1 Introduction

the terms information, computer and network security get confused, but the difference is important

- information security regards all the the prevention of any damage involving data, in any format
- Computer security regards the protection of the phisical machine and the data it contains
- Network security regards the protection of the network and infrastructure of a company

cybersecurity is the ability to protect the use of cyberspace (internet, private networks,...) from cyber attacks

1.1 Remarks on security

Adversaries

Security is characterized by protection against malicious adversaries, with different motivations (money or glory), different capabilities and objectives. This details compone the modelling of a malicious adversary

Mitigation

To mitigate a threat, various strategies are aviable, reguarding people, processes and technologies. This controls are classified in preventive, detective and corrective.
What conditionates which tactic to select is risk management, or the process to identify the probability of an attack and the extention of the subsequent damage

Trust

A library, or dependency, or every third party product to a software, requires trust and dependability, also known as the ability to avoid failures.

Residual Risks

All security controls can mitigate an attack, but do not avoid it completely. In some cases they can contain more vulnerabilities

1.2 Cia Triad

The most important security properties are Confifentiality, Integrity and Availability

Confidentiality

The main objective of confidentiality is to protect personal privacy and proprietary information from unauthorized indiviaduals. Confidentiality covers data in storage, during processing and while in transit

Integrity

In this case our objective is to avoid unauthorized modification or destruction of data, including the authenticity and non-repudiation

Availability

Ensuring timely and reliable access to data and services by authorized users

1.3 Risk

Vulnerability

A vulnerability is a weakness or flaw in a system, procedure, design or network that can be exploited by a threat source. They are characterized by the difficulty in identifying and exploiting them

Threat

A threat is any circumstance or event that could impact organiazational operations or assets via unauthorized access, destruction and modification of data or denial of service. They are characterized by the propensity to attack (intent) and the ability to successfully do it (capability)

Risk

the probability that a threat will exploit a system vulnerability is called risk, and it's calculated in function of the impact and the likelihood of occurrence.

The risk is anilized though a matrix $5x5$ which uses the the severity of the impact and the likelihood to happen as axis and gives point based on the multiplication of the axes

1.4 Secutity policy, service and mechanism

This three things are, in order, the rules set by an organization to protect data, the capabilities to support one or more security requirements and the devices and functions used to protect data and provide security services

2 Security in perspective

2.1 Attacks and impact

Every component of the CIA triad is an objective of attacks. The violation of confidentiality leads to a disclosure of your personal information. In the integrity case impacts on the trustworthiness of data and the violation of availability brings economic damage

Further difficulties come from the ever extending attack surface and the acquisition of cyber-intelligence information. The second case is an issue because corporations don't usually share informations about their security system or the vulnerabilities they found.

2.2 Security and privacy

They are two different but overlapping properties. Privacy can be also used to indicate confidentiality or controlled sharing.

Non-repudiation

It's a protection against an individual falsely denying to having performed a particular action. The opposite is plausible deniability. This two cases are a conflict of privacy and security because one violates the other.

2.3 Legal constraints

The GDPR (General Data Protection Regulation) is a regulation that applies all european companies and non european companies that process europeans personal data. It protects all the data reguarding genetic, metal, cultural, economic and social identities. When it's not followed it applies penalities like fines up to 20 million euros or the 4% of annual global revenue of a company. The GDPR requires that products, systems and processes follow privacy-by-design concepts and a risk-based approach to cybersecurity

2.4 Security and human factors

The human factor can be a great vulnerability in a system, so it's important to provide security training for the employees. The usual concept to follow when creating security policies for the human factor is:

Make it easy to do the right thing, hard to do the wrong thing and easy to recover when the wrong thing happens

3 Authentication - Passwords and more

Passwords are the main human computer authentication system, but more secure and userfriendly alternatives are researched. In a secure system the user identity is used as a parameter for access controll and all relevant events are logged.

The current situation has found that there isn't a perfect authentication system, but a combination of password, OTP and other techniques is more likely to succeed

3.1 Lessons learned

Passwords were created for protection against jokes and abuse of resources, but it was easy to guess passwords or to find the passwords stored in clear. To prevent this password hashing and salting were invented. After a major attack (morris worm) password were stored in a shadowfile readable only by the root user

3.2 Passwords and the web

With the arrival of the internet, new issues with passwords have been discovered: the reuse of the same password for different services, phishing and the need to reset forgotten passwords. They have been made some attempts to outsource the authentication to third party services, and smartphones increase security using the two factors authentication.

3.3 User authentication and digital identity

When logging on to a computer you enter username (announcing who you are) and password (proving to be who you claim to be). This type of authentication is called **user authentication**, in this case, **by password**.

BOOTSTRAPING

The process of identity proofing follows 3 steps:

- Resolution: collection of data/evidence called Personal Identifiable Information (PII)
- Validation: processing of the evidence by an authoritative source, searching for coherence of the information and complaiance against standards
- Verification: the evidence is verified and the user is allowed to proceed

There are different levels of certainty of one user identification, these are called Identity Assurance Levels (IALs), and are divided in 3 levels. With IAL 1, all attributes are self-asserted by the user or should be treated as self-asserted. at level 2 requires either remothe or in-person identification. Lastly, at third level, is required the verification by an authorized representative.

3.4 Attacks and mitigations

One way to get a password is to guess it. This opens the way to two attack types: the brute force, which tries all possible combinations of symbols, and the smarter dictionary, which uses a list of commonly used passwords.
This type of attacks can't be prevented, but the probability to be successful can be reduced. The mitigations are:

- change default passwords
- forbid commonly used passwords
- limit the number of attempts
- don't use password hints or knowledge based
- incourage the use of password generators and managers

Spoofing

Password spoofing is the use of programs with fake login interfaces that captures user and password when a legittimate user gets bamboozled. The countermeadure is to implement mutual authentication between user and OS

Phishing

an attacker impersonates the system to trick a unser into releasing sensible data. It can also use social engineering

Credential stuffing

Is the use of information from compromised databases to be applied on other services

Password file protection

To maintain confidentiality and integrity the file could use cryptographic protection, access controll enforced by the OS, and further measures to slow dictionary attacks

3.5 Hashing and salting

The Hash is a one way function easy to compute but hard to reverse. Password usually get stored in the form of hash. The characteristics of an hash function are the easy computation, compression, one-way and collision resistance.

NB: strong collision resistance is the property to be improbable to produce 2 messages with the same hash code. This can be problematic if your storing passwords. Weak collision is when two passwords retrieve the same hash in the login. This could lead to an exploit of the system security

The principal algoritms in use are RIPEMD-160 and SHA-256 (others have been cracked like MD4, MD5, SHA-1). Hashing can be broken through the use of dictionary or rainbow (hash dictionaries) attacks.

To increase the security salting has been introduced to the hashes. Salting is the practice of appending random values to the end of the password before hashing

3.6 Extensions for password based authentication

Multi factor authentication is characterized by the addition of some properties like knowledge, possession or inherence. The most common is two factor authentication (2FA)

3.6.1 Time based one time passwords

it uses an algoritm to generate the same number on the server and the host, then the user sends the value that is shown by the host, and if the two number are equals, the user is authorized. This methods still hase some weaknesses, like the value could be phished and replayed, or the algoritm could be stolen and used by the attacker to create new OTP

4 Wrap-up

4.1 Security in perspective

- Attacks violate one or more of the CIA properties
- Identifying which properties are violated help in

  understanding the impact and

  identifying which security services should be used to deploy security mechanisms for risk mitigation
- Ensuring security is a difficult task because of several issues

  attribution

  scale of and borderless attacks

  growing attack surface

  lack of collaboration among victims
- Security and privacy overlaps but are different and sometimes conflicting
- Privacy preserving techniques are relevant also from a legal point of view

  The GDPR encapsulates a risk based approach to privacy
- Security is not purely technical, human factors play a crucial role

  Hence the importance of security awareness and security training to improve the security posture