

Week 4

Why are they interested in me?

- Information is a treasure.
- Liabilities.
- High demand.
- Increased competition.
- Increased awareness.
- Increased digitization.

Anonymity:

- Pseudo identity.
 - Example: Student no.
- Pseudo address.
- Untraceable identity.

Anonymity on the internet:

- Anonymous servers.
 - Via encryption.
- Anonymous users.
 - Simple Mail Transfer Protocol (SMTP).
 - Network News Transfer Protocol (NNTP).

Pros and cons of anonymity:

- **Pros:**
 - National security.
 - Whistle blowing.
 - Avoiding intimidation.
 - Self-interest.
- **Cons:**
 - Personal and societal harm.
 - Complicates investigations on disputes and crimes.

Why do we need security?

To prevent:

- Unauthorized access.
- Unauthorized use.
- Theft.
- Physical damage to digital properties.

Security domains:

- **Confidentiality:** means of preventing unauthorized disclosure to third parties.
- **Integrity:** preventing unauthorized modification of files and maintaining the existing situation.
- **Availability:** preventing unauthorized withholding of information.

Types of security:

- **Physical Security.**
 - Prevention of access to physical facilities.
 - Defense mechanisms:
 - Deterrence: create an atmosphere which defend against intruder access.
 - Prevention: stop intruder access.
 - Detection: assume access and monitor who and what intruder is doing.
 - Response: analyze and minimize damage.
 - Physical access control by:
 - Physical security barriers: fences, dogs, sensors, CCTVs, etc.
 - Electronic access control: cards, firewalls, and passwords.
 - Packet filters firewalls.
 - Proxy servers.
 - Stateful inspection (filter + proxy).
- **Information security.**
 - prevention of access to information by encryption, authentication, and other means.
 - Encryption using cryptography.

Types of encryptions:

- **Symmetric Keys:** Encryption and decryption use the **same key**.
- **Asymmetric Keys:** Encryption and decryption use **different keys**, public key and private key.
- **One Way Hash.**

Authentication:

- System gathers information about the user and validates them to assure genuine user access.
- Ensuring message integrity
- Digital signature

Tools:

- Username, password.
- Retinal image.
- Fingerprint.
- Physical locality.
- Identity cards
- Etc.

Authentication: Verify that I am whom I claim.

Ways:

- Login.
- http authentication.
- Certificate.

Authorization: Decides if you have permission to access a resource.

Ways:

- Access control via URL.
- Access control lists.
- Secure methods.

Security Policy:

A document specifying:

- Organizational security guidelines.
- Guidelines about how to handle security incidents.

Privacy:

The ability of individuals or groups to hide or selectively express themselves or information about themselves.

A human value with the following rights:

- **Solitude:** The right to be alone without disturbances.
- **Anonymity:** The right to have no public personal identity.
- **Intimacy:** The right not to be monitored.
- **Reserve:** The right to control one's personal information.
- Is Relative in culture, locality, religion, political system, ...etc.

Types of privacy:

- **Personal privacy** (All personal attributes).
 - **US fourth amendment:** Right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.
- **Information privacy:**
 - Preventing unauthorized access to:
 - Personal information.
 - Financial information.
 - Medical information.
 - Internet activity.
- **Institutional privacy:** Protecting research data, product data, sales data, marketing strategies, etc.

Importance of privacy:

- Guards our personal identity.
- Preserves our autonomy.
- Supports establishing new social relationships.

Privacy acts and policies:

They restrict illegal and harmful privacy violation.

- **Privacy policy:** The institution is bound to tell us the nature, type, usage of information about us.
- **Right to opt out:** The institution is bound to explain our recourse to prevent the transfer of our data to third-party beneficiaries.

- **Safeguards:** The institution must put in place policies to prevent fraudulent access to confidential information.

Legal issues in privacy violations:

Privacy Violations occur due to:

- Inadequate privacy policies.
- Giving up little or more information when shopping, responding to ads, etc.
- Failure of companies to commit and follow up their own privacy policies.
- Internet temptation.
- Intrusion: wrongful entry, seizing, or acquiring possession of the property of others.
- Misuse of information.
- Interception of information.
- Information matching.

Privacy protection:

- **Technical:**
 - Do not reveal personal information inadvertently.
 - Turn on cookie notices in your Web browser, and/or use cookie management, software.
 - Keep a “clean” email address.
 - Don’t reveal personal details to strangers or just-met “friends.”.
 - Realize you may be monitored at work.
 - Use encryption.
 - Contractual: Type and dissemination.
- **Legal:**
 - Protection acts:
 - Children, family, consumer, etc.
 - Freedom of information.
 - Privacy.
 - Financial privacy.
 - Financially services.
- **Ethics.**