4.9.3.2 Internet Security

1) Explain **four** different ways that a firewall can protect computers on a LAN.

[4 marks]

- **Block/allow traffic on specific ports // specified protocols;**
- **Block/allow traffic from specific IP addresses;**
- **Block/allow packets according to specified criteria;**
- **Maintains information about current connections and only allows packets relevant to these connections through;**
- **Act as a proxy server / all traffic to the internet goes via the firewall;**
- **Identify unusual behaviour from a host e.g. a host sending large amounts of data;**
- **Rules can be written to specify conditions under which to block/allow traffic;**

---

2) A message is to be transmitted from computer A to computer B.

a) Explain what the key exchange problem is, in relation to a symmetric cipher.

[2 marks]

- **How to pass the key from the send to the receiver…;**
- **Without it being intercepted;**

The message will be encrypted using asymmetric encryption. To enable computer B to authenticate that the message was sent by computer A, a digital signature will also be sent with the message.

b) Explain how computer B will decrypt the message and verify that it was sent by computer A.

In your response you should refer to the specific keys that will be used in this process.

You do **not** need to explain how computer A will encrypt the message or create the digital signature.

[4 marks]

- **B's private key is used to decrypt the encrypted message and signature**
- **The message is rehashed**
- **A's public key is used to decrypt the digital signature**
- **If the hashes match, B can authenticate that the message was signed using A's private key and therefore verify the sender's identity**

---

3) A virus is a specific category of malware.

a) Define the term 'malware'.

- **A program/software with malicious/intrusive intent**

[1 mark]

b) Describe **three** other different categories of malware.

1 mark for name, 1 mark for description

- **Trojan; a program which misleads the user into thinking it is another piece of software. It needs the user to run the program to execute.**
- **Worm; code which will run autonomously and replicates itself and spreads automatically, often across networks.**
- **Spyware; a program which records data on a host system and forwards it to a third party.**
- **Ransomware; a program that encrypts a user's data and demands payment for the key.**
- **Keylogger; records a user's keystrokes**

[6 marks]

---

4) List **four** different measures that can be used to maintain the security of a computer system. Describe what the measure does and give an example of a threat that it would be effective against.

[8 marks]

1 mark for name, 1 mark for description

- **Antivirus**
  - **scans files to look for malicious code**
  - **quarantines suspicious files**
- **Firewall**
  - **Scans network traffic**
  - **Can block traffic from suspicious hosts/ ip addresses/ ports**
- **MAC address filtering**
  - **A table of allowed/blocked MAC addresses that is checked when allowing devices to connect to a network.**
- **Login/biometrics systems**
  - **Username and passwords/ unique characteristics such as fingerprints used to authenticate a user.**
- **Encryption**
  - **Data is transmitted/stored in an unreadable format (ciphertext)**
  - **Only those with a key can decrypt and read the data**
- **Prevent use of USB ports**
  - **External storage devices can not connected which could be used to upload malware/ steal data**

5) An internet café is evaluating the security for their network.

a) State **two** reasons why using a biometric authentication measure is better than password authentication for staff accounts.

[2 marks]

- **Staff could forget their password while biometric cannot be forgotten.**
- **An unauthorized could learn the password and use it while biometric data can't be used by others.**
- **Lower risk of hacking.**

b) Explain why it would not be appropriate for the café to use MAC address filtering on their wireless network.

[2 marks]

- **In an internet café, there are many different customers/devices,**
- **So maintaining a list of allowed MAC addresses would be impractical.**

6) The email message needs to be sent securely as it contains confidential information. The message will be encrypted using asymmetric encryption. To enable Computer B to authenticate that the message was sent by Computer A, a digital signature will also be sent with the message.

Describe how:

- Computer A will encrypt the message and create the digital signature
- Computer B will decrypt the message and verify that it was sent by Computer A.

In your response you should refer to the specific keys that will be used in this process.

[6 marks]

Transmission

- **A message digest/hash value is calculated from the message contents.**
- **The message digest/hash value is encrypted using A's private key.**
- **The encrypted message digest/hash value is known as the digital signature.**
- **The digital signature is appended to the message.**
- **The message and signature are encrypted using B's public key.**

Reception

- **B's private key is used to decrypt the message and signature.**
- **The message is rehashed // a new message digest/hash is calculated from the message.**
- **A's public key is used to decrypt the digital signature to produce the received message digest.**
- **If received message digest and recalculated message digest match then the sender can be authenticated/then B knows that A sent the message.**

7) Anti-virus software and user training are measures that can be used to reduce the threat posed by viruses.

Describe **four other** measures that can be used to reduce the threat posed by viruses.

[4 marks]

Monitoring

- **Firewall could block packets from sources/computers known to be high-risk // could block packets not part of a current communication (stateful inspection)**
- **Proxy server could receive/check downloaded files**
- **Spam filters can block emails from suspicious sources / email with suspicious content // block pop-ups that could contain harmful links // block downloads based on file types**
- **Digital certificates can be used to verify the source of a downloaded file**
- **Digital signature / checksum to verify that a file has not been changed // that a file came from a known source**

Protection

- **Enable automatic update of applications**
- **Use a virtual machine to execute programs**
- **Set access rights to minimise risk of viruses being able to access important files**
- **Disable execution of macros in documents from outside sources**
- **Restrict execution of software from unverified sources**
- **Backup data and keep it offline**
- **Disable external drives**
- **Use a MAC address allow list so that only known devices can join a network**
- **Use strong passwords / biometric access to make it harder for a hacker to access a computer to install a virus**

Code quality

- **Ensure code does not allow buffer overflow**
- **Test software for security vulnerabilities**
- **Carry out a code review so the code is independently checked by another programmer**
- **Use code analysis software to identify flaws**
- **Only use internet services/libraries from trusted sources**

8) Two computers, A and B, are involved in a secure communication that uses asymmetric encryption. A is sending a message to B.

Each computer has a public key and a private key.

a) Complete the missing words in the following paragraph.

A will encrypt the message using **B's public** key.
The message will be decrypted by **B** using **B's private** key.

[2 marks]

b) The security of the communication could be improved by the addition of a digital signature.

State **two** benefits of including a digital signature.

[2 marks]

- **Detect (unauthorised) changes to message**
- **Authenticate sender's identity**