The CIA Triad — Confidentiality, Integrity, Availability

Three simple rules protect all information: keep it secret, keep it correct, and keep it reachable when you need it.

Introduction

Every security decision in the world comes back to three words: confidentiality, integrity, and availability. Together they are called the CIA Triad — not the spy agency, but the three promises that good security makes about information.

- **Confidentiality** — only the right people can read it.
- **Integrity** — nobody can secretly change it.
- **Availability** — the right people can reach it when they need it.

A university result is confidential (only you should see your marks before you share them), it must have integrity (nobody may change a 60 into a 90), and it must be available (you must be able to open it on result day, not after the server crashes).

In this lesson you will learn each part of the triad, how the three parts can fight each other, and how to check any system against all three.

(Roman Urdu: CIA Triad ke teen usool hain — Confidentiality (raaz rahe), Integrity (cheez badli na jaye), Availability (zaroorat par mil jaye). Har security ka faisla inhi teen par hota hai.)

Beginners often remember only the first part — secrecy. But a secret that nobody can reach is useless, and a correct record that anyone can rewrite is worthless. All three matter, every time.

Key points

- **Confidentiality means "only the right eyes".** Passwords, encryption, and access rules protect it. If a stranger reads your private messages, confidentiality has failed.
- **Integrity means "nothing changed in secret".** Hashes, signatures, and backups protect it. If someone edits your marks and nobody notices, integrity has failed.
- **Availability means "there when you need it".** Backups, spare servers, and protection against overload protect it. If the website is down on exam day, availability has failed.
- **The three parts pull against each other.** Maximum secrecy can destroy availability — a password so complex you forget it locks you out. Perfect availability can destroy secrecy — a file shared with everyone is easy to reach and easy to steal.
- **Good security balances the three.** The right balance depends on the data: a hospital record needs all three at high level; a public timetable needs availability most.

- **Authentication answers "who are you?" and authorisation answers "what may you do?"** A password proves who you are; the system then decides which files you may open.
- **The triad is a test, not a tool.** When you look at any app or system, ask three questions: who can read this, who can change this, and can I reach it when I need it?

Examples

Example 1 — Your exam result, checked against the triad

```
Confidentiality:  only you (and your teacher) can see your marks.
                  Protection: login + password.

Integrity:        nobody can change 60 into 90 without being caught.
                  Protection: the system logs every change.

Availability:     you can open the result on result day.
                  Protection: the server has a backup copy.
```

If any one line fails, the result system has failed — even if the other two are perfect.

Example 2 — When the three parts fight

A student sets a 30-character random password and writes it nowhere:

```
Confidentiality:  EXCELLENT — nobody can guess it.
Availability:     FAILED — she forgets it and cannot log in.
```

Fix: keep the strong password, but store it in a password manager (CS.10). Now confidentiality stays high and availability returns.

Example 3 — A hospital record needs all three at maximum

```
Confidentiality:  only the treating doctor and the patient.
Integrity:        a wrong dose in the record could kill — no secret edits.
Availability:     the doctor needs it in an emergency, at 3 AM.
```

This is why hospitals spend the most on security: all three parts matter at the same time, and failure in any one of them is dangerous.

Example 4 — A public bus timetable needs mostly availability

```
Confidentiality:  LOW — the timetable is public anyway.
Integrity:        MEDIUM — a wrong time misleads passengers.
Availability:     HIGH — people check it on the road, in a hurry.
```

Same triad, different balance. There is no single "correct" setting — the data decides.

Quick recap

- Confidentiality: only the right people can read it.
- Integrity: nobody can secretly change it.
- Availability: the right people can reach it when they need it.
- The three parts pull against each other — security is a balance.
- Authentication is "who are you?"; authorisation is "what may you do?"

Common mistakes

1. **Only thinking about secrecy** — a file nobody can open is safe but useless. Fix: check all three parts, every time.
2. **Mixing up authentication and authorisation** — logging in proves who you are; it does not mean you may open everything. Fix: ask both questions separately.
3. **Forgetting availability in a crisis** — backups that are never tested may not work when you need them. Fix: test a restore, don't just trust the backup exists.
4. **Treating all data the same** — a public poster and a medical record do not need the same protection. Fix: spend the most protection on the most sensitive data.
5. **Adding security that locks out the owner** — a password you cannot remember is a self-attack on availability. Fix: use a password manager, not your memory.

Practice

1. Pick one app you use daily and test it against the triad: who can read your data, who can change it, and can you reach it when you need it?
2. Write one example from your own life where confidentiality failed (someone saw something private) and one where availability failed (a site or file was down when you needed it).
3. A diary app and a bus timetable: which part of the triad matters most for each? Write one line for each.
4. Explain authentication vs authorisation to a friend in two sentences, using a house key and a house rule as the example.
5. Check your own backup: if your phone broke today, which files could you get back, and which would be gone forever? Write the list.

Practice quiz

1. What does confidentiality mean?

- Only the right people can read the information
- The information is always available

- The information can never change
- Everyone can read the information

Answer: Only the right people can read the information

2. What does integrity mean?

- Only the right people can read it
- Nobody can secretly change it
- It is available at all times
- It is stored in two places

Answer: Nobody can secretly change it

3. What is the difference between authentication and authorisation?

- They are the same thing
- Authentication proves who you are; authorisation decides what you may do
- Authorisation proves who you are; authentication decides what you may do
- Authentication is for passwords only

Answer: Authentication proves who you are; authorisation decides what you may do

---

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-cia-triad · More free tools and notes at https://scopetreasure.com