Chapter 9: Security, privacy and data integrity

Terms:

- Data integrity: Data is accurate and up to date.
- Data privacy: Keeping data private. Data protection laws govern how data should be kept privatte and secure.
- Data security: Safeguarding data to provide Confidentiality, integrity and accessibility.

Threats to security

- Lack of proper care
- internal mismanagement
- natural disasters
- unauthorised intrusion
- malicious software

Malware

> Malware or malicious software are developed with intent to harm.

- Types:
  - virus: Self replicating inside other executable code
  - worm: runs independently and transfers itself to other network hosts
  - logic bomb: inactive until some condition is met
  - trojan horse: replaces all or part of previously useful program. Hides in useful program.
  - spyware: collects and transmits it
  - bot: takes control of computer
- Activities:
  - Phishing: sending email pretending to be legitimate source
  - Pharming: setting up bogus/fake website that appears to be a legitimate site
  - Keylogger: Records keyboard usage by user
- User activities that lead to system vulnerability:
  - Weak password
  - Not recognising phising or pharming
  - Not keeping antivirus active and updated
- Vulnerability due to system itself:
  - Lack of security in OS
  - Macro virus with application packages
  - Buffer overflow and similar errors.(in C)

Security measures

For computer system:

- Disaster recovery
- Safe system update
- User authentication:
  - Autorization: Providing right to user
  - Authentication: Ensuring user is who he/she claims to be. Eg. Biometric, password etc.
- Firewall: Hardware/Software that inspects incoming and outgoing connections via network.
- Digital signature: Verifying identity of sender.
- Antivirus and intrusion detection.

For protecting data:

- Backup
- Restricting access to data
- Protecting content(encryption and decryption)

Data validation and verification

- Validation: Checking data is in required format during entry.

  - Ensuring not empty
  - Format check
  - length check
  - range check
  - limit check
  - type check
  - existence check(eg. for files)

- Verification: Making user confirm that data entered was what was intented to be entered.

  - Double entry
  - Visual check before submission

- Check digit: For numbers during storage, some digits are calculated and stored with numbers. Verification is done while reading.

- Verification during data transfer:

  - Parity bit: One bit to ensure even/odd parity
  - Parity bytes + bits(2D parity): Can check and correct error
  - Checksum: Data is broken to blocks and sum is transmitted along with data.
  - Cyclic Redundancy check
  - Hamming code