

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 individuals. 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 organizational 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 analyzed through a matrix 5×5 which uses the severity of the impact and the likelihood to happen as axis and gives point based on the multiplication of the axes

1.4 Security policy, service and mechanism

These 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 regarding genetic, metal, cultural, economic and social identities. When it's not followed it applies penalties 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 remote 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
- encourage the use of password generators and managers

Spoofting

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

Phishing

an attacker impersonates the system to trick a user 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 control 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 algorithms 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 algorithm 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 have some weaknesses, like the value could be phished and replayed, or the algorithm could be stolen and used by the attacker to create new OTP

Smartphones are widely used in MFA, they can provide additional mobile systems to generate password codes, but they also represent vulnerabilities thanks to weak protection of text messages, SIM cloning and the event that the smartphone gets stolen

3.7 Assurance level (NIST)

1. requires at least single factor authentication, provides some assurance the claimant controls the authenticator
2. requires two factor authentication, provides high confidence that the claimant controls the authenticator
3. requires proof of possession, providing very high confidence that the claimant controls the authenticator

3.8 Outsourcing authentication

Securing efficiently the authentication on a system can be difficult for smaller organizations, so the solution is to delegate authentication to trusted third party providers.

Single Sign On (SSO) is one method that uses outsourcing. It's a mechanism that collects your password on the first login, and automatically repeats it on the successive logins. This increases the usability of a system and allows the use of more complex password, at the cost of just one password to compromise.

This mechanism is also an example of the balance between convenience and security

4 Cryptography

4.1 Definitions

- Cryptography is the science and study of secret writing
- Cryptanalysis is the science and study of methods of breaking ciphers
- Cryptology is the combination of cryptography and cryptanalysis
- Cryptosystem is the combination of:
 - E is an encryption algorithm
 - D is a decryption algorithm
 - M is a set of plain texts
 - K is the set of keys
 - C is the set of ciphertextswe can define E and D as $E : M \times K \rightarrow C$ and $D : C \times K \rightarrow M$
- Kerckhoff's principle: the algorithm should not be the secret, but the key

4.1.1 Keys

Are one input to a cryptographic algorithm and the most important part to keep secret. the set of all the possible keys is called key space, and the variance of a key is measured with entropy. Key are important because they're computationally secure

During a connection is common to change the key to limit the amount of data that could be compromised with a single key. So having a strong distribution system is essential

Cryptography is just one part to make a system secure, the keys must stored securely

4.2 Encryption

The encryption process can be applied on blocks of same length or stream of data. The transformation could be through:

- Substitution: each element is mapped into another element
- Transposition: elements are rearranged

4.2.1 Caesar cipher (ROTk)

It's an algorithm based on rotation, mathematically:

$$\begin{aligned} E(x) &= (x + k)(\text{mod } 26) & x \in P \\ D(x) &= (x - k)(\text{mod } 26) & x \in C \end{aligned}$$

it's one of the easiest cipher to break

4.2.2 Vigenere cipher

it's an evolution of the Caesare cipher, it uses the same principle but instead of rotating with the same value, it's used a repeated key

4.2.3 Columnar cipher

The message is written on rows of a table with fixed column length defined by the key (the empty spaces are filled with nulls). In the end the columns are scrambled based on the key and the message gets rewritten from each column

4.3 Modern encryption

With the invention of computers, the algorithms had to evolve because they were too easy to brute force. In this way, new methods arise

4.4 Symmetric keys

A single key is used to encrypt and decrypt and is shared between all intended receivers. It is categorized in two types: stream ciphers and block ciphers. One detail on block ciphers they use both substitution and transposition through S-boxes to obtain confusion and P-boxes to obtain diffusion. These two properties are responsible for the dependency of the key and the fact that if we change one bit, the entire message ciphertext changes

Stream ciphers

converts plaintext one bit at a time with XOR and the key. It's more efficient and it's used for real-time applications

Block ciphers

breaks the message in successive blocks and enciphers them with the same key

4.4.1 Feistel

also called DES, it's a block cipher and follows these procedures

1. splits the blocks in two
2. applies substitution to one half, and the output is XORed with the other half
3. it swaps the two halves

4.4.2 AES

it's the successor to DES. The encryption process is based on a series of table lookups and xor operations. The difference with DES is that the encryption and decryption algorithms are separately implemented, even if closely related. It also mounts larger keys

4.5 Asymmetric keys

It's the base for a secure communication without sharing a secret key. It uses one way functions, those are function easy to compute but difficult to reverse. This is also supported by trapdoor oneway functions, which use a key to easily invert the original function.

During the communication are used two keys, one to encode and another to decode. The two keys are different but mathematically related, although one key doesn't allow to determine the other one. The public key is available to everyone the owner wants, and the private key is kept secret. Then the sender encrypts the message with the public key of the receiver, which decrypts using his private key.

This mechanism can also be used as a digital signature. A private key is unique, so a host can encode something with his private key so that the receiver can verify using the sender public key. This also ensures non repudiation that the receiver

4.5.1 RSA

Is the most used in key exchange, digital signature and encryption of small blocks of data. It uses variable sized encryption blocks and a variable size key. As a mathematical trick it uses the factorization to prime numbers

See FMI

4.5.2 DH

It uses BALZO TATTICOù

5 PKI and TLS

The public key crypto are more secure and supply high levels of integrity, confidentiality and non repudiation. All at the cost of efficiency and the lacking of authentication. PKC is the solution to this cons.

6 Wrap-up

6.1 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

6.2 Passwords and authentication

- Authentication amounts to verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
- Here we focused on user authentication
- Passwords are one of the most widespread and accepted method for user authentication despite their shortcomings
- Adequate security mechanisms should be put in place to protect stored passwords
 - Hashing, salting, access control
- Authentication is only one phase of the identity management lifecycle
 - Also other phases (e.g., identity proofing) may have weaknesses
- Given the importance and difficulty of identity management, it is frequently outsourced to trusted third parties with advantages and disadvantages also from the viewpoint of security (and privacy)