Privacy, safety, and security

Șova Dumitru Ștefan Andrei

dumitru.sova01@e-uvt.ro

15.05.2023

Abstract

In today's world, we are more and more affected by changes in technology, which often leads to a new way of interacting with the world and people around us. The effects of these innovations are in most cases beneficial to us and our society, whether it is the emergence of vehicles that allow us to travel great distances in a short time, or the age of the Internet that has revolutionized the way we share information and communicate with each other. However, progress always has side effects, some of which unfortunately bring new problems that we have to deal with. One such issue is security, privacy, and the safety of our activities in online spaces. This report will look at the broad spectrum of this problem and provide some examples of security risks that the average citizen may face, as well as some solutions, mainly in the form of some already known algorithms. The report will also highlight some new problems that may arise in the online space.

Chapter 1

Introduction

1.1 Selected Titles and Authors

- Brij B. Gupta, Dharma P. Agrawal, Haoxiang Wang, *Computer and cyber security: principles, algorithm, applications, and perspectives.*

- DS Abd Elminaam, HM Abdual-Kader, MM Hadhoud *ANALYSIS AND DESIGN OF SYMMETRIC ENCRYPTION ALGORITHMS.*

1.2 Additional Resources

This paper will also look at other resources, mainly research papers, for a more in-depth look at this problem, those being:

- Michael M. Losavio and Adel S. Elmaghraby, *Cyber security challenges in Smart Cities: Safety, security, and privacy.*

- Douglas Selent, *ADVANCED ENCRYPTION STANDARD* .

- Deris Stiawan, Abdul Hanan Abdullah, Mohd. Yazid Idris, *Characterizing Network Intrusion Prevention System* .

- DS Abd Elminaam, HM Abdual-Kader, MM Hadhoud *ANALYSIS AND DESIGN OF SYMMETRIC ENCRYPTION ALGORITHMS.*

- Spyros Kokolakis, *Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon.*

- Alan F. Westin, *Privacy And Freedom* .

- Siani Pearson, *Privacy, Security and Trust in Cloud Computing.*

- Helen Nissenbaum, *Privacy in Context Technology, Policy, and the Integrity of Social Life.*

1.3 Motivation

The problem of cybersecurity is present in everyone's lives and combined with the emergence of new ways to violate people's privacy, I believe a good understanding of cybersecurity is important. The world of online security is fascinating, not only because it is a new problem that people have never faced before, but also because of the methods and algorithms that people use to protect their privacy and security.

It is a sad truth that nowadays people can access private information about others with a single click. Whereas in the past we had to either befriend someone to find out what they like, where they are from, etc., today most people can access sensitive information with a simple click, meaning information such as where they live, where they work, where they go to school, their hobbies, relationship status, etc. can be viewed by almost anyone. And these are just superficial problems. Hackers can and will steal credit card information, precise locations, and personal data that is not just on a person's Facebook page, passwords, and accounts. Some figures put the damage caused by cybersecurity threats and hacks at 400 billion dollars worldwide, and in the future, those figures will rise to as much as 10.5 trillion dollars annually worldwide.

To combat such problems, I think we have some options:

1. We abandon the use of the Internet as a whole. This is the most extreme scenario, but I believe that for some people, disconnecting from the Internet altogether could actually prove beneficial in getting back in touch with nature and with themselves.

2. We are developing countermeasures for such problems as the ones we will discuss in this paper, namely algorithms for cybersecurity. In addition to these algorithms, we will later discuss a possible solution in machine learning. Some examples of cybersecurity algorithms are (see [2]):

- Symmetric encryption algorithms: Symmetric encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) use a single key for both encryption and decryption.

- Asymmetric encryption algorithms: Asymmetric encryption techniques use two keys: a public key for encryption and a private key for decryption. These algorithms are also known as public-key cryptography. RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are some examples.

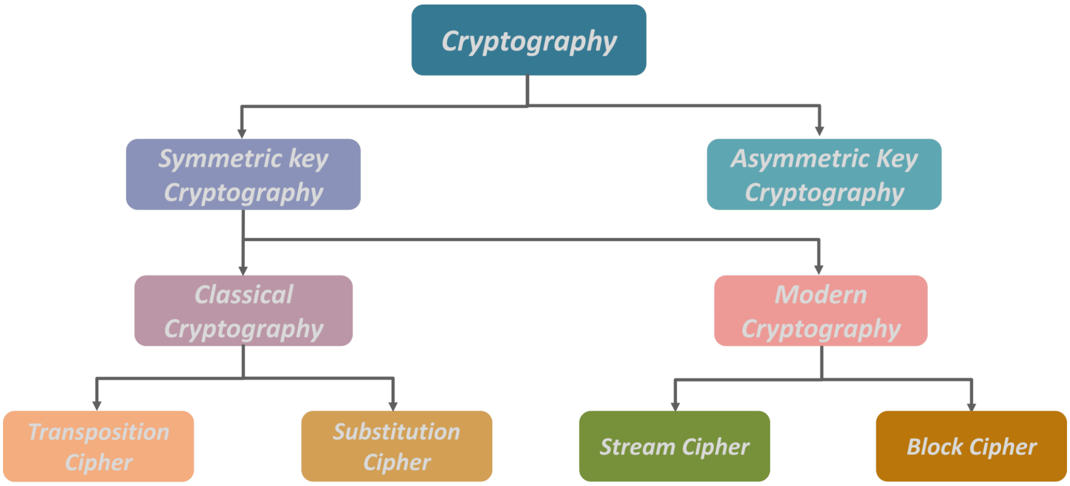
- hash functions: These algorithms take an arbitrary size of input data and produce a fixed-size output (hash). They are commonly used for data integrity checks, digital signatures, and password storage. The hash algorithms MD5, SHA -1, SHA -256, and HMAC are widely used.

- Digital signature algorithms: guarantee the validity and integrity of digital messages and documents. They use the private key to create a unique signature that can be validated with the associated public key. Two examples are the Digital Signature Algorithm (DSA) and RSA-based signatures.

- Intrusion Detection Algorithms: To detect possible security breaches or malicious activity, these algorithms examine network traffic or system logs. They can use methods such as machine learning, data mining, or statistical analysis and can be rule-based or anomaly-based.

- Firewall Algorithms: To enforce network security standards and manage inbound and outbound network traffic, firewalls use a variety of algorithms. Access control lists (ACLs), stateful packet inspection (SPI), network address translation (NAT), and proxy servers are some of these algorithms.
- Intrusion Prevention Algorithms: Intrusion prevention systems (IPS) integrate intrusion detection and prevention functions by actively preventing or reducing detected threats. These algorithms use methods such as anomaly detection, behavioral analysis, and signature-based detection.

We will discuss in detail symmetric encryption algorithms and intrusion prevention algorithms.



Chapter 2

Cybersecurity Concepts

Before we look at the various security algorithms, we must first discuss some basic concepts. From reading [2], we can derive the following basic concepts of cybersecurity:

Cybersecurity can be described as the inclusion and prevention of unauthorized access, damage, and theft of computer systems, networks, and data. Threats such as malware, hacking, and social engineering attempts are all covered. Access controls, encryption, firewalls, and patching are examples of security mechanisms. Risk management identifies vulnerabilities and develops incident-handling procedures. Security policies establish appropriate behavior and user privileges. Users are made aware of secure activities through security awareness. VPNs are used for device and network security. Audits and secure coding are part of application security. Security incident response plans include detection, mitigation, and recovery. Emerging cybersecurity technologies such as cloud security and AI are critical.

Therefore, we can describe cybersecurity as a complex issue that requires a multilayered strategy combining technical and human-centric approaches. Protecting digital assets, security, and privacy is a continuous process that requires constant monitoring, adaptability, and collaboration among the groups affected by these incidents.

It is important to understand these fundamental concepts of cybersecurity, as they provide us with a starting point from which to enhance our privacy and protect ourselves and our loved ones from potential threats.

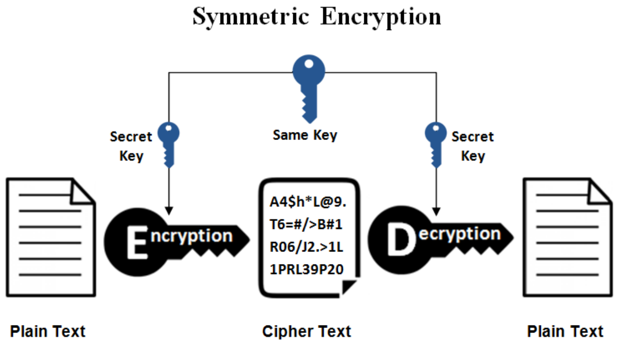
In the next few chapters, we will look at some of the algorithms listed in Chapter 1, some basic concepts about them, their effectiveness, and other applications for security and privacy.

Chapter 3

Algorithms

We will now examine some of the algorithms listed, as well as some other applications and areas where cybersecurity is important.

3.1 Symmetric Encryption Algorithms



From the work of DS Abd Elminaam (see [1]), some key points about protecting online and digital information can be derived, namely that protecting digital information usually involves two separate aspects: maintaining confidentiality to prevent unauthorized disclosure of information and ensuring authentication to verify that messages received are from the intended sender and haven't been tampered with during transmission.

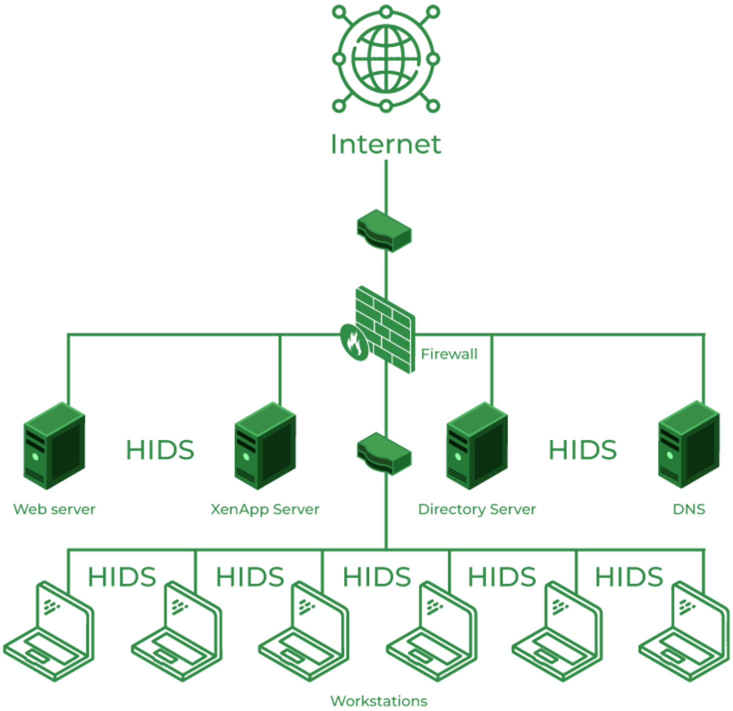
Symmetric cryptography uses a shared secret key to modify the message so that it cannot be retrieved without that key to ensure confidentiality. Symmetric encryption is the name given to this conversion process. Depending on how they handle the message, ciphers, i.e. algorithms for symmetric encryption, can be divided into two main groups: Block ciphers and stream ciphers.

Again (see [1]), we can deduce that an encryption algorithm is designed with the goal of ensuring the confidentiality of messages transmitted over an insecure channel. [1] also tells us that an ordinary encryption algorithm consists of two mathematical operations: an encryption function (E) and a corresponding decryption function (D = E(-1)). The sender (sometimes referred to as Alice) encrypts the original message P (plaintext) before converting it to an encrypted text C = E(P) and sending it over the insecure channel to ensure secure communication. The intended recipient (Bob) determines D(C) = P after receiving C and recovering the plaintext.

An important conclusion that [1] draws is that linear cryptanalysis, a technique used in the study of cryptography to study and decrypt block ciphers and other cryptographic algorithms, is an important and valuable analysis technique in the field of symmetric cryptography. The main point of cryptanalysis and the reason why it's so important is that it helps to identify vulnerabilities, evaluate the security of algorithms, and guide the design and evolution of algorithms. It increases the overall performance of algorithms, enables the potential recovery of secret keys, and ensures a higher level of security.

One algorithm that stood out to me among the group of symmetric algorithms was AES (Advanced Encryption Standard), which [1] calls "the most well-known block cipher based on an SP network." For more information about AES and an example of its implementation, I recommend reading [9], as his article describes both the history and the operation of the algorithm in more detail.

3.2 Intrusion Prevention Algorithms



Another set of algorithms for security is intrusion prevention. According to [10], an IPS (Intrusion Prevention Algorithm) can be described as a real-time product designed to detect and stop malicious network activity. IPS provides a proactive strategy for network defense by combining the methods of firewalls (which operate at multiple levels such as data link, network, transport, and application) and intrusion detection systems (IDS). To prevent attacks on the network, records, and behavior patterns are checked using pattern recognition sensors. The IPS blocks malicious data as soon as an attack is detected and logs relevant data for further investigation.

There are several approaches to this algorithm, namely:

- signature-based detection: this method compares network traffic patterns or other data against a database of recognized attack signatures. If a match is found, the IPS intervenes to stop or mitigate the attack.

- Monitoring network behavior and comparing it to typical or expected patterns are called anomaly-based detection. Any deviation from the usual is considered a potential attack and the necessary action is taken.

- Heuristics-based detection: in heuristics-based detection, predetermined rules and algorithms are used to detect irregular patterns or actions that could be signs of an attack. Based on these characteristics, IPS is able to detect new or undetected attacks.

- Traffic Analysis: to find malicious patterns, strange data streams, or suspicious activities, IPS performs deep packet inspection and analyzes network traffic. Based on network protocols, traffic volumes, and other traffic-related factors, attacks can be detected and stopped.

- Proactive Defense: Using methods such as packet filtering, protocol validation, rate limiting, and session termination, IPS can actively defend against attacks. Attacks must be stopped or mitigated by preventive measures before they can do any damage.

In short, an IPS helps maintain an overall secure and private network environment by detecting and stopping attacks, reducing vulnerabilities, enforcing privacy laws, and providing proactive incident response. It improves the overall security posture and helps protect confidential data from unauthorized access or disclosure.

These algorithms play a critical role in ensuring security and privacy in our network environments. They prevent threats, mitigate vulnerabilities, enforce privacy policies, and enable proactive incident response.

The applications of these algorithms are deeply rooted in our online lives, from privacy to social security. In the following chapter, we will look at these applications, how privacy relates to our freedom, and how this security is being challenged in today's society.

We will also focus on future problems and possible solutions, and how we might be affected by these new challenges.

Chapter 4

Cybersecurity and social life

We have already discussed some reasons why cybersecurity is very important to our social life. From strangers being able to learn a lot about a person by looking at their social profiles (as a quick side note, there are ways to keep your account private, but the vast majority of people leave their accounts public so that anyone can see their profile), to hackers getting into a person's computer and stealing all of their data, I think privacy has taken a bit of a back seat these days like it used to. We could also discuss other ways that companies or the government invade our privacy without us knowing about it, such as how companies like Google can register what a user likes and then show them ads for products that fall into our area of interest (it's not that important, but many people do not realize that, and companies like Google store a whole lot of information about their users).

A big concern people have is how cybersecurity can impact our freedom and how it can help us in our future society, such as how cybersecurity will be implemented in smart cities from now on.

4.1 Our approach to privacy online

It would be unfair to not take into consideration the advancements that were made in the field of cybersecurity and to have at all times a judgemental and doubtful outlook on the current situation of online privacy. However, there is always a risk that something will go wrong, be it a human error, or a successful breach in our firewalls. So, how should one approach this behemoth of an undertaking, it can always feel daunting and disheartening to not know what to do in regard to our safety and well-being. A solution in my opinion is a fundamental change in how we approach what we do online.

There are many ways to reduce the possibility of a privacy breach, for example by using a VPN, or when searching for something, using Incognito Mode. Such examples work well enough, but there are also possible attacks that seem inoffensive at first. As an example, nowadays people can fall prey easily to fake emails forwarded by their "boss" and corrupt their entire organization. Other such events can happen to someone at home or when someone accesses a shady site that he wasn't sure if it was dangerous to enter.

Overall the approach that we have to our online privacy can determine how much will be lost and how we will manage to keep ourselves safe.

4.2 Surveillance and smart cities

The following section was inspired by [8] and [3].

We will discuss a less known issue, but I think one that will become more and more serious in the online space, and that is the problem of surveillance. Although beneficial in combating crime, surveillance could pose a problem if it's made public. For example, there are many cities that have public cameras which anyone can enter and watch live feeds. Not only that but there is a small probability that in cities with more cameras, someone might access them and watch what happens at all times. Now everyone's daily routine can be watched by someone without them knowing, the dangers of it becoming more apparent the more we look into it. I don't think that surveillance cameras are bad, but we can't overlook the new dangers to our privacy and safety.

Other issues that our new, smart cities face include the automation of certain services. Take for example a simple ATM, people used certain tricks with the help of ATMs to steal from people their credit card information. Other problems for our privacy could include police drones or the digitization of services that could lead to scams.

4.3 Machine learning as a solution

The last point that we will focus on is the question of tomorrow. What will happen in the next 50 years? Will we again, get access to new technologies as the people born in the '70s, during the '2000s had to face a problem never before seen, keeping their privacy safe not only from the physical life, but also the online one? There are many such problems that I think will arrive in the future in regard to our privacy. Take for example how today by giving simple instructions, anyone can make a realistic human by using AI, that sometimes looks indistinguishable from a real one. Not only that but AI deep fake voices have begun to also make a big appearance, which in my opinion can create even more problems. Take for example someone that makes a false testimony while using someone's voice without their consent. How will future cybersecurity detect if the voice recording/ video shown is real or fake? This is I feel a problem that the next generations will have to deal with, as we had with the problems that arrived with the birth of the internet.

The silver lining in all of this could be from machine learning. We could develop in the future AIs that could detect if an image, video, or voice recording is generated or not, either by searching for artifacts in the making of the video, searching for any subtle differences in the voice of a recording, or looking for references that an AI might have used to create the fake images. These problems are just now starting to make their appearance, so new solutions need to be implemented fast.

Chapter 5

Conclusion, Related work

5.1 Related work

Some other reads that I recommend are [4] which delves more into a not so cybersecurity focused thought experiment, reviewing if people really care about their privacy and showcasing more abstract ways of thinking, and the other related work that I found interesting includes privacy and trust in Cloud Computing(see [5]),

5.2 Conclusions

I feel deep appreciation for today's world and the systems that we are using right now, but I do feel that as time goes on unfortunately, our privacy and security might get more and more difficult to keep in the evolving state of the internet. For current problems, I do still feel that the current countermeasures are good enough(for example the algorithms discussed), but as mentioned previously, the future could bring some not-so-desirable side effects again.

Bibliography

[1] DS Abd Elminaam, HM Abdual-Kader, MM Hadhoud *ANALYSIS AND DESIGN OF SYMMETRIC ENCRYPTION ALGORITHMS.*

[2] Brij B. Gupta, Dharma P. Agrawal, Haoxiang Wang, *Computer and cyber security: principles, algorithm, applications, and perspectives.*

[3] Michael M. Losavio and Adel S. Elmaghraby, *Cyber security challenges in Smart Cities: Safety, security, and privacy.*

[4] Spyros Kokolakis, *Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon.*

[5] Siani Pearson, *Privacy, Security and Trust in Cloud Computing.*

[6] Helen Nissenbaum, *Privacy in Context Technology, Policy, and the Integrity of Social Life.*

[7] NZ Jhanjhi, Mamoona Humayun2, and Saleh N. Almuayqil, *Cyber Security and Privacy Issues in Industrial Internet of Things.*

[8] Alan F. Westin, *Privacy And Freedom* .

[9] Douglas Selent, *ADVANCED ENCRYPTION STANDARD* .

[10] Deris Stiawan, Abdul Hanan Abdullah, Mohd. Yazid Idris, *Characterizing Network Intrusion Prevention System* .