

4.1 Types of software and interrupts

Name: _____ Class: _____ Date: _____

Total: 29 marks

KEY WORDS interrupt 中断 • operating system 操作系统 • system software 系统软件 • application software 应用软件
• system vs application software 系统

Objective

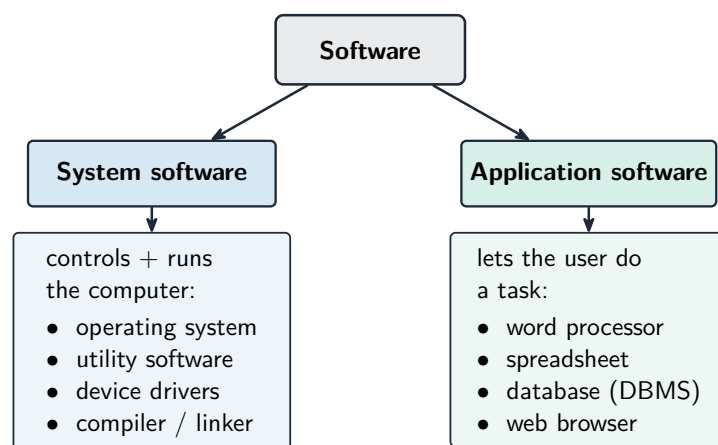
Build the skills to answer exam questions on **software and interrupts** 软件与中断 — **system vs application software** 系统/应用软件, the **operating system** 操作系统, and **interrupts** 中断.

You must be able to:

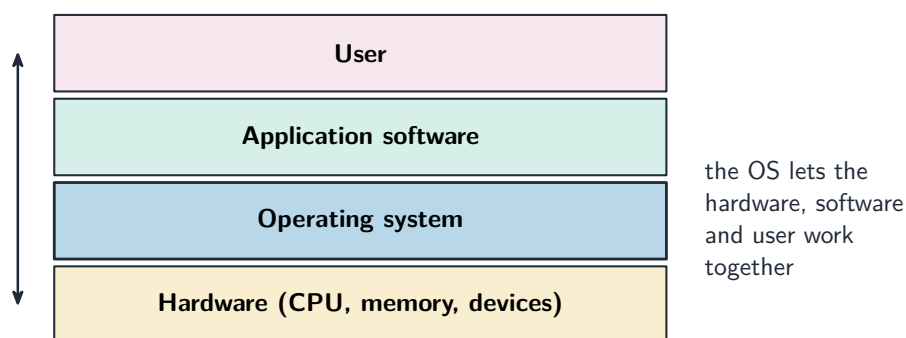
- classify software as system or application
- give the roles of the operating system
- describe an interrupt and how the processor handles it

1 Worked examples

■ Software and the OS



System software runs the computer; application software lets the user do a task



OS roles: manage files, memory, peripherals, multitasking, security; handle interrupts; provide a UI

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

■ 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

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.

2 Practice

2.1 State whether a web browser is system or application software. [1]

2.2 State two roles of the operating system. [2]

2.3 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. [2]

2.4 Give one difference between a virus and a worm. [2]

2.5 Name two ways to prevent a brute-force attack. [2]

3 Exam-style questions

3.1 Which is system software? [1]

- A spreadsheet
- B device driver
- C word processor

- **D** web browser

3.2 A printer runs out of paper while printing.

(a) State the type of interrupt this is. [1]

(b) Describe what the processor does when an interrupt arrives. [3]

3.3 An online shop is worried about security.

(a) Complete the table by naming the threat described and giving one way to prevent it. [6]

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		

(b) Explain the difference between phishing and pharming. [3]

(c) The shop installs a firewall. Describe two tasks a firewall performs. [2]

(d) The shop also uses two-step verification. Explain how it protects an account even if the password is stolen. [2]

(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. [2]

Solutions

2.1 application software.

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

3.1 B. A device driver is system software.

3.2 (a) a hardware interrupt.

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

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

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

2.5 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.

3.3 (a) Phishing, prevented by not clicking links in unexpected email, checking the sender's address, or using an anti-spam filter; data interception, prevented by encrypting the data or using a wireless network key; DDoS attack, prevented by a firewall, a proxy server or filtering the incoming traffic.

(b) Phishing sends the user a message, and the user must click a link or reply for the attack to work; pharming needs no message: malicious code on the computer or the DNS server redirects the user to a fake site; so in pharming the user can type the correct address and still arrive at the fake site.

(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.

(d) A second code is sent to a device the real user holds, such as their phone; the attacker with the password still cannot log in without that code.

(e) Social engineering; staff training, so employees know never to give a password over the phone and always verify who is asking.