A Guide on Cyber Security

Jugersa Smaja | Fabian Brackhane – Institute for Security and Safety GmbH

Co-funded by the
Erasmus+ Programme
of the European Union

Contents

Co-funded by the Erasmus+ Programme of the European Union

1. Introduction to Cyber Security: Threats, Vulnerabilities and Attacks

This chapter will give an insight of Cyber Security and some of its main elements such as threats, vulnerabilities and attacks.

1.1 Why do we need Cyber security?

As the digital age arises, day after day we are preparing ourselves to ‚cope' with the rapid development of technology. Every device around us, is slowly becoming a living thing: It is being named (assigned an IP), it is growing and developing (getting more and more features), and just like humans, these devices are being connected to each other.

The purpose of their use highly depends on the user: Do you want to make use for good or bad? You decide.

Directly related to this decision is the field of cyber security. As we cannot assure the intent of use of the technological devices, it is better to be prepared and secured.

Many people tend to neglect the measurements of security, not knowing the potential dangers this may cause. One of the main aims of this project is to start making a change on this perspective, to make the future generation capable and aware of the dangers that come from the lack of cyber security measures.

In order to make this possible, the following guide will assist the facilitators and trainers to focus on the main aspects of cyber and digital security. These aspects will set the scope of the knowledge needed to grasp on the C4S platform.

1.2 A short history of Cyber Security

The history of cyber security is inextricably linked to the history of the Internet. The problem area of cyber security exists exclusively with interconnected devices. The Internet is essentially nothing other than a computer network of inconceivable size. Since it has become an everyday part of our lives (i.e. after 2000), systematic and coordinated protective measures against intentional and unintentional destructive actions have played a central role.

Co-funded by the Erasmus+ Programme of the European Union

2. Common Terminology

2.1 Cyber Security vs. Digital Security – A definition

Both terms overlap in meaning. Therefore, the context in which they are used is always important.

Cyber Security is defined as a process designed to protect devices, networks or critical systems from threats and possible attacks[1]. In their context, a number of central concepts are encountered, which we will define in the following chapter.

The term Digital Security refers to various ways of protecting a computer's internet account and files from intrusion by an outside user.

2.2 Network

A set of computers sharing resources located on or provided by network nodes. The interconnections of these computers are made up of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods.

2.3 Virtual Machines

The virtualization/emulation of a computer system. Virtual machines are based on computer architectures and provide the functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

2.4 Vulnerability

Vulnerabilities are gaps or system weaknesses that make the threats possible and tempt the threat actors to exploit them. There are existing vulnerabilities regarding different cyber security domains, which get registered by the MITRE Corporation as CVE (Common Vulnerability Exposure) and get assigned a score called CVSS (Common Vulnerability Scoring System) in order to reflect its potential risks[2]. For example, some network security vulnerabilities include XSS (Cross Site Scripting), misconfigurations, SQL Injections, etc[3]. These terms will be explained in the following chapters.

2.5 Cyber Threat

Cyber Threats are described as security circumstances or incidents that could possibly have a negative impact on the network or system. Some of these threat examples include phishing attacks, installation of malwares, possible data breach, etc., which will later be discussed in this chapter.

[1] https://www.ibm.com/topics/cybersecurity

[2] https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

[3] https://www.trustnetinc.com/threats-and-vulnerabilities/

Co-funded by the Erasmus+ Programme of the European Union

2.6 CIA triad

The **CIA triad** (stands for: Confidentiality, Integrity and Availability) is a very respected model that forms the basis for the development of security systems and policies, as it differentiates and guides security teams to pinpoint the ways of addressing concerns.

When all three standards of Confidentiality, Integrity and Availability have been met, ideally the security profile is better prepared and equipped to handle threat incidents[4]:

	**Confidentiality:** Data is accessed only by the authorized parties
	**Integrity**: Data is altered/added/removed only by authorized users
	**Availability**: Data, systems and functions are accessible on-demand according to agreed-upon parameters

[4] https://www.fortinet.com/resources/cyberglossary/cia-triad

Co-funded by the Erasmus+ Programme of the European Union

3. Attack types

A cyberattack consists of a malicious and deliberate attempt of attackers to breach the information system of another (attacking either one of the CIA goals), usually seeking various types of benefits including:

- Achieving Financial Gains (through the: Misuse of Data, Blackmail, Selling the Data, etc.)
- Political Reasons (through the: Stealing of classified data, Interfering with elections/economy, Political Espionage)
- Commercial (products espionage, hurting competitors)
- Proving beliefs (Hacktivism)
- Taking Revenge
- Curiosity/Desire to learn/Hacking for fun

There are different ways that the maliciously intended users, threat actors, or as we simply call them- Hackers, can get to our system. The major routes include[5]:

	**Programming-based Hacking:** The hacker uses the route of finding and exploiting present vulnerabilities inside the system.
	**Physical Access**: The easiest way to get to a system is by having physical access to it.
	**Social Engineering:** Less technical than the above, the art of social engineering consists of numerous ways to psychologically trick or lure the user into performing actions or divulging confidential information[6].

3.1 Physical access

Anyone who has access to a computer or computer system can use it. For good or for bad. A computer should not be freely accessible any more than sensitive documents on paper.

Physical hacking usually opens up a variety of malicious actions a hacker can perform. Some examples include: walking in to a building without a proper authorization, sneaking in, breaking into a facility and stealing sensitive data.

[5] https://www.security.org/digital-safety/

[6] https://en.wikipedia.org/wiki/Social_engineering_(security)

Co-funded by the Erasmus+ Programme of the European Union

3.2 Virtual access: Hacking

In the field of computer security, a system is considered hacked when a security mechanism has been broken or bypassed, with the hack being the action used to achieve the goal. Hacking does not necessarily have to be done with evil intentions. Hacking can also be done to achieve function enhancements or problem solving, or to achieve a goal in an unusual way.

3.2.1 The question of colour: Black, White and Grey Hats

The attackers (**Hackers**) are usually divided into three categories depending on their intent, just as shown on the table below:

 **Black Hat:** A criminal who breaks into computers with malicious intent.	 **White Hat:** Cybersecurity experts which are authorized to hack systems in order to find vulnerabilities.	 **Grey Hat:** Hackers standing in between Black and White. They might engage in non-ethical hacking of the systems, however they usually do not have a malicious intent.

There are of course other categories of Hackers, however Black, White and Grey Hat remain the "classical ones"[7].

3.2.2 Malware

The most preferred and common type of attack is **Malware.**

Malware is an umbrella term used to describe malicious software that gets into the systems, including: Ransomware, Trojans, Worms, Logic Bombs, Spyware, Backdoors, etc. They are designed to do something damaging, depending on the type. The definition for these malware types is shown in the table below:

 **Ransomware:** Malware designed to block the access to a system (through the encryption of the data) until a certain amount of money is paid. **Examples: NotPetya, SamSam, Maze, WannaCry, Locky, GrandCrab, etc.**	 **Trojans:** Maliciously designed malware that gets access to a system by appearing as harmless. **Fun Fact: The name is derived from the infamous Trojan Horse from Ancient Greece that led to the fall of Troy.**

[7] https://www.pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for/

Co-funded by the Erasmus+ Programme of the European Union

 **Worms:** A standalone malware that replicates itself in order to spread to other computers by using different means. **Fun Fact: The first computer worm was devised to be an Anti-Virus software.**	 **Logic Bomb:** A malicious piece of code inserted into a software which sets off harmful actions if certain condition are met. **Fact: Viruses and Worms may contain Logic Bombs in order to spread unnoticed.**
 **Spyware:** Malware designed to gather your personal computer data and forward it to a third-party without consent. **Fact: Data compromised include Login Credentials, PINs, Credit Card details, Browsing Habits, etc.**	 **Backdoor:** A means to access the computer system or encrypted data that bypasses the security mechanisms. **Fun Fact: The infamous SolarWinds attack was assisted by a backdoor installed on the code of the company's software. It remained undetected for a long time.**

3.2.3 Application and Network attacks

This section will cover the common attacks targeted at applications and networks.

Applications are a very attractive target for the attackers as their number of vulnerabilities is increasing. More than 80% of the developers claim that the average application has more than 10 vulnerabilities[8].

OWASP (Open Web Application Security Project) is a worldwide organisation focusing on the security of the applications. A list called OWASP Top 10 is prepared by them in order to communicate the most common risks. Some of the most dangerous ones topping this list are shown below[9]:

 **Broken Access Control:** Access control enforces a certain policy for users to act a certain way and not act outside the intended permissions. Failures can lead to: modifications,	 **Cryptographic Failures:** A lack or failures regarding the cryptography leads to the exposure of the sensitive data such as passwords, credit card details, etc.

[8] https://www.contrastsecurity.com/knowledge-hub/glossary/application-attacks

[9] https://owasp.org/www-project-top-ten/

Co-funded by the Erasmus+ Programme of the European Union

destruction of data or unauthorized information disclosure, etc.	
 **Injection:** Injection happens when the attacker provides malicious inputs to a web application and affecting the normal operation of it. It forces the application to execute malicious commands.	 **Insecure Design:** This category covers all the missing or ineffective control designs that represent weaknesses.

Network attacks, on the other hand, represent attempts to gain unauthorized access to a network in order to perform malicious activity. These attacks are in fact categorized in two types: active and passive. While active attacks involve parties' attempts to modify, encrypt or damage the data, the passive mode is limited to only monitoring and stealing the data on the network without making any alterations. Some of the most common network attacks are shown on the table below:

 **DDoS (Distributed Denial-Of-Service):** This type of attack is an attempt to disrupt the normal traffic of a network by overwhelming it (or its infrastructure) with a flood of internet traffic[10]. **Fun fact:** It can be compared to an unexpected traffic jam in the highway that prevents the cars from getting to their expected destination.	 **Man-in-the-Middle:** The hacker intercepts the data traffic in the communication. The hacker monitors the data being transferred from one point to another, and can as well steal or modify it on the fly.
 **Unauthorized access:** This is an umbrella term to describe the attempts of a hacker to gain entry into a computer system without having permission. There are endless ways to do this, including social engineering techniques, exploiting existing network vulnerabilities, etc.	 **Insider Threats:** This is a security risk involving current or past employees of a targeted organization who already have access to sensitive information (or have privileged accounts) within the network and choose to misuse this access.

[10] https://www.cloudflare.com/en-ca/learning/ddos/what-is-a-ddos-attack/

Co-funded by the Erasmus+ Programme of the European Union

Fact: Amongst the causes of unauthorized access are the lacking protection against social engineering, insider threats or weak passwords.	

3.3 Social engineering

It is very important to be aware of the most common existing social engineering techniques that hackers use, in order to prevent your system from being attacked. Some of these techniques can be found in the table below:

 **Phishing:** Sending malicious email containing dangerous links or attachments pretending to be a legitimate person or business. **Example**: Fake email from your "boss" asking you to download a (malicious) file.	 **Baiting:** The use of bait through online or package delivery in a form of CD/USB stick. **Contains malicious programs – malware.** **Example:** You found a random USB stick in the parking lot, stick it to your laptop and malware gets installed.
 **Tailgating:** Surpassing physical security behind a person who already has access. **Example**: You pretend (impersonate) to be the sanitary of the building and ask an employee who is entering the building to get you in as well.	 **Dumpster Diving:** The criminal searches for valuable and sensitive data inside a rubbish bin. **Example**: The company does not use paper shredders and all private user data is thrown in the closest bin. The criminal gets enough data to plan a targeted attack.
 **Shoulder Surfing:** Stealing sensitive data by physically standing close or in front of the victim's device's screen. **Example:** You take your work device in a public café and the person close to you watches while you type your organisation's username and password.	 **Water Hole Attack:** The attacker guesses/observes which websites are being used and infects one with malware, in the hope that eventually someone will be infected. **Fun Fact:** The name is derived from natural predators as they wait for an opportunity to attack the prey near the water holes.

Co-funded by the Erasmus+ Programme of the European Union

3.4 Threat Actors and Vectors

Under the term “threat actor” we understand any attacker launching a cyberattack on others. When considering cyber-attacks, it is important to realize that there are very different types of actors performing these. Each of them has different intentions, approaches and attributes. Threat actors can be a single person but they can also act as an organized group. Maybe even supported by nation-states (“state actors”). Especially these actors have very specific targets, such as a certain company or the governmental structures of another country.

Attack vectors are the paths that attackers use to gain access to computers and networks. When successful, these vectors will allow attackers to exploit vulnerabilities. Organizations often may think that they aren’t a logical attack target. However, it has become increasingly clear that attackers often try to infiltrate lower-level targets in order to gain access to higher-valued ones. Email and social media accounts are used particularly often as attack vectors.

4. System Overview: Windows and Linux

4.1. Windows

4.1.1 Why is Windows so popular?

The history of Microsoft Windows is closely linked to the Mac OS operating system, from which it was largely inspired. Both had a graphical user interface in common when they appeared in the 1980s. In contrast to earlier operating programs, it was no longer necessary to navigate through a text-based (abstract) user interface. Instead, a far more intuitive, quasi haptic operation was possible, which made it much easier and faster to learn how to use. This circumstance contributed significantly to making Windows a very widespread operating system within a few years, especially among "laymen".

4.1.2. Intuitively Operable (but Vulnerable?)

In the early days of Windows, the importance of the Internet was completely underestimated by its developers. Accordingly, security measures against attacks from the outside were implemented only very inadequately. Even though awareness of this has changed fundamentally in the meantime, there are still some quasi system-inherent vulnerabilities that make Windows systems easier to attack than others. In addition, this operating system is extremely widespread: Anyone who programs a worm or virus designed for Windows can therefore expect to cause far more damage than with other operating systems.

4.2. Linux

4.2.1 Linux as a Hacker’s Choice

The history of Linux is virtually inextricably interwoven with the history of hacking (in a value-neutral sense). Its developer Linus Torvalds originally wrote the operating system to use it to better understand his own computer. Even the original name implies suggestions for the new system - Freax or Buggix - show from which "corner" of the computer world Linux originates. Basically, Linux is based on Unix, a very early operating system from the 1960s. Like Unix, it is not graphically based, but is controlled by written command lines.

Co-funded by the Erasmus+ Programme of the European Union

When used on computers, so-called Linux distributions are usually used. A distribution combines the Linux kernel with various software to form an operating system that is suitable for end use. In the process, many distributors and savvy users adapt the kernel to their own purposes. Linux is used with different frequency: Linux is a constant in the server market as well as in the mobile sector, while it still plays a small but growing role in the desktop and laptop world.

Linux is the most popular choice for hackers due to its flexibility, open-source platform, portability and command line interface and compatibility with popular hacking tools. Windows is a required, but dreaded target for most hackers because it requires them to work in Windows-only environments. Kali Linux is the most popular Linux distribution for hacking and penetration testing among information security professionals. It is an open-source Debian-based Linux distribution developed by Offensive Security that has over 600 hacking tools out of the box.

4.2.2. Linux Specials

Kali Linux offers a wide range of different built-in tools to assist in advanced penetration testing and security auditing, which are its two main reasons of use. The presence of its powerful tools also transforms this operating system into an ethical (and non-ethical!) hacker's Swiss knife.

The tools assist in many information-security tasks, including: penetration testing, computer forensics, reverse engineering and security research.

The tools are also categorized in different families based on their purpose. Some of these categories include: Information gathering tools (used to discover or gather information on a targeted attack – Nmap, Zenmap, etc.), vulnerability analysis tools (check for vulnerabilities or flaws on a system), web application analysis tools (Burpsuite, Httrack, Sqlmap, Vega, etc.), password attacks tools (check and perform attacks against passwords – Hashcat, John, Medusa, etc.), wireless attack tools (checking, breaking or manipulating wireless – Aircrack-ng, Kismet, etc.), forensics tools (to recover or search for cyber evidence – Autopsy, Binwalk, Volatility, etc.), social engineering tools, etc.

5. Attack Mechanisms

5.1. Reconnaissance

This term is mostly used in context of social engineering (cf. chapter 3.3). It means gathering as much information as possible on a target. In networks, reconnaissance methods use tools to send data to the system and then analyse its response. In addition to the internet, reconnaissance also may include actions in the "real" world such as observations or telephone calls. Reconnaissance measures often also are used within penetration tests.

5.2. Threat Modelling and Vulnerability Identification

During this phase of attack, the attacker will further examine the targeted network in order to identify the existing vulnerabilities and validate which ones are exploitable. Later on, the attacker will try to map and create attack vectors (ways/routes to get in!) using all the information gathered during the reconnaissance phase.

Co-funded by the Erasmus+ Programme of the European Union

5.3. Gaining Access (Exploitation)

During the exploitation phase, the attacker tries to take advantage of the vulnerabilities identified by exploiting them. They follow the attack vector defined on the previous phase. If exploitation results successful, this means the attacker has already reached the goal of breaking into the system. Usually, they will also attempt to go as further as they can.

Some standard exploit tactics include: network attacks, web application attacks, social engineering, etc.

5.4. Post-exploitation

As the exploitation phase has been completed and the attacker has already gained access to the targeted network, they will try to perform further malicious actions. The actions from this point are limitless and might include: attempts to escalate privilege, stealing/exfiltrating sensitive data, modifying and altering data and settings, installing malware, maintaining control of the machine for later use, etc.

6. Security Measures

6.1. Endpoint Protection

The term endpoint refers to computer devices such as servers, laptops, desktop PCs and also machines connected to the Internet of Things. These devices can be monitored by an Endpoint Threat Detection and Response. Typically, such systems include Anti-Malware solutions and Intrusion detection, they form a defence-in-depth strategy.

6.2. Hardening

Hardening means the practice of making an operating system or an application more secure compared to its default installation. This measure eliminates vulnerabilities, for example caused from misconfigurations. A typical hardening measure, for example, is to enable ports and protocols only when they are actually needed. Sometimes these are permanently active, for reasons of convenience. Similar to front doors, however, only the port that is actually used should be active ("unlocked"). A second hardening measure is to uninstall unneeded software. For administrators, it is necessary to modify the registry to harden a system.

6.3. Password Policy

Passwords are a security measure that is as widespread as it is misunderstood. While almost everyone uses a password, its security is often criminally overestimated. There are two reasons for this:

1. Many people choose a password that they can remember reasonably well. This often results in passwords that consist of logical terms and possibly numbers, both of which follow a fairly simple regularity.
2. Few know about the mechanisms used to crack passwords. This is usually done using concentrated computer capacity, which tries out thousands and thousands of combinations

Co-funded by the Erasmus+ Programme of the European Union

via simple trial and error. The more "logical" a password is, the faster it can be cracked using such a method.

Therefore, it is generally recommended to use "meaningless" passwords as long as possible: 20 digits, upper and lower case, numbers, special characters and all that mixed aleatorically. Such passwords are difficult (not impossible!) to break. But of course, they are also hard to remember in your head. For this you need a password manager.

6.4. Security Awareness Training

Many people are careless with their data only because they are not aware of the actual potential danger they are in. In awareness trainings, such knowledge gaps can be eliminated and people can be “enabled” to better organize their protective measures. Our program is exactly such a training program.

Co-funded by the Erasmus+ Programme of the European Union