Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology (FEM)

Master's Thesis

Importance and influence of Cybersecurity to keep our society in progress.

Andrew Moheb Soliman Salama

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Andrew Moheb Soliman Salama, BSc

Informatics

Thesis title

Importance and influence of Cybersecurity to keep our society in progress

---

Objectives of thesis

The diploma thesis deals with the principal purpose of Cybersecurity and it's crucial to stand against attacks to keep corporate networks safer and more progressive.

sub-objectives:
- Full Background of Security and Hacking.
- Test some well-known hacking tools and try to nullify them.
- Find out governments' roles towards cybersecurity.

Methodology

The methodology of solving the theoretical part of the diploma thesis will be based on the study and analysis of professional information sources. Based on the knowledge gained in the theoretical part of the work. the practical part will be based on testing several attacks (by hacking tools), using nowadays popular cybersecurity tools. The next step will be collecting reports about the difference before the attacks and after that the change in using the cybersecurity defending tools.

Furthermore, experimental measurements will be performed using appropriate tools. The obtained data will be evaluated. Based on the synthesis of theoretical knowledge and the results of the practical part, the conclusions of the work will be formulated.

The proposed extent of the thesis

50-60 pages

Keywords

Hacking- Cybersecurity- Malware- Ransomware- Cookie Control- GDPR- Government- Computer Crime

---

Recommended information sources

Allsopp, Wil. Advanced Penetration Testing. Print.
Erickson, Jon. Hacking. Print.
Korthals Altes, Willem F. Information Law Towards The 21St Century. Deventer: Kluwer, 1992. Print.
Liska, Allan, and Tim Gallo. Ransomware. Print.
Voigt, Paul, and Axel Von dem Bussche. The Eu General Data Protection Regulation. New York: Springer, 2017. Print.

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Martin Lukáš, Ph.D.

Supervising department

Department of Information Technologies

Advisor of thesis

Ing. Tomáš Vokoun

Electronic approval: 14. 11. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 29. 11. 2023

Declaration

I declare that I have worked on my master's thesis titled “Importance and influence of Cybersecurity to keep our society in progress" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on date ___/___/_____

Signature_____

Andrew Moheb Soliman Salama

Acknowledgments

First and foremost, I would like to thank God, to whom I owe countless blessings that have guided and sustained me throughout this journey. because the God of heaven, he will prosper us; therefore, we his servants will arise and build.

I wish also to express my profound gratitude to my thesis Supervisor: Martin Lukáš, Ph.D. and my consultant, Ing. Tomáš Vokoun, for their unwavering support, invaluable insights, and active involvement throughout the entirety of my dissertation work. their guidance has been instrumental in shaping the quality and direction of this research.

Furthermore, I would also like to convey my gratitude to my parents and extended family members for their steadfast encouragement and belief in my pursuits.

I extend my heartfelt appreciation to my wife, who has been a constant source of motivation and unwavering support, providing me with immeasurable comfort in both my professional and personal endeavours.

Finally, I am deeply thankful to my friends and colleagues whose encouragement and camaraderie have been a source of inspiration and strength throughout this academic journey.

Importance and Influence of Cybersecurity to Keep Our Society in Progress

Abstract.

In a world defined by rapid technological progress and interconnectivity, the indispensable role of cybersecurity in upholding societal advancement is undeniable. This thesis delves into the profound significance of cybersecurity measures as a safeguard against threats to the digital landscape.

The study begins by exploring fundamental security and hacking concepts, providing a comprehensive foundation to comprehend the intricate dynamics underpinning cybersecurity. By investigating security breaches and hacking incidents, the critical need for robust protective measures is established.

Taking a pragmatic approach, the thesis evaluates prominent hacking tools through meticulous testing and analysis, revealing vulnerabilities that illuminate potential avenues for exploitation. The application of countermeasures to neutralize these threats underscores cybersecurity's proactive stance in risk mitigation.

Amid the intricate web of digital vulnerabilities, the thesis emphasizes governments' pivotal role in cultivating a secure digital environment. The exploration of governments' contributions to cybersecurity underscores multifaceted strategies, policies, and regulations crucial for safeguarding vital digital assets. Collaboration between governments, private sectors, and individuals is underscored to fortify the digital landscape against evolving threats. Ultimately, the thesis underscores that cybersecurity's importance extends beyond technology, encompassing social, economic, and political dimensions where the interplay between security and progress is profound. By addressing security foundations, evaluating hacking tools, and highlighting governments' roles, this research offers a comprehensive understanding of the intricate ecosystem shaping cybersecurity's significance in sustaining societal advancement.

As technology advances, this thesis serves as a reminder of the need to strengthen our digital foundations, ensuring a progressive and secure future for our interconnected society.

Keywords: Cybersecurity, Societal progress, Digital landscape, Security breaches, Hacking tools, Protective measures, Government roles, Technological advancement, Risk mitigation, Multifaceted strategies, Vulnerabilities, Collaborative efforts, Progression, Security dynamics, Technological safeguards.

Význam a vliv kybernetické bezpečnosti pro udržení pokroku naší společnosti

Abstraktní.
V světě definovaném rychlým technologickým pokrokem a vzájemným propojením je nezpochybnitelná nedílná role kybernetické bezpečnosti při podpoře společenského pokroku. Tato diplomová práce prozkoumává hluboký význam opatření kybernetické bezpečnosti jako ochrany před hrozbami digitálního prostředí.
Studie začíná prozkoumáním základních konceptů bezpečnosti a útoků hackerů, poskytujících komplexní základ pro pochopení složité dynamiky kybernetické bezpečnosti. Prostřednictvím zkoumání bezpečnostních porušení a incidentů hackerů je stanovena kritická potřeba robustních ochranných opatření.
S pragmatickým přístupem hodnotí tato diplomová práce významné nástroje pro hackování prostřednictvím pečlivého testování a analýzy, odhalující zranitelnosti, které osvětlují potenciální cesty pro zneužití. Aplikace protiopatření k neutralizaci těchto hrozeb zdůrazňuje proaktivní postoj kybernetické bezpečnosti v rámci zmírňování rizik.
Uprostřed složité sítě digitálních zranitelností práce zdůrazňuje klíčovou roli vlád při vytváření bezpečného digitálního prostředí. Prozkoumání příspěvků vlád k kybernetické bezpečnosti zdůrazňuje komplexní strategie, politiky a předpisy, které jsou zásadní pro ochranu klíčových digitálních aktiv. Spolupráce mezi vládami, soukromým sektorem a jednotlivci je zdůrazněna pro posílení digitálního prostředí proti se rozvíjejícím hrozbám. Nakonec tato diplomová práce zdůrazňuje, že význam kybernetické bezpečnosti přesahuje technologii a zahrnuje sociální, ekonomické a politické aspekty, kde vzájemné působení mezi bezpečností a pokrokem je hluboké. Prostřednictvím řešení základů bezpečnosti, hodnocení nástrojů pro hackování a zdůraznění rolí vlád nabízí tato práce komplexní pochopení složitého ekosystému, který formuje význam kybernetické bezpečnosti pro udržení společenského pokroku.
Se vzrůstajícím technologickým pokrokem tato diplomová práce slouží jako připomínka potřeby posílit naše digitální základy a zajistit progresivní a bezpečnou budoucnost naší propojené společnosti.

Klíčová slova: Kybernetická bezpečnost, Společenský pokrok, Digitální prostředí, Bezpečnostní porušení, Nástroje pro hackování, Ochranná opatření, Role vlád, Technologický pokrok, Zmírnění rizik, Multifunkční strategie, Zranitelnosti, Spolupracující úsilí, Postup, Dynamika bezpečnosti, Technologická ochrana.

Table of content

MASTER'S THESIS **1**

ACKNOWLEDGMENTS **5**

ABSTRACT. **6**

TABLE OF CONTENT **8**

1. INTRODUCTION **10**

2. OBJECTIVE AND METHODOLOGY **12**

2.1. OBJECTIVES 12

2.1.1 General Objectives: *12*

2.1.2 Sub-objectives: *12*

2.2. METHODOLOGY 12

3. LITERATURE REVIEW **13**

3.1 OVERVIEW OF CYBERSECURITY: 13

3.1.1 Definition: *13*

3.1.2 The necessity of cybersecurity: *13*

3.1.3 Cybersecurity and Ethics: *14*

3.1.4 Domains of cybersecurity: *14*

3.1.5 The history of data breaches: *15*

3.1.6 Importance of Cybersecurity: *16*

3.2 COMPREHENSIVE CONTEXT OF SECURITY AND HACKING: 16

3.2.1 Attacker Mindset: *16*

3.2.2 The threat landscape: *17*

3.2.3 The progress of Malware: *18*

3.2.4 Viruses and malicious program code: *19*

3.2.5 Security Mindset: *20*

3.2.6 Security awareness *20*

3.2.7 Social Engineering: *20*

3.2.7.1 Social Engineering Methods: 20

3.2.7.2 Social Engineering defences: 21

3.2.8 Hacking and it network security fundamental: *22*

3.2.9 System firewall controls: *23*

3.2.10 Online Privacy and E-Commerce Issues: *24*

3.3. GOVERNMENT IN CYBERSECURITY: 24

3.3.1. Political Cyber Attacks on Governments: *24*

3.3.2. The Primary Cybersecurity Challenges Confronting Governments in 2023: *25*

3.3.3. Enhancing Local Government Cybersecurity: A Proactive Approach: *26*

3.3.4. The Imperative of Comprehensive Cybersecurity Solutions for Government Entities: *26*

3.3.5. The complex definition of cybercrime: *27*

3.3.6. Is Suspicious Activity Uniform Across All Organizations? *27*

3.3.7. Addressing Suspicious Network Activity: *28*

3.3.8. Roles and Laws: *28*

3.3.9. Insufficient Reporting: Reluctance to Report Cyber Incidents: *28*

3.3.10. Legislation and Jurisdiction: Lack of Criminalization of Cyber Offenses and Jurisdictional Complexity: *29*

3.3.11. Cybercrime Undermines the Economy: *29*

3.3.12. Cybercrime Facilitates the Commission of Other Offenses: *30*

3.3.13. Cybercrime Paralyzes Public Services and Can Cost Lives: *30*

3.3.14. Role of the State in Combating Cybercrime: *30*

3.3.15. Human and Material Resources: *31*

3.3.16. Another examples of cyberattacks in real life: *32*

3.3.17. Cyber espionage encompasses: *34*

4. PRACTICAL PART **38**

4.1 ATTACK TESTS WITH HACKING TOOLS 38
4.1.1 SQL Injection Attacks *38*
4.1.2 Phishing Attacks *40*
4.1.3 Https Session Hijack: *44*
4.1.4 Malware attacks: Authentication attacks: *47*
4.1.5 certificate counterfeit: *50*
4.1.6 IOT vulnerabilities: *54*
4.1.7 Crypto jacking: *60*

5. RESULTS AND DISCUSSION **64**

5.1 PRACTICAL RESULTS: 64
5.1.1 Vulnerability Severity and Trends: *64*
5.1.2 Cybercrime Landscape: *65*
5.1.3 Government Commitment to Cybersecurity: *66*
5.1.4 Impact of Cyber Attacks on Industry Sectors: *66*
5.1.5 Global Malware Threat Landscape: *67*
5.1.6 Ransomware Trends: *67*
5.2 DISCUSSION: 68
5.2.1 Vulnerability Severity and Trends: *68*
5.2.2 Cybercrime Landscape: *68*
5.2.3 Government Commitment to Cybersecurity: *68*
5.2.4 Impact of Cyber Attacks on Industry Sectors: *69*
5.2.5 Global Malware Threat Landscape: *69*
5.2.6 Ransomware Trends: *69*

6. CONCLUSION **70**

REFERENCES **72**

LIST OF FIGURES **73**

BIBLIOGRAPHY **74**

1. Introduction

In an era marked by relentless technological advancements and an unprecedented interconnectedness that defines our world, the significance of cybersecurity has transcended its conventional boundaries, emerging as a linchpin for the sustainable progress of societies. This thesis embarks on a comprehensive exploration of the intricate relationship between cybersecurity and societal advancement, synthesizing the essence of two distinct introductions.

As we teeter on the precipice of a digital revolution, the integrity of our technological infrastructure assumes a role of paramount importance, resonating beyond mere technological concerns. The seamless flow of information, the efficacy of commerce, and the functionality of essential services all pivot on the intricate digital networks that traverse the globe. However, this very interconnectedness also exposes these networks to malicious actors who seek to exploit, disrupt, and undermine, underscoring a formidable challenge that cannot be overlooked.

In this landscape of rapid innovation, the realm of hacking stands as an indomitable force capable of reshaping history and exerting global influence on societies. This thesis delves into the multifaceted landscape of cybersecurity, meticulously dissecting the motivations underlying diverse hacking methods and the far-reaching consequences they entail. The comprehension of these intricacies proves pivotal in devising robust strategies to counter the ever-evolving landscape of cyber threats.

Beyond organizational confines, cybersecurity reverberates as a universal concern that intersects with individuals in personal and professional spheres alike. The study navigates the universality of cybersecurity, accentuating its importance in safeguarding data, ensuring financial integrity, and nurturing collective vigilance in an increasingly interconnected world.

Ethical considerations within the realm of hacking remain a contentious arena, prompting inquiries into the alignment of hacking with ethical principles. Our exploration encompasses the realm of ethical hacking, delineating its applications within the cybersecurity spectrum and unveiling the ethical frontiers that guide this practice. As we navigate the intricate ethical maze associated with hacking, we seek to illuminate the boundaries and possibilities that emerge.

Across the global stage, cybercrimes manifest in diverse variations shaped by cultural, economic, and political factors unique to each nation. This analysis sheds light on the assorted nature of cyber threats worldwide, necessitating tailored approaches to cybersecurity within distinct contexts. The understanding of these nuances emerges as a requisite for crafting defence mechanisms that effectively counter these diverse threats.

Within this complex panorama, social engineering attacks emerge as formidable challenges. This study unfurls pre-emptive strategies designed to counteract these manipulative tactics, empowering individuals, and organizations alike to safeguard against these sophisticated and insidious threats. By fostering comprehensive awareness, we fortify our capacity to effectively mitigate the perils posed by social engineering attacks.

As we navigate the intricate terrain where innovation and vulnerability coexist, this thesis strives to comprehensively illuminate the multifaceted tapestry of cybersecurity and hacking. By unravelling the complex interplay between digital advancements and the imperatives of security, this exploration contributes to an enriched understanding of the dynamic forces that underpin the progress of our civilization.

2. Objective and Methodology

2.1. Objectives

2.1.1 General Objectives:

The diploma thesis deals with the principal purpose of Cybersecurity and it's crucial to stand against attacks to keep corporate networks safer and more progressive.

2.1.2 Sub-objectives:

- Full Background of Security and Hacking.
- Test some well-known hacking tools and try to nullify them.
- Find out governments' roles towards cybersecurity.

2.2. Methodology

The methodology of solving the theoretical part of the diploma thesis will be based on the study and analysis of professional information sources. Based on the knowledge gained in the theoretical part of the work. the practical part will be based on testing several attacks (by hacking tools), using nowadays popular cybersecurity tools. The next step will be collecting reports about the difference before the attacks and after that the change in using the cybersecurity defending tools.

Furthermore, experimental measurements will be performed using appropriate tools. The obtained data will be evaluated. Based on the synthesis of theoretical knowledge and the results of the practical part, the conclusions of the work will be formulated.

3. Literature Review

3.1 Overview of Cybersecurity:

3.1.1 Definition:

Cybersecurity refers to the protection of information systems, including hardware, software, and associated infrastructure, along with the data they contain and the services they provide. This protection aims to prevent unauthorized access, harm, or misuse, encompassing intentional harm caused by system operators as well as accidental harm arising from security procedure failures. (Rigby, 2019)

Cybersecurity involves understanding digital attacks and their solutions, focusing on safeguarding confidentiality, integrity, and availability of digital resources. Society's heavy reliance on digital networks has led to a rise in cyberattacks, capturing the attention of intruders and researchers. The prevalence of tools for illicit access to digital content makes cybercrimes a significant concern. As cyberattacks increase due to their accessibility, individuals and society face digital nightmares. Attackers exploit the convenience of technology, leveraging anonymity and geographical constraints. The anticipation is that cybercrime rates and attack sophistication will grow, underscoring the need to comprehend cybersecurity concerns for everyone. (Nitul Dutta, 2022)

3.1.2 The necessity of cybersecurity:

In recent times, society has experienced an unprecedented reliance on technology-driven services, a trend projected to intensify. While services like Google Drive and Dropbox enhance digital convenience, they also expose substantial risks of data breaches, potentially leading to identity theft and sensitive information compromise. Data breaches have triggered global government initiatives to combat cybercrimes and enhance data protection. Prominent examples include Europe's General Data Protection Regulation (GDPR) and California's data breach disclosure mandate. Such regulations emphasize timely breach notification, the presence of data protection officers, and the preservation of data anonymity. Standard-setting bodies like the National Institute of Standards and Technology (NIST) contribute by creating frameworks that aid companies in auditing and fortifying their security infrastructure. Various threat actors contribute to cyberattacks, from sophisticated data theft to simpler yet pervasive methods. As cybercriminals exploit vulnerabilities to escalate attacks, robust cybersecurity becomes imperative, necessitating the implementation of security protocols, standards, and employee awareness initiatives to safeguard data and resources. (Nitul Dutta, 2022)

3.1.3 Cybersecurity and Ethics:

In the context of life, ethics refers to the pursuit of a virtuous existence, encompassing decisions and actions that lead to a good life. Humans strive for goodness and seize opportunities that align with ethical standards, particularly in a technologically advanced age offering various avenues for improvement. Ethics gauges the quality of these opportunities, which can either lead to a positive path or a detrimental one. Instances of ethical lapses are prevalent, exemplified by companies amassing personal data through biometrics and face recognition without consistent rules, risking data breaches. Notable cases involve giants like Facebook, Google, Amazon, and Microsoft, divulging private information. While concrete ethical guidelines are lacking, the fundamental principle is clear: refrain from cyber wrong doings that burden others. Key rules involve avoiding malicious software, cyberbullying, eavesdropping, password misuse, and copyright violations. Ethical quandaries in cybersecurity result in harm or benefit for different users, hinging on the individual's choice between ethical and unethical paths for a good life. Remedies include awareness programs, nurturing ethical values in individuals, and integrating cybersecurity ethics into education to ensure future security professionals prioritize ethical conduct. (Nitul Dutta, 2022)

3.1.4 Domains of cybersecurity:

Cybersecurity encompasses various domains, each playing a crucial role in safeguarding digital systems and data.

- Data Security involves protecting sensitive data from unauthorized access or theft using encryption and access controls.
- Network Security safeguards data as it travels across networks through measures like firewalls and intrusion detection systems.
- Digital Forensics investigates cyber incidents by analysing digital evidence to understand and respond effectively.
- Application Security identifies and addresses vulnerabilities in software to prevent exploitation.
- IAM manages user identities and access to resources.
- Incident Response prepares for and manages cybersecurity incidents.
- Cloud Security addresses challenges in securing cloud-based data and services.
- Risk Management and Compliance assesses and manages cybersecurity risks while ensuring compliance with standards.

- Cryptography secures communication and data through encryption techniques.
- SOC monitors, detects, and responds to security incidents in real-time.
- Penetration Testing identifies vulnerabilities through simulated attacks.
- Mobile Security protects data and applications on mobile devices.
- IoT Security ensures security for connected devices in the Internet of Things.
- ICS Security focuses on safeguarding critical infrastructure systems. (Nitul Dutta, 2022)

3.1.5 The history of data breaches:

Hacking's history stretches further back than commonly known, tracing its origins to 1834. Even in the late 1700s, with France's mechanical telegraph towers, vulnerabilities emerged. Bankers François and Joseph Blanc exploited this system, inserting an extra character to gain trading advantages. Jumping to the late 1980s, the Morris worm marked the first computer virus, rapidly spreading unintentionally. In 2010, Stuxnet showcased targeted industrial cyber espionage, specifically aiming at an Iranian nuclear facility's control systems. Today, cyberattacks encompass ransomware, data theft, and cryptocurrency mining. The growing attack surface and high-profile incidents underscore the vital need for comprehensive data security. It's important to note the Replica of Claude Chappe's optical telegraph on the Litermont near Nalbach, Germany (Photo by Lokilech CC BY-SA 3.0), highlighting historical optical telegraphy's role in communication technology. (Ozkaya, 2019)

Figure 1:Replica of Claude Chappe's optical telegraph on the Litermont near Nalbach, Germany (Photo by Lokilech CC BY-SA 3.0) (Ozkaya, 2019)

3.1.6 Importance of Cybersecurity:

In the contemporary digital era, the significance of cybersecurity has risen exponentially. The proliferation of cloud-based and mobile technologies has ushered in an era of pervasive connectivity and digital transformation. In this landscape, the imperative of safeguarding digital assets has transcended the realm of IT administrators; it has become an indispensable responsibility for all individuals connected to data. The exploration of historical data breaches delves into instances dating back to the 1800s, illustrating manipulations of telegraph networks for financial advantage. Subsequently, the discussion traverses recent instances of cyber threats, exemplified by the late 1980s' Morris worm and the 2010 Stuxnet malware that targeted industrial systems. The evolution of cyberattacks, transitioning from rudimentary viruses to intricate industrial espionage, underscores the escalating demand for robust security measures. Amidst the expanding horizons of digitization and connectivity, the imperative to fortify identities, data, networks, and equipment has assumed paramount significance. Furthermore, the discourse briefly acknowledges the hurdles and vulnerabilities intrinsic to cloud computing, accentuating that security concerns pervade every sphere, irrespective of the target status. (Ozkaya, 2019).

3.2 Comprehensive Context of Security and Hacking:

3.2.1 Attacker Mindset:

Understanding the growing trend of cybercrime requires exploring the psychology of the individuals behind these activities. Cybercriminals possess the technical skills to infiltrate systems, steal data, accumulate wealth, and compromise system integrity. Notably, there are distinct categories of hackers:

- ***Black hats*** are malicious hackers primarily motivated by financial gains.
- ***White hats*** are individuals who identify system vulnerabilities, contributing to proactive measures against attacks.
- ***Grey hats,*** having previously been black hats, now function as security consultants after re-forming.
- ***Hacktivists*** form hacker groups to advocate for social change or make political statements, occasionally targeting influential entities.
- ***Cyber terrorists*** use hacking to cause harm, disrupt critical infrastructure, and spread fear.

It's plausible that grey and white hats would refrain from engaging in cyberattacks, or if they do, it would be to raise awareness about vulnerabilities. Black hats focus on financial motives,

hacktivists aim to convey impactful messages, while cyber terrorists pursue more severe objectives. (Ozkaya, 2019)

3.2.2 The threat landscape:

The "threat landscape" encompasses the collection of observed threats, information about threat agents, and current trends in the cybersecurity realm. Vigilance regarding the threat landscape is crucial for security professionals, often aided by reports from entities like ENISA and NIST. This landscape is dynamic, influenced by tools, resources, vulnerabilities, and attack skills, often available online. Different threat categories include:

- *Unstructured attacks:* Launched without prior environmental knowledge, relying on freely available tools for mass exploitation.
- *Structured attacks:* Planned and prepared, showcasing advanced programming skills and targeting specific entities.
- Social engineering (phishing, spear phishing): Exploits human vulnerabilities, extracting information through deception, often successful due to lack of awareness.
- *Eavesdropping:* Unauthorized network access for intercepting unencrypted traffic.
- *Denial of Service (DoS and DDoS):* Overwhelms systems with data floods, disrupting functionality.
- *Man-in-the-middle attack (MITM):* Intercepts and manipulates communication between server and client, acting as a proxy without victim awareness.
- *Malware:* Disruptive software causing damage or malicious intent, exploiting system vulnerabilities, sometimes remaining undetected.
- *Botnets:* Infected systems remotely controlled by attackers, forming networks with multiple purposes.
- *Cross-site scripting (XSS):* Exploits web app flaws to inject malicious scripts, compromising users without their knowledge, often due to weak input validation.
- *Drive-by download attack:* Malware embedded in legitimate websites redirects unsuspecting users to malware download locations, often spread through emails or links.
- *SQL injection attack:* Attackers exploit poorly configured web applications to manipulate databases, accessing or modifying data.
- *Advanced persistent threat (APT):* Targeted and stealthy attacks against specific organizations or entities, using advanced techniques to stay undetected over extended periods.
- *Web-based attacks:* Targeting internet-facing devices, applications, and services, exploiting vulnerabilities in applications and web browsers.

- *Insider attacks:* Authorized users causing harm, either intentionally or unknowingly, posing a challenging threat to detect and mitigate.
- *Ransomware:* Malicious software encrypts user data, demanding payment for decryption, impacting systems like hospitals and governments.
- *Espionage:* Conducted in cyberspace by governments and entities to compromise sensitive information and disrupt rivals' operations. (Ozkaya, 2019)

3.2.3 The progress of Malware:

The progression of malware is a pivotal component of cyberattacks, involving malicious software designed to achieve nefarious goals like remote computer control, data extraction, and fraudulent revenue generation. Over time, malware has grown in sophistication, capability, and destructiveness. Figure 1 shows some of the most recent large breaches, based on the numbers of compromised records.

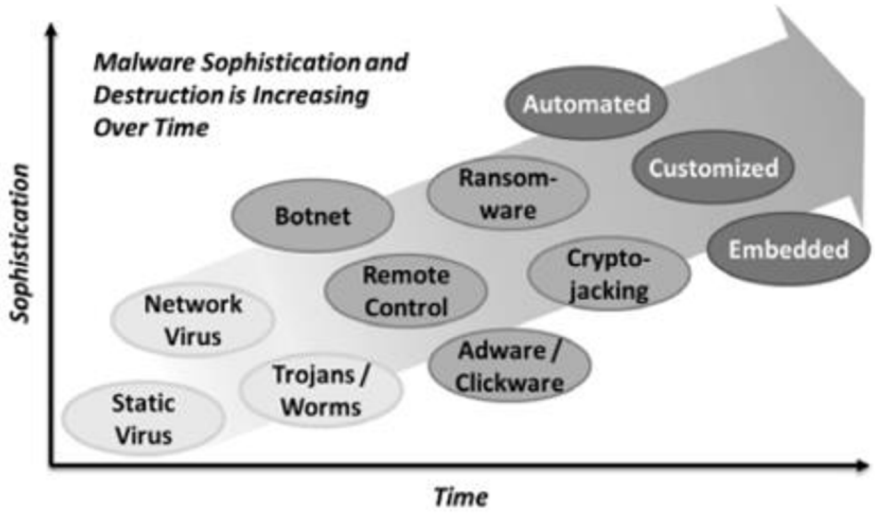


Figure 2: Malware evolves to become more sophisticated and destructive. (Scott Donaldson, 2018)

Various malware types have emerged, encompassing:

- Static viruses embedding in programs or boot processes, necessitating human intervention for propagation.
- Network viruses utilizing networks for autonomous computer-to-computer spread.
- Trojans and worms act independently to propagate and persist.
- Botnet malware linking victim computers to a controlled network for coordinated malicious actions.
- Remote control malware manipulating victim computers without bypassing security.
- Adware and click ware inducing fraudulent revenue via enticing ad clicks.
- Ransomware encrypting files and demanding payment for recovery.

- Crypto jacking malware utilizing victim computers for profitable cryptocurrency transactions.
- Automated malware autonomously spreading across networks to infect multiple systems.
- Customized malware customized to evade conventional security methods.
- Embedded firmware malware posing challenges for removal.

Attackers employ malware to advance financial, geopolitical, or ideological objectives. The evolution from static viruses to sophisticated forms like network viruses and Trojans reflects attackers' adaptability. Instances include compromised factory devices and malware-infested mobile app stores. Grasping these trends is vital for effective cybersecurity. (Scott Donaldson, 2018)

3.2.4 Viruses and malicious program code:

A computer virus is a small program that can replicate itself and infect other computers without user permission or knowledge. It attaches to other systems and spreads as its code is carried to uninfected computers, often through networks, the Internet, or removable storage media. Computer viruses first emerged on early networks like ARPANET in the 1970s, initially displaying messages but later turning malicious. Over time, viruses became more destructive, leading to the introduction of the term "malware" for dangerous software. Various forms of malware emerged, such as Trojan horses and logic bombs, each with their own characteristics. The software industry responded with products to monitor and counteract malware. Malware threats have evolved into complex cybersecurity risks, necessitating constant vigilance and preventive measures. (Moeller, 2016)

Code Type	Characteristics
Virus	Attaches itself to programs and propagates copies of itself to other programs.
Trojan Horse	Contains unexpected functionality that later performs a disguised function
Logic Bomb	Program that only triggers when some other specified event occurs
Time Bomb	Program that only triggers when some other specified time period is met.
Trapdoor	Undocumented software entry point that circumvents system protections.
Worm	Propagates copies of itself through a network
Rabbit	Software code that replicates itself again and again without limit to exhaust the resource.
Scareware	Sometimes called ransomware, can lock up software and then demand a ransom

***Table 1**: Types of Malicious Program Code.* (Moeller, 2016)

3.2.5 Security Mindset:

The concept of a security mindset involves adopting the perspective of potential attackers to better understand how they might exploit vulnerabilities for their benefit. Security attackers, often intelligent and skilled individuals, pursue objectives that conflict with our own interests. Essentially, they seek to exploit what we are aiming to safeguard. While many of their activities are illegal, their elusive nature and international reach often complicate legal investigation and prosecution. The security mindset entails viewing the world from the standpoint of attackers to anticipate and counter potential threats, even in the face of legal challenges and jurisdictional complexities. (Scott Donaldson, 2018).

3.2.6 Security awareness

Expanding on the concept of a security mindset, security awareness involves considering the impact of our actions on our security on a daily basis. It's important to recognize that our choices and behaviours can either heighten or lessen the vulnerability to cyberattacks for us, our families, and our organizations. When we possess security awareness, we constantly evaluate the security implications of our actions, asking ourselves if the potential risks outweigh the benefits. This ongoing assessment helps us anticipate potential issues and plan for contingencies. Examples of security awareness include maintaining a clear distinction between personal and work computing, not permitting unfamiliar individuals to use our devices, refraining from opening suspicious links or attachments, and understanding that certain offers or alerts might be scams. By nurturing a security-focused mindset and practicing awareness, we can minimize the likelihood of mishaps and mitigate the impact when they occur. In doing so, we safeguard ourselves, our loved ones, and our businesses from the inevitable cyber threats. (Scott Donaldson, 2018).

3.2.7 Social Engineering:

3.2.7.1 Social Engineering Methods:

Social engineering, a prevalent hacking technique, involves manipulating individuals into actions detrimental to themselves or others. Its success is rooted in its versatility and the difficulty of thwarting it solely with technology. Various methods of social engineering exist, such as computer-based, phone call-based, in-person, and postal mail-based approaches. Phishing is a prominent tactic where attackers masquerade as legitimate sources to deceive users into divulging logon credentials. Spear phishing targets specific individuals with personalized information, often leading to significant compromises. Another tactic involves

tricking users into executing Trojan Horse programs, often through email or compromised websites. Scammers can impersonate technical support, vendors, or government agencies over the phone, using fear or rewards to manipulate victims. Purchase scams exploit online buyers and sellers, often involving fake checks or undelivered goods. In-person social engineering involves hackers posing as service personnel to gain physical access to secure locations. Attackers utilize either threats or promises to coerce victims, capitalizing on stress-induced vulnerability. Notably, social engineers frequently capitalize on unsuspecting individuals' psychological and emotional responses to orchestrate successful attacks. (Grimes, 2017)

3.2.7.2 Social Engineering defences:

Defending against social engineering attacks requires a dual approach involving education and technology.

Education:

Training is crucial to thwart social engineering. It should incorporate real examples and teach individuals to recognize deceitful tactics. Regular anti-social engineering videos and tests, supplemented by relatable colleagues sharing personal experiences, enhance awareness. Simulated phishing campaigns can also offer valuable lessons.

Software Caution:

Users should avoid installing software directly from websites and instead rely on official vendors. If prompted for third-party software, it's safer to leave the site and visit the authentic vendor's site.

EV Certificates:

Educate users about Extended Validation (EV) digital certificates, which validate site authenticity. EV certificates are highlighted with a green bar, assuring users of a site's legitimacy.

Password Alternatives:

Enhance security by moving away from basic passwords and embracing advanced methods like two-factor authentication and digital certificates.

Anti-Social Engineering Tech:

Anti-malware, web filtering, and email anti-spam tools help combat computer-based social engineering. However, they should complement education, not replace it.

Success Recipe:

Combining thorough training with suitable technology significantly reduces social engineering risks. (Grimes, 2017)

Kevin Mitnick's Insights:

The following chapter profiles Kevin Mitnick, a renowned social engineering expert whose experiences as a former hacker have enhanced his ability to defend clients.

- **Profile: Kevin Mitnick:**

The renowned computer hacker Kevin Mitnick is synonymous with the term "hacker." He gained notoriety in the 1970s, 80s, and 90s, utilizing social engineering and low-level operating system research to execute impressive feats. Despite debatable harm compared to modern cyber threats, Mitnick's exploits have been widely documented, even generating unfounded tales attributed to him. His actions led to extraordinary measures by the government, fearing his potential impact. Mitnick's journey has transformed him into a cybersecurity advocate, contributing to books, working with companies, and running his own security consulting firm. He's an authoritative voice in recognizing and combating the role of social engineering in hacking. His experiences offer valuable lessons for the industry. Mitnick's transformation from hacker to cybersecurity champion underlines the importance of learning from intelligent, reformed individuals in the field. (Grimes, 2017)

3.2.8 Hacking and it network security fundamental:

the evolution of cyber threats in the context of banking and information technology. While traditional bank robberies have become rare due to digitalization, cybercrime has taken their place. Financial assets are now stored electronically, protected by password-based security systems. Perpetrators gain unauthorized access through hacking, exploiting system weaknesses. The four main classes of IT threats are interruptions, interceptions, modifications, and fabrication. These threats have intensified with the growth of the internet, wireless communication, and various computing devices. Internal auditors must be aware of these risks as IT systems become more sophisticated. The text cites an example of a major security breach at Target Corporation, where hackers stole credit card and personal information, resulting in financial losses and legal repercussions. (Moeller, 2016)

The importance of protecting enterprise data in various forms, whether it's stored in centralized databases or on individual devices. The exhibit presented outlines four fundamental ways to safeguard IT data: confidentiality, availability, integrity, and a combination of these known as a secure data environment. Confidentiality emphasizes controlled access and protection against unauthorized spillage, ensuring sensitive data remains confidential. Data integrity is crucial to prevent unauthorized tampering, as exemplified by the breach in the Target case. Availability is achieved through controlled access mechanisms, such as password controls, which ensure

that data is accessible to authorized sources. The concept of secure data encompasses these aspects and adds further layers of security, integrating confidentiality, availability, and integrity. The exhibit underscores the significance of these three fundamental concepts—confidentiality, availability, and integrity—in computer security considerations for internal auditors. Additionally, the exhibit discusses firewalls and virus protections as key elements of securing data, emphasizing the holistic approach to data security. (Moeller, 2016)

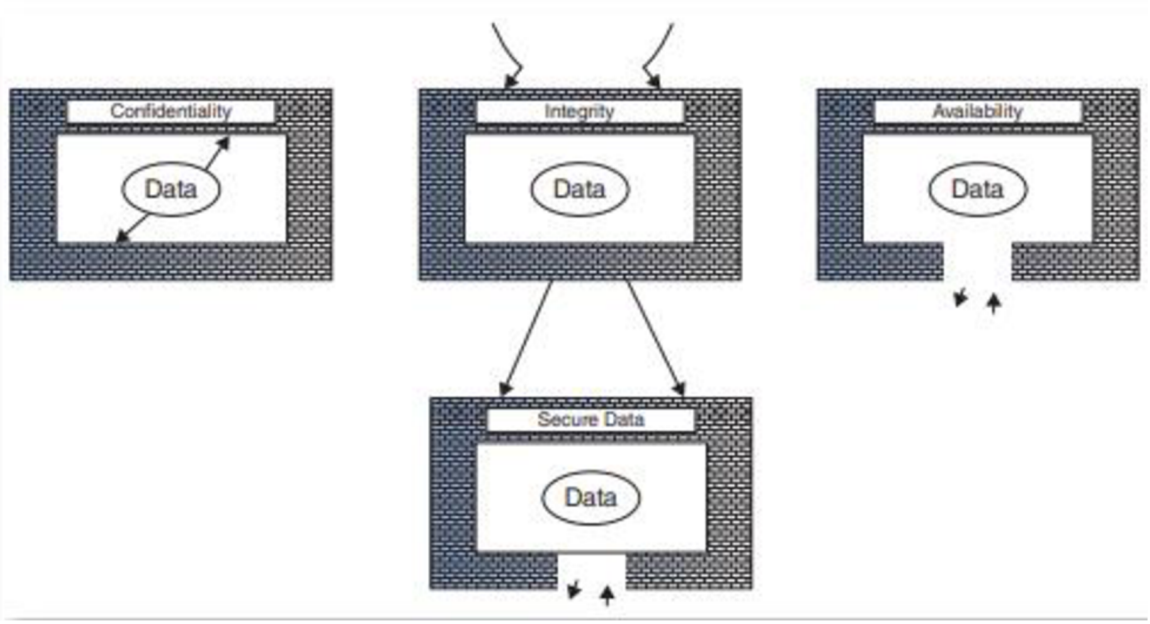


Figure 3: Data Security Concepts (Moeller, 2016)

3.2.9 System firewall controls:

Firewalls are a common type of IT software security that filters traffic between protected internal environments and less secure external ones. They are specialized software that permits or denies specific types of transactions. Firewalls can take the form of screening routers, proxy gateways, or guards. They are crucial for enterprises to safeguard their systems network from the outside world, routing approved traffic while blocking unauthorized access. For internal auditors, understanding how firewalls are set up in the enterprise is more important than the technical details. Different configurations serve various purposes: screening routers segment networks, proxy gateways control external access to data, and guard firewalls restrict certain web content for employees. Firewalls can also monitor message content and report improper access attempts. Proper configuration and regular updates are essential for their effectiveness. However, firewalls aren't foolproof; security can be compromised if external connections bypass them. While strong security tools, firewalls are often targeted by malicious attackers. (Moeller, 2016)

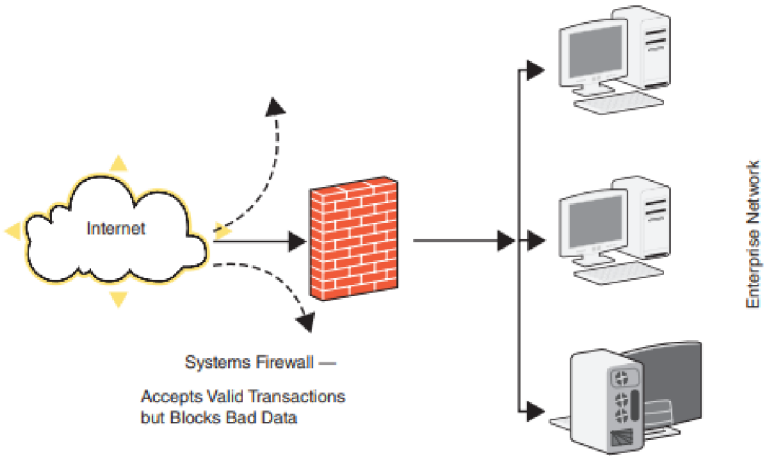


Figure 4: Firewall Diagram (Moeller, 2016)

3.2.10 Online Privacy and E-Commerce Issues:

Issues related to online privacy and e-commerce have received significant media attention. From the introduction of the Electronic Communications Privacy Act in 1986 in the United States to subsequent laws like the Cyber Intelligence Sharing and Protection Act and the Computer Fraud and Abuse Act, various privacy laws have been enacted. However, these laws have struggled to keep pace with evolving technology and have faced criticisms from advocates of financial freedom. It's possible that new U.S. Internet privacy laws might emerge in the future, providing enhanced consumer protections. Such legislation could potentially mandate commercial websites to offer privacy policies, transparently explain data collection practices, and provide effective methods for visitors to control the capture and sale of their personal data to other entities. Internal auditors need to stay informed about these shifting regulations. While some individuals can take steps to safeguard their web surfing activities from being tracked by the websites they visit, these privacy-enhancing strategies might not be accessible or practical for most people. (Damien Van Puyvelde, 2019).

3.3. Government in Cybersecurity:

3.3.1. Political Cyber Attacks on Governments:

Beyond assaults orchestrated by state-sponsored entities, governments encounter threats from various politically-driven groups. In the context of the Ukraine-Russia conflict, several cybercrime groups affiliated with Russia executed attacks targeting the Ukrainian government, Ukrainian enterprises, and their allies in Europe and the United States. Additionally, independent groups have initiated numerous politically-motivated attacks against various governments.

Cyberattacks have become a potent tool for expressing political dissent and executing offensive manoeuvres. Consequently, governments confront cybersecurity challenges of unprecedented magnitude (checkpoint, 2023).

In the face of escalating geopolitical tensions, state-sponsored cyber warfare poses a significant threat to nations. these cyberattacks target critical infrastructure, leading to disruptions in various sectors. Both state and non-state actors now possess advanced technical capabilities, motivation, and financial resources for disruptive attacks. Over 100 governments have developed national cybersecurity defense strategies to address these risks, and a study has benchmarked the cybersecurity strategies of 11 nations to aid others in enhancing their cybersecurity measures (Ankit Fadia, 2020).

3.3.2. The Primary Cybersecurity Challenges Confronting Governments in 2023:

Governmental departments and agencies encounter numerous cybersecurity threats like those faced by other organizations. However, their distinct circumstances, coupled with a lack of awareness and preparedness against cyber threats, expose them to additional risks and more sophisticated adversaries, given their access to vast amounts of sensitive and valuable data.

The following delves into some of the most significant cybersecurity challenges governments confront in 2023 (checkpoint, 2023):

- Hacktivism:

  - Definition: Hacktivism involves employing cyberattacks to advance political or social objectives, often targeting government organizations to protest their actions or policies.

  - Trends: Hacktivist attacks have become more prevalent and sophisticated, with major incidents occurring worldwide. Recent conflicts, like Ukraine-Russia, have fueled attacks supporting one side against the other, posing an elevated threat to government operations.

- Ransomware Attacks:

  - Definition: Ransomware poses a substantial cybersecurity threat, with operators encrypting valuable data and demanding payment for its release. Evolving tactics include double-extortion attacks and ransomware as a service.

  - Trends: The latest trend involves data extortion, where sensitive data is threatened to be exposed if the ransom isn't paid. This evolution amplifies the impact on governments and their associated entities.

- Wipers and Destructive Malware:

  - Definition: Wipers and destructive malware aim to eradicate an organization's access to critical data, making recovery impossible, even with ransom payment.

- Trends: Increasingly used in cyberattacks against governments, destructive malware like WhisperGate and HermeticWiper showcase the prevalence of these tactics.

- Data Breaches:

  - Threat: Government organizations possess vast amounts of sensitive data, including state secrets and personal information about constituents. Data breaches represent a major cybersecurity threat as threat actors become more numerous, sophisticated, and adopt data extortion tactics.

- Weaponization of Legitimate Tools:

  - Concept: Cybercriminals leverage legitimate tools and functions within operating systems or security testing software to make their attacks harder to detect.

  - Impact: The use of legitimate tools enhances cybercriminals' capabilities, as these tools, often free and open source, enable them to exploit built-in functionalities and evade detection.

Governments must navigate these multifaceted challenges by enhancing awareness, preparedness, and cybersecurity measures to safeguard critical data and operations (checkpoint, 2023).

3.3.3. Enhancing Local Government Cybersecurity: A Proactive Approach:

Traditional cybersecurity strategies tend to be reactive, focusing on incident detection and response. This reactive approach often results in organizations scrambling to contain and mitigate the impact of cyber incidents.

Local governments can significantly bolster their cybersecurity by adopting a proactive stance. Collaborating with other organizations through partnerships allows them to glean insights into best practices and stay abreast of the latest threats. Opting for preventative security solutions, designed to block attacks before reaching the organization's systems, proves instrumental in minimizing the threat and potential damage from cyberattacks. Moreover, local governments can strategically design their systems with privacy and security in mind, encouraging constituents to follow suit (checkpoint, 2023).

3.3.4. The Imperative of Comprehensive Cybersecurity Solutions for Government Entities:

Government organizations confront a diverse array of cyber threats, necessitating the protection of expansive IT infrastructures often distributed across multiple departments. Attempting to secure these systems with a patchwork of standalone solutions results in an unwieldy

security infrastructure prone to missing attacks, especially in the absence of in-house cybersecurity expertise.

For effective and scalable security architecture, government organizations are best served by adopting an integrated, comprehensive security platform. This all-encompassing approach not only improves security usability and visibility but also eradicates security blind spots (checkpoint, 2023).

3.3.5. The complex definition of cybercrime:

There is no universally agreed-upon definition of cybercrime. The most common method involves defining key terms used in investigations of cyber offenses. Examining these definitions helps identify key concepts and use them consistently within the framework of a national strategy to combat cybercrime. An example of this method is the Commonwealth Model Law on Computer and Computer Crime of 2017 (the "Commonwealth Model Law"). This legislation begins by defining key terms such as "computer data," "computer data storage medium," "service provider," and "traffic data." After defining these key terms, the Commonwealth Model Law lists the main offenses considered within the scope of cybercrime: 1) unauthorized access, 2) data integrity breaches, 3) interference with the integrity of computer systems, 4) illegal interception of data, 5) illegal devices, and 6) child sexual exploitation content (Stock, 2021).
Concerns over data breaches rank among the primary worries for today's organizations. The expenses associated with these breaches are consistently rising, with the average global cost of a single breach standing at $3.62 million. Apart from the financial implications of such breaches, ensuring robust network security is imperative for any business, as an attack has the potential to compromise the trust of customers.
Indeed, statistics reveal that 60 percent of small companies cease operations within six months of falling victim to a data breach or cyber-attack. Given that both the financial stability and the future viability of a business are at stake, it becomes imperative for organizations of all sizes to implement measures for monitoring suspicious network activity (Robert Johnson, 2019).

3.3.6. Is Suspicious Activity Uniform Across All Organizations?

It is conceivable that suspicious activity may differ across industries and organizations of varying sizes due to divergent motivations behind hacking.For instance, a small business might detect user abuse or irregular database activities as hackers attempt to gain unauthorized access to personal or cardholder information. On the other hand, a financial institution may be more

susceptible to account misuse, unauthorized port access, and malware attacks aimed at pilfering social security and financial data.

Private organizations may face the risk of advanced persistent threats (APTs), which involve multi-phase attacks on an organization's network. While traditionally targeted at governmental entities, APTs can impact small and medium-sized businesses as well.

3.3.7. Addressing Suspicious Network Activity:

As is often the case with challenges, the key to addressing suspicious network activity lies in prevention, and this necessitates the implementation of a robust organization-wide security strategy. Here are several components that should be integral to any comprehensive data security approach:

- Malware protection.
- Implementation of strong password policies.
- Regular scrutiny of network alerts, error reports, performance, and traffic.
- Installation of firewalls.
- Encouraging end users to report any observed suspicious activity.
- File integrity monitoring.
- Periodic risk assessments.
- Formulating incident and failure response strategies.

3.3.8. Roles and Laws:

- In the event of a cybercriminal incident, it is the responsibility of law enforcement and the criminal justice system to intervene (e.g., a unit investigating cybercrime).

- In the case of a cybersecurity incident, the cybersecurity service or entity must be deployed, such as a Computer Emergency Response Team (CERT) or a Cybersecurity Incident Response Team (CSIRT) (Stock, 2021).

3.3.9. Insufficient Reporting: Reluctance to Report Cyber Incidents:

- In most of cases, businesses and individuals who fall victim to cybercrime refrain from reporting the incident to authorities. The lack of reporting on these offenses results in a scarcity of data on the modus operandi of cybercriminals and the technologies employed in their commission. Unfortunately, this phenomenon is widespread.

- Individuals who have been victimized often lack knowledge on how or to whom to report a cybercrime, may perceive reporting as futile, or feel ashamed of falling prey to fraud. As

these incidents typically do not involve fatalities or tangible property loss (usually pertaining to personal data or information), victims may not be aware they have been subject to a criminal act and thus do not report it to authorities.

- Companies that have been targeted by cyber offenses often hesitate to report them, as the dissemination of such information to the public can harm their reputation and undermine investor or market trust. In many countries, data protection regulations address this issue by making it mandatory to report cybersecurity incidents.
- In some instances, victims of cyber offenses find the reporting process burdensome or opaque, leading them to forgo reporting the incident (Stock, 2021).

3.3.10. Legislation and Jurisdiction: Lack of Criminalization of Cyber Offenses and Jurisdictional Complexity:

- Cybercrime often requires conducting cross-border investigations as victims, perpetrators, and infrastructures are frequently located in different countries. This poses a challenge for investigators who may realize that other countries may not necessarily have laws criminalizing such offenses, additional elements are required to prove the commission of the offense, or data retention periods may differ. In some countries, there is no legislation, and consequently, no criminalization related to cybercrime, making these countries a safe haven for cybercriminals.
- It is also crucial that the national legal framework allows sufficient time for the collection, analysis, and dissemination of digital evidence. Too short timeframes may hinder obtaining essential evidence, correct analysis, timely receipt, and lead to dropping charges against cybercriminals.
- To conduct effective investigations across multiple jurisdictions, collaboration with counterparts from other countries is essential to advance the inquiry. This collaboration may involve conducting searches and seizures of physical and/or digital evidence or presenting judicial authorizations such as warrants to entities in the private sector (e.g., telecommunications companies and Internet service providers) (Stock, 2021).

3.3.11. Cybercrime Undermines the Economy:

During the global cyberattack NotPetya in June 2017, the ransomware targeted major logistics operators and their clients. Last-minute redirection, compensation, and maintaining the global supply chain cost the Maersk company no less than 300 million USD. The damage was not limited to this company, as its clients were also severely affected by the incident.

Among others, the pharmaceutical company Merck lost 870 million USD, TNT Express (owned by FedEx) lost 400 million USD, and the chocolatier Cadbury lost 188 million USD. This domino effect of cybercrime was equally visible during the large-scale DDoS attack via the Mirai botnet against the domain name provider Dyn in 2016, thereby paralyzing the operations of most of the 178,000 clients whose Internet domains were hosted by the company. These incidents illustrate the increased sophistication and contagiousness of new cybercriminal methods compared to attacks of the older generation, such as Stuxnet, a computer virus that infected at least four oil and gas companies: Baker Hughes, ConocoPhillips, Marathon, and Chevron.

The Global Risk Report 2020 from the World Economic Forum estimates that the cost of damages caused by cybercrime could reach 6 trillion USD in 2021. A strategy to combat cybercrime defines the measures to be taken to establish good data governance in companies and good personal computer hygiene to limit economic repercussions.

3.3.12. Cybercrime Facilitates the Commission of Other Offenses:

According to the United Nations Office on Drugs and Crime (UNODC), cybercriminal incidents are often orchestrated by criminal networks operating online. These networks use ransom proceeds and illegal profits to finance other forms of major crime or terrorism. A strategy to combat cybercrime supports initiatives related to counter-terrorism and anti-money laundering (CT/AML) and disrupts the financing mechanisms of organized criminal networks.

3.3.13. Cybercrime Paralyzes Public Services and Can Cost Lives:

Ransomware cyberattacks wreak havoc across various sectors, often targeting essential services such as hospitals and healthcare organizations. Lives may be at stake due to the incapacitation of computer systems. For instance, in 2017, the WannaCry ransomware attack targeted the United Kingdom's National Health Service (NHS), rendering medical systems inoperative during critical procedures like heart surgery. Similarly, in September 2020, a hospital in Düsseldorf, Germany, fell victim to a ransomware attack. Due to the hospital's systems being locked, a patient with a life-threatening illness had to be transferred to another hospital, where she died due to delayed treatment.

3.3.14. Role of the State in Combating Cybercrime:

- The state plays a crucial role in the prevention and suppression of cybercrime. It should promote a reporting culture by raising public awareness and facilitating reporting

procedures for individuals and businesses. Moreover, governments can establish compelling regulations to encourage companies to report cybersecurity incidents, thereby strengthening the collection of data on cybercriminal activities.

- Additionally, authorities can work to enhance the confidentiality and security surrounding the reporting process, addressing concerns related to the reputation and trust of businesses. Ultimately, increased international cooperation among states is essential to effectively combat cybercrime, as many attacks transcend national borders.

A strategy to combat cybercrime must align with a cybersecurity strategy to ensure the continuity of essential services.

Advantages of the Strategy of the defence:

Among other benefits, the strategy:

- Informs all individuals who can contribute to and benefit from it.
- Helps better identify a country's vulnerabilities.
- Promotes innovation in the fight against cybercrime.
- Provides an established framework for prevention, detection, and intervention.
- Raises awareness.

Non-governmental entities:

- Academics/think tanks providing insights into current issues and offering research and writing expertise.
- Technology/sectoral organizations capable of identifying major threats to businesses.
- Civil society groups to raise awareness among the public.
- Regional and international organizations to exchange views on cybercrime threats at a regional level. (Stock, 2021)

3.3.15. Human and Material Resources:

The purpose of this audit is to catalogue the available human resources or those holding positions related to cybercrime, such as personnel specializing in cybercrime, digital forensics, or cybersecurity, such as CERT teams.

Examples of services falling under this category include:

- National police (services and units).
- Cybersecurity service (if applicable).
- National Cybersecurity Incident Response Team (CSIRT) and/or CERT.
- National, regional, and local judicial authorities or Ministry of Justice.
- Judges specializing in cybercrime.

- Prosecutors specializing in cybercrime.
- Investigative services.
- Central authority responsible for judicial cooperation treaties.
- National security or intelligence service.
- Other national services specialized in traditional offenses committed using the Internet (e.g., fraud, exploitation, etc.).
- Other national or local police services with active investigative units in the field of cybercrime.

Each of these services should provide the following information:

- A summary of the structure and mission of their service and the relevant units.
- Description of the forms of cybercrime targeted by the service.
- The legal framework within which it operates.
- Current initiatives in the fight against cybercrime led by the service.

3.3.16. Another examples of cyberattacks in real life:

In February 2016, hackers targeted the central bank of Bangladesh, exploiting vulnerabilities in SWIFT, the primary electronic payment messaging system for the global financial system, with an attempt to steal $1 billion. Despite blocking most transactions, $101 million still vanished. This incident served as a wake-up call for the financial industry, highlighting the underestimated systemic cyber risks within the financial system (Nelson, 2021).

The acknowledgment that a major cyberattack poses a threat to financial stability is now considered an axiom—no longer a matter of if, but when. However, governments and companies worldwide continue to grapple with containing this threat, primarily due to the uncertainty surrounding who is responsible for safeguarding the system. Key figures are increasingly alarmed by this challenge. In February 2020, Christine Lagarde, President of the European Central Bank and former head of the International Monetary Fund, cautioned that a cyberattack could trigger a severe financial crisis. In April 2020, the Financial Stability Board (FSB) warned that an inadequately contained major cyber incident could significantly disrupt financial systems, including critical financial infrastructure, leading to broader financial stability concerns. The potential economic costs of such events are substantial, and the impact on public trust and confidence can be severe.

Two ongoing trends further intensify this risk. Firstly, the global financial system is undergoing an unprecedented digital transformation. Banks are in competition with technology companies, and vice versa. The pandemic has elevated the demand for online financial services, normalizing work-from-home arrangements. Central banks globally are contemplating endorsing digital currencies and modernizing payment systems. In this transformative period, where an incident could undermine trust and derail innovations, cybersecurity becomes more crucial than ever.

Secondly, malicious actors are exploiting this digital transformation, posing an escalating threat to the global financial system, financial stability, and confidence in the system's integrity. The pandemic has provided new targets for hackers, following only the health sector, according to the Bank for International Settlements (Nelson, 2021).

Despite the increasing reliance of the global financial system on digital technology infrastructure, it is unclear who is responsible for protecting the system against cyber-attacks. This is partly due to the rapidly changing environment. Without dedicated measures, the global financial system will become more vulnerable to risks as innovation, competition, pandemics, and the digital revolution continue.

While many threat actors focus on financial gain, the number of purely destructive and disruptive attacks has been on the rise. Moreover, those who learn how to steal also gain insights into financial system networks and operations, enabling them to launch more destructive or disruptive attacks in the future or sell such knowledge and capabilities to others. This rapid evolution of risks imposes a burden on a mature response and a well-regulated system (Nelson, 2021).

In 2019, Kaspersky reported detecting over 100 million attacks targeting smart devices in the first six months of the year. This figure marked a significant increase compared to the previous year when only 12 million attacks were detected. The report also emphasized cybercriminals' preference for household devices over corporate devices, citing their increased vulnerability.

In 2020, Kaspersky's honeypots, which consist of networks of virtual copies of various internet-connected devices and applications, identified 426 million attacks on connected objects in the first six months of the year. This represents a fourfold increase in the number of attacks and a 2.5-fold increase in the number of unique IP addresses compared to the same period the previous year (Stock, 2021).

In 2020, Garmin, a company specializing in fitness tracking, experienced a Wasted Locker ransomware attack. The company confirmed paying a ransom of 10 million dollars to the attackers to restore its systems and prevent the public disclosure of user data.

In October 2020, the U.S. Cybersecurity, and Infrastructure Security Agency (CISA) issued an alert about the increasing incidents of ransomware attacks targeting the healthcare and public health sectors (Stock, 2021).

3.3.17. Cyber espionage encompasses:

- Unauthorized entry into systems or devices to retrieve information,
- Social engineering targeting individuals with authorized access to systems or devices to obtain information.

It involves cyber-attacks aimed at acquiring political, commercial, and military intelligence. Cyber espionage shares similar end goals with traditional espionage and takes advantage of the anonymity, global reach, dispersed nature, interconnectedness of information networks, and opportunities for plausible deniability.

Economic and industrial espionage, including cyber espionage, poses a substantial threat to a nation's prosperity, security, and competitive edge. Cyberspace serves as a favored operational domain for various threat actors, including countries, state-sponsored groups, organized crime, and individuals. The introduction of Artificial Intelligence (AI) and the Internet of Things (IoT) introduces new vulnerabilities.

Cyber economic espionage specifically targets and steals trade secrets and intellectual property on a larger scale, significantly impacting competitive advantage and market share. Cybercrime refers to crimes facilitated by or targeting computers, often driven by financial motives such as identity theft or property damage.

Cyberterrorism, as defined by Denning, involves the "convergence of cyberspace and terrorism," encompassing politically motivated hacking and operations intended to cause severe harm, including loss of life or significant economic damage (Nelson, 2021).

- ***Synthesis and Comprehensive Analysis of Selected Cybersecurity Literature:***

While crafting this thesis, a multitude of diverse books have been harnessed to illuminate the complex tapestry of cybersecurity. Each of these books exudes a distinct focus, honing in on precise facets of this multifaceted subject matter. One such exemplar is "Cybersecurity: The Beginner's Guide," a work which unfurls a comprehensive narrative tailored to novices in the realm of cybersecurity. This book serves as an unwavering advocate for heightened

security awareness throughout the tapestry of everyday activities, be it within the confines of the workplace, the sanctuary of one's home, or even amid the peripatetic landscape of travel. Its chapters span an array of dimensions, including the discernment of looming threats, the cultivation of an indomitable security mindset, the fortification of computers, the safeguarding of passwords, the protection of home networks, the insulation of smartphones, the navigation of web-based realms, the imperviousness of emails, the shielding of identities, the sanctuary of privacy, and the guardianship of familial connections in the digital space. Furthermore, it elucidates the importance of integrating cybersecurity within professional milieus and during sojourns to distant lands.

An equally essential tome, "CBOK - The Cyber Security Body of Knowledge," delves fervently into the multifarious domain of cybersecurity. A treasure trove of insights, this book traverses an expansive terrain of cybersecurity themes: the conceptual scaffolding of cybersecurity, the delicate tapestry of risk and its concomitant human and organizational underpinnings, the intricate regulatory landscape, the entwining threads of law, the enigma of computer crime, the intricacies of privacy rights, the ongoing tussle of attacks and defenses, the symphony of security operations, the orchestration of incident management, the labyrinthine realm of forensics, the bedrock of system security, the sanctity of authentication, the sovereign realm of authorization, and the crux of accountability. By distilling these myriad dimensions, the book aspires to furnish a holistic comprehension of the kaleidoscopic realm of cybersecurity.

A riveting addition to this ensemble is the tome titled "Hacking the Hacker: Learn from the Experts Who Take Down Hackers." With an intimate entreaty into the realm of ethical hackers and their panoply of tools, this work thrusts readers into the inner sanctum of cybersecurity. Portraits of ethical hackers, security researchers, and visionary leaders adorn its pages, their narratives a portal into their experiential realms. The tome's ambit encompasses an array of captivating topics: the intricacies of social engineering, the vulnerabilities woven into software architecture, the insidious realm of malware, the enigma of cryptography, the art of intrusion detection, the cataclysmic domain of network attacks, the burgeoning arena of IoT hacking, and more. This volume seeks to demystify hacking, to cast a clarifying light upon its mysteries, and to furnish profound insights into the vast expanse of cybersecurity.

In parallel, the compendium "Understanding Security Issues" assumes a stance akin to its counterpart, the "Beginner's Guide." In this manifestation, the import of cybersecurity

awareness resonates robustly, wielding its influence to enlighten both individuals and businesses. A veritable mosaic of themes adorns its pages, encompassing the panorama of threats, the cultivation of a vigilant security mindset, the anatomy of common cyber assaults, the fortress of computer defense, the citadel of password protection, the sentry post of home network security, the ramparts shielding smartphones, the tapestry of secure web browsing, the bastion of email and call security, the sanctity of identity, the veil of privacy, the guardianship of online familial bonds, and the sagacious considerations permeating the realms of travel. Woven with care, this volume seeks to empower its readers, granting them the tools to mitigate risks and defend their cherished assets.

"Politics, Governance and Conflict in Cyberspace" strides forward, assuming a vantage that stretches beyond mere technical constructs. This title, encompassing the politico-governance strata, unfurls an encompassing exploration of cybersecurity. It delves into the labyrinthine interactions unfurling within cyberspace – interactions spanning individuals, groups, and states. Integrated security risks come to the fore, woven into the narrative tapestry. Employing evocative case studies, the evolution of cyber threats manifests before our eyes, a testament to the fluctuating contours of the digital battlefield. By unearthing themes of cybersecurity governance, strategic underpinnings, non-state threats, the variegated tapestry of deterrence, and the delicate terrain of democracy, this book aims to furnish a cogent vista of the multi-dimensional battlefield that is cyberspace.

Concurrently, "Brink's Modern Internal Auditing: A Common Body of Knowledge" enters the stage, donning a different mantle while enmeshed with cybersecurity's aura. Though not exclusively devoted to cybersecurity, this work converges with the territory by addressing internal auditing in relation to security. Through its pages, the significance of internal controls looms large, casting its gaze upon the meticulous planning and execution of internal audits. The reverberations of information systems upon internal auditing and enterprise governance come under scrutiny, and the book further spotlights the hallowed realm of professionalism and the role of internal auditors in fortifying the security edifice of entities.

Within the structure of this thesis, each book has been carefully dissected, extracting the pertinent information germane to the narrative thread. The meticulous process of curation involves sifting through the volumes, distilling the essence that resonates seamlessly with the thesis's thematic crux. A case in point is the inclusion of "Nitul Dutta 2022," where the bedrock of cybersecurity is excavated, yielding not only a definition of the domain but also delving into its ethical connotations. This book, resplendent with comprehensive and lucid

information, forms the cornerstone of the thesis, expounding upon the fundamental facets of cybersecurity and delineating its principal domains.

Conversely, the pages of (Ozkaya, 2019) unfurl a historical tapestry, chronicling the annals of breaches. This book distinguishes itself by seamlessly interweaving the historical context with the present, underscoring the enduring importance of cybersecurity. A distinctive feature emerges in the form of a juxtaposition between security and hacking, wherein a panoramic overview is sketched, transcending the contours of mere technicalities. This section assumes an eminent place within the thesis, etching the contours of an attacker's psyche while navigating the intricate landscape of the threat milieu.

Turning attention to (Scott Donaldson, 2018), this work emerges as a repository of pivotal information, particularly pertinent to the evolution of malware. It's within these pages that the thesis draws upon the narrative of malware's unfolding saga, augmented by illustrations garnered from this very source. Simultaneously, the canvas broadens to encapsulate the realm of security mindset. A parallel instance unfolds with (Grimes, 2017), wherein the tome's discourse on Social Engineering defenses finds its way into the fabric of the thesis.

Similarly, (Moeller, 2016) furnishes critical insights encompassing the realm of firewalls and control systems. Such instances mirror a deliberate orchestration of sourcing comparable information from congruent literature. This convergence of information from analogous sources serves to buttress the thematic unity of the thesis, culminating in an overarching vista of cybersecurity. Through this deliberate synthesis, the thesis embraces a holistic approach, seamlessly interweaving the introduction to cybersecurity, the intricate choreography of hacking, preventative paradigms, and the pivotal role assumed by governments in safeguarding information realms.

Indeed, the tapestry of this thesis is woven from threads drawn from myriad sources, each tailored to the specific narrative contour it adorns. The distinctive advantage herein resides in its panoramic grasp of cybersecurity. This sets it apart from conventional tomes that isolate specific subjects, leaving the larger panorama unilluminated. Within the folds of this thesis, cybersecurity unfurls in its entirety – from its incipient notions to the labyrinthine realms of hacking, with a concurrent spotlight on prevention strategies and the resolute guardianship assumed by governments. In essence, this thesis epitomizes the holistic introduction to cybersecurity, while delving into the nuances of hacking and mitigation strategies. All the while, it underscores the pivotal role governments play in maintaining the sanctity and functionality of cybersecurity domains.

4. Practical Part

4.1 Attack Tests with Hacking Tools

The first step of our methodological approach involves conducting attack tests using a carefully selected set of well-established hacking tools in the field of computer security. These tools are chosen with great care based on their reputation, reliability, and ability to accurately simulate real attacks. The central objective of this step is to create a diverse range of attack scenarios to deeply explore their complex mechanisms, identify potential vulnerabilities, and understand the tactics employed by attackers.

The selection of these tools is based on a thorough assessment of their features and relevance to our research goals. We will ensure the choice of tools that cover a variety of attack approaches, such as code injection, social engineering, brute-force attacks, and other techniques commonly used by cybercriminals.

During this phase, we will also adhere to ethical and legal standards for attack testing, obtaining all necessary permissions and working in a controlled environment that will not compromise the security of systems beyond our study scope.

The results of these attack tests will serve as an essential foundation for evaluating existing security systems and identifying potential gaps in defence against threats. This step is critical for understanding the real challenges organizations face in terms of cybersecurity and for formulating practical recommendations to strengthen their resilience against attacks.

4.1.1 SQL Injection Attacks

SQL injection is a common and dangerous technique in the field of computer security. It exploits vulnerabilities in poorly designed web applications to gain illegal access to databases by injecting malicious SQL code into data input fields. This technique takes advantage of the fact that many web applications interact with a database to store, retrieve, and manage information.

- ***Description:***

In this type of attack, an attacker attempts to inject malicious SQL code into a legitimate SQL query to access a database. In other words, they insert specially crafted SQL commands into data input fields, such as a search field on a website, with the intention of manipulating the SQL query executed by the application.

- ***Practical Scenario:***

Imagine a highly popular e-commerce website that offers a product search feature. The attacker, aware of this vulnerability, decides to exploit the situation. In the website's search field, instead of entering a typical search query, the attacker enters a malicious query like this:

```
a.sql
1   Laptop' OR '1'='1
2
```

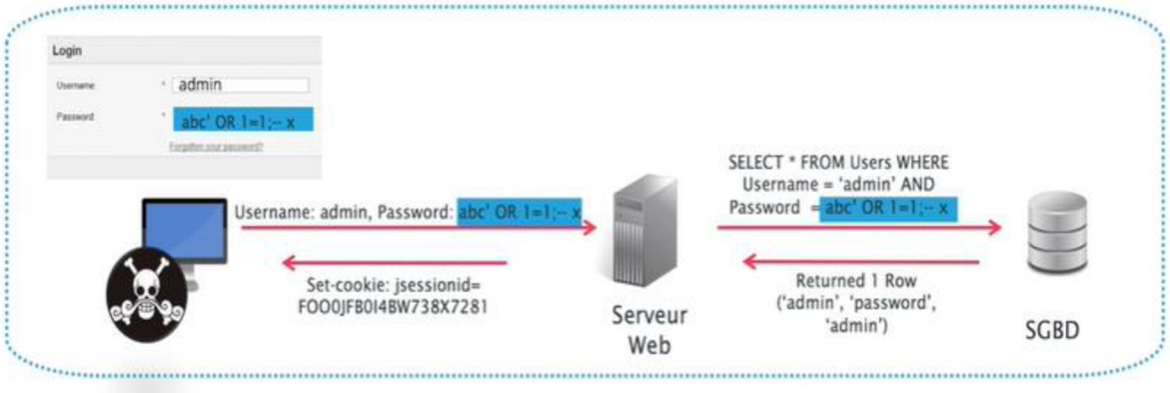
When this query is submitted, the web application will incorporate it into an SQL query intended for the database, which might look like this:

```
a.sql
1   SELECT * FROM produits WHERE nom_produit = 'Laptop' OR '1'='1';
2
```

The part `'1'='1'` is always true in SQL, which means the SQL query will return all rows from the "products" table. As a result, the attacker will have access to all the products listed on the site, including sensitive information such as user data and payment details.

⇨ This illustrates how powerful and devastating SQL injection attacks can be if not properly countered. The consequences can include the leakage of sensitive data, loss of user privacy, and even compromise of the integrity of information stored in the database.

- ***Descriptive Diagram:***



Preventing SQL injection attacks typically involves security practices such as strict user input validation, using prepared statements, or implementing web application firewalls (WAF) to filter out malicious queries. These measures are crucial for safeguarding web applications against this persistent threat.

- ***Practical Defense Code:***

Here's a Python example that utilizes the sqlite3 library to demonstrate a straightforward method for defending against SQL injection:

```python
import sqlite3

def search_users_by_name(name):
    # Establish a connection to the SQLite database
    connection = sqlite3.connect("mydatabase.db")
    cursor = connection.cursor()

    try:
        # Use a parameterized query to safely handle user input
        query = "SELECT * FROM users WHERE name = ?"
        cursor.execute(query, (name,))

        # Fetch and display the results
        results = cursor.fetchall()
        for row in results:
            print("User ID:", row[0])
            print("Name:", row[1])
            print("Email:", row[2])

    except sqlite3.Error as e:
        print("Database error:", e)

    finally:
        # Close the database connection
        connection.close()

# Example usage
user_input = input("Enter a name to search for: ")
search_users_by_name(user_input)

```

In this code, we use a prepared statement with a placeholder (`?`) to safely insert user input into the SQL query. This helps prevent SQL injection by treating the user input as data rather than executable SQL code. This is a fundamental practice for defending against SQL injection in your applications.

4.1.2 Phishing Attacks

- ***Description:***

A phishing attack is a type of cyber-attack where malicious actors impersonate trusted entities or individuals to deceive victims into revealing sensitive information or taking certain actions

that can compromise their security or privacy. Phishing attacks often employ social engineering techniques to manipulate the target's trust, emotions, or curiosity. The ultimate goal of a phishing attack is to obtain personal or confidential information, such as login credentials, credit card details, or sensitive business data.

- ***Scenario:***

Initial Email: The victim receives an email with a subject line that creates a sense of urgency, such as "Urgent Account Verification Required - Action Required Immediately." The email body appears convincing and contains language like "Security Alert" and "Your Account Is at Risk."

Urgent Warning: The email states that due to a recent security breach or system upgrade, the recipient's account is at risk of being compromised. It insists that immediate action is required to secure the account.

Fake Links: The email contains a link, which is prominently displayed as a button, leading to a fraudulent website that closely resembles SecureBank's official site. The link is masked to appear legitimate, and the recipient is urged to click on it to proceed with the account verification.

Data Entry Request: Once the victim clicks on the link, they are directed to a fake login page that looks identical to SecureBank's real website. They are prompted to enter their username and password for account verification.

Capture of Credentials: When the victim enters their login credentials and submits them, the attacker captures this information. The victim is then redirected to a legitimate SecureBank webpage to avoid suspicion.

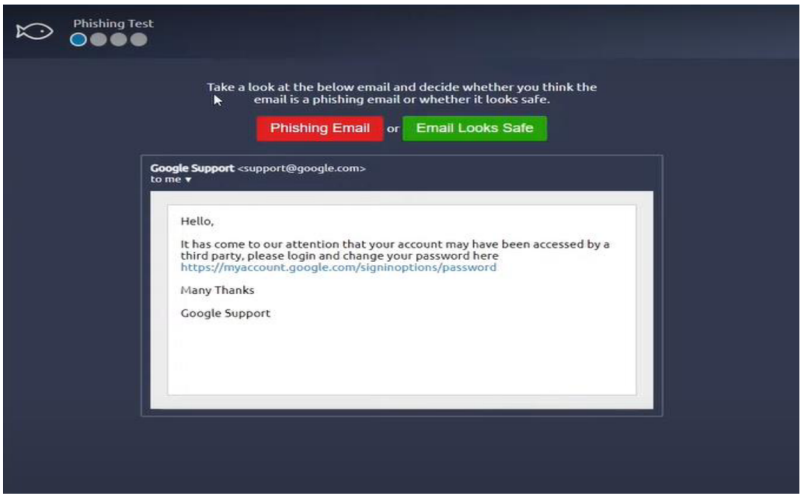
Confirmation: The victim is presented with a confirmation message, assuring them that their account has been successfully verified, which further adds to the illusion of legitimacy.

Consequences: With the victim's login credentials in hand, the attacker can gain unauthorized access to the victim's bank account, make unauthorized transactions, or engage in identity theft.

⇨ This scenario illustrates how phishing attacks can exploit a sense of urgency, fear, or trust in the victim to deceive them into taking actions that compromise their security. It's essential for individuals to exercise caution, carefully inspect emails, and verify the authenticity of the sources and requests they receive to avoid falling victim to such attacks. Organizations also play a crucial role in implementing security measures to detect and prevent phishing attempts.

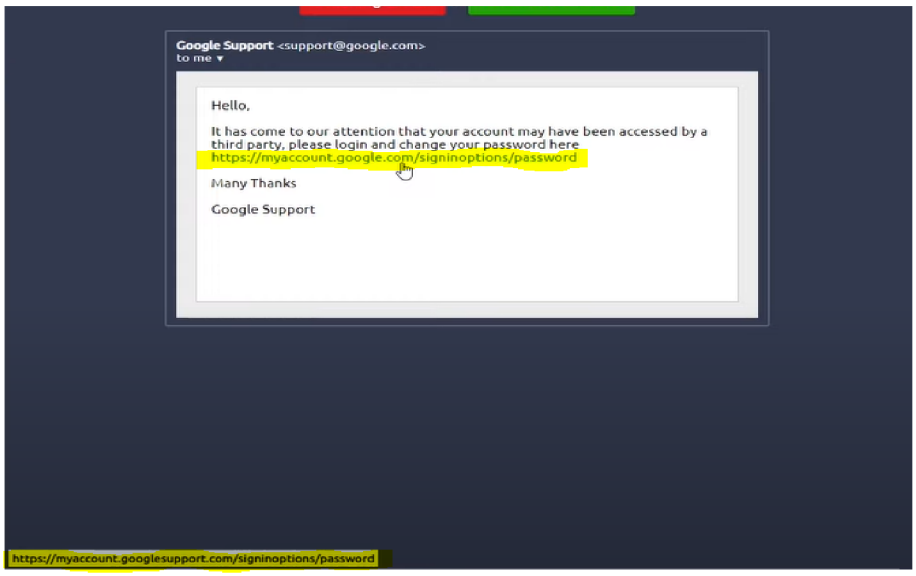
- ***Practical example:***

In this example, the email appears to be from Google Support. However, upon closer examination, it becomes evident that this is a phishing email. The message claims to be from Google, indicating that someone has either changed your password or that you've made a password change from a different location.

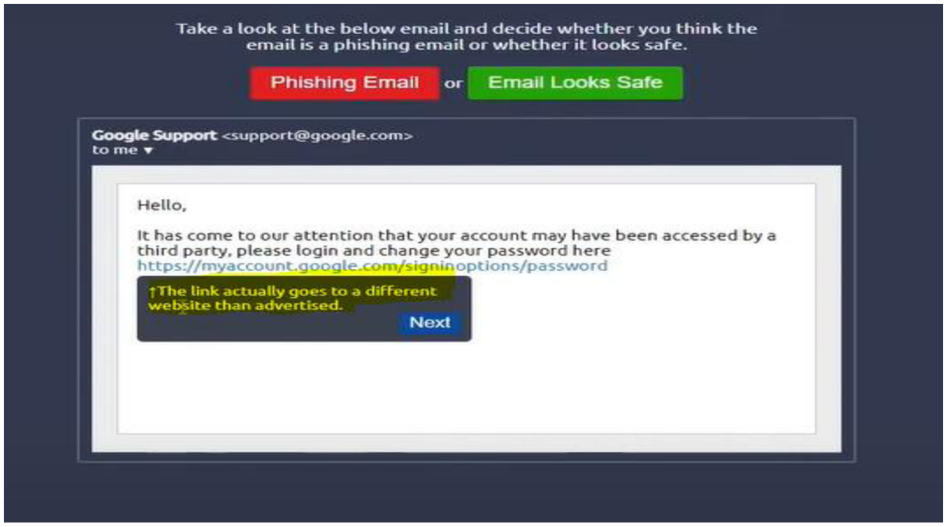


Several factors can help identify phishing emails. The first indicator is the links provided. While the link in the email reads `myaccount.google.com`, it's important to hover over the link to reveal the actual destination. In this case, the real link appears on the bottom left of the screen, showing `myaccountgooglesupport.com`. This discrepancy between the displayed link and the actual destination is a red flag.

The link in the message is crafted by the attacker to make it appear as if it's from Google. However, the real destination is the one that appears in the very far left at the bottom of the screen. This is where the link will take you.



Therefore, the link in the email message is deceptive and designed to convince you that it's from Google, making it a phishing email.



- ***Practical Defense Code:***

Here's an example of Python code that checks if a given URL is potentially a phishing website by examining the domain and using a simple blacklist:

```python
import re

def is_phishing_url(url):
    # Define a list of known phishing domains (you should maintain and update this list)
    phishing_domains = [
        "phishingsite1.com",
        "maliciousphisher.net",
        "fakebankinginfo.org",
        # Add more phishing domains
    ]

    # Extract the domain from the URL
    match = re.match(r'^https?://([^/]+)', url)
    if match:
        domain = match.group(1)

        # Check if the domain is in the phishing domains list
        if domain in phishing_domains:
            return True

    return False

# Example usage
url_to_check = "https://phishingsite1.com/login"
if is_phishing_url(url_to_check):
    print("Warning: This URL may be a phishing website.")
else:
    print("The URL appears to be safe.")

```

- ***Explication:***
- ***is_phishing_url*** function takes a URL as input and checks if the domain part of the URL matches any known phishing domains from the ***phishing_domains*** list.
- You should maintain and update the ***phishing_domains*** list with known phishing domains.

Regular expressions are used to extract the domain from the URL.
The code assumes URLs start with "http://" or "https://". You can adapt the regular expression to handle more URL variations.

4.1.3 Https Session Hijack:

- **Description:**

Session Hijacking occurs when an unauthorized individual gains entry into a user's active session within a system. This unauthorized entity typically acquires a legitimate session ID to infiltrate the system and intercept its data. The notorious WhatsApp Sniffer is recognized as a prevalent form of Session Hijacking attack. The first recorded instance of Session Hijacking took place on Christmas day in 1994 by Kevin Mitnick at the time of the release of HTTP 0.9.

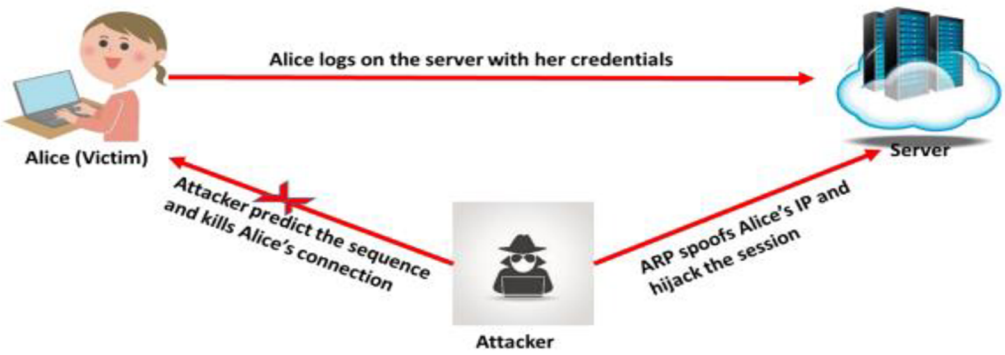


Figure 5: Manipulating the token session executing the session hijacking attack.

Session hijacking encompasses two primary types:

- Active Session Hijacking:

In an active attack, the intruder identifies and seizes an already active session, gaining control over it.

- Passive Session Hijacking:

With a passive attack, the attacker illicitly takes over a session but refrains from actively interfering; instead, they monitor and record the transmitted traffic.

There are two levels at which session hijacking occurs:

- Network Level Session Hijacking:

This involves intercepting packets transmitted between the client and server in TCP and UDP sessions. Various methods are employed, such as TCP/IP hijacking, IP spoofing, RST hijacking, blind hijacking, man-in-the-middle attacks using packet sniffers, and UDP hijacking.

- Application-Level Session Hijacking:

At this level, attackers gain control over HTTP user sessions by obtaining session IDs. Techniques involved here include obtaining session IDs, sniffing, brute force attacks, and exploiting misdirected trust.

Several tools are used for session hijacking, including WireShark for packet sniffing, Juggernaut and Hunt for flow analysis, TTY Watcher for system monitoring and control, IP Watcher, T-Sight, Paros HTTP Hijacker for various functionalities like spidering and filtering, and tools such as Hjksuite Tool, DnsHijacker Tool, and open-source scripts like cookie injector.

- ***Scenario:***
- ***Practical example:***

Setting: An online e-commerce platform that sells various products. Users have accounts to make purchases, view order history, and store personal information.

Step 1: Identifying the Vulnerability:

- An attacker, Jane, discovers a vulnerability in the e-commerce website that allows for session hijacking. Jane notices that the website uses relatively weak session management and lacks proper encryption.

Step 2: Capturing Session Data:

- Jane observes a legitimate user, Alex, browsing the e-commerce site while connected to an unsecured public Wi-Fi network. Through the use of packet sniffing tools, Jane intercepts the network traffic and captures the session ID or authentication token that Alex's browser uses to maintain the active session.

Step 3: Session Takeover:

- With the obtained session token, Jane can now impersonate Alex's session. She crafts a request to the e-commerce website's server using Alex's session ID.

Step 4: Jane Actions:

- Jane, now within Alex's session, gains access to Alex's account and performs unauthorized actions. For example, she can make purchases using Alex's stored payment details or alter shipping information.

Step 5: Covering Tracks and Exit:

- To evade detection, Jane completes the unauthorized actions and then signs out or clears traces of the session hijack by erasing the logs that might reveal her intrusion.

- **Defence coding part:**

a.php

```php
// Enable secure session handling
ini_set('session.cookie_secure', 1);
ini_set('session.cookie_httponly', 1);
session_start();

// Regenerate session ID
session_regenerate_id(true);

// Set session timeout
$session_timeout = 3600; // 1 hour
if (isset($_SESSION['last_activity']) && (time() - $_SESSION['last_activity'] > $session_timeout)) {
    // If session is inactive for more than the timeout, destroy the session and redirect to login
    session_unset();
    session_destroy();
    header("Location: login.php");
    exit();
}

// Update last activity time
$_SESSION['last_activity'] = time();
```

- *Explanation:*

- ***`ini_set('session.cookie_secure', 1);`:*** Sets the session cookie to be transmitted only over secure (HTTPS) connections, making it more challenging for attackers to intercept the session data. It ensures that the session cookie is not sent over unencrypted connections.

- ***`ini_set('session.cookie_httponly', 1);`:*** Restricts access to the session cookie through JavaScript. This measure helps prevent certain types of attacks, particularly cross-site scripting (XSS), by disallowing client-side scripts from accessing the session cookie.

- ***`session_regenerate_id(true);`:*** This function regenerates the session ID. It's a good practice to regenerate the session ID after a successful login or privilege change to prevent session fixation attacks, where an attacker fixes or sets a known session ID, allowing them to hijack the session.

- `*$_SESSION['last_activity'] = time();*`: This line sets or updates the `last_activity` session variable with the current timestamp. This variable is used to track the last time the session was active.

- `*$session_timeout = 3600;*`: Sets the session timeout duration to 1 hour.

- The conditional statement checks if the difference between the current time and the last activity time is greater than the session timeout. If so, it unsets the session, destroys it, and redirects the user to the login page. This prevents sessions from remaining active for an extended period, reducing the window of opportunity for session hijacking.

 The provided PHP code exemplifies fundamental methods to enhance session security and thwart session hijacking. It achieves this by leveraging secure connections through HTTPS, establishing secure session attributes, renewing session IDs, and instituting a mechanism for session timeout.

4.1.4 Malware attacks: Authentication attacks:

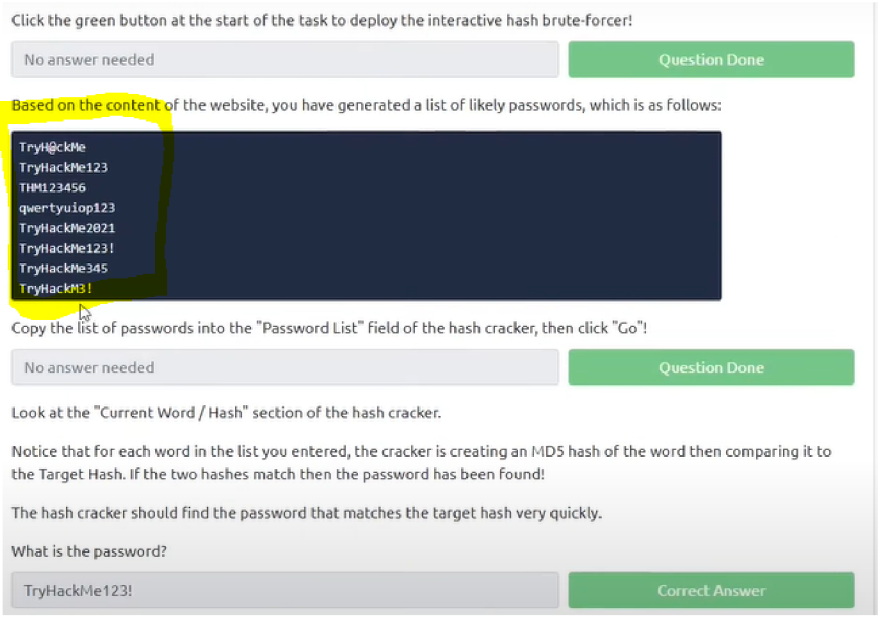
- ***Description:***

  Authentication attacks are a class of cyberattacks focused on compromising the security of user authentication systems, such as usernames and passwords. The goal is to gain unauthorized access to systems, accounts, or data by exploiting vulnerabilities in the authentication process. Here's a description of authentication attacks:

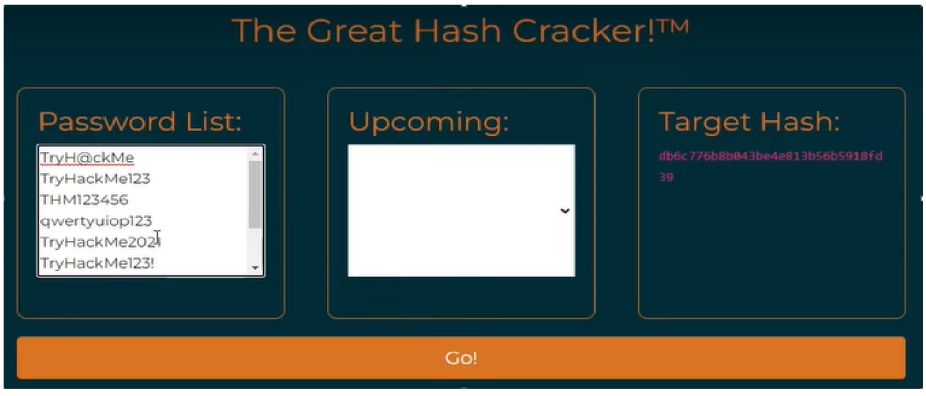
  Authentication attacks target the verification of a user's identity, often by exploiting weaknesses in the authentication mechanisms or through various deceptive techniques. These attacks may involve brute force attempts, where an attacker repeatedly tries different combinations of usernames and passwords, or more sophisticated methods like phishing, where individuals are tricked into revealing their login credentials. Authentication attacks pose a significant risk to the security and privacy of digital systems and can lead to unauthorized access, data breaches, and financial losses.

- ***Practical example:***

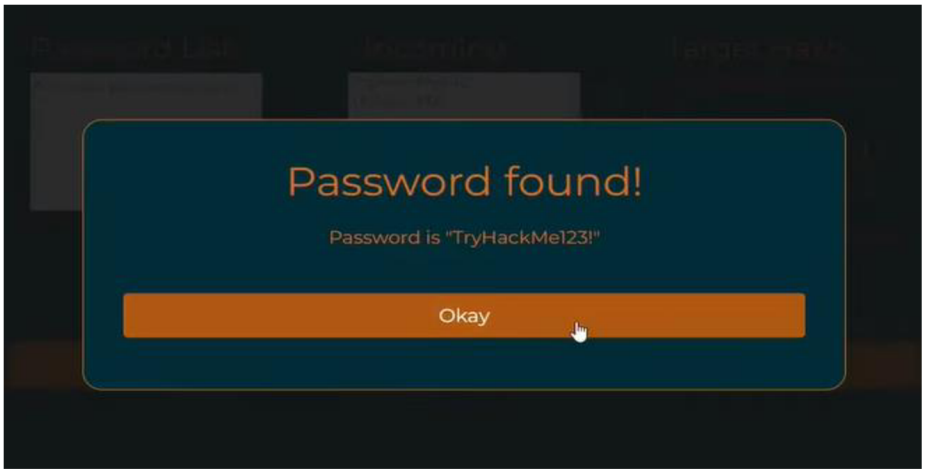
  In this scenario, we have a password list at our disposal.



When we click the 'Go' button, the tool will hash each password in the list. It then compares these hashed passwords with the actual hash. When it finds a match, it decrypts the hash and reveals the corresponding password. To guess the password, we use a word list. For each password in the list, we calculate its hash and compare it with the target hash, which we might have obtained from a leaked password database or a compromised system. When we discover a match, we convert it back to the password and give it a try. For example, by clicking 'Go,' you can see that the password 'tryhackme123' is found.

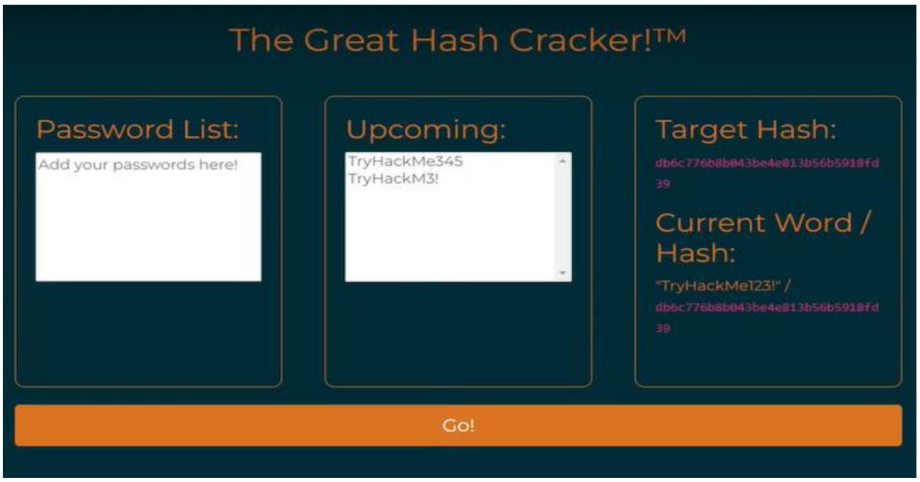


This process simulates how authentication attacks work, but it's important to note that this is only a simulation.



To enhance security and prevent authentication attacks, it's crucial to follow certain security measures. First and foremost, we should use strong passwords. A strong password is characterized by its length, typically above nine characters, and it should include a combination of lowercase and uppercase letters, symbols, and digits.

Additionally, implementing multi-factor authentication is highly effective in countering brute force attacks. Multi-factor authentication requires more than just a password for logging in. For instance, you might need a password and an additional factor, such as an authentication code sent via SMS. For example, when logging into Facebook, they might send you an SMS containing an authentication code (e.g., 123456789). To log in successfully, you'd need to enter this code. This approach prevents unauthorized access even if someone has managed to obtain your password.



These security measures are essential for safeguarding against authentication attacks, ensuring the protection of your accounts and data.

4.1.5 certificate counterfeit:

- **Description:**

Attack certificate counterfeiting typically involves various methods aimed at falsifying or creating counterfeit digital certificates. The objective is to deceive systems or individuals by introducing fake certificates that appear legitimate. This type of attack poses significant security risks as it can compromise the trust established through digital certificates and cryptographic protocols.

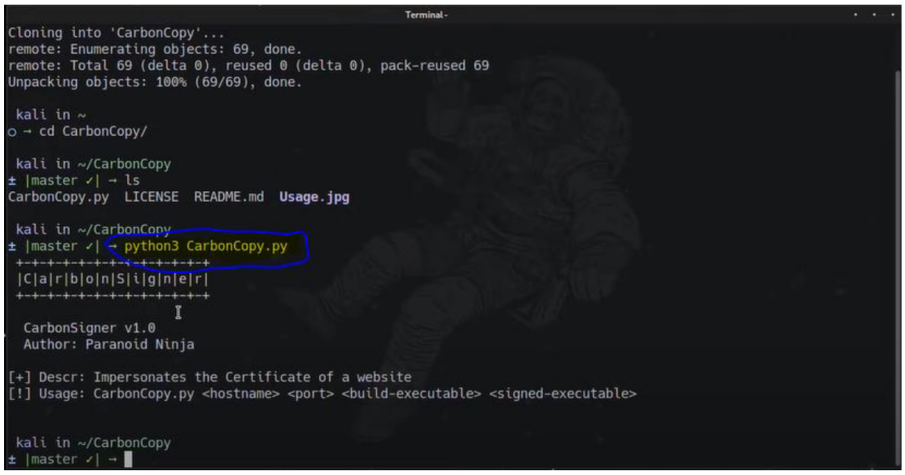
Attackers may employ several techniques to conduct certificate counterfeiting attacks:

- *Forgery:* Creating fake digital certificates that mimic legitimate certificates, often by imitating the credentials of trusted entities. These forged certificates can then be used to intercept or manipulate sensitive information.
- *Impersonation:* Pretending to be a trusted entity or individual by generating a certificate that falsely represents their identity. This can be used to deceive users into interacting with malicious or unauthorized systems.
- *Spoofing Certificate Authorities:* Manipulating or imitating a Certificate Authority (CA) to issue fraudulent certificates. This might involve compromising the CA's infrastructure or imitating its digital signatures.
- *Stealing Private Keys:* Gaining unauthorized access to private keys used in the creation and verification of certificates. With stolen private keys, attackers can generate counterfeit certificates that seem authentic.
- *Altering Certificate Data:* Modifying valid certificates to change the information they contain, such as altering the expiration date or the entities to which they apply.

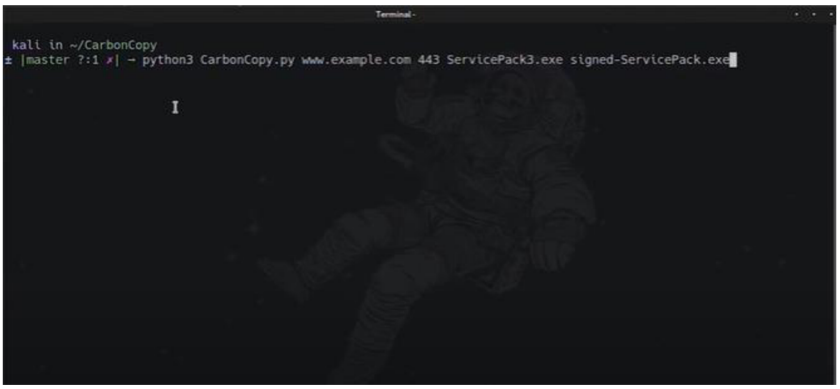
- **Attack coding:**

Example of spoofing the website certificate:

In this example, we are going to use here to spoof .the website certificate is called carbon copy ,it has the ability to self-signed certificates that look exactly the same as the original the best thing about this tool is it not only spoofs certificates but also signs and executable for heavy evasion so that every software can`t detect it is a fake certificate but if the validation process is done on the certificates no local trust anchor will be found in the certificates will be marked as untrusted and rejected. now change the directory to the carbon copy folder here you can see a python script named carboncopy.py , then lunch the script by this command:



You`ve launched the tool successfully now it is time to clone a website certificate to do that type this command:



Now understand the command line first we put the name of the website in which we want to clone the certificate in the second we put the port 443 which is a TCP port used by websites who have SSL in the third we put an evasion executable Service Pack 3.exe at the last we`ve signed the executable with the command signs service pack 3.exe , it was simple now hit enter finally the fake certificate was successfully generated:

hackers do every possible thing to hack us we are not aware of the security problems around us and hackers take advantage of it we are so vulnerable it`s our responsibility to raise security awareness this tutorial is not for illegal purposes it is to let you know how vulnerable we are when we visit a website we do not check whether its certificate is valid or not we do not check what URL is running on the address bar or to what URL its that`s a very bad thing we have to take care of our own security our own .

- **Defence Coding:**

Certainly! Here's an example in Python that demonstrates how you can create a simple system to manage and verify certificates using digital signatures. This example uses the cryptography library, which provides cryptographic functionalities.

Firstly, you'll need to install the cryptography library if you haven't already:

```
pip install cryptography
```

Now, here's an example of how you might generate and verify certificates using digital signatures:

```python
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import ec
from cryptography.hazmat.primitives.asymmetric import utils
from cryptography.hazmat.primitives import serialization

# Function to generate a certificate and its digital signature
def generate_certificate(private_key, data):
    signature = private_key.sign(
        data.encode('utf-8'),
        ec.ECDSA(hashes.SHA256())
    )
    return signature

# Function to verify the certificate's digital signature
def verify_certificate(public_key, data, signature):
    try:
        public_key.verify(
            signature,
            data.encode('utf-8'),
            ec.ECDSA(hashes.SHA256())
        )
        return True
    except utils.InvalidSignature:
        return False

# Generate a private key (usually done by the Certificate Authority)
private_key = ec.generate_private_key(ec.SECP256R1())

# Extract the public key from the private key
public_key = private_key.public_key()
```

```
# Data to be included in the certificate
data = "User: John Doe, ID: 12345, Access Level: 5"

# Generate a certificate with a digital signature
certificate_signature = generate_certificate(private_key, data)

# Verification of the certificate
verification_result = verify_certificate(public_key, data, certificate_signature)

if verification_result:
    print("Certificate is valid.")
else:
    print("Certificate is not valid.")
```

This Python script demonstrates the basic process of certificate generation and verification using elliptic curve cryptography. In a real-world context, security measures, key management, and more robust systems are imperative to ensure the integrity and safety of certificate handling. This code provides a foundational understanding and would need modifications and enhancements to suit specific security protocols and practical application requirements.

So, defending against certificate counterfeiting involves various security measures to ensure the authenticity and integrity of digital certificates. Here are some strategies for defending against certificate counterfeiting:

- *Use Reputable Certificate Authorities (CAs):* Rely on well-established and trusted Certificate Authorities to issue and validate certificates. Trusted CAs implement robust security measures to prevent counterfeit certificates.
- *Implement Robust Encryption:* Use strong encryption methods to secure certificates, ensuring that they cannot be easily forged or manipulated.
- *Regular Certificate Audits:* Conduct periodic audits and validations of certificates to detect any anomalies or signs of tampering. Implement systems that monitor and alert administrators about potential security breaches related to certificates.
- *Enforce Certificate Revocation:* Establish a process to revoke compromised or fraudulent certificates promptly. This typically involves maintaining a Certificate Revocation List (CRL) or utilizing the Online Certificate Status Protocol (OCSP) to inform relying parties when a certificate is no longer valid.
- *Multi-factor Authentication (MFA):* Implement MFA to enhance the security of the certificate issuance and verification process. Multiple layers of authentication make it harder for attackers to counterfeit certificates.
- *Physical Security Measures:* Implement physical security measures for the storage and issuance of physical certificates. This may include using specialized printing techniques, holograms, watermarks, or other physical security features to deter counterfeiting.

- *Regular Software Updates and Patching*: Ensure that all certificate-related software, applications, and systems are up-to-date with the latest security patches to prevent vulnerabilities that could be exploited by attackers.
- *Educate Employees and Users:* Train employees and users to recognize signs of counterfeit certificates and to follow proper security procedures when handling certificates. Awareness programs can help reduce the risk of falling victim to certificate-related attacks.
- *Compliance with Security Standards:*Adhere to industry standards and compliance regulations related to certificate management. Standards like Public Key Infrastructure (PKI) and Secure Sockets Layer (SSL) offer guidance on best practices for certificate issuance and management. By implementing a combination of these strategies, organizations can significantly reduce the risks associated with certificate counterfeiting and enhance the security of their digital assets and communications.

4.1.6 IOT vulnerabilities:

- **Description:**

Attack certificate counterfeiting typically involves various methods aimed at falsifying or An IoT attack refers to a cyber assault directed at Internet of Things (IoT) systems, encompassing physical devices, vehicles, buildings, and various objects integrated with software to facilitate data collection and exchange. With the expanding IoT landscape, there is a corresponding rise in cyber threats. Continue reading to gain insights into IoT attacks and strategies to safeguard your systems (What are IoT attacks?, 2023)

Types of IoT attacks:

IoT attacks constitute cybercrimes aimed at exploiting vulnerabilities in Internet of Things devices, often stemming from weak security measures, outdated firmware, and suboptimal system designs. The following are prevalent types of IoT attacks:

- *Device Spoofing:* This attack involves a malicious device manipulating an authentic device's IP address, MAC address, or other identifying information to masquerade as a legitimate device.
- *Man-in-the-Middle (MitM) Attacks:* In a MitM attack, a hacker intercepts communication between two systems, impersonating the original sender to deceive the recipient into thinking they are receiving a genuine message. MitM attacks are commonly executed to extract sensitive information and disrupt services.

- *Distributed Denial of Service (DDoS) Attacks:* DDoS attacks on IoT devices involve overwhelming the network with constant traffic, such as fake requests, to saturate the system, causing it to crash and denying service to legitimate users.
- *Eavesdropping:* Threat actors engage in eavesdropping, also known as sniffing or spying, to intercept and monitor communication between IoT devices, potentially gaining unauthorized access to sensitive information.
- *Malware Attacks:* Cybercriminals install malicious software on IoT devices to compromise sensitive data, take control of the device, or spy on network activity and conversations.
- *Zero-Day Attacks:* During a zero-day attack, a hacker exploits unpatched vulnerabilities in the software of IoT devices that were previously unknown to cybersecurity experts. These attacks are particularly perilous as there is no available fix during the attack.
- *Password Cracking:* Hackers employ various methods, including brute force attacks, to decrypt system passwords and gain access to IoT devices. Weaker default passwords and poor password practices make it easier for attackers to hijack IoT systems.
- *Firmware Manipulation:* In this type of attack, cybercriminals modify the firmware of an IoT device to alter its functionality, enabling them to perform malicious actions and potentially compromise the device.

- ***IoT-attack scenario :***

Attack Scenario: Manipulating Smart Home Water Dispenser:

Background:

In this scenario, an attacker aims to exploit vulnerabilities in a smart home's water dispenser system, controlled by an IoT network. The central node, responsible for controlling the water dispenser arm, becomes the target.

Steps in the Attack Scenario:

1. *Initialization*:

- The attacker, situated on the external side network (possibly the internet), crafts and sends a deceptive IPv6 CoAP message to the smart home system.

2. *IoT Network Structure:*

- Within the IoT network, two critical nodes are identified:

- Control Node: Manages the water dispenser arm.

- *Internal Node:* Handles various tasks and processes messages for legitimate nodes seeking water within the network.

3. *Malicious Code Activation:*

- The attacker reveals that they've implanted dormant malicious code into the Internal Node during a previous demonstration. This code remained inactive until now.

4. *Targeted Attack:*

- The attack is launched from the external network, specifically targeting messages destined for the Control Node, responsible for managing the water dispenser arm.

5. *Application-Level Modification:*

- The attacker successfully modifies the application-level content of the messages destined for the water dispenser arm. This allows them to control the arm's behavior.

6. *User Interaction:*

- As a demonstration, a normal user initiates a request for more water by sending a standard message. However, when the message passes through the compromised Internal Node, the attacker alters its content.

7. *Unexpected Arm Behaviour:*

- The attacker's manipulation causes the water dispenser arm to behave unexpectedly, contrary to its intended functionality. It fails to dispense water as anticipated.

8. *Exploiting Encryption Gap:*

- The attack was possible due to the absence of end-to-end encryption in application-level messages. The lack of encryption made the inside network susceptible to unauthorized manipulation.

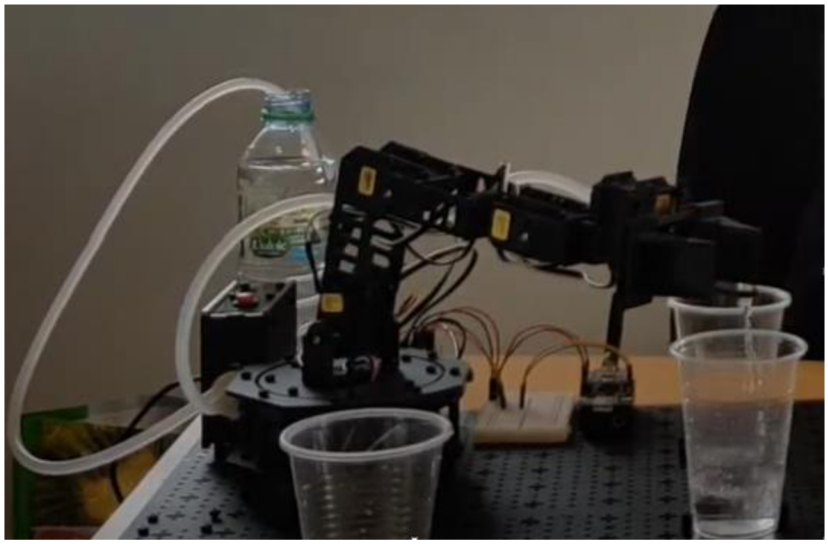


Figure 6: The Experience Before the Impact: A Prelude to the Attack

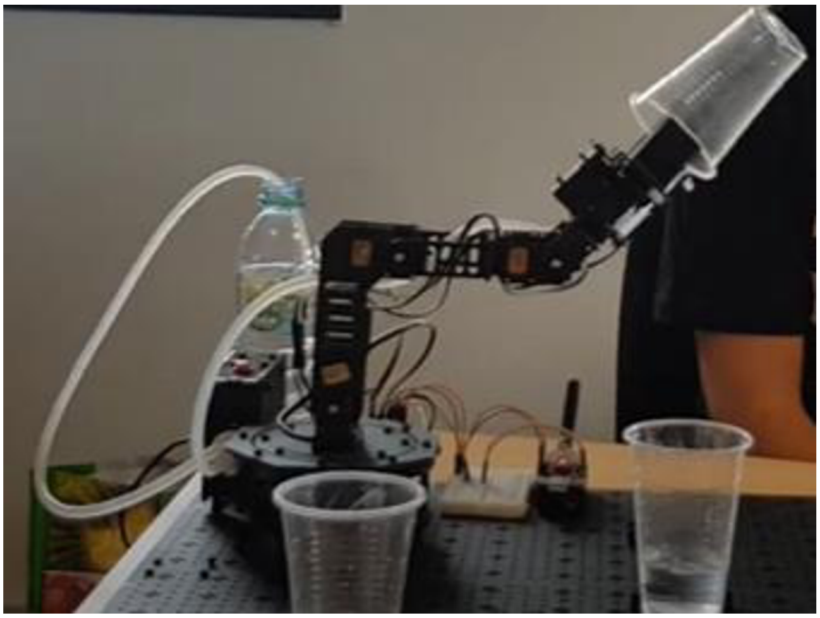


Figure 7: The Experience after the Impact: A Prelude to the Attack

Outcome:

The successful demonstration of this attack highlights the potential risks associated with unencrypted communication in IoT networks, specifically in controlling critical devices like water dispensers. It emphasizes the importance of implementing robust security measures, including end-to-end encryption, to safeguard against unauthorized manipulations and ensure the integrity of IoT systems.

- ***Real-life examples of IoT attacks:***

Exemplifying the potential dangers of IoT attacks, real-life instances underscore the harm inflicted by cybercriminals breaching critical systems. Whether aiming to pilfer sensitive data or disrupt organizational operations, these incidents emphasize the importance of selecting robust IoT security solutions to mitigate risks effectively. Examining historical cases sheds light on the gravity of IoT device attacks.

In 2016, a notorious IoT attack unfolded through the Mirai botnet. Exploiting default login credentials, the Mirai malware infected IoT devices, including cameras and routers. This malicious software orchestrated a botnet of compromised devices, launching a series of distributed denial-of-service (DDoS) attacks. Among the primary victims was the DNS provider Dyn, causing temporary unavailability of services for Netflix, Twitter, and The New York Times.

A particularly alarming IoT attack occurred in 2017 at the medical device company St. Jude Medical. Vulnerabilities were exposed in vital medical devices such as pacemakers, highlighting the potential risks of hacking. The FDA confirmed the susceptibility of some of

St. Jude's implantable cardiac devices, which could empower threat actors to drain batteries or, more alarmingly, administer incorrect shocks—high-energy pulses delivered by devices like implantable defibrillators to rectify life-threatening abnormal heart rhythms.

In 2015, two security researchers demonstrated the manipulation of a Jeep Cherokee's telematics system while on a highway, remotely controlling the car's engine, brakes, and other critical functions. Recognizing the severe implications, Fiat Chrysler invested 1.4 million to address system deficiencies, preventing potential attacks on the car system that could have lethal consequences, such as manipulating the brake system to harm individuals (What are IoT attacks?, 2023).

- ***Defense :***

Securing your IoT devices requires vigilant measures, essential not only for safeguarding data but also for ensuring personal safety. Enhance the security of your IoT devices by adopting the following strategies:

- *Utilize Strong and Unique Passwords:* Change default login credentials and establish robust, unique, and complex passwords. This measure significantly fortifies the protection of your devices.

- *Regularly Update Software and Firmware:* Stay proactive in updating both software and firmware to incorporate the latest security patches and bug fixes. This practice significantly raises the bar for hackers attempting to exploit vulnerabilities.

- *Disable Unnecessary App Permissions*: Many devices come with default settings enabling features like remote access. If these features are unnecessary, disable them to reduce potential points of entry for hackers and enhance overall device security.

- *Implement Two-Factor Authentication (2FA):* Introduce an extra layer of security by enabling two-factor authentication. This measure makes it substantially more challenging for unauthorized users to access your accounts and devices.

- *Secure Network Connections with a VPN:* Enhance the security of your device's data by employing a Virtual Private Network (VPN). A VPN establishes a secure connection between your devices and the VPN server, safeguarding your data from potential interception.

By incorporating these protective measures, you significantly bolster the security posture of your IoT devices, mitigating potential risks and safeguarding both your information and personal well-being.

- ***Defense coding:***

```python
import hashlib
import random
import time
class IoTDevice:
    def __init__(self, device_id, security_key):
        self.device_id = device_id
        self.security_key = security_key
        self.firmware_version = 1
        self.data_store = []

    def authenticate(self, provided_key):
        # Check if the provided key matches the device's security key
        return provided_key == self.security_key

    def update_firmware(self, new_version):
        # Simulate firmware update
        print(f"Updating firmware from version {self.firmware_version} to {new_version}")
        self.firmware_version = new_version

    def secure_communication(self, data, authentication_key):
        # Verify authentication before sending data
        if self.authenticate(authentication_key):
            # Encrypt the data (simulated with a simple hash for illustration purposes)
            hashed_data = hashlib.sha256(data.encode()).hexdigest()
            self.data_store.append(hashed_data)
            print(f"Securely received and stored data from IoT device {self.device_id}")
        else:
            print("Authentication failed. Data not accepted.")

# Simulate a central server managing IoT devices
class IoTServer:
    def __init__(self):
        self.devices = {}
```

```python

    def register_device(self, device):
        # Register a new IoT device with the server
        self.devices[device.device_id] = device
        print(f"IoT device {device.device_id} registered with the server")

    def update_all_firmwares(self, new_version):
        # Update firmware for all registered devices
        for device in self.devices.values():
            device.update_firmware(new_version)

# Example of using the IoTDevice and IoTServer classes
# Create an IoT server
server = IoTServer()

# Register IoT devices
device1 = IoTDevice(device_id="12345", security_key="secureKey123")
server.register_device(device1)

device2 = IoTDevice(device_id="67890", security_key="strongKey456")
server.register_device(device2)

# Attempt to send data without proper authentication
device1.secure_communication(data="Sensor data", authentication_key="wrongKey")

# Proper authentication before sending data
device1.secure_communication(data="Sensor data", authentication_key="secureKey123")

# Simulate a firmware update for all devices
server.update_all_firmwares(new_version=2)

# Attempt to send data after a firmware update
device1.secure_communication(data="New sensor data", authentication_key="secureKey123")
```

- ***Explanation of code:***

- *IoTDevice Class:* The IoTDevice class represents a simulated IoT device. It has attributes like device_id, security_key, firmware_version, and a data_store to store received data securely.
- *authenticate Method:* This method checks if the provided key matches the device's security key.
- *update_firmware Method:* Simulates a firmware update by printing a message and updating the firmware_version attribute.

- *secure_communication Method:* Simulates secure data communication by hashing the data and storing it securely if authentication succeeds.
- *IoTServer Class:* The IoTServer class simulates a central server managing IoT devices.
- *register_device Method:* Registers an IoT device with the server, storing it in the devices dictionary.
- *update_all_firmwares Method:* Initiates a firmware update for all registered devices.
- *Server and Device Instances:* An instance of the IoTServer class (server) is created. Two instances of the IoTDevice class (device1 and device2) are created and registered with the server.
- *Communication and Firmware Update:* Communication is simulated with the secure_communication method, including an attempt with incorrect authentication. A firmware update is initiated for all devices.

4.1.7 Crypto jacking:

- **Description:**

Cryptojacking involves the unauthorized utilization of another individual's computational resources for the purpose of cryptocurrency mining. Hackers aim to seize control of various systems—be it desktops, servers, cloud infrastructure, and similar platforms—to clandestinely mine for cryptocurrencies.

Irrespective of how it's introduced, cryptojacking code commonly operates discreetly in the background while unsuspecting users continue their regular system usage. The sole indicators users might observe are reduced performance, delays in execution, overheating, increased power consumption, or unusually high bills for cloud computing services (Chickowski, 2022).

Figure 8: How cryptojacking works (techtarget, 2022)

Cryptojacking Attack Methods:

There are two main types of cryptojacking attacks:

- ***Web browser-based attacks*** involve using a website or online ad to deliver the cryptojacking malware to the victim's computer. When the victim visits the website or clicks on the ad, the malware is automatically downloaded and installed on their computer. This type of attack is known as "drive-by cryptojacking" because the victim's computer is compromised simply by visiting a website.
- ***Host-based attacks*** involve installing the cryptojacking malware directly on the victim's computer. This can be done through a variety of methods, such as sending the victim a malicious email attachment, using a fake app or game that contains the malware, or compromising the supply chain of a legitimate software provider and inserting the malware into the software.

- ***Examples of Cryptojacking Attacks:***

- *Coinhive:*

Coinhive, introduced in 2017, offered website owners a way to generate revenue by embedding a JavaScript code for in-browser mining. This allowed their visitors' computers to mine Monero cryptocurrency. Despite its legitimate intent, attackers misused it to deploy cryptojacking malware without user consent. Coinhive ceased operations in March 2019 due to regulatory concerns and declining user interest.

- *WannaMine v4.0:*

WannaMine, a cryptojacking malware identified in 2018, spreads through phishing emails with malicious attachments. Once opened, WannaMine installs itself on the victim's computer, mining Monero. The latest version, WannaMine v4.0 (2020), implements evasive measures and data theft capabilities while propagating across networks.

- *FaceXWorm:*

FaceXWorm exploits social engineering on Facebook Messenger, luring users to fake YouTube links that prompt them to download a Chrome extension. This extension hijacks their accounts, spreads to contacts, and starts cryptocurrency mining. Additionally, it steals user credentials and redirects them to fraudulent platforms for payments in cryptocurrency.

- *Black-T:*

Black-T, a variant by cybercriminal group TeamTNT, targets AWS credentials, exploiting Docker daemons and APIs to mine Monero. The malware includes advanced features like countering other cryptojacking worms, password scraping, and network scanning, using tools like pnscan, masscan, and zgrab.

- Each of these instances showcases diverse tactics used in cryptojacking attacks, emphasizing the evolving and sophisticated nature of these malicious activities.

- ***Defense:***

To defend against cryptojacking, implementing good cybersecurity practices is crucial. Here are some measures and code examples that could be used to detect and prevent cryptojacking:

1. *Using malicious script blockers:* You can use browser extensions to detect and block crypto mining scripts.

Sample JavaScript code to detect mining scripts:

2. *Utilizing browser extensions or anti-cryptojacking software:* Extensions like NoCoin for browsers like Chrome or Firefox can help in blocking mining scripts.

```javascript
// Checking for script loads from known mining domains
var scriptSources = document.getElementsByTagName('script');
var cryptoMiningDomains = ['exampledomain.com', 'anotherdomain.com']; // Add known mining domains here

for (var i = 0; i < scriptSources.length; i++) {
    var src = scriptSources[i].src;
    for (var j = 0; j < cryptoMiningDomains.length; j++) {
        if (src.includes(cryptoMiningDomains[j])) {
            console.log('Mining script detected: ' + src);
            // Block or alert the user
        }
    }
}
```

3. *Monitoring system resource usage:* Watch for abnormal system resource usage, such as high CPU and memory usage, which could indicate cryptocurrency mining activity.

Sample Python code to monitor CPU usage:

```python
import psutil

# Checking CPU usage
cpu_usage = psutil.cpu_percent(interval=1)  # interval in seconds
if cpu_usage > 70:  # Adjust this threshold as needed
    print("Abnormally high CPU usage. Suspicious activity detected.")
    # Action to stop or report suspicious activity
```

4. *Keeping software and operating systems up to date:* Ensure all your software, browsers, and operating systems are updated to benefit from the latest security patches.

5. *Using security tools and antivirus software:* Employ antivirus programs and security software to detect and remove malicious software, including cryptojackers.

- ***Instances of real-world cryptojacking:***

- *WatchDog focuses on Docker Engine API endpoints and Redis servers:* A simulated trap set up by the security research team at Cado Labs uncovered an intricate cryptojacking assault that specifically targets vulnerable Docker Engine API endpoints and Redis servers. This attack has the capacity to spread akin to a worm. The responsible party behind this assault is the

WatchDog attack group, notably prolific during late 2021 and 2022, orchestrating multiple cryptojacking campaigns.

- *Alibaba ECS instances targeted for cryptocurrency mining:* In late 2021, researchers at TrendMicro reported that TeamTNT, among others such as the Kinsig gang, were among the initial hacking groups to extensively transition their cryptojacking efforts toward cloud-based services. These groups conducted campaigns aimed at installing miners on Alibaba Elastic Computing Service (ECS) instances while actively disabling security features to avoid detection.

Also, in 2021 witnessed cryptojacking emerging as the third most prominent cybersecurity threat, as highlighted by the European Union Agency for Cybersecurity (ENISA). This underscored a notable and worrisome trend within the sphere of cyber threats.

In parallel, Google's Cybersecurity Action Team unveiled a significant discovery during the same year. They attributed a substantial 86% of compromised cloud platforms to incidents of cryptojacking. This revelation highlighted the extensive impact of cryptojacking, notably within cloud-based systems, emphasizing the pressing need for elevated security measures within cloud environments.

Adding to this, Cisco's 2020 disclosure revealed that a notable 69% of its customer base had been impacted by cryptomining malware. This statistic illuminated the widespread nature of the threat, affecting a considerable portion of Cisco's clients.

The collective evidence from these reports underscores the considerable prevalence and impact of both cryptojacking and cryptomining threats. This accentuates the urgent requirement for robust cybersecurity measures to counter these threats and safeguard digital systems, encompassing both cloud-based infrastructures and various user environments (TechTarget, 2022)

5. Results and Discussion

5.1 Practical results:

5.1.1 Vulnerability Severity and Trends:

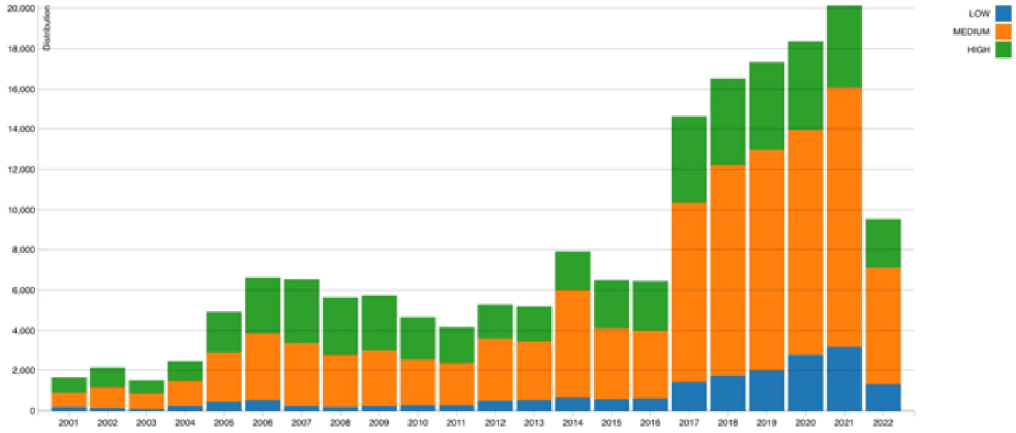


Figure 9: Vulnerability Severity Distribution over time (NVD, 2023)

The chart above illustrates the distribution of vulnerability severity reported to the National Vulnerability Database (NVD) from 2011 to 2022. It reveals a steady increase in the number of vulnerabilities reported from 2011 to 2016, followed by an exponential surge in 2017. This surge may be attributed to a more extensive cataloguing of software products in the NVD. Notably, the trend continues to show a consistent increase each year thereafter. This observation underscores the growing importance of addressing vulnerabilities in the cybersecurity landscape.

5.1.2 Cybercrime Landscape:

2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Figure 10: Phishing Attack Data (Kolesnikov, 2023)

In the ever-evolving landscape of cybersecurity, it is crucial to stay informed about the various cyber-attacks that threaten individuals and organizations. The impact of these attacks is substantial, both in terms of financial losses and reputation. The FBI's Internet Crime Report for 2022 revealed that the public reported a total of 800,944 cybercrime complaints. Phishing attacks were the number one crime type, with 300,497 complaints reported. The total losses due to phishing attacks exceeded $10.3 billion. Phishing attacks remain the most common cyber-attack, with approximately 3.4 billion daily spam emails. They encompass various deceptive techniques to trick individuals into revealing sensitive information or engaging in malicious activities through disguised emails or websites. Phishing attacks are responsible for 90% of data breaches. This is because phishers often assume the identity of a reliable and credible entity in electronic communications.

5.1.3 Government Commitment to Cybersecurity:

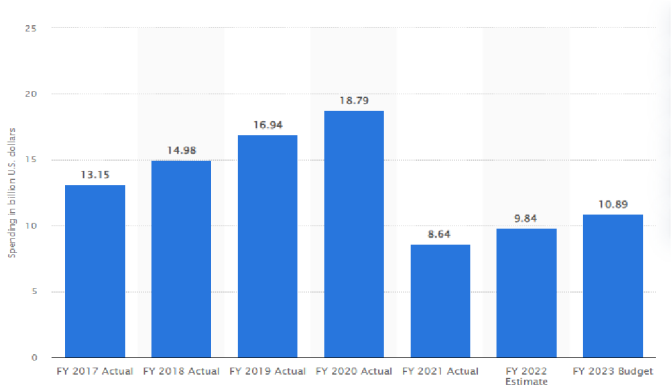


Figure 11: Proposed budget of the U.S. government for cyber security in FY 2017 to 2023 (in billion U.S. dollars) (Petrosyan, statista, 2022)

For the fiscal year 2023, the government of the United States proposed a 10.89 billion U.S. dollar budget for cybersecurity, representing an increase from the previous fiscal year. These federal resources for cybersecurity are set to support a broad-based cybersecurity strategy for securing the government and enhancing the security of critical infrastructure and essential technologies.

5.1.4 Impact of Cyber Attacks on Industry Sectors:

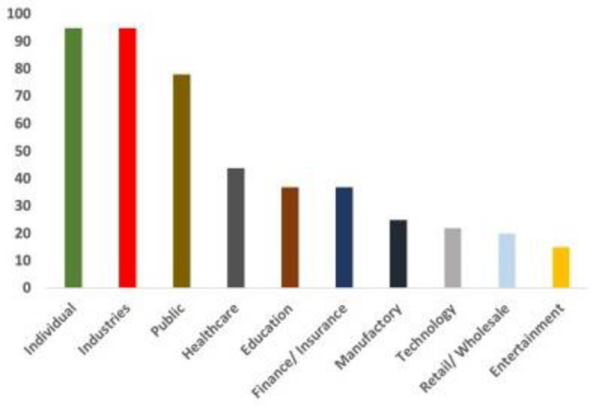


Figure 12: Top 10 targeted industry sectors in the first quarter of 2020 (B. Christiaan, 2020)

Comparing the first quarter results in 2020 and 2019, statistics show a 71% increase in mobile malware and 689% in PowerShell malware. For publicly disclosed incidents, Fig. 4 illustrates the top 10 sectors targeted in the first quarter of 2020. For example, attacks on the individual sector increased 59% compared to the same quarter in 2019. Malware attacks have a serious impact on the economy. In 2017, cybercrime cost 600 billion dollars in the USA alone, and increased by approximately 50% in 2018, and the financial damages exceeded 1 trillion USD.

5.1.5 Global Malware Threat Landscape:

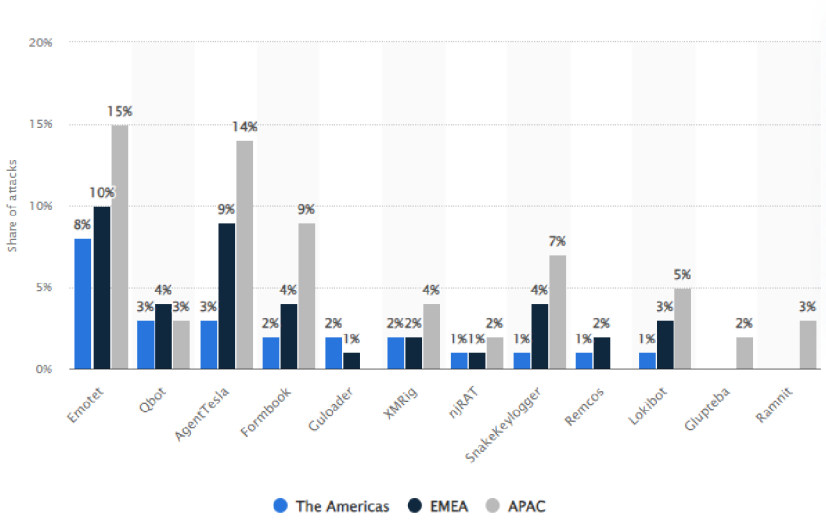


Figure 13: Most frequently detected malware threats in global regions in 2022, by type and region (Petrosyan, statista, 2023)

In 2022, the most prevalent malware threats to corporate networks across the globe were from the malware family Emote. This type of malware infection represented roughly 15 percent of all reported attacks in the Asia Pacific (APAC) region. The second-highest number of attacks across all regions came from the Agent Tesla malware family.

5.1.6 Ransomware Trends:

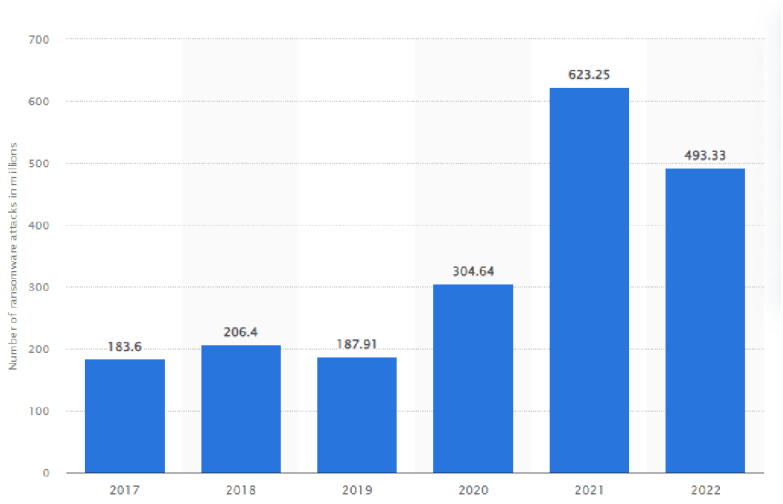


Figure 14: Most frequently detected malware threats in global regions in 2022, by type and region (Petrosyan, statista, 2023)

Figure 6 presents the annual number of ransomwares attempts globally from 2017 to 2022. It illustrates the escalating trend of ransomware incidents over this period. Ransomware attacks have seen a significant increase, representing a considerable threat to organizations worldwide. In the following sections, we will discuss and analyze the implications of these results in the context of our thesis objectives and the broader cybersecurity landscape.

5.2 Discussion:

The results presented in this chapter shed light on several critical aspects of the cybersecurity landscape, ranging from vulnerability trends to the economic impacts of cyber-attacks. These findings carry significant implications for our understanding of cybersecurity and the strategies required to safeguard individuals, organizations, and nations.

5.2.1 Vulnerability Severity and Trends:

The observed increase in vulnerability reporting is a clear indication of the expanding attack surface in the digital realm. The surge in 2017 suggests that as more software products are catalogued in the National Vulnerability Database (NVD), the number of reported vulnerabilities naturally rises. This underscores the importance of proactively addressing vulnerabilities. As the digital ecosystem continues to grow, it is crucial to remain vigilant and prepared for potential threats. Organizations must invest in robust vulnerability management and mitigation strategies.

5.2.2 Cybercrime Landscape:

The prevalence of phishing attacks, as indicated by the FBI's Internet Crime Report, highlights a disturbing trend. The financial losses and reputation damage associated with these attacks are substantial. The widespread use of deceptive techniques and social engineering in phishing attacks underscores the need for increased awareness and education among individuals and organizations. Enhanced email security measures and user training are essential components in mitigating the impact of phishing attacks. Furthermore, the fact that phishing attacks are responsible for 90% of data breaches emphasizes their central role in cybersecurity challenges.

5.2.3 Government Commitment to Cybersecurity:

The allocation of a substantial budget for cybersecurity by the U.S. government in fiscal year 2023 indicates the recognition of cybersecurity as a national priority. This budget increase signifies the government's commitment to securing critical infrastructure and emerging technologies. It is vital that governments worldwide prioritize and invest in cybersecurity to protect national security and economic interests.

5.2.4 Impact of Cyber Attacks on Industry Sectors:

The alarming increase in malware attacks, with a 71% rise in mobile malware and 689% in PowerShell malware, demonstrates the evolving tactics of cybercriminals. The financial repercussions of these attacks are staggering and growing year by year. Organizations must invest in robust cybersecurity measures to safeguard their operations and customer data. The increasing cost of cybercrime underlines the urgency for organizations to prioritize cybersecurity investments to mitigate financial losses and reputational damage.

5.2.5 Global Malware Threat Landscape:

The global malware threat landscape, characterized by the prevalence of Emote and Agent Tesla malware families, illustrates the complexity and diversity of cyber threats. These findings emphasize the need for organizations to maintain up-to-date threat intelligence and deploy advanced threat detection and prevention systems to counteract these evolving malware strains.

5.2.6 Ransomware Trends:

The steady increase in ransomware attempts highlights the persistence of this threat. Ransomware has emerged as a significant menace, causing financial and operational disruption worldwide. Organizations must adopt a multi-faceted approach to ransomware prevention, including robust backup and recovery strategies, employee training, and advanced threat detection.

In conclusion, the results presented in this chapter underscore the critical importance of cybersecurity in an increasingly interconnected and digital world. They provide valuable insights into the evolving threat landscape and serve as a call to action for individuals, organizations, and governments to prioritize cybersecurity measures and proactively address emerging vulnerabilities and cyber threats. It is imperative to continuously adapt and fortify our cybersecurity strategies to safeguard our digital assets and protect against the ever-present and evolving threat of cybercrime.

6. Conclusion

Throughout this thesis, the complex interactions between internet crimes, human behaviour, and security protocols have been explored, with a focus on the importance of cybersecurity for protecting society. Nevertheless, it has been emphasized that cybersecurity should not be associated only with companies and governments but should also include individuals, as they are the main victims.

In the face of increasing internet crimes and ongoing struggles, a question has been raised about whether we are truly heading in the right direction to reduce the impacts of internet crimes or if we are seeking to profit from them. The importance of addressing the main vulnerability, which is individuals, has been confirmed. Cybersecurity should be comprehensive and include all segments of society, not just limited to companies and governments.

For example, a working man uses secured devices (laptop and mobile phone) with protection applications from his company, but his personal mobile phone gets hacked, causing data leakage during a company meeting or through devices at home. This shows that violations are not limited to direct communication but may involve third parties, as seen in the case of Target in 2013.

Therefore, we need to work on securing everyone. Efforts to combat internet crimes must be shifted from users to cybersecurity companies and governments. This cannot be achieved without effective government involvement. We have launched some recommendations to enhance the level of security by integrating cybersecurity concepts into school curricula, a vital step towards raising awareness among students and empowering them to face internet challenges. Encouraging the simplification of internet security concepts and promoting digital resilience through the use of strong passwords and avoiding open networks are crucial. On the other hand, the government's role in securing cyberspace has been highlighted through its active participation in protecting citizens from internet crimes and providing free government applications for financially limited individuals. Enhancing cybersecurity through mandatory subscription at reasonable costs strengthens overall security levels. Emphasis must be placed on adopting international laws to combat internet crimes to ensure international cooperation in facing digital challenges. In the industrial field, governments issue strict cybersecurity standards covering both local and imported companies, aiming to enhance security and prevent internal breaches. Internet service providers are encouraged to provide firewall applications to their customers, considering the firewall as an essential part of digital services.

Finally, today's world is a digital one, with our focus shifting more towards digital aspects than physical ones. Given this transformation, it is anticipated that most crimes will have a digital nature. We hope that cybersecurity becomes more than just a solution for companies but a broadly understood concept in our society. We can dream of creating a world where internet crimes are significantly reduced, although achieving a world completely free from them may be impossible.

References

Ankit Fadia, M. N. (2020, semptember 16). *Follow the leaders: How governments can combat intensifying cybersecurity risks.*

B. Christiaan, D. T.-R.-M. (2020, september 23). Retrieved from sciencedirect: https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html

checkpoint. (2023). *Cybersecurity Challenges for Governments in 2023.* Retrieved from https://www.checkpoint.com/about-us/contact-us/

Damien Van Puyvelde, a. A. (2019). *Cybersecurity : Politics, Governance and Conflict in Cyberspace.* cambridge: Polity Press.

Grimes, R. A. (2017). *Hacking the Hacker : Learn from the Experts Who Take down Hackers.* Indiana: John Wiley & Sons, Incorporated.

Kolesnikov, N. (2023, August 30). Retrieved from techopedia: https://www.techopedia.com/cybersecurity-statistics

Moeller, R. R. (2016). *Brink's Modern Internal Auditing : A Common Body of Knowledge.* USA: John Wiley & Sons, Incorporated.

Nelson, T. M. (2021). *The assessment that a major cyberattack poses a threat to financial stability is axiomatic—not a question of if, but when.*

Nitul Dutta, N. J. (2022). *Cyber Security: Issues and Current Trends.* Singapore: Springer.

NVD. (2023, september). Retrieved from NIST: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

Ozkaya, D. E. (2019). *Cybersecurity: The Beginner's Guide* . Mumbai: Packt Publishing.

Petrosyan, A. (2022, september 12). Retrieved from statista: https://www.statista.com/statistics/675399/us-government-spending-cyber-security/

Petrosyan, A. (2023, April 5). *statista*. Retrieved from Most prevalent malware 2022, by type and region: https://www.statista.com/statistics/1238995/top-malware-threats-by-type-region/

Rigby, Y. (2019). *The Cyber Security.* uk: Cybok.

Robert Johnson, I. P. (2019, Jan 2). *cybercrime MAGAZINE.* Retrieved from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Scott Donaldson, C. W. (2018). *Understanding Security Issues.* Berlin: DEG Press. Retrieved from https://ebookcentral.proquest.com/lib/techlib-ebooks/detail.action?docID=5157542.

Stock, J. (2021). *Guide sur la stratégienationale de lutte contre la cybercriminalité.*

List of figures

Figure 1:Replica of Claude Chappe's optical telegraph on the Litermont near Nalbach, Germany (Photo by Lokilech CC BY-SA 3.0) (Ozkaya, 2019) 15

Figure 2: Malware evolves to become more sophisticated and destructive. (Scott Donaldson, 2018) 18

Figure 3: Data Security Concepts (Moeller, 2016) 23

Figure 4: Firewall Diagram (Moeller, 2016) 24

Figure 5: Manipulating the token session executing the session hijacking attack. 44

Figure 6: The Experience Before the Impact: A Prelude to the Attack 56

Figure 7: The Experience after the Impact: A Prelude to the Attack 57

Figure 8: How cryptojacking works (techtarget, 2022) 60

Figure 9: Vulnerability Severity Distribution over time (NVD, 2023) 64

Figure 10: Phishing Attack Data (Kolesnikov, 2023) 65

Figure 11: Proposed budget of the U.S. government for cyber security in FY 2017 to 2023 (in billion U.S. dollars) (Petrosyan, statista, 2022) 66

Figure 12: Top 10 targeted industry sectors in the first quarter of 2020 (B. Christiaan, 2020) 66

Figure 13: Most frequently detected malware threats in global regions in 2022, by type and region (Petrosyan, statista, 2023) 67

Figure 14: Most frequently detected malware threats in global regions in 2022, by type and region (Petrosyan, statista, 2023) 67

Bibliography

Ankit Fadia, M. N. (2020, semptember 16). *Follow the leaders: How governments can combat intensifying cybersecurity risks.*

B. Christiaan, D. T.-R.-M. (2020, september 23). Retrieved from sciencedirect: https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html

checkpoint. (2023). *Cybersecurity Challenges for Governments in 2023.* Retrieved from https://www.checkpoint.com/about-us/contact-us/

Damien Van Puyvelde, a. A. (2019). *Cybersecurity : Politics, Governance and Conflict in Cyberspace.* cambridge: Polity Press.

Grimes, R. A. (2017). *Hacking the Hacker : Learn from the Experts Who Take down Hackers.* Indiana: John Wiley & Sons, Incorporated.

Kolesnikov, N. (2023, August 30). Retrieved from techopedia: https://www.techopedia.com/cybersecurity-statistics

Moeller, R. R. (2016). *Brink's Modern Internal Auditing : A Common Body of Knowledge.* USA: John Wiley & Sons, Incorporated.

Nelson, T. M. (2021). *The assessment that a major cyberattack poses a threat to financial stability is axiomatic—not a question of if, but when.*

Nitul Dutta, N. J. (2022). *Cyber Security: Issues and Current Trends.* Singapore: Springer.

NVD. (2023, september). Retrieved from NIST: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

Ozkaya, D. E. (2019). *Cybersecurity: The Beginner's Guide* . Mumbai: Packt Publishing.

Petrosyan, A. (2022, september 12). Retrieved from statista: shttps://www.statista.com/statistics/675399/us-government-spending-cyber-security/

Petrosyan, A. (2023, April 5). *statista*. Retrieved from Most prevalent malware 2022, by type and region: https://www.statista.com/statistics/1238995/top-malware-threats-by-type-region/

Rigby, Y. (2019). *The Cyber Security.* uk: Cybok.

Robert Johnson, I. P. (2019, Jan 2). *cybercrime MAGAZINE.* Retrieved from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Scott Donaldson, C. W. (2018). *Understanding Security Issues.* Berlin: DEG Press. Retrieved from https://ebookcentral.proquest.com/lib/techlib-ebooks/detail.action?docID=5157542.

Stock, J. (2021). *Guide sur la stratégienationale de lutte contre la cybercriminalité.*