

6. Security, Privacy, and Data Integrity

6.1 Data Security

- **Difference** between data security, privacy, and integrity
 - **Data Security:** Ensuring that data is **protected against unauthorized access, modification, or destruction**
 - **Data Privacy:** Ensuring that **personal data** is **kept confidential**
 - **Data Integrity:** Ensuring that data is **accurate, reliable, and consistent**
- We need to protect **both** the **security of data** and the **security of the computer system**

Security of Computer Systems

- Protection of the **system**
- Prevent **access of viruses** to the system
- Prevent **hackers** from entering the system

Different Measures (Stand-alone PCs & A Network of Computers)

- **User Accounts & Password**
 - Each has a Username and Password associated with login details
 - Has assigned privilege which gives him access to only his workspace, preventing the user from having admin rights
 - Can assign privilege to files so users without privilege don't have access
 - Cannot access the system without a valid username and password
- **Authentication Techniques:** i.e., digital signatures and biometrics
 - *Digital Signatures:* mathematical algorithm/encrypted data attached to electronically transmitted document
 - *Password:* Case-sensitive, unique string of letters, numbers, and special characters
 - *Biometric Scans:* retina, fingerprints, palm
- **Firewalls**
 - A set of programs, located at the network gateway, that *protects the resources of a private network from users from other networks*
 - All *incoming and outgoing* network traffic goes through it into the computer system and is **filtered**
 - **Block** signals that do not meet the requirements
 - Applications can have *network access restricted*
- Encryption
- Anti-Virus Software, Anti-Spyware
 - Scan the computer's hard drive and memory for known spyware signatures
 - Monitor system behaviour for suspicious activities
 - Often include features like real-time protection, system scanning, and the ability to quarantine or delete harmful software
 - Regular updates and scans are necessary to protect against new and evolving spyware threats

Security of Data

- Protection of **data on the system**
- Prevent **corruption of data**
- Prevent **hackers** from using the data

Different Measures

- **Encryption**
 - Conversion of data to code by **encoding** it
 - Data stored in an **incomprehensive** state
 - **Doesn't prevent** illegal access but **appears meaningless**
 - Necessary to use **decryption software** to decode data - Keys complex algorithms; cannot crack
- **Access Rights**
 - Different users are assigned **different authorization levels** which prevent them from accessing all the data to increase security
 - To **stop users from editing data** they are not permitted to

Threats to Computers and Data

- **Malware** (virus, spyware)
 - **Virus**
 - Program code that can **replicate** themselves
 - Can be **disguised** as legitimate software; Run in the **background**
 - **Intention of deleting/corrupting** files to cause computer to malfunction
 - **Spyware**
 - **Gathers information** by monitoring the user on the device, i.e., monitoring the webcam or the key pressed on user's keyboard
 - Can be **disguised** as legitimate software; Run in the **background**
 - Information **sent back to the third party** who sent the spyware
- **Hackers**
 - **Illegal access** to a computer system **without permission/knowledge**
 - Done with the intent of **causing harm** to a computer system or user
- **Phishing**
 - Being sent a **legitimate-looking email**
 - May contain **links** that, when clicked, take the user to a fake website
 - **Trick** user into entering their personal information into these fake websites
 - **Taking away** information like passwords and bank details
- **Pharming**
 - **Malicious code** installed on the user's computer/web server
 - **Redirects** user to a fake website
 - Users **do not have to take any action**, unlike phishing
 - Creator of malicious code can **gain personal data**, leading to **identity theft**

Methods to restrict the risks

- restricting **Malware** → using anti-malware software like anti-virus software and anti-spyware
- restricting **Hackers**
 - Strong passwords
 - Firewalls
 - Software that can detect illegal activity
 - Virtual Private Network (VPN) → hides your IP address when browsing the web, so the hackers cannot locate your web location and hack you
- restricting **Phishing**
 - **Be aware** of new phishing scams
 - **Do not click links** unless you are certain that it is safe

- Using **modern browsers** that alert users to pharming/phishing attacks
- Look for "**https**" instead of "**http**" to ensure that the website is secure/encrypted
- Frequently **change passwords**
- restricting **Pharming**
 - Antivirus software → so the malicious code won't be installed on the server
 - Using **modern browsers** that alert users to pharming/phishing attacks
 - Checking the **spelling** of websites to avoid fake sites
 - Look for "**https**" instead of "**http**" to ensure that the website is secured/encrypted

6.2 Data Integrity

- **Transmission Errors:** interference in communications link may cause bits to be wrongly received → hence, we need to check data integrity

Data Validation

- Check that the data entered is **sensible**
- Data can be valid but this doesn't mean that it is accurate
- Example: checking data is the right type of characters

Methods of data validation

1. **Range check:** data must be *between a set of values*
2. **Format check:** data must *follow the correct pattern*
3. **Length check:** data must *have an exact number of characters*
4. **Presence check:** data must be *filled in*; the field is not left empty
5. **Existence check:** data must *exist* (e.g., a barcode must correlate to an item)
6. **Limit check:** data must be *within one of the limits* (the upper or lower limit)
7. **Check Digit**
 - one digit is used to be an answer to an **arithmetic** operation of the other digits in the data
 - if the arithmetic operation result of the other digits do not equal to that check digit, the data entered is incorrect
 - Example: the last digit of the barcode is a check digit for all digits before it

Data Verification

- Check that the data entered is **the same as the original**
- Example: double entry

Methods of data verification

- During **Data Entry**
 - **Visual Check:** compare the entered data with the original visually
 - **Double Entry:** data is entered twice, sometimes by different people; then, the computer system compares both entries
- During **Data Transfer**
 - **Parity Check**
 - parity can be **even or odd**
 - transmitting device counts the **number of 1 bits** in the byte
 - if there is an even/odd number of 1s, then the parity is even/odd

- a parity bit is used to make sure that the binary pattern has the correct parity
- receiving device on receipt of byte counts the number of 1 s
- even the number of 1s in odd parity gives an error, and vice versa
- **Checksum**
 - the checksum value is calculated **from the data** before transmission
 - it is calculated by **adding up the individual bits or bytes of a message**
 - this calculated value is **transmitted with the data**
 - **receiving** computer recalculated the checksum from the received data
 - if the checksum **received** and **calculated** match, no error has occurred
 - if the checksum **received** and **calculated** do not match, an error has occurred