AP COMPUTER SCIENCE PRINCIPLES • EXERCISE SHEET

5.6 Safe Computing

Name: _____ Class: _____ Date: _____ **Total: 49 marks**

KEY WORDS malware 恶意软件 • encryption 加密 • authentication 身份验证 • phishing 网络钓鱼 • multifactor authentication 多因素身份验证

Objective

Build the skills to answer exam questions on **safe computing** 安全计算: what personal data is collected, how it can be misused, how systems are protected, and how unauthorised access is actually gained.

You must be able to:

- say what **personally identifiable information (PII)** 个人身份信息 is, and give the benefits *and* the risks of putting it online
- explain how **aggregation** 聚合 turns harmless separate data into private knowledge
- describe **authentication** 身份验证 measures, including **multifactor authentication** 多因素身份验证
- explain how **encryption** 加密 protects data, and distinguish **symmetric** 对称 from **asymmetric** 非对称
- name and describe the routes to unauthorised access: phishing, keylogging, rogue access points, malicious links, unsolicited attachments, untrustworthy downloads
- distinguish a **computer virus** 计算机病毒 from **malware** 恶意软件 generally

1 Worked examples

Study these first. Each one shows the method for a question type used later.

■ PII: the benefit and the risk are the same fact

PII is any information that identifies, links to, relates to or describes an individual - a name, an address, an ID number, a fingerprint, a date of birth.

The exam almost always wants **both sides**, because the convenience and the danger come from the same stored data:

Benefit	Risk from the same data
stored card details make purchases quick	the same details enable identity theft
search history gives better suggestions	the same history is sold for targeted marketing
location data gives directions and recommendations	the same trail shows where you live and when you are out

Two further facts the exam tests directly: once information is online it is **difficult to delete**, and it can be used in ways never intended - an email is forwarded, a post is screenshotted, a photo outlives the account it was posted from.

■ Aggregation - the idea most answers miss

Disparate pieces of data, each harmless alone, can be **combined** to create knowledge the person never disclosed.

Example. Geolocation shows a house each night. Cookies show visits to a diabetes forum. A social post names an employer. Separately: three ordinary facts. Aggregated: home address, likely medical condition, and workplace - enough to stalk, to defraud, or to plan a crime.

When a question says "explain how this data could be misused", **name a second source and combine them**. A single-source answer rarely earns full marks.

■ Protecting a system

- **Strong password** - easy for the user to remember, hard for someone who knows them to guess. Length and unpredictability, not just symbols.
- **Multifactor authentication (MFA)** - access is granted only after presenting **several separate pieces of evidence**, typically at least two steps. Each step is another layer an attacker must break, so a stolen password alone is no longer enough.
- **Antivirus / malware scanning** helps protect against infection.
- **Regular software updates** fix the errors and design flaws every real system has - the reason "install updates" is a security measure and not just maintenance.
- **Review app permissions**, because users can control what programs collect.

■ Encryption

Encryption encodes data to prevent unauthorised access; **decryption** decodes it.

- **Symmetric** - **one shared key** encrypts and decrypts. Fast, but the key itself has to reach the other person safely.
- **Asymmetric** - a **public/private key pair**. The public key encrypts, only the private key decrypts, so nothing secret has to be sent in advance.

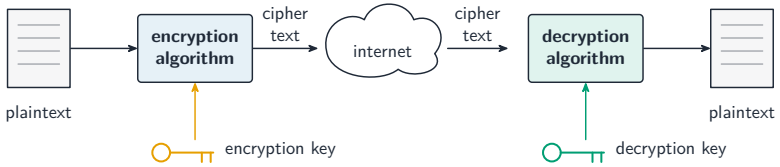
Certificate authorities issue digital certificates that validate who owns a public

key. Without them you could encrypt perfectly - to an impostor.

■ **How access is actually gained**

Route	What it does
Phishing	tricks a user into *handing over* information
Keylogging	records **every keystroke**, capturing passwords as they are typed
Rogue access point	a wireless access point giving unauthorised access to a secure network; data on public networks can be intercepted, analysed and **modified**
Malicious link	disguised in a page or an email
Unsolicited attachment	from an unknown sender **or a known sender whose account was compromised**
Untrustworthy download	free-ware and share-ware sites can carry malware

Virus vs malware. *Malware* is the whole category: software intended to damage a system or take partial control of it. A *virus* is one kind - it **copies itself** and often attaches to a legitimate program, running when that program runs.



2 Practice

2.1 State what PII is and give **three** examples. [4]

2.2 For each item, give one benefit to the user and one privacy risk.

(a) A shopping site storing your card details. [2]

(b) A search engine keeping your search history. [2]

(c) A map app recording your location. [2]

2.3 Explain what is meant by **aggregating** personal data, and give an example of private knowledge that could be deduced from two ordinary sources. [3]

2.4 Explain why "just delete the post" is not a complete answer to an online privacy problem. [2]

2.5 Describe **multifactor authentication** and explain why it protects an account whose password has already been stolen. [3]

2.6 State what makes a password strong, according to the course. [2]

2.7 Name the threat described in each case.

(a) A program silently records every key the user presses. [1]

(b) A wireless access point set up to give outsiders entry to a company network. [1]

(c) An email appearing to be from a bank asks the user to confirm a password. [1]

(d) A free video converter downloaded from an unknown site installs hidden software. [1]

2.8 State the difference between a **computer virus** and **malware**. [2]

2.9 Explain why regular software updates are a security measure, not just maintenance. [2]

3 Exam-style questions

3.1 PII stands for personally identifiable [1]

- **A** internet
- **B** information
- **C** interface
- **D** index

3.2 Encryption protects data by [1]

- **A** deleting it
- **B** encoding it so only authorized users can read it
- **C** compressing it
- **D** sorting it

3.3 Which best describes the role of a certificate authority? [1]

- **A** it encrypts the data before it is sent
- **B** it validates who owns an encryption key
- **C** it stores a copy of every private key
- **D** it scans downloads for malware

3.4 A user connects to free airport Wi-Fi and signs in to email. The network is a rogue access point. Which statement is correct? [1]

- **A** data on the network can be intercepted, analysed and modified
- **B** the data is safe because the login page loaded normally
- **C** only unencrypted attachments are at risk
- **D** a strong password prevents interception

3.5 A fitness app records each run: route, start time and duration. It offers to publish a weekly summary to the user's social media, and asks for permission to read the phone's contacts "to find friends". The user re-uses one password across the app, their email and their bank.

(a) Identify **two** pieces of PII the app holds and state how each could be misused. [4]

(b) Explain how combining the published run summaries with the user's social media posts could reveal information the user never chose to share. [3]

(c) The user believes the contacts permission is harmless because they have nothing to hide. Give **two** reasons this reasoning is unsafe. [2]

(d) The app's password database is stolen. Explain the specific consequence of the user's password re-use, and describe **two** measures that would have limited the damage. [5]

(e) The app now encrypts all data sent to its servers. Explain what encryption does and does not protect against here, referring to at least one threat that remains. [3]

Solutions

2.1 information about an individual that identifies, links to, relates to or describes them; any three of: name, address, ID or passport number, date of birth, phone number, email address, fingerprint or other biometric, place of work.

2.2 (a) faster purchases with no re-typing; the stored details enable identity theft or fraudulent purchases if the store is breached. (b) more relevant results and suggestions; the history can be used for targeted marketing, or reveal interests the user never stated. (c) directions and local recommendations; the record shows where the user lives, works and when their home is empty.

2.3 aggregation is combining disparate pieces of data - each harmless alone - to create knowledge about an individual. Example: geolocation gives a home address and cookies from a health forum suggest a condition, so together they identify a specific person's likely medical condition, which neither source stated. Accept any two genuinely separate sources with a deduced conclusion.

2.4 once information is placed online it is difficult to delete - it may already have been forwarded, retweeted, screenshotted or copied by others, so the original's removal does not remove the copies.

2.5 MFA grants access only after the user presents several separate pieces of evidence, typically at least two steps; each step is an additional layer that must be broken; so a stolen password is only one factor and the attacker still cannot reach the account without the second.

2.6 it is easy for the user to remember but difficult for someone else to guess even knowing that user - so not a birthday, a pet's name or anything posted publicly.

2.7 (a) keylogging. (b) rogue access point. (c) phishing. (d) untrustworthy download / malware from freeware.

2.8 malware is the general category - software intended to damage a computing system or take partial control of its operation; a virus is one kind of malware that copies itself and often attaches to a legitimate program, running when that program runs.

2.9 every real-world system has errors or design flaws that can be exploited to compromise it; an update fixes those flaws, so an unpatched system stays exploitable by an attack that is already publicly known.

3.1 B.

3.2 B.

3.3 B. A certificate authority validates ownership of an encryption key, on a trust model. Without it, an attacker's key could be accepted as the recipient's.

3.4 A. Data sent over public networks can be intercepted, analysed **and modified**. A normal-looking page proves nothing, and a strong password does not stop interception of the traffic.

3.5 (a) any two of: **location/route data** - reveals home address and daily pattern, enabling stalking or a burglary timed to an absence; **timestamps** - show when the home

is regularly empty; **contacts** - allow phishing of friends from a trusted name; **name and account identity** - supports identity theft.

(b) each source alone is ordinary, but a run that starts and ends at the same point every morning identifies the home, while a social post names the employer or school; combined they give a named individual, a home address and a predictable time window - none of which the user posted.

(c) any two of: the data is not only about them - the contacts belong to other people who did not consent; data collected now can be used later in ways not intended, and cannot be deleted once shared; aggregation means harmless data becomes harmful in combination; a breach of the app exposes it regardless of the user's own conduct.

(d) the attacker now holds a working password for the **email and bank accounts as well**, because re-use means one breach compromises every account sharing that password; and the email account is the reset route for the others, so control of it can unlock accounts that used a different password. Measures - any two of: a unique password per account, so a breach is contained; multifactor authentication, so a stolen password is not sufficient; a password manager, which makes unique passwords practical.

(e) encryption encodes the data in transit and at rest so an interceptor cannot read it. It does **not** protect against threats that bypass it: a phishing message that gets the user to hand over the password, keylogging that captures it as it is typed, or malware on the device that reads the data after decryption; nor does it help once the attacker holds a valid credential, because the system then decrypts for them.