🧠 Lecture 17 – Cybersecurity Fundamentals: CIA Triad, Hashing, Vulnerabilities, Threats, and AAA Model

---

🔺 1. CIA Triad

📘 Definition:

The **CIA Triad** is the **core model of cybersecurity** that defines three main principles — **Confidentiality, Integrity, and Availability**.
It provides the **framework for building secure systems** and **protecting data**.

🧩 A. Confidentiality

🔹 Meaning:

Only **authorized people** should have access to sensitive information.
It ensures **data privacy** and prevents **unauthorized disclosure**.

🔹 Example:

- Your bank account details should only be visible to you and your bank.
- Company confidential files should not be accessible to outsiders.

🔹 How to Achieve:

- **Encryption:** Converts data into unreadable format.
- **Access Control Lists (ACLs):** Restrict user access.
- **Multi-Factor Authentication (MFA):** Verifies identity using password + OTP.

🔹 Tools & Techniques:

- AES (Advanced Encryption Standard)
- VPN for secure transmission
- File permissions in OS

🧩 B. Integrity

🔹 **Meaning:**

Ensures that **data has not been changed or modified** without permission.
Data must remain **accurate, complete, and trustworthy**.

🔹 **Example:**

If a salary report or exam result file is altered without approval, data integrity is lost.

🔹 **How to Achieve:**

- Use **Hashing algorithms** (MD5, SHA1, SHA256, etc.).
- **Digital Signatures** to verify authenticity.
- **Checksums** for file verification.

🔹 **Tool:**

- **Hash Calculators**
    - MD5File.com
    - VirusTotal.com
    - Pelock Hash Calculator

These sites can calculate the **hash value** of files or text to verify their integrity.

🧩 C. Availability

🔹 **Meaning:**

Authorized users must have **timely and reliable access** to data and systems whenever needed.

🔹 **Example:**

If your company's website is down due to a DDoS attack, availability is lost.

🔹 **How to Achieve:**

- Use **Redundant Servers** and **Backups**.
- Apply **Disaster Recovery Plans**.

- Maintain **updated hardware** and **network security**.

✅ CIA Triad Summary

Principle	**Purpose**	**How It's Maintained**
Confidentiality	Keep data private	Encryption, MFA
Integrity	Keep data unmodified	Hashing, digital signatures
Availability	Keep data accessible	Backup, redundancy, DDoS protection

---

⚙️ 2. Hash Value and Integrity Verification

🔹 **Definition:**

A **hash value** is a **unique numeric or alphanumeric code** generated by applying a **hash function** to a file or text.
It represents the **content's fingerprint** — even a tiny change in the file changes the hash completely.

🔹 **Purpose:**

- To **verify data integrity**.
- To **detect tampering or corruption**.
- To **authenticate** downloaded files.

🔹 **Example:**

If a file has this original hash:

5d41402abc4b2a76b9719d911017c592

and after download it changes to:

7c6a180b36896a0a8c02787eeafb0e4c

It means the file was **modified** or **corrupted**.

🔹 Common Hash Algorithms:

Algorithm	Full Form	Bit Size	Description
MD5	Message Digest 5	128-bit	Fast but weak (not secure for cryptography)
SHA-1	Secure Hash Algorithm 1	160-bit	More secure than MD5 but now outdated
SHA-2	Secure Hash Algorithm 2	256/512-bit	Currently used for modern systems
SHA-512	Secure Hash Algorithm 512-bit	512-bit	Very strong and secure

---

⚠️ Important Concept:

"Downloading a file does not cause harm — installing or executing it does."

- Malware only activates **when the file is executed**.
- That's when its **code runs** and starts performing malicious activity.

🧩 3. Vulnerability

🔹 Definition:

A **vulnerability** is a **weakness or flaw** in software, hardware, or human behavior that can be **exploited** by an attacker.

🔹 Example:

- Unpatched operating systems
- Weak passwords
- Misconfigured firewalls
- Phishing-prone employees

🔹 **Types of Vulnerabilities:**

1. Technical Vulnerabilities

Found in systems, software, or configurations.

- SMB (Server Message Block) protocol vulnerabilities
- RDP (Remote Desktop Protocol) exposure
- Outdated antivirus or software
- Unpatched operating systems

Solution:
Regular updates, system hardening, and patch management.

2. Human Vulnerabilities

Caused by user actions or negligence.

- Clicking phishing links
- Sharing passwords
- Disgruntled employees leaking data

Solution:
Security awareness training and strict access policies.

💀 4. Threat

🔹 **Definition:**

A **threat** is a potential event or person that can **exploit a vulnerability** and cause **damage** to data or systems.

🔹 **Example:**

- A hacker launching a DDoS attack.
- An insider stealing sensitive company data.

◆ Common Threat Types:

- **Remote attacks** – attacker gains unauthorized system access.
- **Malware attacks** – viruses, worms, ransomware, trojans.
- **DDoS attacks** – flooding network to make it unavailable.

◆ Common Threat Actors & Their Motivations:

Threat Actor	Motivation	Example
Cyber Criminals	Financial profit	Ransomware, phishing
Nation States	Political or military advantage	Government-backed attacks
Terrorist Groups	Ideological violence	Attacks on critical infrastructure
Thrill Seekers	Fun or challenge	Website defacement
Insiders	Revenge or dissatisfaction	Disgruntled employee leaking data
Hacktivists	Political/social message	Anonymous hacking groups

---

⚖️ 5. Risk

◆ Definition:

Risk is the **probability and potential impact** of a negative incident happening due to a threat exploiting a vulnerability.

◆ Formula:

Risk = Threat × Vulnerability

🔹 **Example:**

If a company has:

- Weak RDP password (**vulnerability**)
  and
- Hackers trying to brute-force it (**threat**),

then the **risk** of unauthorized access is high.

🔹 **Risk Management Process:**

1. **Identify** vulnerabilities and threats.
2. **Assess** risk level (high, medium, low).
3. **Mitigate** using security controls.
4. **Monitor** continuously.

🔐 6. AAA Model (Authentication, Authorization, Accounting)

📘 Definition:

The **AAA Framework** is used to **control and track user access** in network and system security.

🧩 A. Authentication

🔹 **Meaning:**

Verifying **who the user is**.
It confirms the user’s identity before granting access.

🔹 **Example:**

- Username + Password
- OTP (One-Time Password)
- Biometric login

🧩 B. Authorization

🔹 **Meaning:**

Defines **what the authenticated user can do**.
It decides the **level of access** or **permissions** for each user.

🔹 **Example:**

- Admin can install software.
- Employee can only read or modify documents.

🧩 C. Accounting

🔹 **Meaning:**

Tracks **what users do** in the system after they log in.
Helps in **auditing, monitoring, and reporting**.

🔹 **Example:**

- Login logs
- File access logs
- Command history

✅ AAA Example in Real Life:

1. You log into your company network → **Authentication**
2. You access only your department folder → **Authorization**
3. System logs your activity → **Accounting**

🧾 7. IT Asset Disposal (Scraping in Companies)

When IT teams remove old or faulty hardware, they perform **scraping (secure disposal)** to ensure **confidential data doesn't leak**.

🔹 **Items to be Scrapped Securely:**

- **Papers or documents** (shredded)

- **Toner cartridges**
- **RAM and Hard Drives (HDD/SSD)**
- **Network devices** (e.g., L3 Switches)

🔹 **Reason:**

- To prevent sensitive company information from going outside.
- To comply with data protection regulations (like ISO certification).

🧩 Summary Chart

Concept	**Description**	**Example**
CIA Triad	Security framework	Confidentiality, Integrity, Availability
Hashing	Verify data integrity	MD5, SHA256
Vulnerability	Weakness in system	Outdated OS, weak password
Threat	Potential attack	Hacker, malware, insider
Risk	Threat × Vulnerability	Data breach risk
AAA Model	Access control framework	Authentication, Authorization, Accounting

---

✅ Final Takeaway:

- **CIA Triad** defines *what* to protect.
- **Hashing** ensures *data integrity*.
- **Vulnerability + Threat = Risk*.
- **AAA** defines *how* to control access.
- **Scrapping** ensures *data doesn’t leak* after device disposal.