Chapter 2
Information System Security

What is an information system?

What is an information system?

Information System (IS)

- **A set of resources** designed to **collect**, **classify**, **store**, **manage**, and **distribute** information within an organization.
    - The IS should enable and support the organization's mission.

Key point: Information is the ***"nerve center"*** or ***"lifeblood"*** of every company, administration, organization, etc.

What is an information system?

An organization's information system contains a set of **assets**

- **Primary assets,** such as business processes and information.

- **Supporting assets,** everything that enables the organization to function, including employees, company premises, hardware, software, and more.

The security of the information system therefore consists in ensuring the protection of all these assets.

What is an information system?

- **Security** aims to **reduce the risks** weighing on the information system in order to **limit their impact** on the organization's operations and business activities.
- Managing security within an information system is **not intended to create <u>obstacles</u>**.
- On the contrary
  - It **contributes to the quality of service** that users are entitled to expect.
  - It **ensures the level of protection** that staff members are entitled to expect.

Safety vs. Security

Safety vs. security

- **Differences Between Safety and Security**

  “**Safety**” and “**Security**” have different meanings depending on the context.

  The interpretation of these terms can vary according to individual perspectives.

What is an information system?

Safety (Sûreté): It refers to the **protection against malfunctions and unintentional accidents**.

It can be defined as the **set of mechanisms implemented to ensure the system's continuous operation under required conditions**.

Examples of risks

- Access point overload
- Disk failure
- Execution error, etc.

Statistically measurable: (e.g., the average lifespan of a disk is *X* thousand hours)

Countermeasures: Backup, proper system sizing, equipment redundancy, etc.

What is an information system?

Security (Sécurité): It refers to the **protection against deliberate malicious actions**.

It can be defined as a **set of mechanisms designed to protect information from users or processes that are not authorized to handle it**, while ensuring access for authorized ones.

Examples of risks

- Service blockage (Denial of Service)
- Information modification
- Data theft, etc. => DAD (Disclosure, Alteration, Destruction)

Not statistically measurable, but it is possible to **assess risk levels and potential impacts in advance**.
Countermeasures: Access control, security monitoring, patches and updates, hardened configuration, filtering, etc.

Why Are Hackers Interested in Information Systems?

Motivations Behind Cyberattacks?

The motivations behind attacks are numerous, including

- **Financial** (accessing information, then monetizing or selling it)
  - User data, emails
  - Internal organizational information
  - Client files
  - Passwords, bank account numbers, credit card details
- **Use of resources** (then resale or offering them “as a service”)
  - Bandwidth and storage space
  - Compromised machines (*botnets, C&C, C2*)
- **Blackmail / Extortion**
  - Denial of service (DoS)
  - Data modification
- **Espionage**
  - Industrial or competitive
  - State-sponsored
- **Other motives** (activism, ideology, personal challenge, etc.)

The Organization of Today's Attackers

The new economy of cybercrime

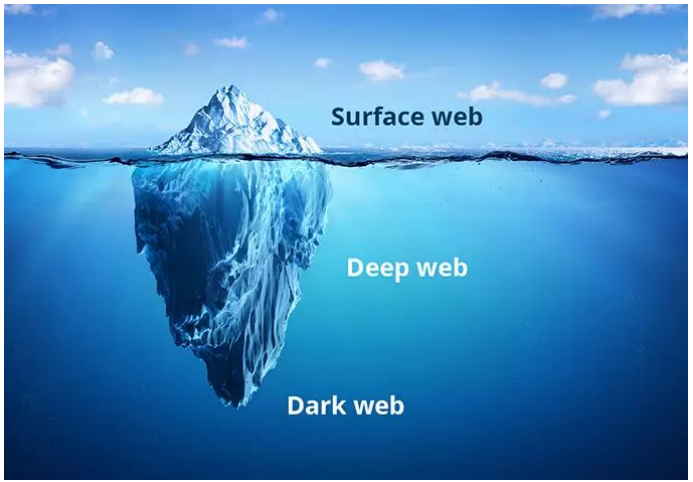
A majority of attacks are committed by **organized, professional groups** and involve

- Groups specialized in **developing malicious software**.
- Groups responsible for **operating and commercializing services** that enable cyberattacks.
- One or more **hosting providers** that store malicious content, either dishonest hosts or hosts that have themselves been compromised and are controlled by attackers.
- Groups in charge of **selling stolen data**, e.g., bank card data.
- **Financial intermediaries** who collect the money and typically rely on networks of **mules**.

Dark Web

Some figures to illustrate the cybercrime market

- The average rental price for **1 hour of a botnet** (used to overwhelm a website) is **$9**.
- The commercial price of the **Citadel** malware (used to intercept card numbers) is **$2,399**, plus a **$125 monthly subscription**.
- **100,000 email addresses (no passwords) = $50**.
- Data for **a single bank card**: **$5–$20**.



Impacts of Cybercrime on Privacy

A non-exhaustive list of impacts

- **Defamation** (damage to reputation)
- **Disclosure of personal information**
- **Harassment / Identity theft**
- **Theft and reuse of logins/passwords** to perform actions in the victim's name
- **Ransomware**: data encrypted in exchange for a ransom
- **Fraudulent account access** and malicious deletion of all data
- **Financial impact** and permanent data loss
- **Stolen credit card numbers** used for online purchases
- **Blackmail**: disclosure of photos or compromising information if ransom is not paid

Impacts of Cybercrime on Privacy

A non-exhaustive list of impacts

- **Defamation** (damage to reputation)
- **Disclosure of personal information**
- **Harassment / Identity theft**
- **Theft and reuse of logins/passwords** to perform actions in the victim's name
- **Ransomware**: data encrypted in exchange for a ransom
- **Fraudulent account access** and malicious deletion of all data
- **Financial impact** and permanent data loss
- **Stolen credit card numbers** used for online purchases
- **Blackmail**: disclosure of photos or compromising information if ransom is not paid

It is essential to anticipate these risks and exercise sound judgment when using the Internet, smartphones, etc.

Some Examples of Attacks

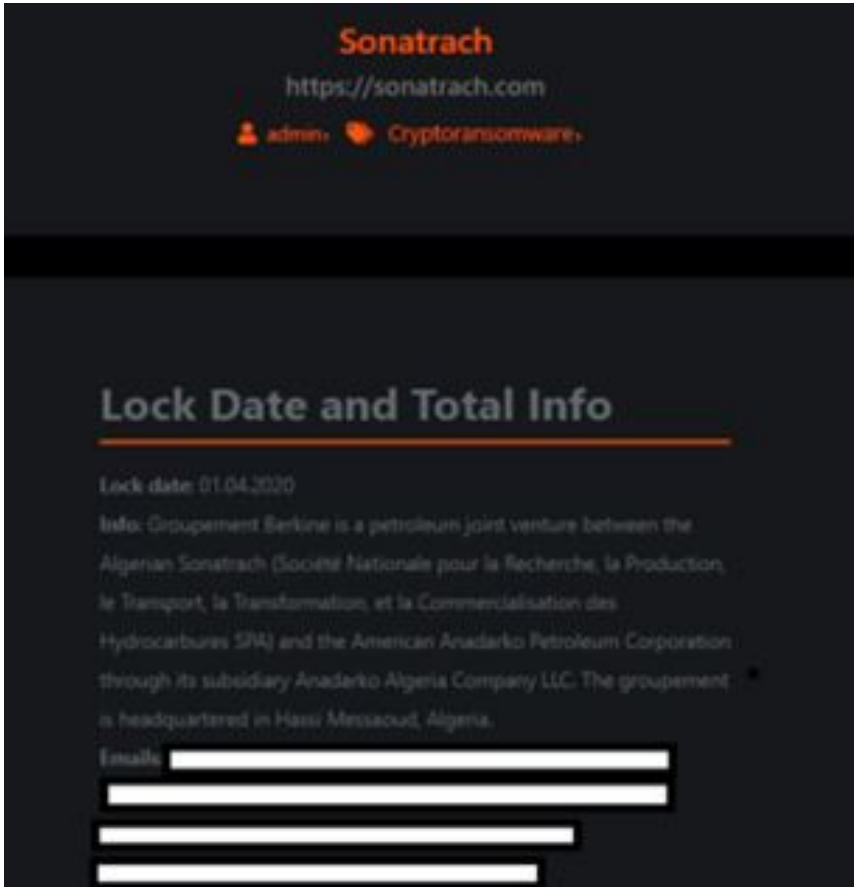
Some Examples of Attacks

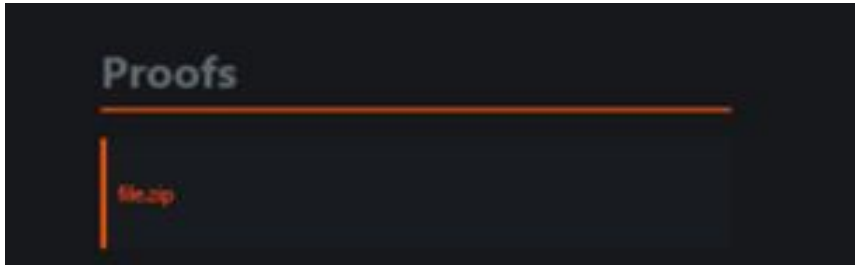
Sony Pictures Entertainment Attack (2014)

- On **November 24, 2014**, multiple Sony computers displayed the message: “If you don’t obey us, we’ll release data shown below to the world.”

- The attackers were known as **GOP (Guardian of Peace)**.
- **Internal data released included:**
  - Social Security numbers and passport scans of actors and directors
  - Internal passwords
  - Unreleased company scripts
  - Marketing plans
  - Legal and financial data
  - Four full, unreleased films
- **Impacts**
  - High risk of **identity theft** for affected individuals
  - **Competitors** gained visibility into Sony’s **strategic plans**

Some Examples of Attacks





Some Examples of Attacks

Sonatrach Cyberattack (April 2020)

- In **April 2020**, **Sonatrach** was targeted by a cyberattack.
- A notorious cybercrime gang called **Maze** successfully stole confidential data from Africa's largest company.
- Around **500 MB of sensitive documents** were leaked, including information on the company's **strategies, budgets, and production**.
- Maze is known for **hacking to extort money from major companies worldwide**.
- According to **Middleeasteye**, by publishing Sonatrach's **banking data and strategic documents**, Maze may have **demanded a ransom from Africa's largest oil company in exchange for recovering the data**.

The need for cybersecurity

Introduction to Security Services

- How to define the security level of an information system asset?
- How can we assess whether this asset is adequately protected?

Introduction to Security Services

Three Criteria for Evaluating Security (Known as C.I.A.)

1. **Confidentiality**
   The property that assets are **accessible only to authorized individuals**.

2. **Integrity**
   The property that assets and information are **accurate and complete**
   (i.e., any unauthorized modification should be detectable and correctable).

3. **Availability**
   The property that assets are **accessible when needed** by authorized individuals
   (i.e., the asset must be available during its intended usage periods).

Introduction to Security Services

The “Non-repudiation / Proof” Criterion

The **Proof** criterion is a complementary aspect often associated with C.I.A. (Confidentiality, Integrity, Availability).

Proof: The property of an asset that allows one to **reconstruct, with sufficient confidence, the circumstances under which the asset is used**. This includes:

- **Traceability** of actions performed
- **Authentication** of users
- **Attribution** of each action to its responsible party

=> AAA Triad (Authentication, Authorization, Accounting)

Example of Security Evaluation

To assess whether an asset is properly secured, it is necessary to **audit its levels of Confidentiality, Integrity, Availability, and Proof**.

Evaluating these criteria on a scale allows determining if the asset is adequately protected.

The **security requirement** can originate from

- **Internal:** inherent to the company's business processes

- **External:** derived from legal or regulatory obligations

Example of Security Evaluation

Example of audit results for an asset on a scale (Low, Medium, High, Very High):

Criterion	Level
Confidentiality	Very High
Integrity	Medium
Availability	Very High
Proof (Non-repudiation)	Low

Conclusion: The asset has an **adequate level of security**.

Example of Security Evaluation

Not all assets in an information system need to achieve the same levels of **C.I.A.P.** (Confidentiality, Integrity, Availability, Proof).

Example

A simple **static company website** designed to promote services online

- **Confidentiality:** Low ⚠️ (public information, no sensitive data)
- **Integrity:** High ✅ (content must be accurate and unaltered)
- **Availability:** High ✅ (site must always be accessible)
- **Proof / Non-repudiation:** Low ⚠️ (no sensitive actions to trace)

Concepts of Vulnerability, Threat, and Attack

Vulnerability

A **vulnerability** is a weakness in a system. This weakness can exist at the level of

- **Design**
- **Implementation**
- **Installation**
- **Configuration**
- **Use of the system**
- **Insufficient protective measures**

Once this weakness is **exploited**, it can cause **losses or damage to the organization**.

Threat

A **threat** is a potential cause of an incident that could cause damage to an asset if it **exploits a vulnerability**.

Threats can be

- **Intentional:** e.g., a hacker or a former employee seeking to harm the organization
- **Accidental:** e.g., a natural event like a fire or a flood

Attack

An **attack** is a **malicious action intended to compromise the security of an asset**.

- An attack represents the **realization of a threat** and requires the **exploitation of a vulnerability**.

- Therefore, an attack can **only occur (and succeed) if the asset has a vulnerability**.

Implication

- The main task of **security experts** is to ensure that the information system **has no vulnerabilities**.

What is Cybersecurity?

What is Cybersecurity?

Cybersecurity is the **set of solutions and techniques implemented** to not only:

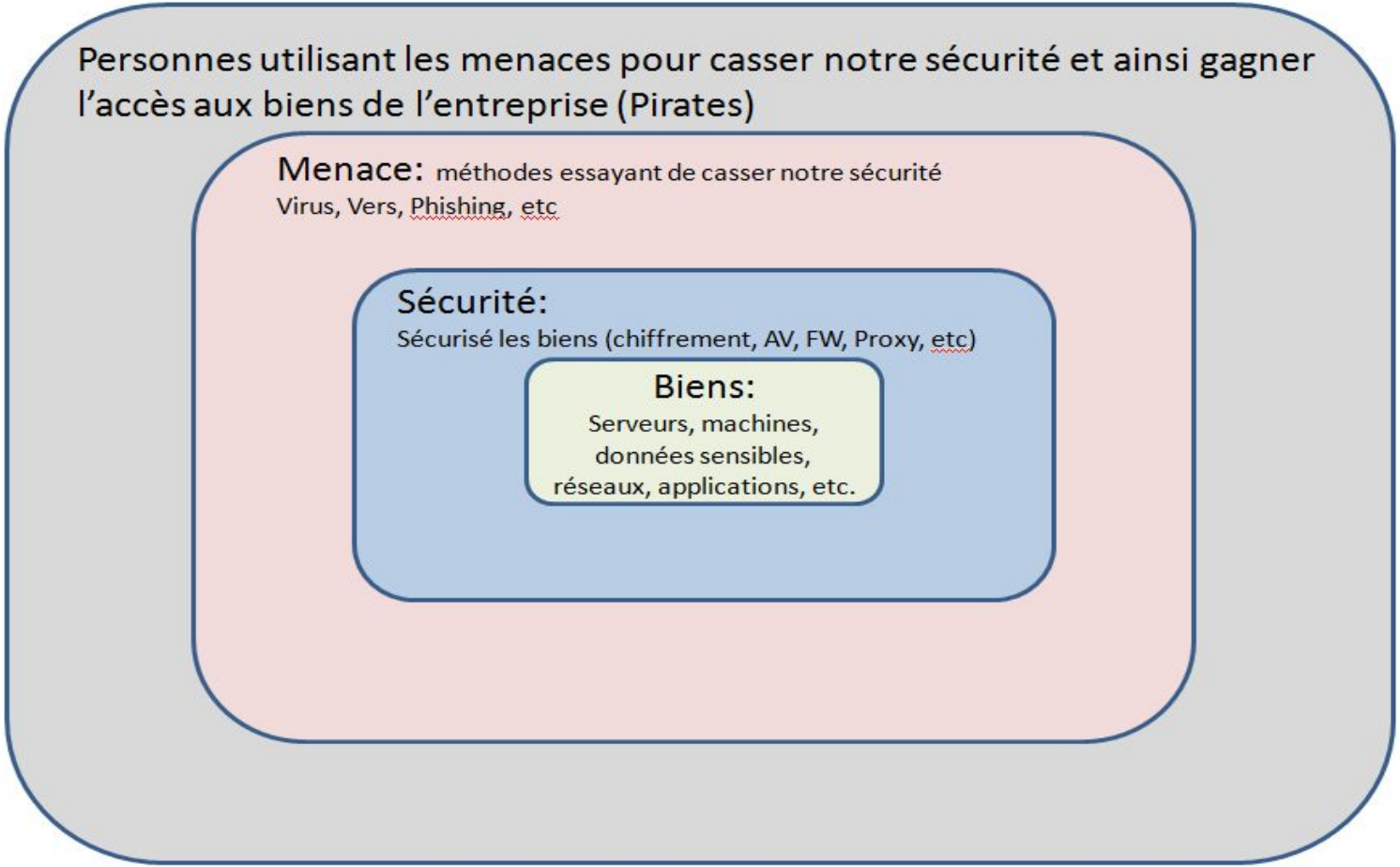
1. **Protect an organization's assets** (including sensitive data, IT systems, networks, and software applications) **against cyberattacks**.

   But to also

2. **Respond effectively if an asset is attacked**, using methods such as **forensic analysis** and **reverse engineering**.

3. **Restore the normal operation** of assets after an attack.

Cybersecurity also involves **protecting the organization's reputation and image**.


Personnes utilisant les menaces pour casser notre sécurité et ainsi gagner l'accès aux biens de l'entreprise (Pirates)
Menace: méthodes essayant de casser notre sécurité
Virus, Vers, Phishing, etc
Sécurité:
Sécurisé les biens (chiffrement, AV, FW, Proxy, etc)
Biens:
Serveurs, machines,
données sensibles,
réseaux, applications, etc.

Approaches to Securing Assets

Approaches to Securing Assets

1) **Risk-based Security**

2) **Defense-in-Depth Security**

3) **Zero Trust Security**

1) Risk-Based Security

This approach involves **choosing an appropriate level of security** based on the **potential consequences of an attack** (hacking or unauthorized access to a company asset).

The goal is to **identify and manage risks throughout the deployment process**.

By determining risk levels, the organization can **deploy the necessary countermeasures** and create a secure system.

1) Risk-Based Security

Typically, this approach includes five phases

1. **Identification:** Identify the assets to protect, potential threats, and possible actors.

2. **Protection:** Implement measures to **protect the identified assets**.

3. **Detection:** Set up processes to **detect potential attacks** (e.g., firewall, IDS, IPS, proxy, etc.).

4. **Response:** Define methods and procedures to **respond effectively to attacks** if they occur.

5. **Recovery / Healing:** In case of an attack, **engage procedures to restore normal system operation** or recover lost data.

Defense-in-Depth Security

This approach involves **securing each subsystem of an organization or system**.

The goal is to **keep malicious actors as far as possible from the organization's assets** by using **multiple layers of defense**.

Examples of fortifying system security

- **Protect data** with encryption
- **Secure applications** that contain sensitive data
- **Authenticate users** for access to machines, servers, applications, etc.
- **Protect the internal network** (e.g., IDS)
- **Protect the perimeter** using tools like VPNs for geographically separated networks
- **Physically secure buildings** (e.g., badge access systems)
- **Raise user awareness**: most IT security breaches occur due to user mistakes

Zero Trust Security

This approach ensures **secure access to all system resources**, regardless of their location.

The goal is to have **visibility into all actions performed by any user** on the resources and to **maintain a record of all activities**.

- This involves **logging and inspection**.
- The approach is based on **least privilege**, meaning users should only have access to the resources they need to **perform their job correctly**.

Quiz Time

Quiz 1

In a **SIEM** system, which of the following is the primary function?

A) Execute antivirus scans only
B) Aggregate, correlate, and analyze logs from multiple sources
C) Backup user data
D) Configure firewalls automatically

Quiz 2

A **SOAR** platform is mainly used to:

A) Automate and orchestrate firewalls
B) Automate incident response and orchestrate workflows
C) Encrypt hard drives
D) Monitor network speed

Quiz 3

What is the main difference between **EDR** and **XDR?**

A) EDR is for endpoints only; XDR collects data across endpoints, network, and cloud for unified detection
B) EDR is hardware-based, XDR is software-based
C) XDR is only for mobile devices
D) EDR replaces SIEM completely

Quiz 4

Which type of firewall **filters traffic based on IP address, port, and protocol only**?

A) Stateful firewall
B) Packet-filtering firewall
C) Application firewall
D) Next-generation firewall

Quiz 5

You want to **block access to a specific website for all employees**. Which solution is most suitable?

A) Proxy server
B) VPN
C) EDR
D) SSH

Quiz 6

What is the **main purpose of a proxy server** in cybersecurity?

A) To encrypt all network packets
B) To hide the client’s IP address and control web traffic
C) To detect malware at the file system level

Quiz 7

Which command checks if a remote host (e.g., 8.8.8.8) is reachable, and stops after 3 attempts?

A) `ping -a 3 8.8.8.8`
B) `ping -c 3 8.8.8.8`
C) `ping -t 3 8.8.8.8`
D) `ping 8.8.8.8`

Quiz 8

What is the primary difference between an IDS and an IPS in the SOC context?

A) IDS blocks traffic, IPS only logs it
B) IDS monitors and alerts, IPS actively blocks traffic
C) IDS replaces the firewall
D) IDS only works on endpoints

Quiz 9

What is the main role of a **firewall**?

A) To prevent viruses from entering a computer
B) To filter network traffic based on security rules
C) To encrypt user files
D) To back up data

Quiz 10

The **HTTPS** protocol mainly relies on

A) SSH
B) SSL/TLS
C) AES
D) HTTPv2
E) RSA

Quiz 11

The main goal of **phishing** is to

A) Infect computers with a virus
B) Steal login credentials and personal information
C) Block servers
D) Destroy hard drives

Quiz 12

Which tool is commonly used for **packet capture and network analysis**?

A) Wireshark
B) Nmap
C) Metasploit
D) Hydra

Quiz 13

What is the main difference between a **virus** and a **worm**?

A) There is no difference
B) A worm cannot spread on its own
C) A worm self-replicates and spreads automatically
D) A virus infects only servers

Quiz 14

What is the key concept of **asymmetric cryptography**?

A) One single key for encryption and decryption
B) Two distinct keys: one public and one private
C) Encryption based on a password
D) Automatically reversible encryption

Quiz 15

What is a **ransomware**?

A) A spyware
B) A malicious program that encrypts files and demands money for decryption
C) A backup tool
D) A phishing technique
E) A denial of service

Q & A

amine.merzoug@univ-batna2.dz

https://staff.univ-batna2.dz/merzoug-amine