1.6 Security, privacy and data integrity

Explain difference between the terms security, privacy & integrity of data.

- Data Security:

Making sure only that only the people who have access to the data are the only ones who can access the data is referred to as data security. Data security policy is applied to ensure data privacy.

- Data integrity:

Maintaining validity of data is referred to as data integrity. It is making sure that data is correct & not corrupted.

- Data Privacy:

Data privacy refers to appropriate use of information. It means that data should only be used for intended purpose.

Show the appreciation for the need for both the security of data & the security of the computer system.

Computer-based information systems are vulnerable to crime and abuse, natural disaster and human error. Loss, alteration, misuse, theft of these data may result in big loss for the organization. So it is important to keep data safe from the various hazards to which it may be subjected.

Describe security measures designed to protect computer systems, ranging from the stand-alone PC to a network of computers, including:

- User accounts:
  Each user who is permitted to access computer system should be provided User id and password, which will give them a certain level of access rights.

- Firewalls
  Firewall can be hardware or software(or a combination) that sits between LAN and WAN. The firewall interrogates all data packets that are intended for the LAN. There are two strategies for doing this:
  - Proxies
  - Stateful inspection

  With proxies, a proxy server stops the packets of data at the firewall and inspects them before they are allowed onto the LAN. Once the packets have been checked and found to be satisfactorily, they are passed through the LAN. The message does not pass through firewall but is passed to the proxy. This method tends to degrade network performance but offers better security than stateful inspection.
  Stateful inspection tracks each packet and identifies it. To do this, the method uses tables to identify all packets that should not pass through the firewall. This is not as secure as the proxy method because some data do pass through the firewall. However, the method uses fewer network resources.

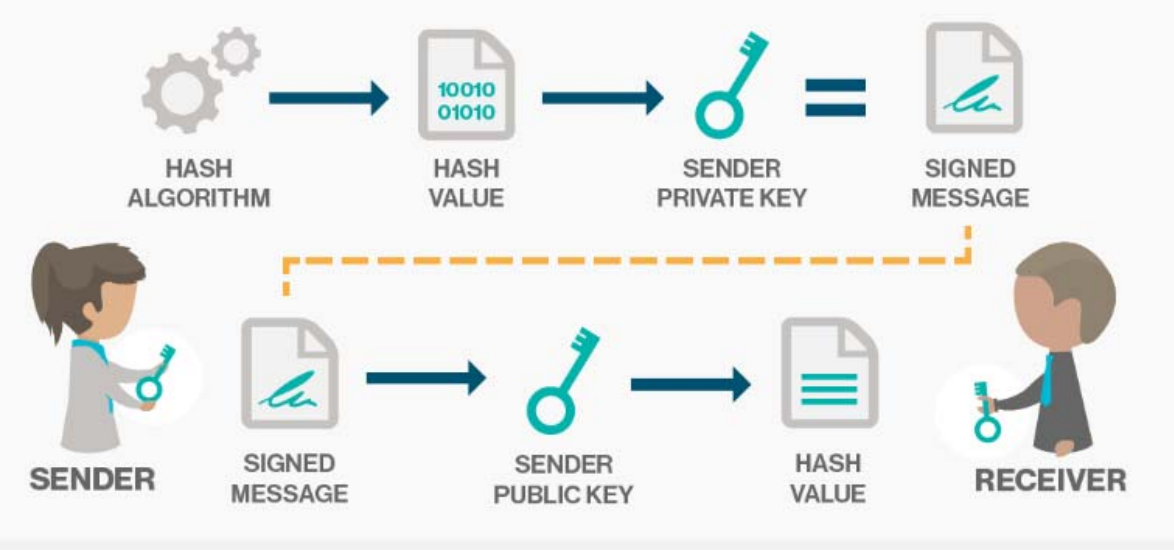
- Password
  Most password schemes use tables to store the current password for each authorized user. These tables will be stored on disk and will be backed up along with other vital system files, and in addition may be printed out in a dump of system files. So, password lists should not be stored in plain form but should be encrypted.

Bikash Agrawal

In networking system, unauthorized users can gain entry to a networked computer through their own computer. One way to prevent this is to use a call back procedure so that when a remote user logs in, the computer automatically calls them back at a pre-arranged telephone number to verify their access request before allowing them to log on.

- Digital Signature
  A **digital signature** is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**. Authentic means that receiver knows who created the document and that it has not been altered in any ways.

  The **Digital Signature Standard (DSS)** is based on a type of public key encryption method that uses the **Digital Signature Algorithm (DSA)**. DSS is the format for digital signatures that has been endorsed by the US government. The DSA algorithm consists of a private key that only the originator of the document (signer) knows and a public key.



Describe data security methods

- Data backup
  It is the process to make a copy of the data in the file, so that if the disk is destroyed, the data can be recovered. This copy is known as backup. In most applications, the dta are so valuable that it makes sense to produce more than one backup copy of file. Some of these copies are stored away from the computer system in case of a hazard, such as fire.

  A file that is frequently altered needs to be backed up more often than one that is very rarely changed.

- A disk-mirroring strategy
  Disk mirroring is a technique used to protect a computer system from loss of data and other potential losses due to disk failures. In this technique, the data is duplicated by being written to two or more identical hard drives, all of which are connected to one

disk controller card. If one hard drive fails, the data can be retrieved from the other mirrored hard drives.

- Encryption

Encryption involves applying a mathematical function, using a key value, to a message that can only be read by the sender and the intended receiver. There are number of terms used with encryption.

- Plain text describes the original unaltered text as created by the sender.
- Encryption algorithm is the calculation which is used to change the plain text into the encrypted text.
- Chipper text is the message text after the encryption has been performed.
- Decryption is the process of converting the message text back to the original plain text.

The aim of encryption is not to prevent unauthorized access but to make it impossible for them to "unscramble" the message, i.e. produce the plain text from it.

- Authorization

Authorization is a process by which a server determines if the client has permission to use a resource or access a file. Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access. The type of authentication required for authorization may vary; passwords may be required in some cases but not in others. In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

Show awareness of what kind of errors can occur and what can be done about them

The data held in a computer system may become incorrect or corrupted in many different ways and at in many stages during data processing.

- Errors on input
- Errors in operating procedure
- Program errors
- Viruses
- Transmission errors

To protect against errors, standard procedures may be documented & folloed for both input and output.

Input

- Data entry must be limited to authorize personnel only.
- Data may be verified to guard against entry errors.
- Data control tools can be used.

Output

- All output should be inspected.
- Printed output containing sensitive information should be shredded after use.

Data validation for input data

Data validation means accuracy of input data. Validation is a check on data input to the system by comparing the data input with a set of rules that the computer software has been programmed to implement. If the data input does not match up with the rules then there must be an error.

- Presence Check: Data must be present in certain field.
- Range Check: is there a low/high limit?
- Format check: If data is in particular predefined format
- Length check: if numbers of characters in data are as defined
- Character check: if names consists of alphabets only or other characters too

Data verification for data entry:

Verification means checking the input data with the original data to make sure that there have been no transcription errors (transcription means copying of data). The standard way to do this is to input the data twice to the computer system. The computer then checks the two data values (which should be the same) and if they are different, the computer knows that one of the inputs is wrong. It won't know which one is wrong but it can ask the operator to check that particular input.

a) Checksum:

Data will normally be sent from one place to another as a block of bytes rather than as individual bytes. The computer can add numbers together without any trouble, so another checking procedure is to add all the bytes together that are being sent in the block of data. The carry, out of the byte, is not taken into account, so the answer is an 8 bit number, just like the bytes. This answer is calculated before the data is sent, and then calculated again when it is received, and if there are no errors in the transmission, the two answers will match. If, however, the two bytes are different there must be at least one checksum that has been corrupted and the whole block of data has to be re-sent.

b) Parity Check:

All data is transmitted as bits (0s and 1s). The Number of 1s in a byte must always be either an odd number or an even number. If two devices that are communicating data decide that there will always be an odd number of 1s, then if a byte is received that has an even number of 1s, an error must have occurred. E.g. the byte 01011000 has 3 ones in it. 3 is an odd number, so it fits the rule that it must have an odd number of ones. When it is sent there is an error in transmission so that the first bit is received as a one. So, the byte received is 11011000. This has 4 ones in it, which is an even number, so there must be an error. The receiving device would ask for it to be sent again.

Notes:

• If two mistakes are made in the same byte they will cancel each other out and the faulty data will be accepted. This problem can be overcome, and in the same way, a clever way of correcting error mistakes can be implemented. This method is not part of this course.