Security
29 May 2022 01:59

Security

① Data Integrity

- Is making sure that data is correct / valid
- Ensures that data received is same as the data sent
eg Parity Check

② Data Privacy

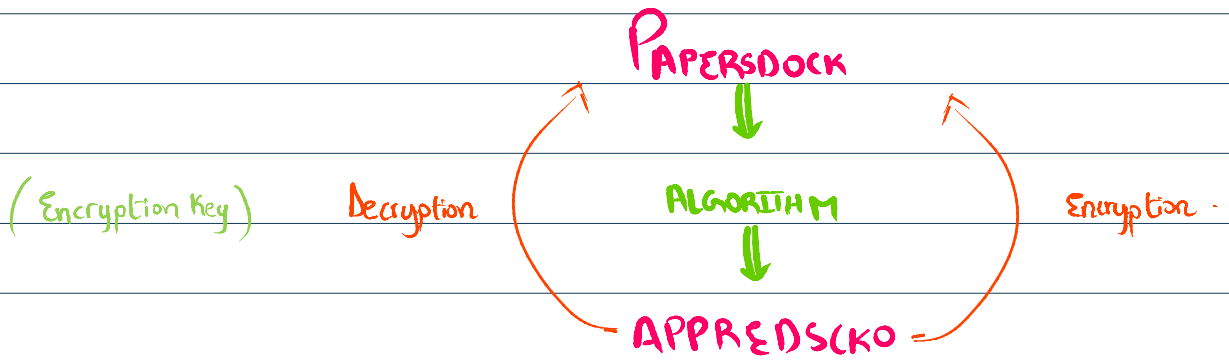
- Keeps data confidential
- Only seen by authorized personals

③ Security

- Is to keep data safe
- Prevention of data loss
- e.g data backup.

Security Measures To Protect Computer

① Encryption

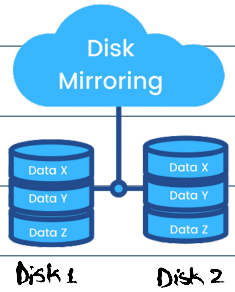


- Encryption scrambles the source code
- Using an encryption key
- If the file is accessed without authorization it will be meaningless
- It requires a decryption key to unscrammble the algorithm.

② Data Backup

- A copy of data will have been made and stored elsewhere
- If the original data is lost, the backup can be used to restore the data.

③ Disk Mirroring

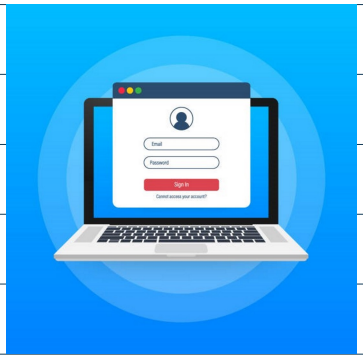


- The data is stored on two disks simultaneously
- If the first data disk drive fails, the data is accessed from the second disk.

④ Firewall

- Prevents unauthorized access to the data
- Monitors incoming and outgoing traffic
- Blocks transmission from unauthorized sources / website
- Maintains an allow list
- Can be software or hardware both
- Can help to prevent hacking

⑤ User Account



- user has an username and password
- access to resources can be limited to specific account
- A person cannot access system without valid username and password.

⑥ Anti Malware

- Scans for malicious code (harmful code)
- Quarantines or deletes any malicious software found
- Scans can be scheduled at regular intervals.

⑦ Access Rights

- Different Access Rights for individual / group
- To stop users from editing program.

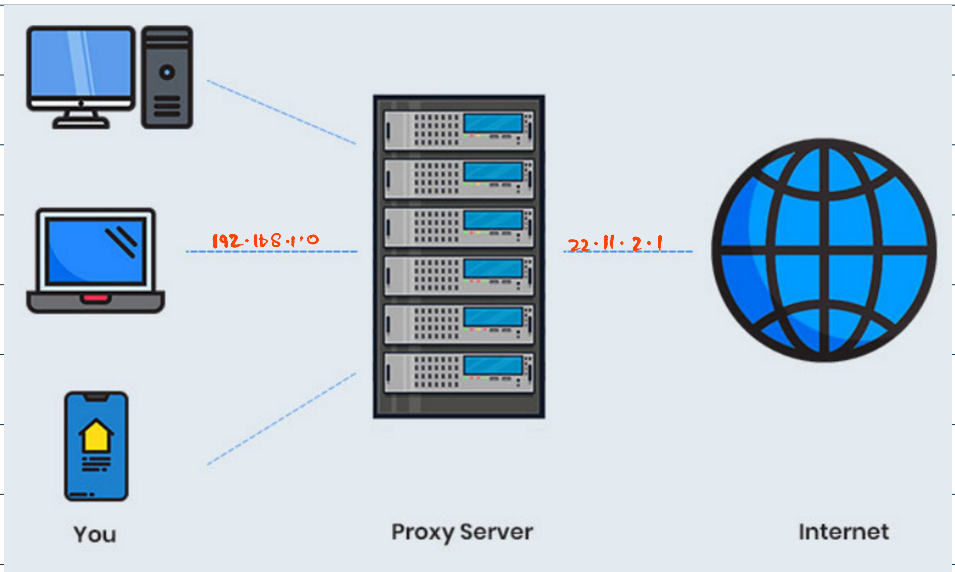
⑧ Physical Measure

- Locked doors / Keyboards
- Secure method of access

What are the other methods to proted data online?

- Running up to date anti virus
- Use of proxy server
- Strong biometrics / password

Proxy Server



Acts as the middle man and hides the public IP address of the user

What are the factors to consider when planning a data backup?

- How often should the data be backed up

e.g at the end of each day as students progress may be edited each day.

- What medium should the data be backed upto.

e.g external harddisk as it has larger capacity

- Where should the backup be stored

e.g off site as if the building is damaged only the original data are lost.

What is backed up?

eg only the updated file.

When should the backup take place?

e.g over night.

MALWARE

Malware is software that is intentionally designed to cause damage to a computer or server

TYPES OF MALWARE

viruses , worms , logic bombs , trojan horses , Spyware

Explain the term virus ?

- Milicious Code
- that replicate / copies itself
- can cause loss of data
- can cause computer to crash
- can fill up hard disk with data .

What are the ways to protect from virus ?

- Use anti-virus
- update anti-virus on regular basis
- avoids downloads from unknown sources
- use a firewall
- avoid suspicious website .

(1) Virus

Programs or program code that can replicate itself by inserting itself into another piece of software with the intention of deleting or corrupting files .

Problem: Computer may stop working or files may get lost.

Solution: run anti-virus software.

(2) Worms

A standalone piece of software which can reprodue itself automatically does not require a host.

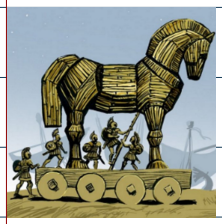
Problem: could corrupt user's computer // delete data // consume bandwidth

Solution: run anti virus software in the background // keep OS up to date // not connected on internet.

(3) Logic Bombs

Code embeded in a program on a computer. When certain conditions are met (such as specific date) they are activated to carry out tasks such as deleting files or sending data to a hacker.

(4) Trojan Horses.



Same as that greek horse story, where the soldiers hid inside a horse and when they entered the city, they attacked.

Malicious program often disguised as Legitimate software with the intent of harming the computer.

(5) Spyware

Software that gathers information by monitoring for example key presses on user's keyboard

The information is then sent back to the person who sent the software.

Solution: Anti-Spyware Software.

PHISHING

someone sends email to users, when clicked takes the user to fake website so they could obtain somebody's confidential data or to install malware.

Problem: Identity fraud // misuse of financial data

Solution: Ignore suspicious email and undergo frequent security awareness training.

PHARMING

Malicious code installed on user's computer or webserver. The code redirects the user to fake website.

DATA INTEGRITY

Validation: Checks that the data entered is reasonable.

Verification: Checks that the data entered is same as the original.

VALIDATION

Range Check: Checks whether data entered is between a lower and and upper limit

Range Check: Checks whether data entered is between a lower and and upper limit

e.g using 13 as months or -120 as age

Format Check: Check whether data has been entered in the agreed format

e.g format of date is dd/mm/yyyy

Length Check: Checks whether data has the required number of characters.

e.g phone number should contain 7 numbers

Presence Check: Checks to make sure a field is not left empty when it should contain data

e.g verification code should be present

Existence Check: Checks if data in a file or a file name actually exists

e.g registered name is found.

Limit Check: Checks only one of the limits (such as the upper limit or lower limit)

e.g 1.5 litre only.

Check digit: Is an additional digit added to a number.

Methods For Calculating Checkdigit

(1) Each digit in the number is given a weighting e.g 7, 6, 5, 4, 3, 2, 1 starting from Left.

(2) The digit is multiplied by its weighting and then each value is added to make a total.

(3) The total is divided by 11 and remainder subtracted from 11

E.g

4	1	5	6	7	1	0
7	6	5	4	3	2	1
(7x4)	(6x1)	(5x5)	(4x6)	(3x7)	(2x1)	(1x0)
28	+ 6	+ 25	+ 24	+ 21	+ 2	+ 0

= 106

$$11 \overline{)106} \quad 9 \quad -99 \quad 7$$

Remainder = 7

11 - 7 = (4) → Check digit.

VERIFICATION

Is a way of preventing errors when data is entered manually using a keyboard or when data is transferred from one computer to another

Verification During Data Entry

(1) Double Entry

(2) Visual Check

Double Entry: Data is entered twice, using two different people and then compared.

Visual Check: Entered data is compared with the original document.

Verification During Data Transfer

(1) Check Sum

(2) Parity Check

(3) Automatic Repeat Request

Checksum

- bytes sent as a block
- bytes added up before transmission
- results of addition is sent with the data block
- same calculation is carried out at receivers end
- the two values are compared.

0 1 0 1 1 0 1 1 1 0 0 0 1 1 1 0

Block 1 | Block 2

0 1 0 1 1 0 1 1 | 1 0 0 0 1 1 1 0

```
  1 1 1 1
+ 0 1 0 1 1 0 1 1
  1 0 0 0 1 1 1 0
  ---------------
  1 1 1 0 1 0 0 1
```

Apply 1's compliment

Sender ⇒ (0 0 0 1 0 1 1 0) ⇝ checksum

The checksum block will be sent with the data and the receiver will add all the blocks and the answer should be ALL 1's if it is transferred correctly

```
    1 1 1 1
  0 1 0 1 1 0 1 1
  1 0 0 0 1 1 1 0
  ---------------
  0 0 0 1 0 1 1 0
  ---------------
  1 1 1 1 1 1 1 1
```

Correct transfer.

Parity Check

Even Parity (Even number of 1's)

Odd Parity (Odd number of 1's)

Even Parity (Even number of 1s)

Odd Parity (Odd number of 1's)

5 Parity checks are often used to check for errors that may occur during data transmission.

(a) A system uses **even parity**.

Tick (✓) to show whether the following three bytes have been transmitted correctly or incorrectly.

Received byte	Byte transmitted correctly	Byte transmitted incorrectly
11001000		✓
01111100		✓
01101001	✓	

[3]

(b) A parity byte is used to identify which bit has been transmitted incorrectly in a block of data.

The word "F L O W C H A R T" was transmitted using nine bytes of data (one byte per character). A tenth byte, the parity byte, was also transmitted.

The following block of data shows all ten bytes received after transmission. The system uses **even parity** and column 1 is the parity bit.

	letter	column 1	column 2	column 3	column 4	column 5	column 6	column 7	column 8	
byte 1	F	1	0	1	0	0	1	1	0	✓
byte 2	L	1	0	1	0	1	1	0	0	✓
byte 3	O	1	0	1	0	1	1	1	1	✓
byte 4	W	1	0	1	1	0	1	1	1	✓
byte 5	C	1	0	1	0	0	0	1	1	✓
byte 6	H	0	0	1	0	1	0	0	0	✓
byte 7	A	0	0	1	0	0	1	0	1	✗
byte 8	R	1	0	1	1	0	0	1	0	
byte 9	T	1	0	1	1	0	1	0	0	
parity byte		1	0	1	1	1	1	1	0	

(i) **One** of the bits has been transmitted incorrectly.

Write the byte number and column number of this bit:

Byte number ..... 7 .....

Column number ..... 6 .....

[2]

How a parity block check can identify a bit that has been corrupted?

- Each byte has a parity bit
- An additional parity byte is sent with vertical and horizontal parity
- Each row and column must have an even/odd number of 1's
- Identify the incorrect row and column
- The intersection is the error.

- Identify the incorrect row and column
- the intersection is the error.

Automatic Repeat Request

ARQ uses acknowledgement (a message sent to the receiver indicating that data has been received correctly) and timeout (time interval allowed to elapse before an acknowledgement is received.
when receiving device detects an error, it asks for the data packet to be resent. If no error is detected then positive acknowledgement is sent
The sending device will resend the data if it receives a request to resent after negative acknowledgement or timeout has occured.

Digital Signature

Public and Private Keys

Sender

Receiver

PRIVATE KEY

email

PRIVATE KEY

PUBLIC KEY

PUBLIC KEY

PUBLIC KEY (receiver)

PUBLIC KEY (sender)

HASHING ALGORITHM.

· Hashing algorithms are mathematical function that produces a hash key.

0 5 4 1 9 7 2 2

5 5 16 4

30 Hash key 10 20

30

Sender

Receiver

email

email Encrypted

Hashing Algorithm ✓

(54) Hash key (Digest)

Encrypt Sender's Private Keys (Digital Signature)

Decrypt by Public Key of sender

✓ Hashing Algorithm

54 Hash Key

Explain how digital signature is used to ensure email is authentic ?

· Email message put through hashing algorithm to produce a digest ✓

· Digest is encrypted with sender's private key to create digital signature

· The digital signature can only be decrypted with matching sender's public key.

. The digital signature can only be decrypted with matching sender's public key.

Explain how digital signature is used to ensure that data is not altered?

. Email message put through agreed hashing algorithm to produce a digest
. Digest is encrypted with message by sender's private key to create digital signature.
. The digital signature and the message is decrypted with public key of sender.
. Then the receiver passes the email to same hashing algorithm and produces digest
. The digest received by sender is matched with digest of receiver
. If both digest are same then data is not altered.