Firewall

The entrance to a network can be protected by openning and closing certain ports, which prevents data packets using those ports from entering and leaving the network.

Packet filtering

Packets of data are inspected by fire wall to check which port they are attempting to access, they are checked if they are trying to enter a closed port or open one. If port is closed, it may if the packet is verified, temporarily open the port to allow it in, then close it again.

Proxy servers

Proxy means ‘on behalf of’, they server different functions, one of which is anonymous web browsing. It makes request to a webserver, rather than you sending the request. Client sends request to proxy server, the proxy server then redirects this and sends a new data packet to the web server. Unlike being routed through routers, the routers would just keep the source IP so if data is intercepted, then it is known what the client’s ip address is. Using proxy servers however, if the proxy server is sending the request for data from web server, and the data is intercepted, the source IP of the user isn’t there so the interceptor won’t know where the original user is sending the request from.

Proxy servers can also be used for filtering undesirable online content, like advertisements, since data is received by proxy server first, then brought to user.

Malicious software

Malware annoys users or damages their data.

* Worm is a standalone program that does not require a user to run it in order for it to spread.
* Viruses are embedded into a file, and need a user to spread it and activate it.
* Trojans are malicious software programs that pretend as innocuous or useful applications.
* Backdoor – give attackers remote control over infected system
* Banking – steal financial information
* Ransomware – encrypt files and demand payment
* Spyware – record keystrokers or steal personal data, e.g what websites user is visiting

Phishing:

* Using emails to manipulate a victim into visiting a fake website and giving away personal informtion
  + They may be identified for looking urgent and have mistakes in their email such as spelling mistakes, and things that make them look unofficial.

Buffer overflow:

* Buffer overflow occurs when a program accidentally writes data to a location too small to handle it
  + E.g if there is 3 spots for data, if a hacker forces 2 pieces of data to be written when the 2/3 spots are already taken. The last bit will be taken up by one, while the 2nd one is written elsewhere, which might cause the 2nd bit of data to be overwritten into a location that is shouldn’t be written into, e.g an instruction, resulting in the loss of the instruction.
  + buffer overflow can cause programs to crash because you don’t have the correct instructions to run the code.
  + Attackers can also inject their own code and get the user’s computer to do what they want them to do.
  + Privilege escalation – in some cases, attackers gain higher system privileges.
* Stack overflow: overwrite the stack memory, potentially altering function return addresses.
* Heap overflow – overwrites dynamically allocated memroy, leading to unpredictable behaviour.
* Buffer overflow can be prevented using safe programing languages – e.g python, which automatically doesn’t allow an excess amount of data being written at a time.
* Use bound checking functions, which limits the amount of data copied or written into a buffer, ensuring that the operation does not exceed the buffer’s allocated size.

SQL injection:

* A malicious user can enter SQL commands via online databae forms to change the processing
* Can be avoided by using validation and sanitization e.g restrict user input length and allowed characters
  + Limiting database privileges for the application to prevent full access to the database
  + Use protection / security methods like firewalls.

Monitoring:

* Monitoring can protect against the threat of hacking, which can introduce malware.
  + Packet sniffers – analyse packet payload and-ord headers to detect suspicious activity.
    - E.g if an internal server is communicating with an unknown IP, it could indicate a breach.
    - Can detect suspicious outgoing data, e.g large file transfers to unapproved destinations with important data.
    - Can detect multiple failed login attempts from a single IP, indicating a brute force attack
    - Packet sniffers can also be used offensively to analyse data packets on another network to search for data that the hacker deems useful to hack.
  + User access logs – records details about who accesses a system, when, and from where
    - May include timestamp, username, IP, login tsatus, authentication method, session duration, actions performed
    - Can be used to detect brute force attacks, suspicious remote logins, unauthorised access to admin accounts, or other suspicious activity

Prevention:

* Up to date patches to an operating syste and application programs reduce vulnerabilities in the system
* Up to date anti malware software can prevent the spread of infection.