Exercise walk-through

Cyber security ▪ 5.3

eXercise

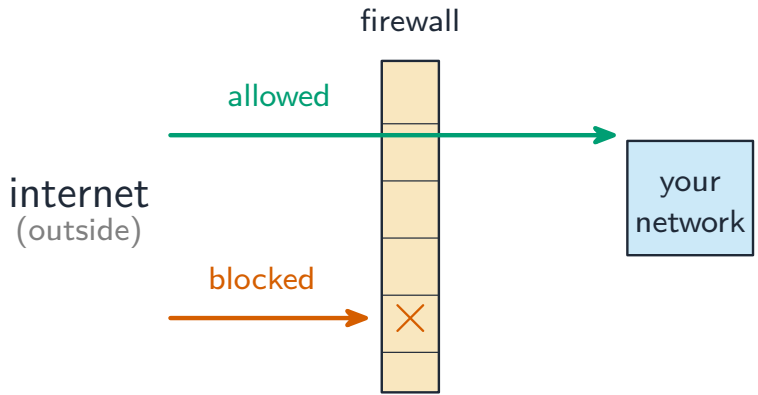
You must be able to

- describe threats (brute force, DDoS, phishing, pharming, social engineering)
- describe the types of malware
- describe security methods (firewall, authentication, anti-malware)

Method — Threats and protection

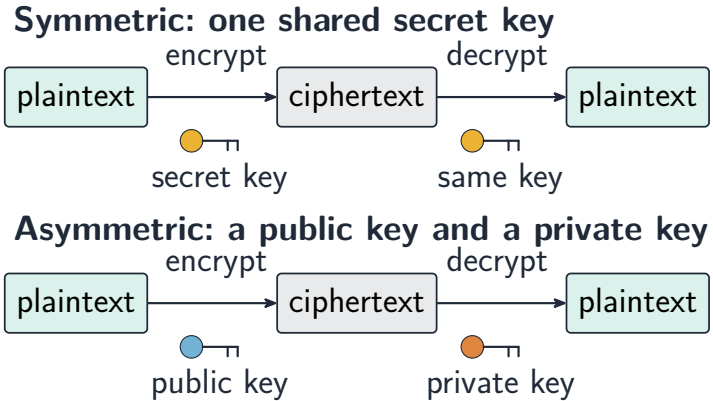
- **threats:** brute force, data interception, DDoS, hacking, malware, pharming, phishing, social engineering.
- **malware:** virus, worm, Trojan, spyware, adware, ransomware.

Method — Threats and protection



A firewall between the internet and a private network

Method — Threats and protection



Encryption is a key security measure against interception

Method — Keeping data safe: which measure answers which risk

Encryption 加密 scrambles data with a key so that an interceptor gets **ciphertext** 密文 they cannot read; the plaintext is recovered with the key. It does not stop the data being taken, it makes what is taken useless. **Symmetric encryption** uses the same key to encrypt and decrypt, so the key itself must be exchanged safely; **asymmetric encryption** uses a public key to encrypt and a matching private key to decrypt, so nothing secret has to be sent.

Secure sockets layer (SSL) and its successor TLS encrypt the traffic between a browser and a web server. The browser checks the site's **digital certificate**, then the two agree a session key. You can tell it is in use because the address begins `https` and a padlock appears.

Firewall 防火墙: examines traffic entering and leaving the network, compares it with a set of criteria, blocks what fails, logs traffic, and can block named sites or addresses.

Method — Keeping data safe: which measure answers which risk

Proxy server 代理服务器: sits between the user and the internet, so the web server never sees the user's own address. It can filter traffic, keep a cache of pages so they load faster, and act as a firewall.

Access rights 访问权限: each user gets only the permissions their role needs (read, read-and-write, none), so a person who is not authorised cannot see or change a file even after logging in.

Authentication 身份验证: passwords, biometrics (fingerprint, face, iris), and two-step verification, which sends a one-time code to a device the real user holds.

Worked example. A hospital keeps patient records on a server used by doctors and receptionists. Suggest measures. Encrypt the records so a stolen copy is unreadable; use access rights so receptionists see only appointment details while doctors see the medical notes; use biometrics or two-step verification, so a stolen password alone is not enough; put a firewall between the server and the internet to block unauthorised traffic.

Practice 2.1 ▪ 1 mark

State what a brute force attack is.

Solution 2.1

Method: Threats and protection

Worked steps

trying many passwords very quickly until the right one is found B1.

Practice 2.2 ▪ 1 mark

State what ransomware does.

Solution 2.2

Worked steps

it locks your files and demands payment to unlock them B1.

Practice 2.3 ▪ 2 marks

Give the name of the data before and after encryption.

Solution 2.3

Method: Keeping data safe: which measure answers which risk

Worked steps

Plaintext before, ciphertext after B1 B1.

Practice 2.4 ▪ 2 marks

Identify two tasks performed by a proxy server.

Solution 2.4

Method: Keeping data safe: which measure answers which risk

Worked steps

Any two of: it filters traffic; it keeps a cache of web pages so they load faster; it hides the user's IP address from the web server; it acts as a firewall B2.

Practice 2.5 ▪ 2 marks

Explain why encryption does not stop data being intercepted.

Solution 2.5

Method: Keeping data safe: which measure answers which risk

Worked steps

Encryption only scrambles the data B1; an interceptor can still take a copy, but without the key the ciphertext is meaningless to them B1.

Exam-style 3.1 ▪ 1 mark

A firewall protects a network by:

A scanning for viruses

B checking data in/out and blocking what is not allowed

C encrypting files

D hiding the IP address

Solution 3.1

A scanning for viruses

B checking data in/out and blocking what is not allowed ✓

C encrypting files

D hiding the IP address

Worked steps

B. A firewall checks data in/out and blocks anything not allowed.

Exam-style 3.2 ▪ 2 marks

A company wants to protect its data.
(a) Describe what a phishing attack is.
(b) State two methods (other than a firewall) to keep data safe.

Solution 3.2

Method: Keeping data safe: which measure answers which risk

Worked steps

(a) fake emails/messages M1 that trick you into giving away private details A1.
(b) any two of: authentication (password/biometrics/two-step); anti-malware; access levels; automatic updates; proxy server B1 B1.

Exam-style 3.3 ▪ 2 marks

State the difference between a virus and a worm.

Solution 3.3

Method: Threats and protection

Worked steps

(a) The readable plaintext is scrambled using a key so that it becomes ciphertext **B1**, which cannot be understood without the matching key to decrypt it **B1**.
(b) SSL, or its successor TLS **B1**; the address begins with `https` or a padlock is shown in the address bar **B1**.
(c) Any two of: it examines the traffic entering and leaving the network; it compares that traffic with a set of criteria and blocks anything that fails; it keeps a log; it blocks named sites or IP addresses **B2**.
(d) Each user is given only the permissions their job needs **B1**, so a receptionist who

Solution 3.3

logs in cannot open or change files reserved for doctors B1.
(e) After the password is accepted, a one-time code is sent to a device the real user holds, such as their phone B1; the user must enter that code to complete the log-in B1; a thief who has only the password still cannot get in without the device B1.
(f) With asymmetric encryption the bank publishes a public key that anyone may use to encrypt B1, so no secret key has to be sent over the internet where it could be intercepted, unlike symmetric encryption B1.

Exam-style 3.3 ▪ 2 marks

An online bank protects its customers' data.
(a) Explain what happens to data when it is encrypted, using the terms plaintext and ciphertext.
(b) Identify the protocol that encrypts the connection between a customer's browser and the bank's server, and give one way the customer can tell it is being used.
(c) Describe two tasks a firewall performs for the bank's network.
(d) Bank staff have different access rights. Explain how access rights protect customer data even from someone who has logged in successfully.
(e) The bank adds two-step verification. Describe how it works and explain why it is safer than a password alone.
(f) Explain one advantage of asymmetric encryption over symmetric encryption when a customer first connects.

Solution 3.3

Method: Keeping data safe: which measure answers which risk

Worked steps

(a) The readable plaintext is scrambled using a key so that it becomes ciphertext B1, which cannot be understood without the matching key to decrypt it B1.
(b) SSL, or its successor TLS B1; the address begins with `https` or a padlock is shown in the address bar B1.
(c) Any two of: it examines the traffic entering and leaving the network; it compares that traffic with a set of criteria and blocks anything that fails; it keeps a log; it blocks named sites or IP addresses B2.
(d) Each user is given only the permissions their job needs B1, so a receptionist who

Solution 3.3

logs in cannot open or change files reserved for doctors B1.
(e) After the password is accepted, a one-time code is sent to a device the real user holds, such as their phone B1; the user must enter that code to complete the log-in B1; a thief who has only the password still cannot get in without the device B1.
(f) With asymmetric encryption the bank publishes a public key that anyone may use to encrypt B1, so no secret key has to be sent over the internet where it could be intercepted, unlike symmetric encryption B1.