



Information Security and It's Elements

Lecture 1

Information Security

Definition

Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.

Information Security Management System (ISMS)

A set of guidelines and processes created to help organizations in a data breach scenario.

By having a formal set of guidelines, businesses can minimize risk and can ensure work continuity in case of a staff change.

ISO 27001 is a well-known specification for a company ISMS.

Types of InfoSec

- Application Security
- Cloud Security
- Cryptography
- Infrastructure Security
- Incident Management
- Vulnerability Management

Core Principles of Information Security

- The CIA Triad

The CIA triad, also known as the information security triad, is a widely recognized model that represents the core principles of information security. It stands for Confidentiality, Integrity, and Availability, and these three principles form the foundation of a secure and well-rounded information security framework.

1. **Confidentiality**– No unauthorized access
2. **Integrity** – No unauthorized modifications
3. **Availability**– Information available to authorized users only



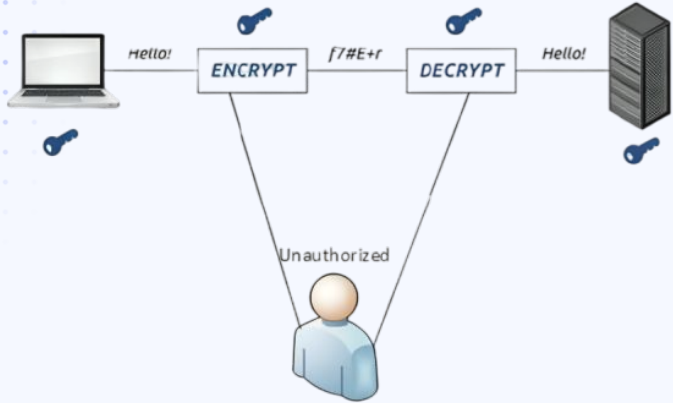
What is Information Security?

Information Security is the practice of protecting information from unauthorized access or harm.

Cyber Security is the protection of computer systems, networks, and data from digital threats and attacks.



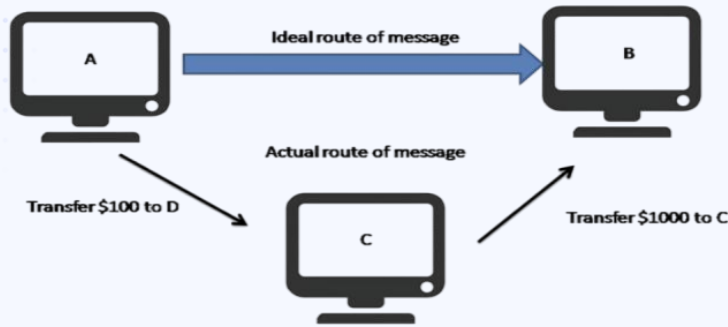
The CIA Triad (Confidentiality)



Confidentiality: Ensuring that information is accessible only to authorized individuals and protected from unauthorized access or disclosure.

For example, when you log into your email account, you expect that only you can read your emails, not anyone else.

The CIA Triad (Integrity)



Integrity: Maintaining the accuracy, completeness, and trustworthiness of information by preventing unauthorized modification or tampering.

Example: Imagine you submit an online application form for a job. Integrity ensures that the information you entered (e.g., your personal details, qualifications, and work experience) remains unchanged and accurate when it reaches the employer's database. If someone maliciously alters your application data during transmission, integrity mechanisms would detect and prevent such unauthorized changes.

The CIA Triad (Availability)



**99.999%
Availability**

Availability: Ensuring that information and systems are accessible and usable when needed by authorized users, and protected from disruptions or outages.

Consider an e-commerce website during a sale event. Availability ensures that the website remains operational and responsive despite a surge in visitor traffic. If the website crashes or becomes unavailable due to high demand, customers may not be able to complete their purchases, impacting the business's revenue and customer satisfaction.

Examples of CIA Triad

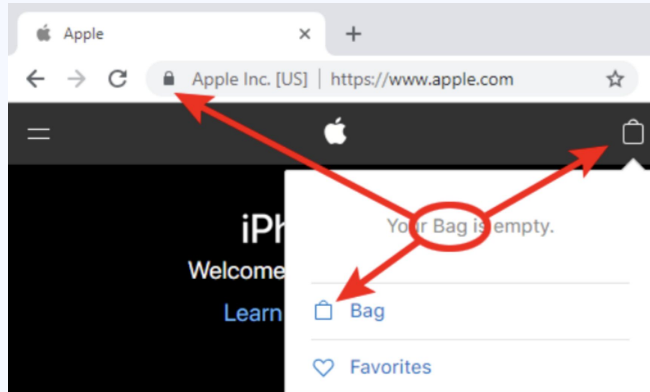
- To have a better understanding of how the CIA triad works in practice, consider an ATM that allows users to access bank balances and other information. An ATM incorporates measures to cover the principles of the triad:
 - The two-factor authentication (debit card with the PIN code) provides **confidentiality** before authorizing access to sensitive data.
 - The ATM and bank software ensure data **integrity** by maintaining all transfer and withdrawal records made via the ATM in the user's bank account
 - The ATM provides **availability** as it is for public use and is accessible at all times.

Other Key Principles

- Authenticity
- Non-repudiation
- Accountability
- Privacy
- Least Privilege
- Defense-in-Depth
- Risk Management

Authenticity

- Verifying the origin and integrity of information

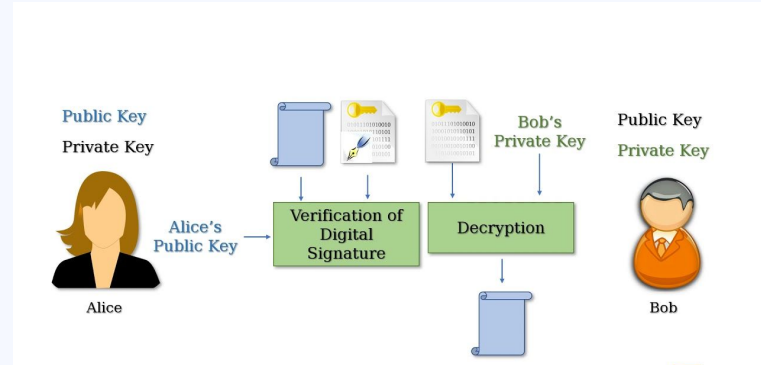


- Imagine you purchase a product online from a reputable e-commerce website. Before entering your payment details, you notice a padlock icon and "https://" in the website's URL, indicating a secure connection.
- This authenticity ensures that the website is legitimate and encrypts your data during transmission, protecting it from unauthorized access or tampering by malicious parties. By verifying these security indicators, you trust that your transaction details are safe and proceed with confidence in making the purchase.

Non Repudiation

- Non-repudiation is the ability to prevent an electronic message or transaction that someone cannot deny the validity of something

For example, if you take a pen and sign a (legal) contract, your signature is a nonrepudiation device.



Accountability

- Tracing actions and holding individuals responsible
- We need to ensure that an authenticated user behaves according to the rules, business conduct, and ethics of the organization. In other words, we need to hold an authenticated user accountable for all his activities.



- For example, we can review the organization's records or information to ensure an authenticated user is held responsible for any wrongdoing.

Privacy


- Safeguarding personal information and respecting privacy rights
- When we host parties, we welcome guests into our home. We give them access to the living hall, kitchen, restrooms, and other common areas. However, do we allow them any access to sensitive information such as your social-security-number (SSN), mother's maiden name, credit card, and bank account information? No. This information is our private information. This information belongs to only us and must be protected at all costs.



Least Privilege

Granting minimal access privileges based on job roles

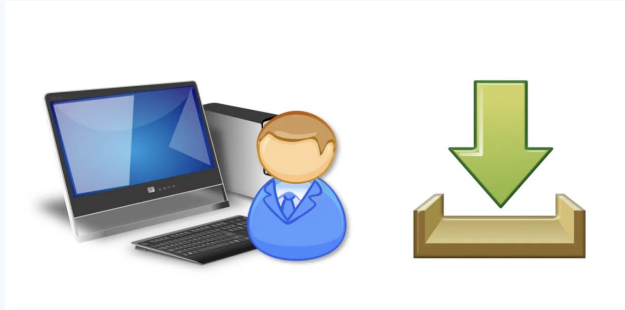
For example, if a database user needs to view a table, he should not have the right to update or delete a table. It helps in protecting data and functionality from faults and malicious behavior



User ID	Name	Email Address
12345	John	john@example.com
12346	Adam	adam@example.com
12347	Amit	amit@example.com
12348	Kumar	kumar@example.com
...

User ID	Name
12345	John
12346	Adam
12347	Amit
12348	Kumar
...	...

Similarly if a user job is only to use a system for a particular purpose then he should not install additional software on the system that require administrator privileges.



It helps in reducing the cyber attack surface and preventing the spread of malware also

Defense-in-Depth

Defense-in-Depth: Using multiple layers of security measures for protection

For example, Banks use Defense in Depth by having armed guards and vaults to protect money, unlike regular stores that just use alarms and cameras. This way, even if one security measure fails, others are in place to keep the money safe.



Each layer of security is represented by icons: a firewall (flame and brick wall), multi-factor authentication (OTP on a phone), biometric security (fingerprint), encryption or physical locks (padlock), and access control (login screen). These layers work together to defend against threats

Risk Management

Identifying, assessing, and mitigating risks to information assets

- Identifying Risks: The company identifies threats such as hacking and phishing that could affect their sensitive customer data.
- Assessing Risks: The company understands that a data breach could lead to financial loss and damage their reputation.
- Mitigating Risks: The company implements security measures like encryption, strong passwords, and regular updates. They also continuously monitor their systems and review security practices to address new threats and keep data secure.





Thanks !
