4.9.3.2 Internet Security

Firewall

A **firewall** is a piece of hardware or software that controls access to and from a network.

Firewall rules determine which network traffic is allowed through or blocked.

Packet filtering

- Packets of data are inspected by the firewall as they arrive to check which port they are trying to access.
- If the traffic is to be allowed through, the firewall will open the port for the duration of the connection.

Stateful inspection

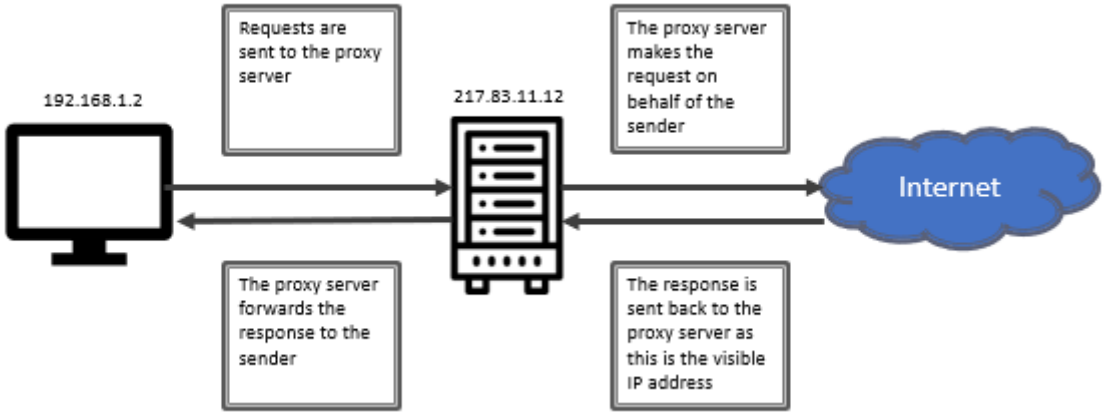
- Stateful inspection keeps track of active connections and uses this information when deciding whether to allow or block packets.
- The firewall maintains a state table containing details of active connections.
- A packet belonging to an established connection can be allowed through, while unexpected packets can be blocked according to the firewall rules
- E.g. is the packet part of an existing, valid connection?
  - ➢ If yes, then allow through
  - ➢ If no, then allow or block based on firewall rules

Proxy Server

A **proxy server** makes a web request on behalf of your own computer.

This hides the IP address of the device that made the real request behind that of the proxy server.

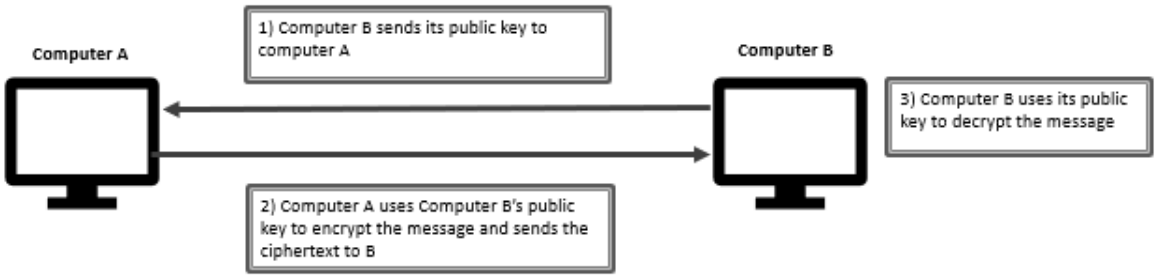
The web server sees the proxy server's IP address rather than the client's IP address.



Symmetric Encryption

Encryption is the act of encoding a plaintext message into and unreadable format (ciphertext). This stops intercepted messages from being understood if they are intercepted during transmission.

Symmetric encryption uses one key, the same key to encrypt and the decrypt the data being transferred.



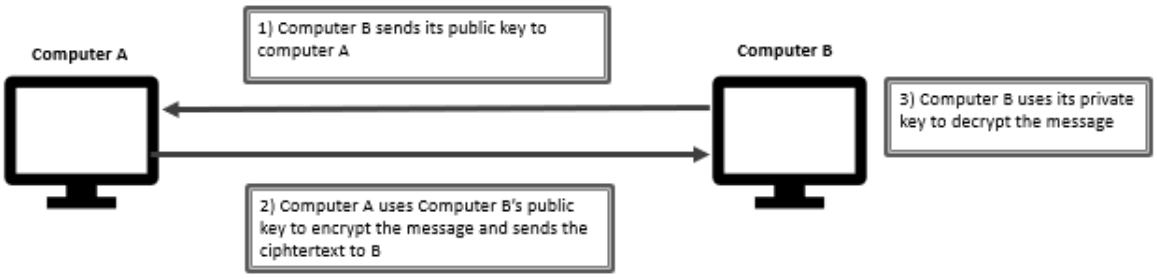
The main problem is securely exchanging the shared key. If the key is sent over an insecure network, an attacker could intercept it and decrypt the messages.

Asymmetric Encryption

Asymmetric encryption uses two separate keys, a public key to encrypt data and private key to decrypt data.

The public key can be sent openly over the network because it does not need to be kept secret.

As the private key is never transmitted over the network it cannot be intercepted and an attacker cannot decrypt the intercepted message without the recipient's private key.

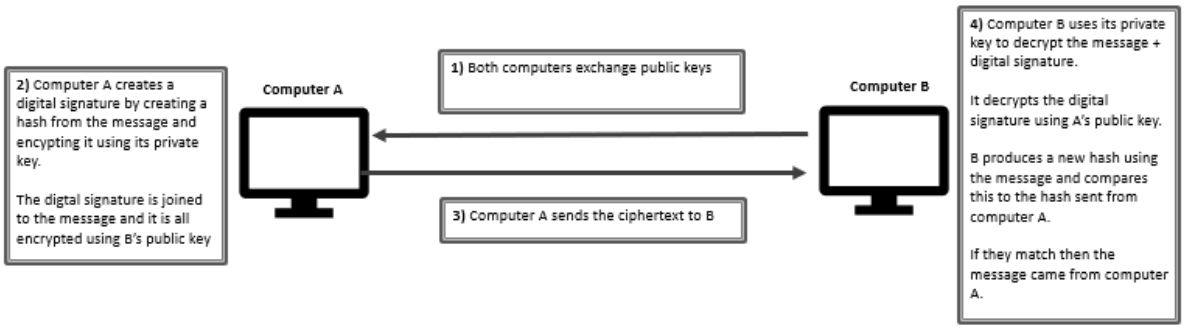


Digital Signatures

In order to verify the integrity of a message, the sender can add a digital signature to a message.

A calculation is carried out on the message to produce a value called a hash (or message digest). The hash is encrypted with the sender's private key to form the digital signature.

A digital signature is used authenticate the sender and verify that the message has not been altered.



Digital Certificates

A digital certificate links a public key to the identity of a person or organisation. A Certificate Authority (CA) verifies the identity and digitally signs the certificate.

A digital certificate can be provided to allow others to verify that a public key belongs to the claimed person or organisation.

These are provided by a Certificate Authority (CA) and provide:

- A serial number
- Name of the CA
- Expiry date
- Name of the holder
- Holder's public key
- CA's digital signature to verify the certificates origin

HTTPS uses digital certificates to help verify the identity of the website and establish a secure connection.

Malware

Malware is a piece of software with malicious intent.

Virus

- A virus infects by attaching itself to a legitimate host program.
- When the program executable is run, the virus activates and begins to replicate, corrupt files or damage systems.

Worm

- Worms are self-replicating and do not need interaction to run.
- They spread automatically over networks using vulnerabilities or open ports.
- Can carry payloads such as ransomware

Trojans

- Trojans disguise themselves as a legitimate program.
- The user is tricked into installing or running the program.
- Once inside it performs malicious actions such as spying or opening backdoors.

Vulnerabilities Exploited by Malware

Malware can exploit weaknesses in software, operating systems or user behaviour.

- Unpatched software — known security vulnerabilities may be exploited.
- Open ports/network vulnerabilities — worms can spread between vulnerable devices.
- Weak security practices — users may be tricked into installing a Trojan.
- Poor input validation — vulnerabilities such as buffer overflows can be exploited.

Protections Against Malware

Improved code quality, monitoring and security measures can reduce the risk and impact of malware.

Measures include:

- **Keep software and operating systems patched** to remove known vulnerabilities.
- **Use input validation and bounds checking** to reduce vulnerabilities such as buffer overflows.
- **Use strong passwords and two-factor authentication** to reduce unauthorised access.
- **Use access rights/permissions** to limit what compromised programs or users can access.
- **Monitor systems and network activity** to detect unusual behaviour.
- **Use anti-malware software** to detect and remove malicious software.