Exercise walk-through

Types of software and interrupts ▪ 4.1

eXercise

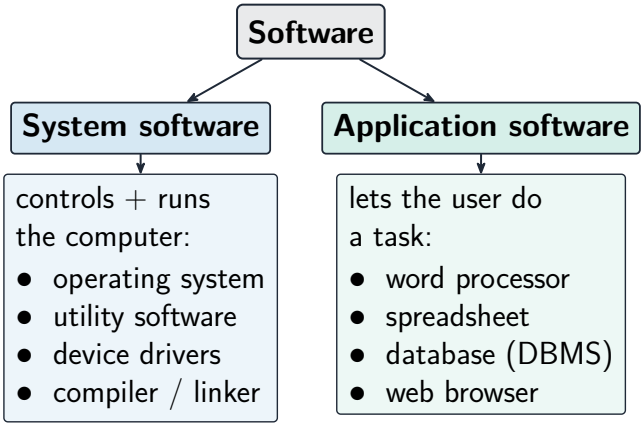
You must be able to

- classify software as system or application
- give the roles of the operating system
- describe an interrupt and how the processor handles it

Method — Software and the OS

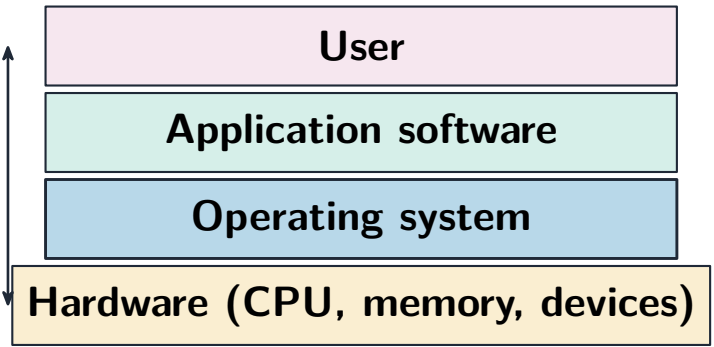
- an **interrupt** tells the processor something needs attention now.

Method — Software and the OS



Software tree: system vs application

Method — Software and the OS



the OS lets the hardware, software and user work together

The OS sits between hardware and applications/user

Method — Naming the threats, and matching each to its prevention

Learn each threat as a pair: what it does, and what stops it.

Threat	What it does	Prevention
brute-force attack 暴力破解	tries every combination until a password works	strong passwords, a limit on log-in attempts, two-step verification
data interception 数据拦截	uses a packet sniffer to read data as it travels	encryption, a wireless network key (WPA)
DDoS attack 分布式拒绝服务	floods a server with requests so real users cannot get through	firewall, a proxy server, filtering traffic
hacking 黑客攻击	gains unauthorised access to a system	firewall, strong passwords, access rights
malware 恶意软件	virus, worm, trojan horse, spyware, ransomware, adware	anti-malware software, do not open unknown attachments
phishing 网络钓鱼	a fake email or message tricks the user into giving details	do not click links in unexpected mail, check the address, anti-spam filters
pharming 域名劫持	malicious code redirects the user to a fake website	anti-malware, check the site's certificate and the URL
social engineering 社会工程	manipulates a person into breaking security (a fake phone call, tailgating)	staff training, verify who is asking, clear procedures

Method — Naming the threats, and matching each to its prevention

Malware, distinguished. A **virus** attaches to a file and needs the user to run it; a **worm** copies itself across a network without help; a **trojan horse** is disguised as a useful program; **spyware** records keypresses; **ransomware** encrypts files and demands payment.

Phishing or pharming? Phishing starts with a message the user must act on. Pharming needs no message: code on the computer or the DNS server sends the user to a fake site even when they type the correct address.

Worked example. A user types the correct bank address and reaches a page that looks right but is not the bank. Identify the threat and give two preventions. The threat is pharming, because no message was involved and the correct address was used. Preventions: run anti-malware to remove the redirecting code, and check the site's security certificate and the padlock before entering any details.

Practice 2.1 ▪ 1 mark

State whether a web browser is system or application software.

Solution 2.1

Method: Software and the OS

Worked steps

application software B1.

Practice 2.2 ▪ 2 marks

State two roles of the operating system.

Solution 2.2

Method: Software and the OS

Worked steps

any two of: managing files; managing memory; handling interrupts; providing a user interface; managing peripherals; multitasking; security B1 B1.

Practice 2.3 ▪ 2 marks

Identify the threat in each case: an email says your account will close unless you confirm your password; a server is flooded with requests until it stops responding.

Solution 2.3

Method: Naming the threats, and matching each to its prevention

Worked steps

Phishing B1; a DDoS (distributed denial of service) attack B1.

Practice 2.4 ▪ 2 marks

Give one difference between a virus and a worm.

Solution 2.4

Method: Naming the threats, and matching each to its prevention

Worked steps

A virus attaches itself to a file and needs the user to open or run it B1; a worm copies itself across a network on its own, without any user action B1.

Practice 2.5 ▪ 2 marks

Name two ways to prevent a brute-force attack.

Solution 2.5

Method: Naming the threats, and matching each to its prevention

Worked steps

Any two of: use a strong password with a mix of characters; limit the number of log-in attempts; use two-step verification; add a delay after failed attempts B2.

Exam-style 3.1 ▪ 1 mark

Which is system software?

A spreadsheet

B device driver

C word processor

D web browser

Solution 3.1

A spreadsheet

B device driver ✓

C word processor

D web browser

Worked steps

B. A device driver is system software.

Exam-style 3.2 ▪ 1 mark

A printer runs out of paper while printing.
(a) State the type of interrupt this is.
(b) Describe what the processor does when an interrupt arrives.

Solution 3.2

Method: Software and the OS

Worked steps

(a) a hardware interrupt B1.
(b) the processor stops what it is doing and saves its place M1; it runs the interrupt service routine to deal with it M1; then restores its place and carries on A1.

Exam-style 3.3 ▪ 6 marks

An online shop is worried about security.
(a) Complete the table by naming the threat described and giving one way to prevent it.

Description	Threat	Prevention
customers are sent an email asking them to confirm their card details		
data is read by a packet sniffer as it travels over the wireless network		
the site is flooded with requests until real customers cannot connect		

Exam-style 3.3 ▪ 6 marks

(b) Explain the difference between phishing and pharming.
(c) The shop installs a firewall. Describe two tasks a firewall performs.
(d) The shop also uses two-step verification. Explain how it protects an account even if the password is stolen.
(e) An employee receives a phone call from someone claiming to be from the IT department, asking for their password. Identify this threat and state one way staff can be prepared for it.

Solution 3.3

Method: Naming the threats, and matching each to its prevention

Worked steps

(a) Phishing, prevented by not clicking links in unexpected email, checking the sender's address, or using an anti-spam filter B2; data interception, prevented by encrypting the data or using a wireless network key B2; DDoS attack, prevented by a firewall, a proxy server or filtering the incoming traffic B2.
(b) Phishing sends the user a message, and the user must click a link or reply for the attack to work B1; pharming needs no message: malicious code on the computer or the DNS server redirects the user to a fake site B1; so in pharming the user can type the correct address and still arrive at the fake site B1.

Solution 3.3

(c) Any two of: it examines the traffic entering and leaving the network; it checks that traffic against a set of criteria and blocks what fails; it keeps a log of traffic; it can block access to named sites or IP addresses **B2**.
(d) A second code is sent to a device the real user holds, such as their phone **B1**; the attacker with the password still cannot log in without that code **B1**.
(e) Social engineering **B1**; staff training, so employees know never to give a password over the phone and always verify who is asking **B1**.