social networks. The network is made more durable against random failure and user-friendly by these well-connected nodes. However, as Albert-Laszl'o Barab'asi, Reka Albert, Hawoong Jeong, and Albert-Laszl'o Barab'asi demonstrated, they also ‘make such networks susceptible to targeted assault. The network may be quickly unplugged if the densely linked nodes are removed.

For a variety of reasons, these strategies could potentially become increasingly applicable to network attack and defence. The capture of Saddam Hussein included the application of multilayer social network analysis, demonstrating the effectiveness of early social network approaches. Second, topology will become increasingly important as individuals attempt to attack (and defend) local networks arranged ad hoc using technologies like Wi-Fi and Bluetooth. Third, social networking sites have a lot of social network information that can be used to track people; if a phisherman uses Google mail, the police can look for the people who introduced him, and then for everyone else they introduced, when searching for contacts. More traditional services like Google mail also use introductions to attract new customers. Fourth, individuals will invest in cell-structured organisations and other covert strategies to undermine social structure when it begins to be used against wrongdoers (and against citizens by oppressive governments). Finally, topological knowledge has the potential to be used for a variety of practical purposes. People may be better able to judge the reliability of 'nearby' devices, for instance, and you may not need to filter traffic as rigorously if it originates from a small number of sources rather than the whole Internet. This is not completely obvious since systems evolve over time in ways that call into question the assumptions of trust made by their designers, but it may still be something to consider.

CONCLUSION

Probably the most noteworthy area of security engineering is preventing and identifying assaults that are launched across networks, especially the Internet. Given that the attacker's toolset includes a wide variety of vulnerabilities, the issue is unlikely to be resolved very soon. In an ideal world, humans would execute precisely crafted programs on reliable platforms. In fact This won't occur constantly or even often in life. In the business environment, there is reason to believe that firewalls can prevent the worst assaults, proper configuration management can stop the majority of the remainder, and intrusion detection can stop the majority of the remaining threats. Home users are less advantageously situated, and the majority of the computers joining the massive botnets in operation today are domestic PCs connected to DSL or cable modems.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Hacking methods rely on both social engineering strategies to trick users into executing malicious programs and the opportunistic exploitation of vulnerabilities unintentionally introduced by large suppliers. The majority of the negative outcomes are just the same negative outcomes from a generation ago that have been relocated online, on a greater scale, and with a speed, degree of automation, and global dispersion that catch law enforcement off guard. The Internet is not a catastrophe, despite all of this. A security engineer may sometimes get depressed while thinking about the issues we've covered in this chapter. However, the Internet has greatly benefited billions of people, and online crime rates are far lower than those of traditional crime. The $200 million to $1 billion lost in the USA to phishing in 2006 was far less than regular fraud involving things like checks, not to mention the drug trade or even the trade in stolen automobiles. I'll go into more depth about this when we get to policy in Part III.

REFERENCES

[1] X. Wang and X. Zhang, "Wireless Network Attack Defense Algorithm Using Deep Neural Network in Internet of Things Environment," *Int. J. Wirel. Inf. Networks*, 2019, doi: 10.1007/s10776-019-00430-1.

[2] R. Peng, D. Wu, M. Sun, and S. Wu, "An attack-defense game on interdependent networks," *J. Oper. Res. Soc.*, 2021, doi: 10.1080/01605682.2020.1784048.

[3] H. Zhang, L. Jiang, S. Huang, J. Wang, and Y. Zhang, "Attack-Defense Differential Game Model for Network Defense Strategy Selection," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2018.2880214.

[4] S. Goyal and A. Vigier, "Attack, defence, and contagion in networks," *Rev. Econ. Stud.*, 2014, doi: 10.1093/restud/rdu013.

[5] W. Fang, W. Zhang, W. Chen, T. Pan, Y. Ni, and Y. Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey," *Wireless Communications and Mobile Computing*. 2020. doi: 10.1155/2020/2643546.

[6] Y. Zhu, L. Yu, H. He, and Y. Meng, "A Defense Strategy Selection Method Based on the Cyberspace Wargame Model," *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/4292670.

[7] M. N. U. Islam, A. Fahmin, M. S. Hossain, and M. Atiquzzaman, "Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques," *Wirel. Pers. Commun.*, 2021, doi: 10.1007/s11277-020-07776-3.

[8] S. Yoon, J. H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson, and H. Lim, "Attack Graph-Based Moving Target Defense in Software-Defined Networks," *IEEE Trans. Netw. Serv. Manag.*, 2020, doi: 10.1109/TNSM.2020.2987085.

[9] X. Liu, H. Zhang, Y. Zhang, H. Hu, and J. Cheng, "Modeling of Network Attack and Defense Behavior and Analysis of Situation Evolution Based on Game Theory," *Dianzi Yu Xinxi Xuebao/Journal Electron. Inf. Technol.*, 2021, doi: 10.11999/JEIT200628.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

A Brief Study on Telecom System Security

Dr. Thimmapuram Reddy
Assistant Professor, Department of Engineering Physics, Presidency University, Bangalore, India,
Email Id-ranjethkumar@presidencyuniversity.in

ABSTRACT: ***Global connectedness has been revolutionized by the quick development of telecommunications networks, which has also changed many facets of contemporary culture. The need for the creation and execution of strong security measures arises from the fact that these systems are becoming more and more dependent on telecommunications, which also exposes them to numerous security risks. The topic of "Telecom System Security Warfare" is examined in this abstract within the field of "Security Engineering," with a particular emphasis on the difficulties, tactics, and technologies related to safeguarding telecommunications networks and systems. The importance of telecom system security warfare in protecting telecommunications networks and systems. In order to remain ahead of sophisticated threats, it emphasizes the need of continual research, innovation, and information exchange. It also emphasizes how crucial it is to ensure regulatory compliance and include security concerns from the beginning of design in order to promote a secure telecom environment.***

KEYWORDS: ***Cordless Phones, Phone Phreaking, System Security, Security Warfare.***

INTRODUCTION

For a variety of reasons, the protection of telecommunications networks is an essential case study. First, the reliability of fixed and mobile phone networks is deteriorating and many distributed systems rely on them in ways that are sometimes not visible. In contrast to cellular networks, which normally employ batteries with a maximum 48-hour lifespan, POTS, or the "plain old telephone system," traditionally needed exchanges to have backup generators with enough diesel to withstand a six-week interruption in the energy supply. What's worse is that electricity providers use cell phones to guide their engineers while fixing problems. The energy providers began purchasing satellite phones as a backup when consumers understood that this may lead to major issues in cases when outages lasted more than two days [1]–[5].

Early attacks on phone companies were made by enthusiasts (called "phone phreaks") to obtain free calls; later, criminals began to use the phone system's flaws to avoid police wiretapping; finally, the introduction of premium rate calls provided the justification for widespread fraud; finally, after the liberalization of the telecoms markets, some phone companies began attacking each other's customers; and finally, some phone companies have even attacked one another. The defensive measures implemented at each level were not only exceedingly costly but also often insufficient for a variety of reasons. With the Internet, history is moving much more quickly but otherwise following the same pattern. On the Internet, some of the legal concerns that emerged with landline phones like wiretapping have come up once again. VOIP at the customer level and telecom providers' use of IP networks as the underlying technology generate additional interactions, as do recent advancements in telecom. One example is Skype's two-day outage in August 2007 after Microsoft's Patch Tuesday. Systems are typically not being developed to the previous standards and are becoming far more complicated and interrelated. The introduction of the abstract establishes the significance of security engineering in the telecom industry. It draws attention to the particular security difficulties telecom systems confront, such as the requirement to safeguard private communications, secure infrastructure parts, stop unauthorized access, and identify and lessen assaults. The significance of preventative security measures to defend against developing threats is emphasized in the abstract.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

The paper then explores the idea of "telecom system security warfare," which includes the tactics and methods used to stop harmful actions that attack telecom networks. It examines the numerous fronts of this conflict, such as threat intelligence, network security, and data security. The need of using a thorough and multi-layered strategy to reduce vulnerabilities and safeguard crucial assets is covered in the abstract. The paper also talks about certain security technologies and techniques used in telecom system security warfare. It examines network segmentation, firewalls, intrusion detection and prevention systems (IDPS), secure protocols, and encryption methods. The abstract focuses on the significance of ongoing surveillance, vulnerability analysis, and incident response procedures in preserving the reliability and integrity of telecom systems.

The paper also examines new developments and difficulties in telecom system security warfare. It talks on how the security landscape would change as a result of technologies like 5G, the Internet of Things (IoT), cloud computing, and virtualization. In order to handle growing threats and guarantee adequate security measures, the abstract also emphasizes the significance of cooperation between stakeholders, including telecom providers, governmental organisations, and security experts.

DISCUSSION

Phone Phreaking

Communication services have long been abused. Prior to Sir Rowland Hill, the receiver was responsible for covering the cost of shipping. Recipients were permitted to view a letter and reject it rather than paying for it since unsolicited mail became a significant concern, particularly for prominent persons. Soon after, people devised plans to include brief notes on the covers of letters that their correspondents rejected. Although regulations were introduced to prevent this, they were never really successful.

With the advent of the telegraph, a new set of abuses emerged. People took use of the early optical telegraphs, which employed semaphores or heliographs to operate, to make foreknowledge bets on horse races; if you could find out which horse had won before the bookmaker could, you were in a good position. People would pay the operators or 'hack the local loop' by using a telescope to see the final heliograph station. Attempts to solve the issue via legislation failed in this instance as well. The difficulties became worse once the electric telegraph reduced expenses; the more communication and flexibility that were added to and on top of the service resulted in increased complexity and volume of misuse. The phone was not going to be any different [4]–[7].

Attacks on Metering

Metering methods are still being attacked. To reduce the expenses of coin collection and vandalism, several nations have switched their payphones over to chip cards. As I noted in the chapter on tamper resistance, some implementations have been subpar, and bad guys have produced tonnes of fake phone cards. Other assaults use a technique known as clip-on, which involves physically connecting a phone to another person's line in order to use their service. Foreign students would connect their own phone to a domestic line in the 1970s to make international calls, which may result in a hefty cost for an unwary homeowner. The majority of phone companies were insistent that homeowners pay and could threaten to blacklist them if they didn't, even though the cable was often the phone company's legal obligation up to the service socket in the house. The financial motive for clip-on fraud has mostly vanished since long distance calls are very inexpensive. However, the issue is still significant enough that the Norwegian phone company devised a method in which a challenge and answer are exchanged between an authentication device located in a wall socket and the exchange software prior to the issuance of a dial tone.

A family in the North East of England's Cramlington town suffered greatly as a result of clip-on scam. Hearing a discussion on their line was the first indication that anything was wrong. The cops then showed up and informed them that there had been

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

complaints about annoying phone calls. The complainants were three women, each of whose phone numbers was one digit off from the one that this family allegedly made a tonne of calls to. In addition to the nuisance calls, there were calls to groups of numbers that turned out to be payphones when the family's account was inspected. These calls had begun abruptly at the same time as the nuisance calls. The family's connection was diverted when they subsequently reported a problem to the phone provider, which resolved the issue.

The family's line had been tampered with at the distribution cabinet, according to the maintenance person's report, but the phone company denied there had been a tap. (The phone provider subsequently said that this story was inaccurate.) It discovered out that a drug dealer had previously lived nearby, and it appeared logical to assume that he had tapped their line to contact his couriers at the payphones. He not only reduced his phone expense by using another family's line rather than his own, but he also had a greater chance of avoiding police observation. However, despite the fact that the dealer had already been sentenced to six years in prison, both the police and the local phone company declined to enter the home where the dealer had resided, stating it was too risky.

The request to provide testimony on clip-on for the defence was denied by the Norwegian phone carrier. In the end, the subscriber was found guilty of making harassing phone calls in a case that was generally seen as a miscarriage of justice. At the time, there was debate about whether the police and phone company's decision to close ranks was just a bureaucratic reaction or a sign of something more sinister. Since the attacks of September 11, it has come to light that several phone companies have been providing the authorities with easy access to networks for years, sometimes without a warrant. The inevitable outcome was a strategy of concealing up everything that may wander into this area, even if doing so resulted in unintended consequences. All of this will be covered in more detail in the book's third section. Another variation on the topic is taking the dial tone from cordless phones. This developed to such an extent in Paris in the 1990s that France Telecom defied convention and disclosed that it was taking place, alleging that the victims were using cordless phones that had been illegally imported and were simple to spoof. I have yet to come across any cordless phones with respectable air link verification, whether they are licenced or not. The DECT standard, which the new digital cordless phones utilise, permits challenge-response systems, but the hardware so far marketed seems to convey nothing more complicated than the handset's serial number to the base station.

Insecure End Systems

Insecure terminal equipment and feature interaction are the next significant weaknesses of contemporary phone networks after direct assaults on the systems held on phone company property. Several instances of crooks taking advantage of people's answering machines have occurred. The same method may be used for at least two distinct objectives, such as deceiving a victim into dialing a premium rate number or, in a somewhat more nefarious scenario, secretly emailing a voicemail message via the victim's answering machine. Dial tone is provided by phone company switches twelve seconds after the other side hangs up, which causes an issue. The tones required to call his colleague's number and the secret message may then be recorded on your answering machine by a terrorist who wishes to transmit an untraceable command to a colleague. He then makes a second call, asks the machine to replay its messages, and hangs up. However, businesses and government agencies are the targets of the very significant frauds committed employing vulnerable end systems. By the middle of the 1990s, attacks against corporate private branch exchange systems (PBXes) were huge business and costing companies billions of dollars annually. Refiling calls, also known as direct inward system access (DISA), is often available on PBXs. The normal use is for the sales team of the business to dial a 0800 number, enter a PIN or password, and then dial out once again to take advantage of the affordable long distance rates a big business can acquire. As you could anticipate, bad guys learn about these PINs and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

exchange them. The outcome is referred to as dial-through fraud.

In many circumstances, the manufacturer sets the PINs to a default value, which the client never modifies. In other instances, thieves who monitor phone traffic in hotels to steal credit card information also record PINs; phone card numbers and PBX PINs are a lucrative side business. Prudent people believe that any PBX will have at least one back door installed by the manufacturer to give easy access to law enforcement and intelligence agencies (it's said to be as a condition of export licensing). Many PBX designs have fixed engineering passwords that allow remote maintenance access. Of sure, people will find and misuse such features. One incident included Scotland Yard's PBX being infiltrated and being used by criminals to refile calls, costing the Yard a million pounds, for which they sued their phone installation. The thieves evaded capture all along. This was especially poignant since one of the reasons why criminals commit such crimes is to have access to communications that won't be bugged. The authorities are still hesitant to look into these crimes against businesses, in part because the phone providers aren't very cooperative. Presumably because they don't enjoy being held responsible. Their legislation were contested. In a different instance, Chinese criminals engaged in labor market trafficking smuggled illegal workers into Britain from Fujian, China.

They hacked the PBX of an English district council and used it to reroute over a million pounds' worth of calls to China before being forced to work in sweatshops, on farms, and other places. The gang was stopped by the authorities when many of its workers perished while shell fishing in Morecambe Bay and were drowned by the incoming tide. The council filed a lawsuit against the phone firm to recover its money after seeing the mismatch in its phone bills. Despite having provided the vulnerable PBX, the phone provider said it was not at fault. The criminals' goal in this situation was to avoid being seen as well as to save money. In fact, they used a compromised PBX in Albania to route their calls to China, making sure that the cross-border portion of the call, which is most likely to be monitored by the agencies, was between whitelisted numbers; the same ruse appears to have been employed in the Scotland Yard case, where the thieves made their calls through the USA.

Mobile Phones

Mobile phones have evolved from being an expensive luxury in the early 1980s to one of the major success stories in technology. By 2007, we had over a billion subscribers. This year, it's predicted that over a billion phones will be sold, and the number of customers might reach two billion. Most individuals in wealthy nations own at least one mobile device, and several new electronic services are being created on top of them. Scandinavia has set the standard in this area: in Helsinki, you can purchase a can of Coke and a ferry ticket by sending a text message to the vending machine. Additionally, you may use the camera on your phone to scan a bar code at a bus stop to get a text message 90 seconds before the next bus comes, saving you from having to wait outside in the snow [8]–[10]. Even in developing nations, where the landline network is often deteriorated and consumers formerly had to wait years for phone service to be supplied, growth is brisk. The introduction of mobile phone service in certain areas has linked remote settlements to the outside world. Mobile phones are often used by criminals as well, and not simply for communication. In fact, mobile phone units have essentially replaced paper money in many parts of the third world. If you are abducted in Katanga, the kidnappers will instruct your Kinshasa relatives to get cell phones and text them the secret codes. In affluent nations, criminals are primarily interested in communications, and the majority of police wiretaps increasingly target mobile phones. As a result, both as a component of the underlying infrastructure and as a means of service delivery, mobile phones are crucial to the security engineer. They have a lot to say about fraud strategies and defences, too.

So, Was Mobile Security a Success or a Failure?

Depending on who you ask, mobile phone security has either been successful or unsuccessful. It was unsuccessful from a cryptographic standpoint. Once

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

they were made public, the Comp128 hash function and the A5 encryption technique were both compromised. In reality, Kerckhoffs' Principle, which states that the choice of the key, rather than the mechanism's obscurity, should determine the level of cryptographic security, often uses GSM as an example. The mechanism will eventually leak, thus it's preferable to have the public examine it now rather than after 100 million units have been produced. Of course, most cryptographers didn't find GSM security to be a complete failure since there were many chances for research paper writing.

GSM was a success in the eyes of the phone companies. The challenge-response system in GSM has prevented cloning, and as a result, the stockholders of GSM providers like Vodafone have gained enormous profits. The cryptographic flaws weren't important since they were never used, at least not in a manner that seriously hurt call revenue. The extended conference call hoax is one of a few frauds that continue, although overall, the GSM architecture has proven beneficial to the phone companies. GSM was likewise acceptable in the eyes of the crooks. The method of operation only changed, with the expense being borne by credit card companies or by specific victims of "identity theft" or street robbery. It did not stop them from stealing phone service. Calls from unknown numbers continued to be made; in fact, the growth of the prepaid phone market made them much simpler. Both of these adjustments pleased the phone companies. Naturally, GSM does little to combat dial-through fraud.

GSM looked good from the perspective of the big-country intelligence services. They already have easy access to both domestic and international traffic, and the weaker A5 version makes it easier to launch tactical attacks on emerging nations. Additionally, the second wave of GSM technology is adding additional tasty features, such operator-remote control of phones. There appears to be nothing that can prohibit you from secretly turning on a target's mobile phone without his knowledge and listening to the discussion taking place in the room if you can subvert or pose as the operator.

Things are not nearly as rosy from the perspective of the police and low-resource intelligence agency. GSM networks' increased technological complexity isn't the issue; instead, the phone company can carry out court-ordered wiretaps although it may be difficult to track down the suspect's mobile phone number. The advent of prepaid mobile phones is the issue. This promotes crimes like extortion and stalking while also lowering the signal to noise ratio of traffic analysis algorithms and making it more difficult to target wiretaps. From the perspective of the client, GSM was once promoted as being 100 percent secure. Was it correct? The air link's encryption undoubtedly prevented casual listening, which was sometimes annoying with analogue phones. (There have been some high-profile instances of celebrities being humiliated, such as the British example where Prince Charles was caught speaking to his lover Camilla Parker-Bowles before to his divorce from Princess Diana and the American case involving Newt Gingrich.) However, the majority of phone tapping worldwide is carried out by powerful intelligence organisations, for whom encryption doesn't really matter.

When we consider invoicing, the situation for the customer is considerably worse. The many scams committed by premium rate operators and phone providers cannot be stopped by the cryptographic verification of devices. In fact, the phone company may claim in court that your smartcard and PIN had to have been entered into the handset that made the call, making it tougher to contest erroneous charges. Third-generation smartphones will function similarly. The proliferation of prepaid phones, which might reduce exposure, was made easier by GSM, which is the only slight compensation. Therefore, the subscriber doesn't benefit much from the security measures included into GSM.

From the perspective of the phone company, they were created to provide "security" by offloading most of the toll fraud risk while continuing to let legitimate or fraudulent premium rate business to flow. The only consolation for the average user in the long term is that the complexity of phones and services is likely to increase, which may put pressure on the government

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

to adopt transparent billing systems. There are many forces working in favour of this, such the increasing susceptibility of platforms to malware, and many forces working against it, like the phone companies' aim to conceal pricing so they may overcharge consumers. I don't only mean this in the literal sense of how often phone companies mislead their clients; I also mean it in the figurative sense of how confusion pricing is a key component of phone company economics. The following part, in which I examine the economics of telecommunications and how they relate to fraud and abuse, has a more in-depth discussion of this.

CONCLUSION

The case study of phone fraud is intriguing. For many years, people have cheated phone providers, but lately, the phone companies have retaliated forcefully. Systems were initially not at all safeguarded, making it simple to dodge fees and divert calls. Out-of-band communication was used as a preventative measure, however this approach was found to be insufficient due to the system's quickly expanding weaknesses. These may include user-targeted social engineering assaults made possible by PBXs' subpar design and administration, as well as the exploitation of several tricky feature interactions. The efforts made to protect GSM and its third generation successor on the mobile front make for an intriguing case study. Their engineers focused on dangers to communications security rather than threats to computer security, and they prioritized the interests of the phone corporations above those of the users. While not wholly in vain, their efforts failed to provide a clear-cut answer.

Overall, environmental changes, such as deregulation, which allowed for the entry of several new phone companies, are to blame for the security issues in the telecommunications industry. However, the introduction of premium rate numbers was the primary modification. When it came to manipulating the system, free calls or calls that were difficult for the police to intercept were about the only significant benefits that could be obtained. Phone companies used to sell a service with a negligible marginal cost of provision, but suddenly there was real money at stake. The protective systems in place could not keep up with this progress. The big phone providers' business models, however, are increasingly based on confusion pricing as a result of how threatened they are by price competition. Therefore, there are simply no incentives for a redesign of the billing processes.

REFERENCES

[1] R. Anderson, *20 Telecom System Security*. 2006.

[2] H. A. Bouhamida, S. Ghouali, M. Feham, B. Merabet, and S. Motahhir, “PV Energy Generation and IoT Power Consumption for Telecom Networks in Remote Areas,” *Technol. Econ. Smart Grids Sustain. Energy*, 2021, doi: 10.1007/s40866-021-00103-0.

[3] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, “Security and Trust in the 6G Era,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3120143.

[4] W. M. Cheng and S. M. Wang, “Research on the general algorithm and benefit of real-time positioning advertising system—based on the use of 5G base station data,” *Futur. Internet*, 2021, doi: 10.3390/fi13080187.

[5] Z. H. Xiang *et al.*, “A tuneable telecom wavelength entangled light emitting diode deployed in an installed fibre network,” *Commun. Phys.*, 2020, doi: 10.1038/s42005-020-0390-7.

[6] D. Garcia-Retuerta, P. Chamoso, G. Hernández, A. S. R. Guzmán, T. Yigitcanlar, and J. M. Corchado, “An efficient management platform for developing smart cities: Solution for real-time and future crowd detection,” *Electron.*, 2021, doi: 10.3390/electronics10070765.

[7] M. Al-Hawamdeh and S. Alkshali, “The Impact of Information Technology on Information System Effectiveness in Jordanian Telecommunication Companies,” *Comput. Inf. Sci.*, 2020, doi: 10.5539/cis.v13n1p90.

[8] V. Rotondi, R. Kashyap, L. M. Pesando, S. Spinelli, and F. C. Billari, “Leveraging mobile phones to attain sustainable development,” *Proc. Natl. Acad. Sci. U. S. A.*, 2020, doi: 10.1073/pnas.1909326117.

[9] M. A. Carrillo, A. Kroeger, R. Cardenas Sanchez, S. Diaz Monsalve, and S. Runge-Ranzinger, “The use of mobile phones for the prevention and control of arboviral diseases: a scoping review,” *BMC Public Health*, 2021, doi: 10.1186/s12889-020-10126-4.

[10] I. Forenbacher, S. Husnjak, I. Cvitić, and I. Jovović, “Determinants of mobile phone ownership in Nigeria,” *Telecomm. Policy*, 2019, doi: 10.1016/j.telpol.2019.03.001.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Managing the Development of Secure Systems

Mr. Ajay Mishra
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-ajaykumarmishra@presidencyuniversity.in

ABSTRACT: ***A key component of security engineering is managing the creation of secure systems, which makes sure that strong security features are implemented into software and hardware throughout the development lifecycle. The main factors, difficulties, and best practices for managing the development of secure systems are summarized in this abstract. The introduction of the abstract emphasizes the significance of developing safe systems as well as the dangers of doing so. It focuses on the need of a proactive and organized approach to security, including security concerns into each stage of the development process. The abstract then looks at the core tenets of creating safe systems. This comprises determining the need for security, modelling threats, evaluating risks, and setting security goals. In order to achieve a thorough and successful security policy, the abstract highlights the need of integrating security specialists and stakeholders early in the development process. The paper also discusses the difficulties and complications involved in overseeing the creation of secure systems. It talks about the need of secure testing procedures, safe configuration management, and secure coding practices. It also discusses the value of secure coding standards and development frameworks in fostering standardised and secure software development procedures. The significance of security testing and assessment in the development lifecycle is highlighted in the abstract. It describes numerous testing methods, including code review, vulnerability scanning, and penetration testing, to find and fix security flaws. It also highlights the need of ongoing monitoring and development to guarantee that systems continue to be secure over time.***

KEYWORDS: ***Control Systems, Risk Management, Security, Software.***

INTRODUCTION

We've covered a wide range of security applications, methods, and issues up to this point. If you work as an IT manager or consultant and are being paid to create a safe system, you are probably already searching for a methodical strategy to choose security objectives and defences. This brings up the subject of system engineering, risk analysis, and lastly the key to writing safe code: managing a team [1]–[4]. Business schools believe that management education should be primarily case study-based, with specialized courses in fundamental subjects like law, economics, and accounting. In this work, I mostly adhered to their paradigm. We reviewed the principles, including protocols, access control, and cryptography, before examining several applications with numerous case studies.

The next step is to tie everything together and talk about how to approach a generic security engineering issue. Organizational concerns are important here in addition to technological ones. In order to account for the administrative and work-group demands on the people who will run your control systems, such as guards and auditors, it is crucial to understand their capabilities. You should also collect input from them as the system develops. Your development staff has to be taught appropriate methods of thinking and functioning. Success is a combination of abilities, work habits, and attitudes. There are conflicts: how can you persuade people to act like criminals while yet having them work fervently for the success of the product?

DISCUSSION

Managing a Security Project

Choosing what to safeguard and how to do so is often the most difficult aspect of the project manager's job. The key differentiators between the top teams and the underperformers are threat modelling and requirements engineering. Understanding the choice between risk and reward is the first fatal flaw. Naturally, security personnel give too much attention to the former and too little to the latter. The security

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

consultant may make a loss-reduction pitch about "how to increase your profits by 15%" if the client has a turnover of $10 million, profits of $1 million, and theft losses of $150,000; however, it may be in the shareholders' best interests to double the turnover to $20 million, even if this triples the losses to $450,000. With the same margins, the profit has increased by 85% to $1.85 million.

Therefore, if you are the company's owner, avoid making the mistake of thinking that the only solution to a vulnerability is to patch it and be wary of consultants who can only discuss "tightening security." Often, it's already too tight, so all you really need to do is adjust the focus just a little bit. However, the security team whether internal programrs or outside consultants typically has a motive to exaggerate the hazards, and since it has greater knowledge on the issue, it may be difficult to refute. The same forces that cause a country to overreact to terrorist attacks also operate in businesses.

1. **A Tale of Three Supermarkets:**

My little example case study to make this point involves three stores. The wages of the checkout and security workers as well as stock loss because of theft are among the significant operational expenses of operating a retail chain. Cutting personnel isn't always an option, and working them harder could result in greater loss since checkout lines irritate your consumers. What then might technology do to assist?

In South Africa, one supermarket made the decision to fully automate. Every piece of product would have an RFID tag attached so that a full trolley load could be instantly scanned. If it had been successful, cutting staff numbers and making theft more difficult might have been accomplished using the same RFID tags. Although there was a pilot, barcodes were able to outperform the concept.

Customers had to utilise a unique trolley that was big and unsightly, and the RF tags were also expensive. The difficulty in accurately reading tags attached to objects that carry electricity, such canned beverages, hasn't changed despite significant investment in RFID.

Another store in a European nation intended to employ RFID to combat a hard core of professional thieves who they claimed were responsible for many of their losses. They discussed developing a face-recognition system to notify the guards anytime a known criminal entered a shop after later realising this wouldn't work. However, existing technology is unable to do so with sufficiently low error rates. Finally, civil recovery was decided upon. When a shoplifter is caught, the supermarket sues her in civil court for wasted time, lost wages, solicitors fees and anything else they can think of.

Once they have a judgement in their favour for a few thousand dollars, they then go to the woman's home and seize all of the furniture. All is OK thus far. However, rather of boosting sales, their management chose to take revenge on small-time burglars. Their stock price began to decline shortly after they started to lose market share. Instead of being the root of their downfall, their decision to shift resources from marketing to security may have accelerated it. When I published the first edition in 2001, Waitrose in England, which had recently implemented self-service scanning, looked to be performing the best. You swipe your shop card in a machine that gives you a handheld barcode scanner as you enter their store. As you take items from the shelf and put them in your shopping bag, you scan each item. At the exit, you scan your purchases to get a printed list, swipe your credit card, and go to the parking lot.

This can sound hazardous, but the self-service supermarket did too when all the products were behind the counter in conventional grocers' stores. In actuality, a number of sophisticated control systems are in operation. By limiting access to those with store cards, you can both keep out known shoplifters and promote the store card. It may be humiliating to lose your card (whether by being caught stealing or, more often, falling behind on your payments) since possessing one gives you a trusted status that neighbours you encounter while shopping can see. And because there are no rewards for gaming the system, trusting individuals eliminates a large portion of the motivation for cheating. Of course, it is always possible to arrange for the system to 'break' when the suspect approaches the checkout, giving the staff a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

non-confrontational option to examine the bag's contents, should the security officer at the video screen see someone loitering suspiciously close to the racks of $100 bottles of wine [5]–[9].

2. **Risk Management:**

Risk management procedures inside a corporation are often the source of security regulations. One of the biggest sectors in the world is risk management, which encompasses a substantial portion of the legal profession as well as security engineers, insurers, road safety companies, and fire and casualty services. However, it is surprising how little is really understood about the topic. Engineers, economists, actuaries, and attorneys all approach the issue from various angles, speak in different languages, and come to wildly divergent conclusions. Strong cultural influences are also at play. For instance, if we differentiate between uncertainty, where even the chances are unknown, and risk, where the odds are known but the result is not, most individuals are more uncertainty-averse than risk-averse. A risk is often handled intuitively when the probabilities are immediately apparent, but even here, our responses are influenced by the numerous cognitive biases mentioned. People are free to project whatever worries or biases when the science is unclear or ambiguous. But risk management is more than simply actuarial science with a touch of psychology. Governments and corporations alike are important organisations.

Profit is the reward for risk, and the goal of business is to make money from it. Security measures may often significantly alter the risk/reward equation, but ultimately, it is the responsibility of the board of directors of a corporation to strike the correct balance. They may consult with attorneys, actuaries, security engineers, as well as their marketing, operations, and finance teams, for help on this risk management duty. Attacks on information systems are only one aspect of a strong business risk management plan; there are also operational risks that are not related to IT, such as fires and floods, as well as legal risks, currency rate risks, political risks, and many more. Company executives must guarantee that advisors from many disciplines collaborate closely enough to avoid groupthink in order to make wise judgments. This is a challenging responsibility for them.

The regulations created by the Big Four audit firms in reaction to Sarbanes-Oxley have mainly shaped the practice of risk management. A typical company will demonstrate that it is upholding its obligations by maintaining a risk register that lists the major threats to its financial performance and rates them in some fashion. Senior managers who are in charge of monitoring risks and choosing any necessary solutions are given the title of "owners" of such risks. Thus, operational risks like fires and floods will be addressed by insurance; exchange-rate and interest-rate risks may be assigned to the finance director, some of which he will hedge; and system risks may end up with the IT director.

3. **Organizational Issues:**

It should go without saying that advisors should respect one other's duties and cooperate rather than compete with one another. The counsellors could, however, get close to one another and establish a consensus view that gradually departs from reality given the nature of human nature. Therefore, the CEO or another responsible management has to probe deeply and stir the pot a little. It's crucial to hire new individuals often and to have a diverse group of expertise. One of the most significant changes after Enron is the expectation that businesses periodically switch out their auditors. As a security engineer, you may be relied upon to do this work when you are brought in as an impartial outsider to confront groupthink.

Maybe a third of the consulting projects I've worked on had at least one client firm employee who knew precisely what the issue was and how to resolve it; they simply needed a reliable mercenary to take down the bulk of their coworkers who were stuck in a rut. (This is one reason why well-known consulting companies with a reputation for quality and certainty may have an edge over specialists, but a generalist consultant may find it challenging to determine which of the 10 distinct opposing viewpoints from insiders has to be taken seriously. Even while government has somewhat different objectives and organisational systems, the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

same fundamental ideas still hold true. Because employees are more used to complying with standards than to case-by-case requirements engineering, risk management is often more difficult. Empire-building is a concern in the public sector in particular. James Coyne and Normal Kluksdahl provide a well-known example of information security gone awry at NASA. In order to cover the void created by the DoD's withdrawal, a security team was established at the Houston Mission Control Centre when military participation in Space Shuttle operations came to an end. This team was given a challenging mandate, it gained independence from both development and operations, its demands became more unconnected to financial and operational limitations, and its relationships with the rest of the organisation grew more hostile. Ultimately, it had to be removed or nothing would have been accomplished.

The essential argument is that knowing the qualifications and skills of the guards (and the auditors, and the checkout employees, and everyone else inside the trust perimeter) is insufficient when doing a security needs analysis. Many systems fail because their creators had unreasonable expectations regarding motivation, which is crucial. Structures within organisations matter. Additionally, there are risk dynamics that might cause instability. For instance, a low fraud rate at first may cause individuals to become careless and complacent until things unexpectedly blow up. Additionally, an externally caused change in the organisation, such a merger or political unpredictability, might erode morale and consequently control. During my earlier years, I travelled as a security consultant to countries where local traumas were driving up bank fraud, including Hong Kong in 1989. Therefore, you must account for how human frailties manifest themselves in organizational behavior while creating your ideas.

Methodology

Typically, software projects go over budget, take longer than anticipated, and contain more defects than anticipated. This is frequently referred to as "Cheops' law" after the Great Pyramid's constructor. The term "crisis" is scarcely relevant for a situation that has now persisted (like computer vulnerability) for two generations. By the 1960s, this had come to be known as the software crisis. Anyway, Brian Randall coined the phrase "software engineering" in 1968, and it is described as: "Software engineering is the establishment and use of sound engineering principles in order to obtain economically reliable software that operates effectively on real machines."

This included the wish that the issue could be resolved using a proven scientific framework and a set of design guidelines, much like how ships and aeroplanes are constructed. Much development has been achieved since then. The outcomes of the advancement, nevertheless, were unanticipated. People thought that by the late 1960s, we would reduce the 30% or more failure rate that was then recorded for big software initiatives. The failure rates for major projects are still about 30% now, but they are significantly higher. Before we tumble down the complexity mountain, the tools help us climb farther, but the failure rate seems to be exogenous, determined by things like risk appetite among firm managers1.In any case, managing complexity is what software engineering is all about. There is also the unintentional difficulty of programming with ineffective tools, such the assembly languages that certain early computers only supported; creating a contemporary application with a graphical user interface in such a language would be very time-consuming and prone to mistakes. Dealing with significant and complicated challenges has inherent complexity as well. For instance, the administrative systems of a bank may include tens of millions of lines of code and be too complex for any one individual to comprehend. Technical tools are mostly used to cope with incidental complication. The most crucial of them are high-level languages, which allow programrs to create code at an appropriate degree of abstraction and conceal most of the tedious work of dealing with machine-specific details. Additionally, there are formal approaches that make it possible to verify especially error-prone design and programming activities. Intrinsic complexity often necessitates the use of methodological methods that break the issue down into smaller, more manageable subproblems and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

limit how much they may interact. There are several tools available on the market to assist you in doing this, and the one you choose may depend on your client's policies.

Top-down and iterative techniques are the two main types, however. The waterfall model has the advantages of requiring early clarification of system objectives, architecture, and interfaces; simplifying the job of the project manager by giving them specific deadlines to work towards; potentially increasing cost transparency by allowing for separate charges to be made for each step and for any late specification changes; and being compatible with a wide range of tools. It's often the best strategy when it can be made to work. If the requirements are well understood before beginning any development or prototype work that is the crucial question to ask. This is the case, for example, when developing a cryptographic processor to implement a known transaction set and pass a specific degree of evaluation or while creating a compiler in the security realm. In Figure 1 shown the waterfall model.

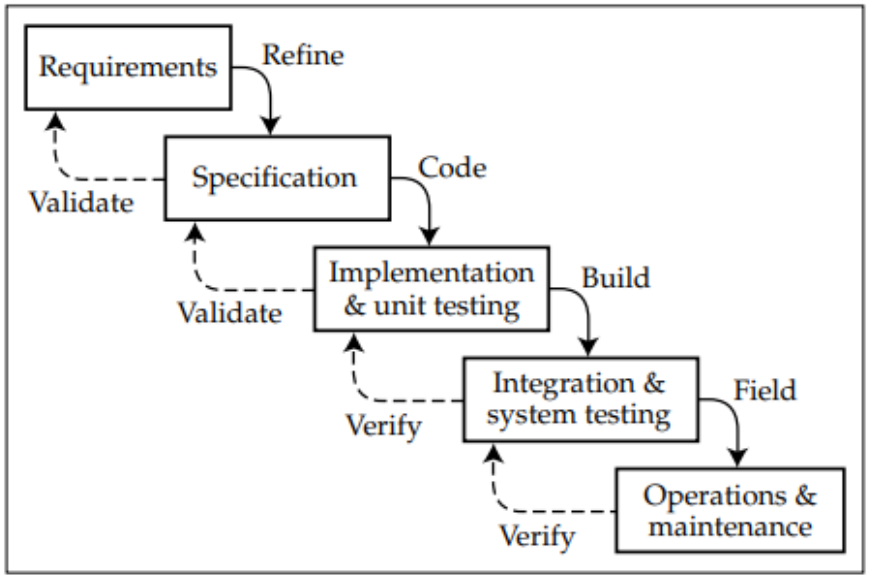

Figure 1: Illustrate the waterfall model.

Security Requirements Engineering

A security target, which is a more thorough description of the security controls that a particular implementation offers and how they relate to the control goals, is created by further refining the security policy model. The security goal serves as the foundation for a product's testing and assessment. The process of creating a security policy and getting the system owner's approval on it is known as requirements engineering. The policy model and the target together may be referred to as the security policy. The toughest and often most important part of managing secure system development is security requirements engineering. The "rubber meets the road" there. It sits at the crossroads of the trickiest technological problems, the fiercest bureaucratic power conflicts, and the tenacious attempts at blame shifting [10]–[13].

The approaches that are now accessible constantly lag behind those that are available to the rest of the system engineering community. The crucial realization, in my opinion, is that creating a security strategy or security aim is not fundamentally different from creating code. You may utilise a top-down, waterfall technique, a restricted iterative strategy like the spiral model, or a continual iterative process like the evolutionary model, depending on the application. In each situation,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

we must include risk management tools and let the risk assessment guide the creation or growth of the security policy.

Once the system is put into operation, risk management must continue as well. It may be impossible to forecast the applications of new inventions, and this also holds true for their bad side: fresh assaults are just as unpredictable as anything else that will happen in the future. In the 1970s, phone companies spent a lot of time finding out how to prohibit people from making free calls, but as premium-rate numbers started to surface, the main challenge was preventing fraud. We feared that thieves would hack bank smartcards, so we added a lot of back-end security to the early electronic purses; nonetheless, pay-tv smartcards were the target of assaults, while bank fraud specialists focused on mag-stripe fallback and phishing. People were concerned about the security of credit card information used in online purchases, but it turned out that refunds and disputes posed the biggest danger to online firms.

The street, as they say, "finds its own uses for things." Therefore, you can't expect to fulfil the protection needs perfectly on your first try. The policies and processes that were put in place when a system was originally constructed were often weakened when the environment (and the product) changed but the protection did not. Spending a lot of money trying to come up with new attacks is pointless if you're operating a business; that's research, and it's better left to academics like myself. What you do want is a method for preventing your developers from creating systems that are susceptible to known problems like stack overflows and weak encryption, as well as a system for tracking and responding to shifting protection requirements. As it is more typical than in the preceding part, we'll start by examining the scenario of changing protection needs.

CONCLUSION

It's challenging to oversee a project to construct or improve a secure system. Creating a product with the assistance of professionals, such as an antivirus monitor or encryption program, was formerly thought of as "security software." Nowadays, it's common to write systems that must do actual tasks, such as online applications or devices that monitor network traffic, and to avoid any flaws that would leave them vulnerable to attack. To put it another way, you want software security, which is distinct from security software.

The trickiest aspect of the procedure is often comprehending the criteria. Security requirements engineering might be a one-time effort, a limited iterative process, or a continual development, much as building the system itself. As systems grow and survive longer, whether as packaged software, internet services, or devices, evolution is becoming more prevalent. Changes in size, organizational structures, and most importantly, the environment, where the changes may be in the platform you use, the legal context in which you operate, or the dangers you face, complicate security needs. Systems are deployed, become well-liked, and then come under assault.

Writing secure code must be seen in this light; the main challenge is understanding what you're attempting to do. Even with a strict specification or ongoing input from users who are hacking your product, you're not out of the woods yet. It can be difficult to find the right candidates, keep them informed about attacks, and support them with knowledge in the areas where they'll actually use it, reinforce this with the appropriate tools and lingo, and, most importantly, foster an environment where they can work to advance their security capabilities.

REFERENCES

[1] R. Anderson, “Managing The Development Of Secure Systems,” *Secur. Eng. A Guid. To Build. Dependable Distrib. Syst.*, 2008.

[2] Z. Wang, N. Luo, And P. Zhou, “Guardhealth: Blockchain Empowered Secure Data Management And Graph Convolutional Network Enabled Anomaly Detection In Smart Healthcare,” *J. Parallel Distrib. Comput.*, 2020, Doi: 10.1016/J.Jpdc.2020.03.004.

[3] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, And K. Jones, “A Survey Of Cyber Security Management In Industrial Control Systems,” *Int. J. Crit. Infrastruct. Prot.*, 2015, Doi: 10.1016/J.Ijcip.2015.02.002.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

[4] G. Lacava *Et Al.*, "Cybersecurity Issues In Robotics," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, 2021, Doi: 10.22667/Jowua.2021.09.30.001.

[5] E. C. Villarosa, "Developing A Record Archiving System In Eastern Visayas State University-Burauen Campus," *Int. J. Multidiscip. Acad. Res.*, 2021.

[6] M. N. Mujiono, "The Shifting Role Of Accountants In The Era Of Digital Disruption," *Int. J. Multidiscip. Appl. Bus. Educ. Res.*, 2021, Doi: 10.11594/10.11594/Ijmaber.02.11.18.

[7] A. Saidane And S. Al-Sharieh, "A Compliance-Driven Framework For Privacy And Security In Highly Regulated Socio-Technical Environments: An E-Government Case Study," In *Research Anthology On Privatizing And Securing Data*, 2021. Doi: 10.4018/978-1-7998-8954-0.Ch043.

[8] M. Ramachandran, "Software Security Requirements Management As An Emerging Cloud Computing Service," *Int. J. Inf. Manage.*, 2016, Doi: 10.1016/J.Ijinfomgt.2016.03.008.

[9] F. F. Alruwaili, "Artificial Intelligence And Multi Agent Based Distributed Ledger System For Better Privacy And Security Of Electronic Healthcare Records," *Peerj Comput. Sci.*, 2020, Doi: 10.7717/Peerj-Cs.323.

[10] D. Mellado, E. Fernández-Medina, And M. Piattini, "Security Requirements Engineering Framework For Software Product Lines," *Inf. Softw. Technol.*, 2010, Doi: 10.1016/J.Infsof.2010.05.007.

[11] D. Mažeika And R. Butleris, "Integrating Security Requirements Engineering Into Mbse: Profile And Guidelines," *Secur. Commun. Networks*, 2020, Doi: 10.1155/2020/5137625.

[12] J. Boutahar, I. Maskani, And S. E. G. El Houssaïni, "Experimental Evaluation Of Security Requirements Engineering Benefits," *Int. J. Adv. Comput. Sci. Appl.*, 2018, Doi: 10.14569/Ijacsa.2018.091158.

[13] S. Prabhakaran And K. Selvadurai, "Performance Analysis Of Security Requirements Engineering Framework By Measuring The Vulnerabilities," *Int. Arab J. Inf. Technol.*, 2018.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

System Evaluation and Assurance

Mr. Narender Singh
Assistant Professor, Department of Mechanical Engineering, Presidency University, Bangalore, India,
Email Id-narendersingh@presidencyuniversity.in

ABSTRACT: ***Critical components of security engineering that guarantee the efficiency and dependability of security systems are system assessment and assurance. The main ideas, approaches, and difficulties involved in evaluating and validating the security of systems are highlighted in this abstract, which offers an overview of the significance of system evaluation and assurance in the context of security engineering. The definitions of system evaluation and assurance and their importance in the larger subject of security engineering are given at the beginning of the abstract. It highlights their importance in locating weaknesses, evaluating risks, and confirming the efficiency of security controls and systems. The abstract emphasizes the need of a methodical and thorough approach to assessing and guaranteeing system security. The importance of frameworks and standards in system assurance and assessment is also covered in the abstract. It examines widely used standards that provide direction and criteria for assessing and guaranteeing system security, including ISO/IEC 27001, the NIST Cybersecurity Framework, and Common Criteria. The need of coordinating assessment and assurance efforts with these standards is emphasised in the abstract in order to guarantee consistency and dependability. The abstract also covers the advantages of independent third-party certification and review. It emphasises the need of external evaluations in fostering trust and confidence in the security of systems, particularly in areas essential to the economy or the government. The abstract also discusses the difficulties and factors to be taken into account when hiring outside assessors.***

KEYWORDS: ***Open Source Software, Security Engineering, System Evaluation, System Security.***

INTRODUCTION

It examines widely used standards that provide direction and criteria for assessing and guaranteeing system security, including ISO/IEC 27001, the NIST Cybersecurity Framework, and Common Criteria. The need of coordinating assessment and assurance efforts with these standards is emphasised in the abstract in order to guarantee consistency and dependability. The abstract also covers the advantages of independent third-party certification and review. It emphasises the need of external evaluations in fostering trust and confidence in the security of systems, particularly in areas essential to the economy or the government. The abstract also discusses the difficulties and factors to be taken into account when hiring outside assessors.

In this book, I've covered a lot of ground, some of it extremely challenging. However, I saved the most difficult for last. These are concerns with assurance whether the system will function—and evaluation how you persuade others of this. How do you decide whether to ship the goods, and how do you persuade your insurance to buy the safety case. Assurance ultimately boils down to the issue of how much the system has been beaten up by talented, motivated individuals. But what really is "enough"? And what exactly is the "system"? How do you handle those who defend the incorrect item since their model of the criteria is outdated or just incorrect? How then can you account for human fallibility? Many systems are ineffective for their intended purpose because they are difficult for average people to use or are intolerant of mistake, even if they can be managed perfectly by attentive, experienced specialists [1]–[4].

However, if assurance is difficult, assessment is much more so. It's about persuading your employer, your clients, and, in the worst case scenario, a jury that the system is truly fit for purpose and that it operates as intended (or that it did operate as intended at a certain point in the past). Evaluation is difficult and vital since, often, one principle bears the risk of failure while another bears the expense of protection. Third-party assessment frameworks, such as the Common

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Criteria, are often employed to increase transparency since this clearly causes tension.

DISCUSSION

The evolution of dependability may be much worse for software engineers than it is for biological species, but it is much worse for security engineers. Let's look at a more straightforward example rather of getting into the intricate maths. Consider a sophisticated product like Windows Vista that has 1,000,000 problems with a 1,000,000,000-hour MTBF. Imagine that Brian is the army assurance specialist whose duty it is to stop Ahmed as he attempts to hack into the U.S. Army's network to get a list of informers in Baghdad while Ahmed is working in Bin Laden's cave. He must thus become aware of the bugs before Ahmed does.

Ahmed can only complete 1000 hours of testing every year since he must travel around to elude the Pakistani army. Brian is in charge of the government's program to dispatch consultants to crucial industries like power and telecoms to learn how to hack them (excuse me, to advise them how to protect their systems). He also has the full source code for Vista, dozens of PhDs, control over the commercial evaluation labs, inside information on CERT, and a deal to share information with other UKUSA member states. Brian tests for 10 billion hours annually.

Ahmed discovers a bug after a year, while Brian has discovered 10,000. However, there is only a 1% chance that Brian has discovered Ahmed's problem. Even if Brian sends 50,000 recent graduates in computer science to Fort Meade to go through the Windows source code, he will still only complete 100,000,000 hours of testing annually. He will discover Ahmed's virus eight years later. Ahmed will have discovered nine more by that time, and it's doubtful that Brian will be aware of them all. Even worse, Bill will no longer be resolving bug reports from Brian since they have accumulated to such a firehouse.

To put it another way, thermodynamics is on Ahmed's side. Anything that is vast and sophisticated may be broken by an attacker with even relatively modest resources. As long as there are enough distinct security flaws to compile statistics, nothing can be done to stop this. Real-world vulnerabilities are connected rather than independent; for example, if 90% of your vulnerabilities are stack overflows and you use compiler technology to catch them, then there was only one vulnerability for modelling reasons. Nevertheless, it has taken several years to kind of cure that specific weakness, and new ones continue to emerge. In other words, you can't simply depend on a big, complicated commercial off-the-shelf product if you're truly in charge of Army security. Mandatory access restrictions must be used, and they must be implemented in something easy to verify, such a mail guard. The secret to escape the statistical trap is simplicity.

Evaluation

Evaluation is defined as "the process of assembling evidence that a system meets, or fails to meet, a prescribed assurance target" in a practical sense. (It overlaps testing and is sometimes mistaken for it.) As I previously said, this proof may only be required to persuade your manager that the task has been accomplished. However, it is often necessary to reassure principals who will depend on the system. The core issue is the conflict that results from having diverse parties execute and rely on the protection [5].

When you construct a burglar alarm to standards established by insurance underwriters and get it validated by inspectors at their labs, the strain is often easy and controllable. When building to government security requirements that attempt to balance dozens of competing institutional interests, or when employing your company's auditors to assess a system and inform your boss that it is appropriate for purpose, it may sometimes be still apparent but more difficult. It becomes more difficult when there are several principals involved, as when a smartcard vendor needs an evaluation certificate from a government agency (which wants to promote the use of a feature like key escrow that is not in anyone else's interest) in order to sell the card to a bank, which then wants to use it to shift fraud liability to its customers. Although it may look very shady, none of the parties involved may have engaged in behavior that is obviously unlawful.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

Managers may exhibit crookedness as an emerging characteristic as a result of adhering to their own individual and departmental motivations.

To reduce their risk of being fired when things go wrong, managers, for instance, often purchase goods and services from reputable suppliers while knowing they are inferior or even faulty. (About 20 years ago, it was believed that "no one ever got fired for buying IBM"). Corporate solicitors applaud this as due diligence rather than denounce it as fraud. In the end, it could be difficult for someone who depends on a system—in this example, the bank's customer—to have their voice heard and to seek restitution from the bank, the vendor, the evaluator, or the government when anything goes wrong [2], [3], [6].

The words "assurance" and "evaluation" are frequently understood to apply only to the specific technical aspects of the system, ignoring system issues like usability, not to mention organizational issues like appropriate internal control and sound corporate governance. This is a serious and widespread problem. The assurance that the prescribed processes are followed, that there are no significant mistakes in the accounting, that relevant laws are being followed, and a host of other things are also important to company directors. However, a lot of assessment methods (particularly the Common Criteria) studiously exclude the organizational and human components of the system. The examination of these components is assumed to be the responsibility of the client's IT auditors, or even a system administrator putting up configuration files, if any consideration is given to them at all.

Having stated that, the following will concentrate on technical assessment. To divide assessment into two situations is practical. The first situation is one in which the relying party does the review; examples of this include insurance evaluations, NASA's independent verification and validation of mission-critical code, and the Orange Book, an older generation of military evaluation standards. The second situation is one in which someone other than the party depending on the assessment does it. These days, the Common Criteria are often meant.

Ways Forward

A more practical method of product assessment and assurance would take into account the product's actual behavior in use as well as its technical attributes. A UK government email system that required users to restart their PC whenever they changed compartments so frustrated users that they made informal agreements to put everything in common compartments effectively wasting a nine-figure investment is one example of how usability is ignored by the Common Criteria but is in reality of utmost importance. It is certain that official concealment will continue to save the guilty persons from punishment. In order to mitigate the impacts of human frailty, characteristics like those we discussed in the context of accounting systems in Chapter 10 are crucial. In most applications, it is necessary to make the assumption that individuals are often dishonest, usually inept, and always careless.

The reality of huge, feature-rich programs that are updated regularly must also be faced. You cannot wish away economics. In order to give buyers the impression of stability, evaluation and assurance schemes like the Common Criteria, ISO9001, and even CMM attempt to corral a highly dynamic and competitive sector into a bureaucratic straightjacket. However, given how the market operates, the best thing consumers can do is support well-known companies, such as Microsoft now and IBM in the 1970s and 1980s. These brands are created and maintained by powerful commercial forces, and security plays a little role. I've probably provided you with enough tips at this point on how to game the system and make it seem secure, at least long enough for the issue to be someone else's. I'll assume for the duration of this book that you're really trying to safeguard a system and prefer risk mitigation over due diligence or other forms of responsibility dumping.

We've seen a few of these systems above (nuclear command and control, pay-tv, prepayment utility metres, etc.), and there are still plenty of systems where the system owner loses if the security fails. These systems provide many fascinating technical examples.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

1. *Hostile Review:*

It's crucial that the design undergo a hostile assessment if you actually want a protective property to hold. It should be completed prior to the system going into service since it will ultimately be. As shown by several case studies, The attacker's intent is virtually everything; positive feedback from those who want the system to work is essentially pointless in comparison to contributions from those who are actively seeking to undermine it. Contractual and adversarial methods of hostile review are traditional.

The Independent Validation and Verification (IV&V) program employed by NASA for human space travel is an example of the contractual technique; contractors were recruited to comb over the code and were given a bonus for each fault they discovered. In the examination of nuclear command and control, Sandia National Laboratories and the NSA competed to uncover flaws in each other's designs as an illustration of the conflictual method. Hiring many specialists from various consultant companies or colleges and rewarding them with repeat work goes a long way towards merging the two. Whoever identifies problems and enhances the design the most obviously wins. Another is having several distinct accrediting organisations: Similarly, back when there were no standards enforced by organisations like VISA and SWIFT, banks would construct local payment networks, with each having the design reviewed by its own auditors. Although there are some extremely terrible legacies banking and voting systems, neither strategy is perfect.

2. *Free and Open-Source Software:*

The free and open-source software movement broadens the openness tenet to include implementation specifics in the architecture. The first security product with publicly accessible source code was presumably the PGP email encryption tool. Many users rely on the open-source Linux operating system and Apache web server to secure their information. The government is also pushing for the use of open source [7], [8]. The concept of open-source software is not totally new; in the early years of computers, the majority of system software providers made their source code available. When lawsuit pressure forced IBM to establish a "object-code-only" policy for its mainframe software, in spite of harsh opposition from its user community, this openness began to wane in the early 1980s. IBM is a pillar of open source and the pendulum has just started to swing again. There are many compelling reasons both for and against open source software. As Raymond famously said, "To many eyes, all bugs are shallow," bugs are more likely to be detected and solved if everyone in the world has access to examine and interact with the program. This is particularly true if the program is maintained via collaboration, as is the case with Linux and Apache. Additionally, it could be harder to add backdoors to such a product.

Open source is often defended by defence contractors with the claim that if software is huge and complicated, there may be few or no skilled, motivated individuals researching it, and significant flaws may take years to discover. For instance, a programming flaw in PGP versions 5 and 6 enabled an attacker to create a second escrow key without the key holder's consent ; this flaw existed for years before it was discovered. 'Maintenance passwords' for back doors have also existed in programs like sendmail and lasted for years before being eliminated. The concern is that there could be attackers who are sufficiently motivated to spend more time than the community of reviewers finding vulnerabilities or exploitable features in the published code. First off, because the average volunteer considers building code more gratifying than detecting flaws, there could not be enough reviewers for many open goods. Many students work on open-source projects because they believe that being able to point to a system that they contributed to that an employer uses will help them land good jobs in the future. However, this strategy might not be as effective if all they could point to were a collection of bug reports that necessitated security upgrades. It's also possible that even after a product had withstood 10,000 hours of community scrutiny, a foreign intelligence agency that invested a meagre 1000 hours might discover a new vulnerability. The probability are simple enough to calculate using the dependability

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

growth models that were mentioned. Other counterarguments include the observation that active open source projects add functionality and features at a dizzying rate compared to closed software, which can lead to unpleasant feature interactions; that such projects can fail to reach consensus about what the security is trying to achieve; and that there are special cases, like when protecting smartcards against various attacks, where a proprietary encryption algorithm embedded in the chip hardware can force the use of a proprietary encryption algorithm; So where is the benefit balance? According to Eric Raymond's influential analysis of the economics of open source software, there are five factors that determine whether a product would benefit from an open source strategy: it must be sensitive to failure, be based on common engineering knowledge rather than proprietary techniques, require peer review for verification, be sufficiently business-critical that users will cooperate in finding and removing bugs, and be sensitive to failure. All these checks are passed by security.

3. Semi-Open Design:

Where a totally open design isn't practicable, choosing a partially open one may often still have advantages. For instance, even when some of the implementation details are not public, the architectural design may. Using an open base and adding private components on top is another method for semi-open design. Apple's OS/X, which mixes the OpenBSD operating system with specialized multimedia components, may be the most well-known example in this regard. In other applications, a widely used proprietary product like Windows or Oracle may be 'open enough'. Let's say, for instance, that you are concerned about a legal assault. Instead than having opposing specialists go through code to determine if the system was safe at the time of a disputed transaction, you may depend on the history of publicly reported vulnerabilities, fixes, and assaults. As a result, we see that an increasing number of ATMs utilise Windows as their operating system (albeit the version they use has had a lot of the superfluous features removed).

CONCLUSION

Knowing when a security engineering project is complete might sometimes be the most difficult component. There are several approaches for assurance and assessment that may be used. They may be quite helpful when used in moderation, particularly for start-up businesses looking to cultivate positive work habits and establish a reputation but whose growth culture is still flexible. However, the help they can provide is limited, and excessive use of bureaucratic quality control measures may be quite harmful. I compare them to salt in that a few shakes on your fries may be beneficial, but a few ounces are obviously not.

But even if the situation seems bleak, hopelessness is not warranted. Things steadily improve as individuals gain knowledge of what operates, what is attacked and how, and as protection needs and processes become more ingrained in working engineers' skill sets. Security may only be achieved correctly on the fourth attempt, but that is still preferable than never, which was the norm fifteen years ago. Life is complicated. Success involves handling it. Overcomplaining about it can only lead to failure.

REFERENCES

[1] A. M. Yamaguchi and S. Tsukahara, “Quality assurance and evaluation system in japanese higher education,” *Avaliação Rev. da Avaliação da Educ. Super.*, 2016, doi: 10.1590/s1414-40772016000100004.

[2] Z. Zhou, Q. Zhi, S. Morisaki, and S. Yamamoto, “An Evaluation of Quantitative Non-Functional Requirements Assurance Using ArchiMate,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2987964.

[3] X. Q. Zhang, C. Q. Jiang, C. H. Xu, and J. J. Lin, “RS-UM based information system security assurance evaluation model,” *Chongqing Daxue Xuebao/Journal Chongqing Univ.*, 2012.

[4] M. P. Egido, “Teachers’ perceptions of quality assurance education policies in Chile,” *Educ. e Soc.*, 2019, doi: 10.1590/es0101-73302019189573.

[5] C. Li, Z. Dai, X. Liu, and W. Sun, “Evaluation system: Evaluation of smart city shareable framework and its applications in China,” *Sustain.*, 2020, doi: 10.3390/su12072957.

[6] R. Sadagopan, J. A. Bencomo, R. L. Martin, G. Nilsson, T. Matzen, and P. A. Balter,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3S, March 2022

"Characterization and clinical evaluation of a novel IMRT quality assurance system," *J. Appl. Clin. Med. Phys.*, 2009, doi: 10.1120/jacmp.v10i2.2928.

[7] E. Menéndez-Caravaca, S. Bueno, and M. D. Gallego, "Exploring the link between free and open source software and the collaborative economy: A Delphi-based scenario for the year 2025," *Technol. Forecast. Soc. Change*, 2021, doi: 10.1016/j.techfore.2021.121087.

[8] K. Mansouri *et al.*, "Open-source QSAR models for pKa prediction using multiple machine learning approaches," *J. Cheminform.*, 2019, doi: 10.1186/s13321-019-0384-1.