Chapter 9: Security, privacy and data integrity

⇒ Data Privacy

→ it is about keeping data private rather than allowing it to be available in the public domain.

→ There is a legal framework in place to penalise offenders who breach others privacy. This framework is provided by a "data protection law."

→ aspects of "data protection law"

→ it is focused on ~~dat~~ personal/private data that a person gives to an organisation.

→ The data given, allows the organisation to use the data but only for purposes understood and agreed by the individual.

→ Data protection laws oblige organisations to ensure the privacy and the integrity of this data.

→ Unfortunately, having laws doesn't mean adherence to them but they do act as a ~~deter~~ deterrent.

⇒ Data Security

→ Data security must be achieved before Data integrity or Data privacy

→ Data security does not guarantee data integrity or privacy.

→ System Security - (why needed?)

→ to ensure that the system continues to carry out tasks users need

→ to ensure that only authorised users have access to the system

→ Definition - a requirement for data to be available for use when needed. Data can be recovered if lost or corrupted.

⇒ ~~Threats to security~~

⇒ Threats to the security of a computer system

1. user not taking appropriate care
2. Internal mismanagement
3. Unauthorised intrusion into the system
4. Natural Disasters
5. malicious software entering the system.

⇒ Malware

→ malicious software that has the intention of causing harm to a system

→ Example

→ Virus - replicates itself inside other executable files code

→ Worm - runs independently and transfers itself to other network hosts

→ Logic Bomb - stays inactive until some condition is met.

→ Trojan Horse - replaces all or part of previously useful program

→ Spyware - collects info and transmits it to another system

→ Bot - takes control of another computer and uses it to launch attacks

→ The virus category is often subdivided according to the software that the virus attaches itself to. Ex. boot sector virus and macro virus

→ Malware classified in terms of activity involved

→ Phishing - sending e-mail or electronic message from an apparently legitimate source requesting confidential information

→ Pharming - setting up a bogus website which appears to be legitimate

→ Keylogger - recording key-presses on the keyboard by the user of the system.

⇒ System Vulnerability (because of user activity)

1. Use of weak passwords, directly related to the user, makes it easy for a hacker to guess.
2. User not recognising a phishing or pharming attack, and as a result gives away sensitive info.
3. Actions that might introduce malware in the system.
   → attaching a portable storage device
   → opening an email attachment
   → accessing a website
   → downloading a file from the internet

⇒ System Vulnerability (within the system)

1. Over time, there is a tendency for operating systems to increase in complexity, which leads to more opportunities for weak security. Os has regular updates, which fixes security issues.

2. A very specific vulnerability is "BUFFER OVERFLOW". Programs written in C programming language, of which there are very many, do not automatically carry out array bound checks. A program can be written to deliberately write code to the part of memory that is outside the address range defined for the array, set up as a buffer. The program overwrites what is stored there so when a later program reads this overwritten section it will not execute as it should.

⇒ Security measures for protecting computer systems.

→ Disaster Recovery

→ measures are needed to ensure that the system continues working whatever event occurs. Such measures come under disaster recovery which is based on risk assessment. The plan has provision for an alternate system to brought into action. This alternate system has to be remote to the main system.

→ User Authentication

→ The main security feature of a user account is authentication of the user. There is a password for accessing each account, the pwd should be complex and long. There is a alternative method to passwords, "BIOMETRICS" "SECURITY TOKEN".

→ keep good practice. Don't leave computers open and unattended.

→ Firewall

→ a hardware device that acts like a security gate. It checks all incoming and outgoing traffic. It can be used as a software also MONITORS and CONTROLS NETWORK TRAFFIC.

→ Digital Signature

→ It confirms the identity of an user electronically. Ex. email.

→ Anti-virus Software

→ it carries out regular checks to detect any malware and remove or deactivate it.

→ Intrusion ~~detection~~ detection

→ it will take input an audit record of system use and look for examples that do not match expected system activity.

⟹ Security measures for protecting data

→ Data loss

Disk gets corrupted
Disk is destroyed
System crashes
file erased or overwritten by mistake
Location of file is forgotten

→ Prevention

full back up weekly
two generations of full backup
incremental backup daily basis.

UPS / backup generator

→ Restricting access to data

If a user has logged in he should not have access to all the data in the system. The solution is have an authorisation policy which gives different access rights to different files for different individuals.

→ Protecting data content, if someone breaks through security measures, we can encrypt data for further protection.

⟹ Validation of data entry

→ it can only filter out data of wrong type, wrong format, out of range

→ Data validation is implemented by software associated with a data entry interface.

Examples -

1. a prescence check - field should not be empty
2. a format check - dd/mm/yyyy
3. a length check - number of characters ex. phone no.
4. a range check - month in a date should not exceed 12
5. a limit check - max no. of years in age
6. a type check - only a numeric value or only char
7. an existence check - check if file exists

⟹ Verification of data entry

→ it means getting the user to confirm that the data entered was what was intended to be entered.

→ Double entry - method of verification. Ex. Pwd are asked to re-enter.

→ Visual Check - read through the data entered, before sending

⟹ Check digit

→ Sender while sending data attaches an extra digit in the 13th bit, which is calculated using a formula. The reciever uses the formula and checks if the digit matches, if it matches data has been recieved correctly, if it does not reciever asks sender to send again. Ex. Barcode, ISBN

⟹ Parity Check

→ Even / Odd, count number of one's.

⟹ Check sum

→ The sum of binary numbers is calculated and supplied as a checksum value. The reciever does same calculation if the checksum matches then no error, if it does not then error position of error cannot be determined.