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, regarding 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 regarding 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

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 cn be difficult for smaller organizations, so he solution is to delegate authentication to trusted third party providers.

Single Sign On (SSO) is one method the uses outsourcing. It's a mechanism that collects your password on the first login, and automatically repeats it on the successives logins. This increases the usabilty 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 algoritm

  D is a decryption algoritm

  M is a set of plain texts

  K is the set of keys

  C is the set of ciphertexts

  we can define E and D as $E : M \times K \to C$ and $D : C \times K \to M$
- Kerckhoff's principle: the algoritm 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 keyspace, 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 lenght 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 algoritm based on rotation, matematicaly:

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

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 lenght 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 algoritms 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 share between all intended receivers. it is categorized in two types: stream cyphers and block cyphers. One detail on block cyphers they use both substitution an transposition through S-boxes to obtain confusion and P-boxes to obtain diffusion. This two properties are responsable of the dependency of the key and the fact the if we change one bit, the entire message cyphertext changes

Stream ciphers

converts plaintext one bit at a time with xor and the key. it's more efficient and it's used for realtime 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 procedure

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 pubblic 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.

5.1 Digital signature

Some data that vouches the origin and integrity of a message, it uses the private key to "sign" the message so that the recipient can use the public key of the sender to verify the origin. This system used hash fucntion to enable the signature, but today hash functions are considered deprecated, plus this method still doesn't guarantee the real identity of the user

5.2 Public Key infrastructure

The main requirements on the public key are to be bound on the identity of the party controlling the private key and that this bound is still valid. These two requirements can be satisfied via PKI.

The initial proposal to bound public keys and identities were bulletin boards. In IoT the public key were hardcoded in the software and in internet applications is widely spread the use of digital certificates signed by a Trusted Third Party (TTP)

The PKI binds the entity to the public key through a process of registration and issuance by a Certificate Authority (CA). Then is the Registration Authority that assures a valid and correct registration. The last component of the PKI is the Validation Authority who provides informations of the entity on behalf of the CA

5.2.1 Digital Certificates

This certificates bind a public key and a person/service/hardware component/... and it contains the issuer, the subject (or user), the public key and the digital signature of the issuer.

The certificates are stored in a certificate distribution system, togheter with the Certificate Revocation List (CRL)

Proccedure to obtain a certificate:

1. The user generates a public and private key-pair or is assigned one by some authority
2. The user requests the certificate to the CA server
3. The CA answers with the certificate including public key and digital signature
4. The user gathers the information required by the CA
5. The user send a certificate request (CSR) to the CA including public key and additional data. The request is digitally signed by the user
6. The CA verifies the identity of the user and generates a certificate binding the user identity with his public key

7. The CA issues the certificate signed by the CA to the user

5.2.2 Requirements on PKI

- The TTP must be able to check a party identity
- The relying parties shall be able to check the time and general validity of the certificate

  One way to do this is through CRLs, the other is through the OCSP, or Onlne Certificate Status Protocol
- The cryptographic software of the relying party must be updated according to the latest known vulnerabilities. The software validating certificates shall also work correctly

5.3 SSL and TLS

The Secure Sockets Layer and his successor the Transport Layer Security are protocols developed to secure comunications between client and server

5.3.1 TLS in the browser

His goal is to provide the user with identity of page origin. HTTPS (HTTP + TLS) provides the authentication of the web server and bidiractional encryption against man-in-the-middle, eavesdropping and tampering attacks while protecting privacy and integrity of exchanged data

5.3.2 TLS overview

TLS is composed of two main protocols: the handshake protocoll which consist in the use of the public key criptography tto share a secret simmetric key between client and server, and the record protocol which uses the key obtained through the handshake to encrypt the communication. It also uses some additional protocols like the Change Cipher Protocol to switch to simmetric key encryption, and the Alert Protocol to report failures

The handshake protocol step by step:

1. The clients sends a hello message containing the supported cipher suite

   A cypher suite is the set of algoritms used to secure a network connection

   They usually include key exchange, bulk encryption and message authentication code algoritms

   it also can include signatures and authentication algorithms to authenticate server and clint
2. The server answers with a hello message containg the chosen protocol and cipher suite, plus the session ID
3. IF the client has requested an authenticated connection, the server must send an X.509 certificate.

   it is also the step with the server key exchange

4. the client verifies the server certificate and answers with his own certificate and his part in the client key exchange

   the key exchange contains the pre-master key which is used to calculate the master key

   the master key is obtainad using a pseudo random function

5. The server sends a change cipher spec, which determins the beginning of the use of the new cipher

   it's also sent the finished, or an hash generated from the entire handshake, used to signal the completition of the algoritm

6. At this point every message is sent using the shared key

TLS provides authentication for both server and client by encrypting the clint's choosen key with the server public key, then the server uses the public key of the client to decrypt the data sent by the client in phase 4. If this exchange fails, the session terminates.
This entire communication is encrypted, this provides confidentiality within the session.
Lastly TLS uses a Message Authentication Code (MAC) to provide data integrity. The MAC uses an algorithm composed of cryptographic functions which are similar to hash functions and digital signatures but use differetn security requirements

5.3.3 TLS Vulnerabilities

TLS suffers in securities issues because of logical flaws, compatibility with old cipher suites and implementation issues

RC4NOMORE: An attack born in 2017, it used guesses and observation of occurences of the cipher RC4 to authenticate as the victim

Poodle: an exploit of SSL 3.0. The attacker impersonates the server to downgrade the connection to SSL 3.0, then uses a vulnerability of the protocol to break the entire thing

Bleichenbacher attack: a vulnerability of SSL, it guesses the padding by looking at the server response. In TLS is fixed as decryption failures are hidden from the attacker

Heartbleed: find in the extension heartbeat which kept connections open. The message was composed of the data and datalenght, from which the server replayed with the same message. But if the data was shorter than the declared lenght, the server would fill the missing space with data from his memory, which could have contained sensible information

All this vulnerabilities were using the weakness of the ciphers or failures in the logic, which in successive updates were patched. Right now the best mitigations for TLS vulnerabilities are proper configuration of the TLS server

5.3.4 TLS 1.3

This new version containes:

- Clean-up: removal of unsafe or unused feature, like a smaller cipher suites Poodle
- Security: application of modern techniques

- Privacy: more extensive encryption
- Performance: Faster handshake (1 RTT and 0 RTT)
- Backwards compatability

NB: forward secrecy or perfect forward secrecy is the property that session keys will not be compromised even if long-term secrets are compromised

5.3.5 Ephemeral Diffie-Hellman

This variant of the normal DH from the fact that DH uses the same private key. In EDH, a temporary DH key is generated for every connection. On the other side this doesn't allow for authentication, in fact, in TLS is used Authenticated Encryption with Associated Data (AEAD) cyphers.

6 Single Sign On, SAML, SPID, CIE

6.1 SSO

SSO operates inside of security domains, or applications trusting a common security token for authentication.
The basic concept is:

1. an user access the application
2. the service provider refers for authentication with the identity provider
3. the identity provider ask the user for credential and after the user is authenticated, provides authentication evidence to the service provider
4. the service provider gives to the user an authentication token

Using this system, the credential never leave the authentication domain, but the service provider must trust the authentication domain, plus the authentication transfer must be protected

6.2 SAML

The Security Assertion Markup Language is a common language and flow between systems that want to provide an SSO experience, and it's XML based.

SAML distinguishes two main entities: and identity provider, who authenticates the user and provides authorisation information, and the service provider, which relies on the information provided by the IsP. IdP e SP share metadata in any form and mean possible, sharing at least the entity ID and the cryptographic keys.
There are also federations, or groups of entities, which establish the initial trust among resources.

The authentication flow follows this procedure:

1. A user tries to access an SP
2. The user is redirected to a Discovery Service
   it allowes the user to choose the IdP
3. The user goes back to the SP with the ID of the IdP
4. The user is redirected to the IdP
5. the Authentication is performed
6. THe user goes back to the SP with the authentication

NB: SAML can support other resources, and resources can support multiple SAML profiles. The most used is redirect

SAML is composed of the authentication context, metadata and the main content, which is it self composed of profiles, bindings, protocols and assertions.

Assertions

The assertion are a set of statements made by the authority, and is classified in authentication assertion (which describes the issuer, the issued, validity period,...), attribute assertion (defining specific details about the subject) and authorization assertion (defines what the subject is entitled to do)

Protocols

This section defines the communication and cryptographic protocols used for the exchange

Bindings

SAML uses a mechanism called SAML binding to transport the messages between the actors. There are various types like SAML URI, HTTP redirect, HTTP POST,...

Profiles

The combination of protocols, assertions and binding define a profile which creates a federation and enables federated SSO. This profiles can be Web browser SSO, Single Logout, artifact resolution...

The two types of web SSO are
IsP initiated SSO

1. A user is challenged to supply credentials to the IdP site
2. The user provides credentials and a local security context is created
3. The user accesses to the SP through the IdP, which triggers the SSO service to be called
4. The SSO service builds a SAML assertion
5. The browser issues an HTTP POST request to send the SAML to the SP
6. Final access is allowed or denied to the user by the SP

The opposite is a SP initiated SSO

1. A user attempts to access a resource on the SP
2. The SP sends a redirect in response
3. The SSO service checks for a pre-existing logon security context, if missing requires the user to provide credentials
4. The user provides a valid credentials and a local security context is created
5. The IdP creates a SAML assertion
6. The browser issues an HTTP POST request to the SP
7. The access is allowed or denied to the user

6.2.1 Authentication Context

It indicates how a user athenticated at an IdP. It can be required by an SP to enstablish a level of assurance (LOA)

6.2.2 Metadata

A SAML metadata document describes a SAML deployment which is used to enstablish trust and interoperability. The minimum required is the entity ID, cryptographic keys and protocols endpoints (bindings and URLs). It's important to remember that the keys are both used for encryption and digital signature. In this case is required that each party knows each other in advance.

6.3 SAML Security

Only providing assertion to enstablish trust may lead to man-in-the-middle or replay attacks. SAML fights this vulnerabilities by relieng on a Public Key infrastructure. It also uses SSL/TLS to grant authentication and confidentiality, and the use of XML Signature improves the message integrity. Other mechanism used are expiration timers and unique identifiers for the messages

regarding privacy instead, SAML uses persisten pseudonyms and one-time identifiers between an identity and a service provider and creates a specific authentication context in which the user is allowed to use only certain operations

6.4 National Identity Infrastructures - Spid

The Spid is based on SAML 2.0 and is managed by the AGency for Digital Italy (AgID).
The trust is achieved thorugh the intermediation of the agency, a third party guarantor, a process of accreditation of digital identity providers, attribute authorities and service providers.

All the entities that have passed the accreditation process are listed in the federation registry. For each record is stored the SAML identifier, name of the subject, type of entity, URL to the service provider's metadata and a list of qualified attributes.

6.4.1 CIE

Used to store personal information, the eletronic Id Card is provided with a NFC cip with encryption

6.5 European Identity Infrastructure

An european service used for identification between nations of the EU. Uses various eIDAS-Nodes to connect the different country's services. The communication between a connector and a service relies on SAML

Currently EIDAS is under discussion with a focus on digital wallets, or a user controlled app that permits to select what personal information to share with a service. This gives self-sovereign identity,

decentralized identifiers and verifiable credentials.
Currently the EU is developing a European Self-Sovereign Identity Framework, or ESSIF, with the use of decentralized identifiers and european blockchain services.

7 Access Control

The access control is composed of various mechanism and actors, but we will focus on the subject, or entity, the access control module and the policy decision point (or PDP). This elements (with the exception of the subject) are contained inside an outer and an inner boundary.

Some remarks regarding the access control isolation boundaries:

- The outer boundary prevents the by-passing of the guard

8 Wrap-up

8.1 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

8.2 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)

8.3 SAML

- SAML allows service providers to outsource identity management and focus on their core business

  Reduced administration burden

  Improved interoperability, usability, security and privacy

- SAML profiles are useful use case scenarios

  Web SSO most widely adopted

  SSO has increasing importance and is gaining wider and wider adoption

- SAML is ideal starting point to build infrastructures for digital identity management

  Key enablers in an increasing digital world (SPID, eIDAS)

  First line of defense against attackers