

AP Cybersecurity | Unit 5

5.1 CIA Triad for Applications

Solutions

Reference scenario

Separate three security goals for a student-record application.

Unauthorized reading: confidentiality

Unauthorized grade change: integrity

Service outage: availability

5.1.1

An attacker changes a posted exam schedule while the site stays online. Which goal is most directly affected?

Integrity: the information was altered without authorization. The site being reachable does not make the information trustworthy.

5.1.2

Why do backups support recovery but not automatically prevent unauthorized disclosure?

Backups can restore lost or damaged data, but a person may still read an exposed copy. Backup access must also be controlled and sensitive copies protected.

AP Cybersecurity | Unit 5

5.2 Roles, Permissions, and Data Ownership

Solutions

Reference scenario

Review permissions for a shared finance document.

Public link: edit allowed

Reviewer role: needs read only

Owner: finance manager

Former contractor: still listed

5.2.1

A reviewer needs comments but not deletion rights. What principle guides the assigned role?

Least privilege: select the narrowest approved role that supports reviewing and commenting without unnecessary destructive actions.

5.2.2

What should a periodic access review compare?

Compare current people and roles with actual permissions, sharing links, inherited access, and business need. Record owner approval and remove obsolete or excessive access.

AP Cybersecurity | Unit 5

5.3 Cryptography, Hashing, and Data Movement

Solutions

Reference scenario

Choose a cryptographic mechanism based on the required property.

Goal A: private transfer

Goal B: compare a downloaded file with a trusted digest

Goal C: recover readable stored data with a key



5.3.1

Can Base64 encoding protect a secret from a person who receives the encoded text? Explain.

No. Base64 is a reversible representation format without a secret key. Confidentiality needs an appropriate encryption and access-control design.

5.3.2

Why is a salted, deliberately slow password-hashing scheme preferable to storing plaintext passwords?

It avoids directly exposing readable passwords in the stored record and raises the cost of guessing against a stolen database. It still needs secure authentication, access controls, and operational protection.

AP Cybersecurity | Unit 5

5.4 Application Attacks, Logs, and Recovery

Solutions

Reference scenario

A user can request another student record by changing an identifier in the application request. Identify the missing control.

Authenticated user: student A
Requested record owner: student B
Server result: record returned
Ownership check: absent

5.4.1

Why is client-side input validation insufficient as the only protection for an application endpoint?

A client can send requests outside the expected interface. The server must validate input and enforce authorization for every relevant operation.

5.4.2

After correcting the record-ownership check, give one positive and one negative regression test.

Positive: student A can read their own permitted record. Negative: the same authenticated student cannot read student B records by changing an identifier. Verify the denial does not expose sensitive details.