“Sapienza” Università di Roma
Ingegneria dell’Informazione,
Informatica e Statistica
Dipartimento di Informatica

Cybersecurity

Appunti integrati con il libro "Computer Security: Principles and Practice", W. Stallings, L. Brown

Author
Simone Bianco

5 gennaio 2024

Indice

Information and Contacts

Appunti e riassunti personali raccolti in ambito del corso di *Cybersecurity* offerto dal corso di laurea in Informatica dell'Università degli Studi di Roma "La Sapienza".

Ulteriori informazioni ed appunti possono essere trovati al seguente link: **https://github.com/Exyss/university-notes**. Chiunque si senta libero di segnalare incorrettezze, migliorie o richieste tramite il sistema di Issues fornito da GitHub stesso o contattando in privato l'autore :

- Email: **bianco.simone@outlook.it**
- LinkedIn: **Simone Bianco**

Gli appunti sono in continuo aggiornamento, pertanto, previa segnalazione, si prega di controllare se le modifiche siano già state apportate nella versione più recente.

Suggested prerequisites:

Preventive learning of material related to the *Computer networks* course is recommended

Licence:

1

Introduction to cybersecurity

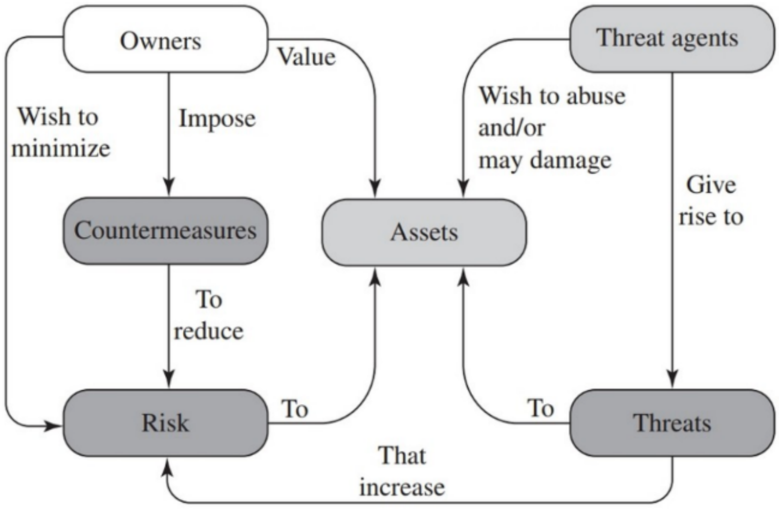
1.1 Fundamental concepts

The National Institute of Standards and Technology (NIST) defines **computer security** as the prevention of damage, protection and restoration of computers, electronic communications systems and services and any other type of digital structure.

In this course, we define **computer security** as measures and controls that ensure **confidentiality**, **integrity** and **availability** of information system assets including hardware, software and information being processed, stored, and communicate.

In order to talk about cybersecurity, first we have to give the following **essential definitions**:

- **Threat**: any circumstance or event with the potential to adversely impact organizational operations
- **Threat agent** (or *Adversary*): anyone who conducts or has the intent to conduct detrimental activities
- **Countermeasures**: a device or a technique that has the objective of impairing detrimental activities
- **Risk**: a measure of the extent to which an entity is exposed to a thread, such as the impact that would arise if an unaccounted event occurs and his likelihood of occurrences
- **Vulnerability**: weakness in an information system, internal controls, implementation, etc... that could be exploited or triggered by a thread source



Osservazione 1

The security of a system, application or protocol is always relative to the set of desired properties and the capabilities of the potential threat agent

Example:

- Standard file access permission in Linux or Windows systems are not effective against an adversary who can boot the system from a CD

Definition 1: Types of attacks

In order to distinguish between kinds of threats, we define the following **types of attack**:

- **Active attack**: an attempt to alter system resources or affect the operation.

  In particular, we establish four categories of active attack: **replay**, **masquerade**, **modification of messages** and **denial of service**

- **Passive attack**: an attempt to learn or make use of information from the system that does not effect the system resources

  In particular, we establish four categories of passive attack: **release of message contents** and **traffic analysis**

- **Inside attack**: initiated by an entity inside of the system's *security perimeter*, namely an **insider** who is authorized to access the system resources, using them in an unapproved way

- **Outside attack**: initiated by an entity outside of the system's *security perimeter* who is

1.2 Confidentiality, Integrity and Availability (CIA)

Definition 2: Confidentiality

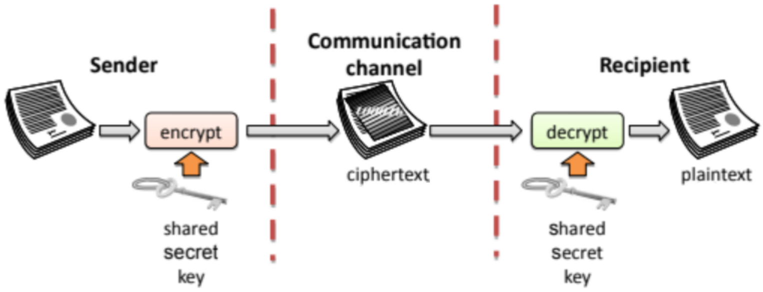
We define **confidentiality** as the avoidance of the unauthorized disclosure of information

Example:

- Confidentiality involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content

In order to **ensure** confidentiality is preserved, three main tools are used:

- **Encryption**: the transformation of information using a secret called *encryption key* in order to make the transformed information readable only by those who know another (or the same) secret, namely the *decryption key*



- **Access control**: rules and policies that limit access to confidential information to established people and/or systems
- **Authentication**: the determination of the identity or role that someone has, usually done through a number of different factors, such as something the person has, knows or is
- **Authorization**: the determination if a person or system is allowed to access resources based on an policy
- **Physical security**: the establishment of physical barriers to limit access to protected computational resources

Definition 3: Integrity

We define **integrity** has the property that something must not be altered in an unauthorized way

Examples:

- Integrity involves the use of backups, checksums, data correcting codes, etc...

Definition 4: Availability

We define **availability** as the property that something is accessible and modifiable in a timely fashion by those who are authorized to do so

Examples:

- Availability involves the use of physical protections and computational redundancies

The concepts of confidentiality, integrity and availability establish what is know as the **CIA security triad**. In order to be secure, a system should try to minimize the number of fallacies that conflict with the triad.

However, other concepts are used to describe the security of a system:

- **Authenticity**: the ability to determine that statements, policies and permission issued by a person are genuine.
- **Accountability**: the requirement for actions of an entity to be traced uniquely back to that same entity through the use of activity records
- **Anonymity**: the property that certain records or transactions are not to be attributable to any individual

1.3 Threat consequences and types

We can categorize events based on their ability to pose a threat on one or more concepts of the CIA triad or based on the type of attack implied by those events.

The first categorization can be reduces to the following types of events:

- **Unauthorized disclosure**: a circumstance or event whereby an entity gains access to data for which the entity is not authorized. This type of event is a threat to **confidentiality**
- **Deception**: a circumstance or event that may result in an authorized entity receiving false data and believing it to be true. This type of event is a thread to either **system integrity** or **data integrity**
- **Disruption**: a circumstance or event that interrupts or prevents the correct operation of system services and functions. This type of event is a threat to **availability** or **system integrity**
- **Usurpation**: a circumstance or event that results in control of system services or functions by an unauthorized entity. This type of event is a threat to **system integrity**

Instead, the second categorization can be reduces to the following types of attacks:

- **Interception**: the eavesdropping of information intended for someone else during its transmission over a communication channel
- Falsification: unauthorized modification of information, such as the *man-in-the-middle attack*, where a network stream is intercepted, modified and retransmitted to the original receiver
- **Denial of service (DoS)**: the obstruction or degradation of data service and/or information access
- **Masquerading**: the fabrication of information that is supposed to be from someone who is not actually the author
- **Repudiation**: the denial of commitment or data reception, such as the attempt to back out of a contract or protocol that requires the different partied to provide receipts acknowledging that data has been received
- **Inference** (or *correlation/traceback*): the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information

2 Authentication