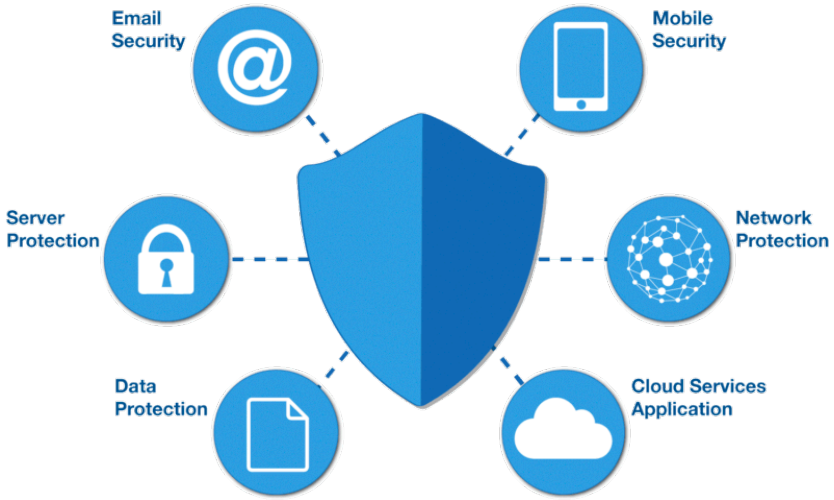
Cybersecurity: an Introduction



Tecnologie Internet

a.a. 2022/2023

Michele Amoretti

Summary

- Cybersecurity
- Security objectives: the CIA triad
- Challenges
- The OSI security architecture
- Security attacks
- Security services
- Security mechanisms
- Fundamental security design principles
- Attack surfaces and attack trees
- A model for network security
- Standards

Cybersecurity

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Major areas covered in cybersecurity are:

1) Application Security

2) Information Security

3) Network Security

4) Disaster recovery

Security objectives: the CIA triad

Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the ***integrity***, ***availability***, *and* ***confidentiality*** *of information system resources (includes hardware, software, firmware, information/data, and telecommunications).*
[from NIST Computer Security Handbook]

Other security objectives: **authenticity** and **accountability**.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity

Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Data integrity assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

System integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Availability assures that systems work promptly and service is not denied to authorized users.

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability

The security goal that generates the requirement for **actions of an entity to be traced uniquely to that entity**.

Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.

Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Challenges

1. Security requirements seem to be straightforward, but the mechanisms used to meet those requirements **can be quite complex**.

2. In developing a particular security mechanism or algorithm, one must always **consider potential attacks** on those security features.

3. Because of point 2, the procedures used to provide particular services are often **counterintuitive**.

4. Having designed various security mechanisms, it is necessary to decide where to use them.

5. Security mechanisms typically involve more than a particular algorithm or protocol.

Challenges

6. The great advantage that the attacker has is that he or she need only to find a single weakness, while **the designer must find and eliminate all weaknesses to achieve perfect security**.

7. There is a natural tendency on the part of users and system managers to **perceive little benefit from security investment** until a security failure occurs.

8. Security requires **regular, even constant, monitoring**, and this is difficult in today's short-term, overloaded environment.

Challenges

9. Security is still too often **an afterthought** to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The OSI security architecture

Security attack: Any action that compromises the security of information owned by an organization.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

The OSI security architecture

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

[RFC 4949]

Security attacks

Passive attacks are very difficult to detect because they do not involve any alteration of the data.

Two types of passive attacks:

- **interception (snooping)**
- **traffic analysis**

Both interception and traffic analysis attack confidentiality.

Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

However, it is feasible to prevent the success of these attacks, usually by means of encryption.

Security attacks

Active attacks involve some modification of the data stream or the creation of a false stream.

Four types of passive attacks:

- **spoofing** (attacks authenticity)
- **tampering** (attacks integrity)
- **replay/reflection** (attacks authenticity)
- **denial of service** (attacks availability)

It is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities.

Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

Security services

A security service is a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.
[RFC 4949]

- Confidentiality
- Data integrity and message authentication
- Peer entity authentication (identification)
- Authorization and access control
- System integrity and availability
- Accountability and non-repudiation

These security services meet all the CIA triad +autenticity + accountability requirements.

Confidentiality

This security service protects data against unauthorized disclosure.

Information is not made available to unauthorized entities.

Related to
- data —> data confidentiality
- entities involved in the communication —> anonymity

Data integrity and message authentication

Data integrity is the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

- protects against unauthorized changes to data by ensuring that changes to data are detectable
- in general it can only detect a change

Data origin authentication provides for the corroboration of the source of a data unit. This service verifies the identity of a system entity that is claimed to be the original source of received data. Usually provided with data integrity.

Message authentication is the ensemble of data integrity and data origin authentication.

Peer entity authentication (identification)

Provides for **the corroboration of the identity of a peer entity in an association**. Two entities are considered peers if they implement to same protocol in different systems; for example two TCP modules in two communicating systems.

Peer entity authentication is provided for use at the establishment of a connection, or at times during the data transfer phase of a connection.

It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

Authorization and access control

Authorization is the verification of the permission to access a resource or system (manage access rights/privileges).

Access control is the ability to limit and control the access to a system (protection of system resources against unauthorized access).

System integrity and availability

System integrity is the quality that a system has when it can perform its intended function. Achieved by protecting system resources against unauthorized change, loss, or destruction.

Availability is the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

Accountability and non-repudiation

Accountability is the property of a system or system resource that ensures that the actions of an entity may be traced uniquely to that entity.

Audit is a service that records information needed to establish accountability.

Non-repudiation provides protection against false denial of an action and prevents either sender or receiver from denying a transmitted message.

Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message (proof of origin).

Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message (proof of receipt).

Security mechanisms

Security services are provided by means of different security functions/mechanisms.

The following security mechanisms may be incorporated into the appropriate protocol layer:

- **Encipherment**
- **Digital signature**
- **Access control**
- **Data integrity check**
- **Authentication exchange**
- **Traffic padding**
- **Routing control**
- **Notarization**

Security mechanisms

Relationship between security services and mechanisms

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Fundamental security design principles

Economy of mechanism means that the design of security measures embodied in both hardware and software should be as simple and small as possible.

Fail-safe defaults means that access decisions should be based on permission rather than exclusion. That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.

Complete mediation means that every access must be checked against the access control mechanism.

Open design means that the design of a security mechanism should be open rather than secret. For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny.

Fundamental security design principles

Separation of privilege is defined as a practice in which multiple privilege attributes are required to achieve access to a restricted resource.

Least privilege means that every process and every user of the system should operate using the least set of privileges necessary to perform the task.

Least common mechanism means that the design should minimize the functions shared by different users, providing mutual security.

Psychological acceptability implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.
See also: **least astonishment**.

Fundamental security design principles

Isolation is a principle that applies in three contexts.
1) public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering;
2) the processes and files of individual users should be isolated from one another except where it is explicitly desired;
3) security mechanisms should be isolated in the sense of preventing access to those mechanisms.

Modularity in the context of security refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.

Layering refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.

Attack surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system.

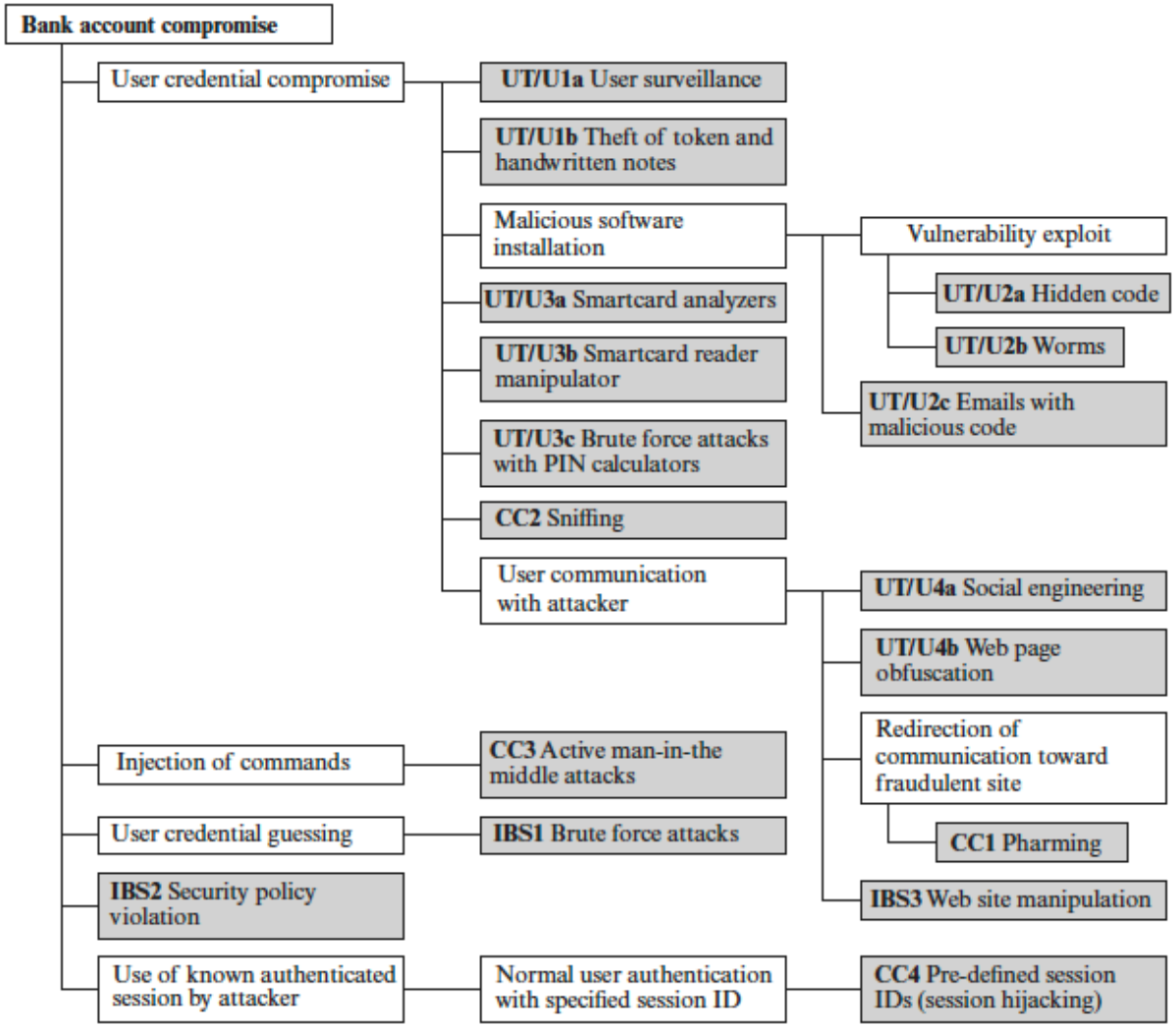
Network attack surface refers to vulnerabilities over an enterprise network, wide-area network, or the Internet.

Software attack surface refers to vulnerabilities in application, utility, or operating system code.

Human attack surface refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

Attack trees

An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.



A model for network security

There are four basic tasks in designing network security services:

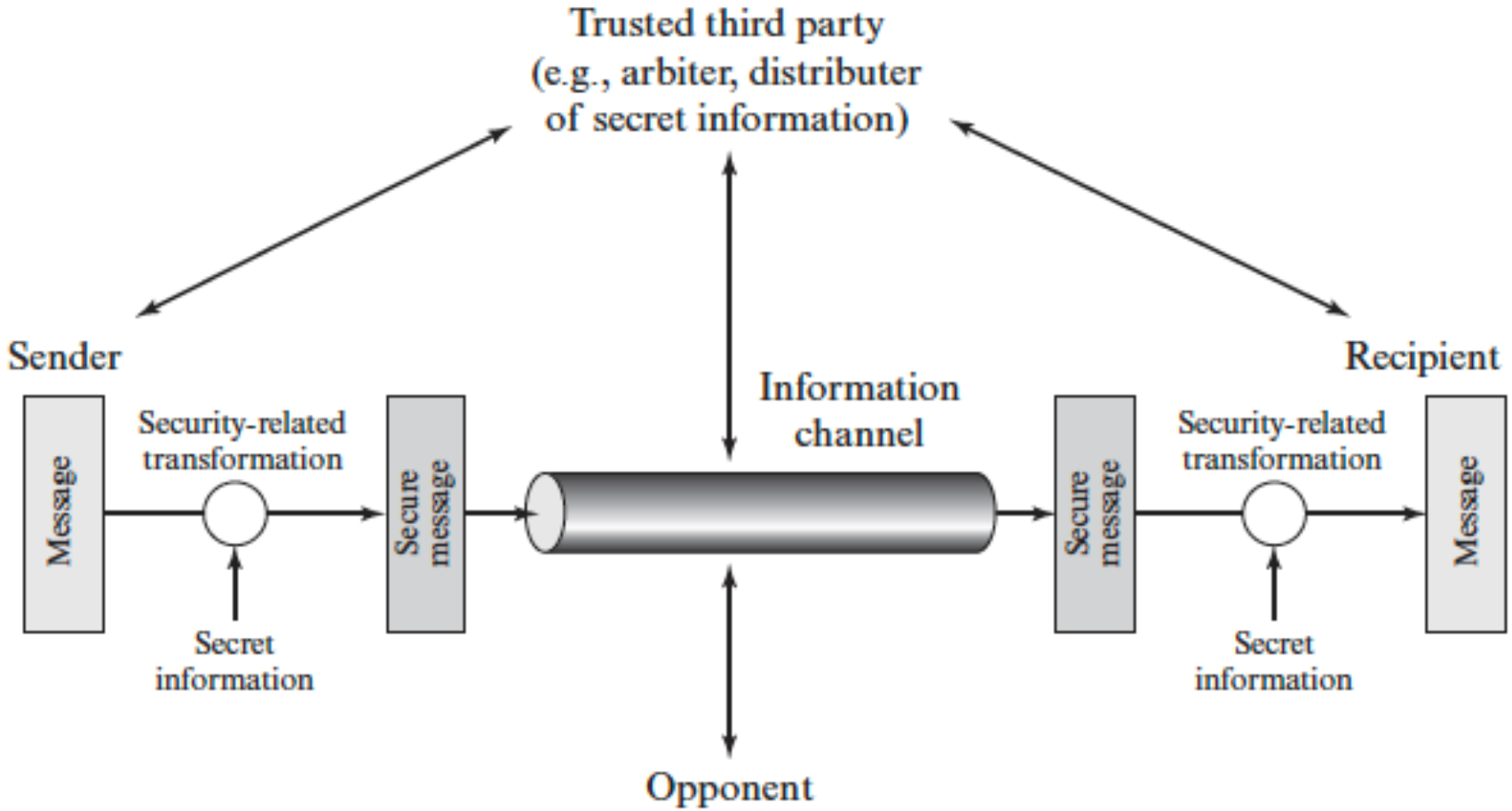
1. Design an **algorithm** for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate some **secret information** to be used with the algorithm.

3. Develop methods for the **distribution and sharing** of the secret information.

4. Specify a **protocol** to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

A model for network security



Standards

National Institute of Standards and Technology (**NIST**) is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact.

Internet Society (ISOC), including **IETF** and **IAB**

International Telecommunication Union (ITU), in particular the **Telecommunication Standardization Sector (ITU-T)**

International Organization for Standardization (ISO)

Plan of the Lectures (Services and Mechanisms)

- Confidentiality
  - Secret key cryptography (5.2)
  - Public key cryptography (5.4)

- Data integrity and message authentication
  - Secret key cryptography (5.2)
  - MAC (5.3)
  - Public key cryptography (5.4)
  - Digital signature (5.5)

- Accountability and non-repudiation
  - Public key cryptography (5.4)
  - Digital signature (5.5)

- Peer entity authentication (5.7)
  - Secret key cryptography (5.2)
  - Public key cryptography (5.4)

Other topics:
- Key Distribution (5.6)
- TLS (5.8)

References

William Stallings, ***Cryptography and Network Security - Principles and Practice***, 7th edition, Pearson, 2017

IETF, **RFC 4949 - Internet Security Glossary**, https://tools.ietf.org/html/rfc4949