AP CYBERSECURITY • EXERCISE SHEET

5.2 Protecting Applications and Data: Managerial Controls and Access Controls

Name: _____ Class: _____ Date: _____ **Total: 51 marks**

KEY WORDS access control models 访问控制模型 • in transit 传输中数据 • in use 使用中数据 • regulated 受监管 • principle of least privilege 最小权限原则

Objective

Build the skills to answer exam questions on **data states** 数据状态 and classification, **managerial controls** 管理控制 for applications and data, **access control models** 访问控制模型, and **Linux permissions** Linux 权限.

You must be able to:

- name the three states of data and the control that protects each
- explain why regulated data is labelled, and what a policy must then specify
- say what a cryptography policy and a web application security policy each contain
- choose the right access model (RBAC, RuBAC, DAC, MAC) from a scenario, using subjects, objects and operations
- apply the two Bell-LaPadula properties ("write up, read down")
- read and write Linux permissions in both the numeric and the symbolic method
- apply the **principle of least privilege** 最小权限原则

1 Worked examples

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

■ The three states of data

Ask **where the data is right now**, then name the control that fits that place.

State	Where it is	What protects it
At rest	stored on a drive	physical security of the drive, plus encryption so a stolen disk is useless
In transit	moving between devices	protect the cable or link, plus encryption so an intercepted packet is unreadable
In use	being processed by software or read by a person	access control - and note the data **must be unencrypted** to be processed, so this is the hardest state to protect

More sensitive data earns a higher degree of security, and **regulated** data (health, financial, personal) is **labelled** so that the storage, transmission and handling rules the law requires can actually be applied.

■ Naming what a policy contains

A policy is a *managerial* control: it does not stop an attack itself, it states what must be in place.

- A **cryptography policy** names the approved algorithms for each use, the minimum or maximum **key lengths**, and how keys are **generated** and **stored**.
- A **web application security policy** states when an application must be assessed, how the assessment is carried out (which tools or framework), and the **timeline for fixing** each vulnerability according to its risk.

The give-away in a question is a *rule about a rule*: "keys must be at least 256 bits" is a policy line, not a control acting on data.

■ Choosing the access control model

First name the three parts: **subjects** (users or applications), **objects** (files or applications), **operations** (access, modify, add, remove). Then ask **who decides**:

Model	The decider	Give-away
RBAC	your role	"everyone in role X can..."
RuBAC	a rule or condition	time of day, location, device
DAC	the object's owner	"the file's owner grants access"
MAC	central levels	"secret", "top secret", clearance

Bell-LaPadula is a MAC model built for governments and the military. Two properties, and the exam wants both:

- **Simple Security Property** - a subject may **not read above** its level.
- *** (Star) Security Property** - a subject may **not write below** its level.

Together: **write up, read down (WURD)**. Reading down is safe because you already have that clearance; writing up is safe because it cannot leak a secret downwards.

Example. A "Secret" analyst may read a "Confidential" file (reading down) and may write into a "Top Secret" report (writing up), but may not read the "Top Secret" file, and may not paste its contents into a "Confidential" one.

■ **Linux permissions - both methods**

Order never changes: **read (4), write (2), execute (1)**, for **owner, group, others**.

`ls -l` prints ten characters: a file-type character then three sets of three.

```
-rwxr-x---
 ^^^ owner: read+write+execute = 7
    ^^^ group: read+execute    = 5
       ^^^ others: none        = 0     ->  chmod 750
```

A `+` at the end of the string means extra permissions are set beyond these three sets.

Numeric method - `chmod ### filename`, one digit per entity: `chmod 640 report.txt`.

Symbolic method - `chmod entity +/- permission filename`, where `u` = user owner, `g` = group, `o` = others, `a` = all: `chmod g+w report.txt` adds write for the group without touching anything else.

Choose symbolic when you want to **change one thing**, numeric when you want to **set the whole state**.

2 Practice

2.1 Name the state of the data in each case, and give one control that protects it.

(a) A patient database on an office server's hard disk overnight. [2]

(b) A card number travelling from a shop terminal to the bank. [2]

(c) A spreadsheet open on an accountant's screen. [2]

2.2 Explain why data **in use** is the hardest state to protect. [2]

2.3 A hospital collects regulated patient data.

(a) State why the hospital labels these data. [1]

(b) State **two** things the law may require the policy to specify. [2]

2.4 State **two** items a cryptography policy would contain, and **two** a web application security policy would contain. [4]

2.5 Name the access-control model in each case.

(a) "Access allowed only during business hours." [1]

(b) "Every user with the role 'nurse' can open patient charts." [1]

(c) "The document's owner chooses who else may edit it." [1]

(d) "A user cleared to Confidential cannot open a file marked Secret." [1]

2.6 A subject is cleared to **Secret** under Bell-LaPadula. State whether each action is allowed, and name the property that decides it.

(a) Reading a Confidential file. [2]

(b) Reading a Top Secret file. [2]

(c) Writing into a Top Secret report. [2]

2.7 Write the chmod number for each requirement.

(a) Owner read+write, group read, others nothing. [1]

(b) Owner read+write+execute, group read+execute, others read+execute. [1]

(c) Owner read+write, nobody else anything. [1]

2.8 A file listing shows `-rwxrw-r--`.

(a) Write the equivalent chmod number. [1]

(b) Write the symbolic command that removes write access from the group, changing nothing else. [1]

(c) Explain why the symbolic method is safer than re-typing a numeric value here. [1]

3 Exam-style questions

3.1 "Every user with the role 'nurse' can open patient charts" describes [1]

- **A** RuBAC
- **B** RBAC
- **C** DAC
- **D** MAC

3.2 The permission string -rw-r—— corresponds to which chmod number? [1]

- **A** chmod 444
- **B** chmod 640
- **C** chmod 740
- **D** chmod 777

3.3 Under Bell-LaPadula, a subject at Confidential attempts to write into a Secret file. This is [1]

- **A** denied by the Simple Security Property
- **B** denied by the Star Security Property
- **C** allowed, because writing up is permitted
- **D** allowed, because reading down is permitted

3.4 Which is a **managerial** control rather than a technical one? [1]

- **A** a firewall rule blocking port 23
- **B** a document stating the minimum key length for stored data
- **C** full-disk encryption on every laptop
- **D** an intrusion detection system

3.5 A university research group stores anonymised medical data used by three kinds of user: research staff, an external statistician on a six-month contract, and undergraduates who may read but never change the data. The data are copied nightly to a backup server across the campus network. A file currently shows `-rwxrwxrwx`.

(a) Name the state of the data during the nightly copy, and state the control that protects it. [2]

(b) Choose an access-control model for the three kinds of user and justify the choice, naming the subjects, objects and operations involved. [4]

(c) The statistician's contract restricts access to weekdays. Name the model that adds this and explain how it works alongside your answer to (b). [2]

(d) The current permissions break the **principle of least privilege**. State what least privilege means, explain the specific danger of `-rwxrwxrwx` here, and give the chmod number you would set instead, justifying each digit. [5]

(e) The group writes a cryptography policy for the backup. State **two** parameters it must specify and explain why a policy is needed when encryption software is already installed. [3]

Solutions

2.1 (a) at rest; physical protection of the drive, or encryption so a stolen disk is unreadable. (b) in transit; protect the link, or encrypt so an intercepted packet is unreadable. (c) in use; access control limiting who may view or edit.

2.2 the data must be **unencrypted** to be processed, so encryption cannot protect it at that moment and the only defence left is access control over who or what may use it.

2.3 (a) so that the storage, transmission and handling rules the law requires can be applied to exactly those data. (b) any two of: how the data must be stored; how they may be transmitted; who may handle them; retention or disposal rules; breach reporting.

2.4 cryptography policy - any two of: approved algorithms for each use; minimum or maximum key lengths; key-generation requirements; key-storage requirements. Web application security policy - any two of: when an application is subject to assessment; how the assessment is carried out (tools or framework); timelines for remediating vulnerabilities by risk level.

2.5 (a) RuBAC / rule-based. (b) RBAC / role-based. (c) DAC / discretionary. (d) MAC / mandatory.

2.6 (a) allowed - reading down, permitted by the Simple Security Property, which only forbids reading *above* your level. (b) not allowed - the Simple Security Property forbids reading above your level. (c) allowed - writing up, permitted; the Star Security Property only forbids writing *below* your level.

2.7 (a) 640. (b) 755. (c) 600.

2.8 (a) 764. (b) `chmod g-w` followed by the filename. (c) it changes only the one permission asked for, so an owner or others setting cannot be altered by mistake while re-typing three digits.

3.1 B. Access follows the role, so RBAC.

3.2 B. Owner rw = 6, group r = 4, others none = 0.

3.3 C. Writing up is allowed; the Star Property forbids writing *below* your level, and the Simple Property governs reading, not writing.

3.4 B. A statement of a required parameter is a rule about what must be in place - managerial. The other three act on traffic or data directly.

3.5 (a) data **in transit**; encrypt the transfer, and protect the physical campus link.

(b) **RBAC**. Subjects are the three groups of users, objects are the data files, operations are read and modify. Each of the three kinds of user maps cleanly onto a role, so access is granted once per role rather than per person, and a new undergraduate inherits the correct access on the day they are added, with nothing to revoke individually when the statistician's contract ends. Accept DAC only if the answer argues the owner should decide *and* notes the loss of central consistency.

(c) **RuBAC**. A rule-based layer evaluates the condition - weekday - and allows or denies on top of the role the subject already holds, so the two work together rather than replacing each other.

(d) least privilege = each entity is given exactly the access it needs to do its job and no more. `-rwxrwxrwx` grants **everyone** write and execute, so an undergraduate who should only read can alter or delete the research data, and any compromised account on the system can too. Set **640**: owner 6 = read+write for the researcher who maintains the file; group 4 = read only, which is all the undergraduates need; others 0, because nobody outside the project should reach it at all. Accept 750/740 with justification tied to whether the file must be executed.

(e) any two parameters: approved algorithm, minimum key length, key-generation requirements, key-storage requirements. A policy is still needed because installed software can be configured weakly - a short key, a deprecated algorithm, or a key left beside the backup it protects - and the policy is what makes the required setting checkable and auditable. Encryption is a technical control; the policy is the managerial control that says what "encrypted" must mean here.