Information Security and Principles

Course Code: CSC5311 Course Title: Information Security Management

Dept. of Computer Science
Faculty of Science and Technology

Lecturer No:	1	**Week No:**		**Semester:**	Summer 24-25
Assistant Professor:	Dr. Rajarshi Roy Chowdhury (rajarshi@aiub.edu)				

Lecture Outline

1. Information security
2. Types/areas of IS
3. The CIA triad
4. OSI
5. The DAD triad
6. AAA

Information Security

Information security (InfoSec) refers to the practice of reducing/protecting **information assets and systems** from unauthorized access, use, disclosure, modification, or destruction. It ensures that data remains confidential, accurate, and available to authorized users.

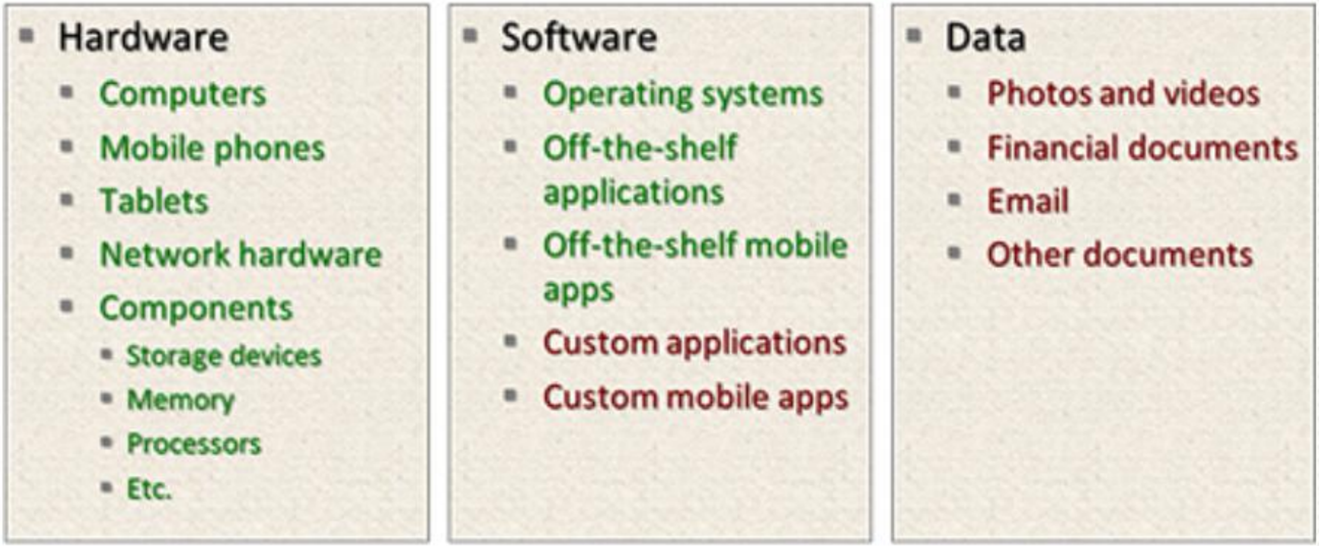
It is **not a tool** rather than policies, technology, awareness, risk management and compliance (Adhering to regulations).

Information assets: Anything of value to an organization that involves data or information in either digital or physical format. **Examples**: Data, Documents, credentials, emails, media, etc.

Information Security

Information systems: A structured setup consisting of hardware, software, people, processes, and data, utilized to collect, process, store, and distribute information. Some examples of Information Systems: Transactional systems, Communication systems, Security systems, etc.

Information Assets Valuation

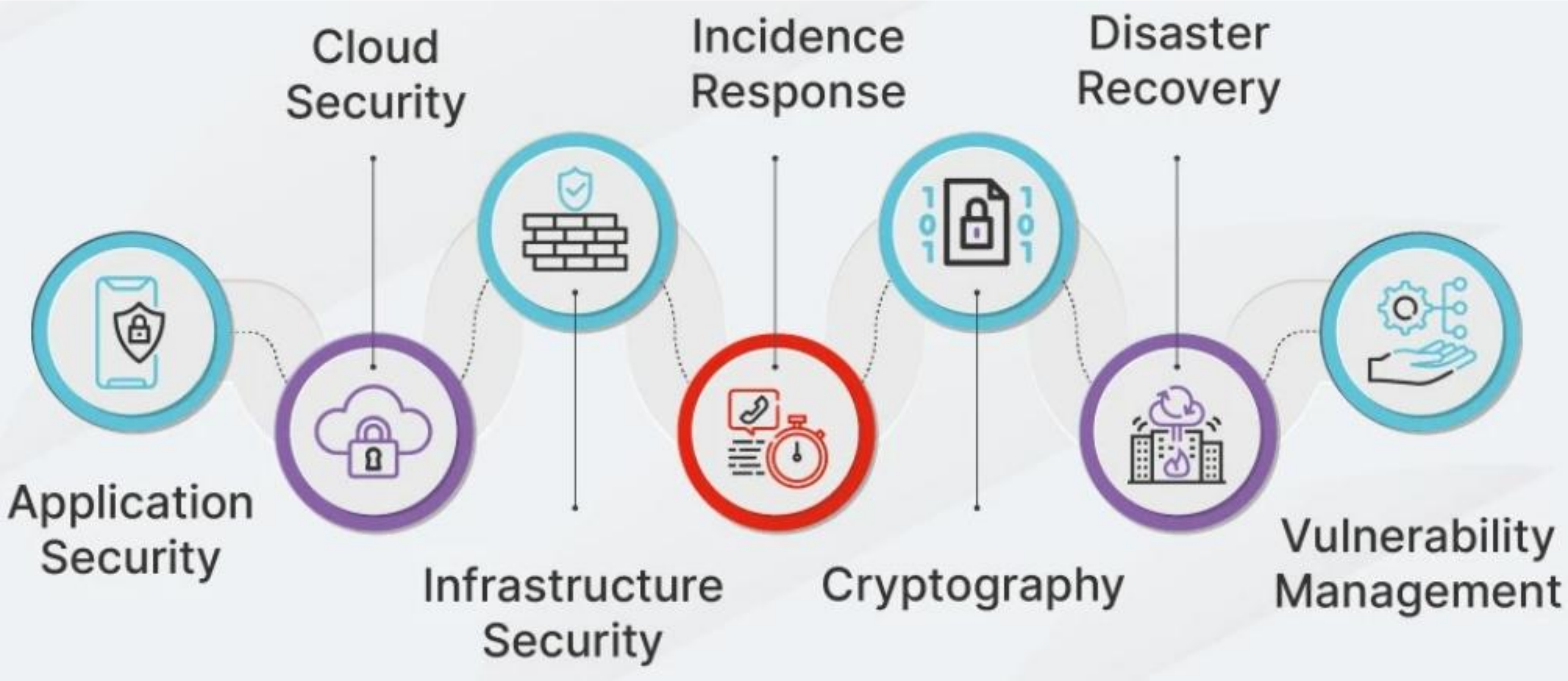


- Hardware
  - Computers
  - Mobile phones
  - Tablets
  - Network hardware
  - Components
    - Storage devices
    - Memory
    - Processors
    - Etc.

- Software
  - Operating systems
  - Off-the-shelf applications
  - Off-the-shelf mobile apps
  - Custom applications
  - Custom mobile apps

- Data
  - Photos and videos
  - Financial documents
  - Email
  - Other documents

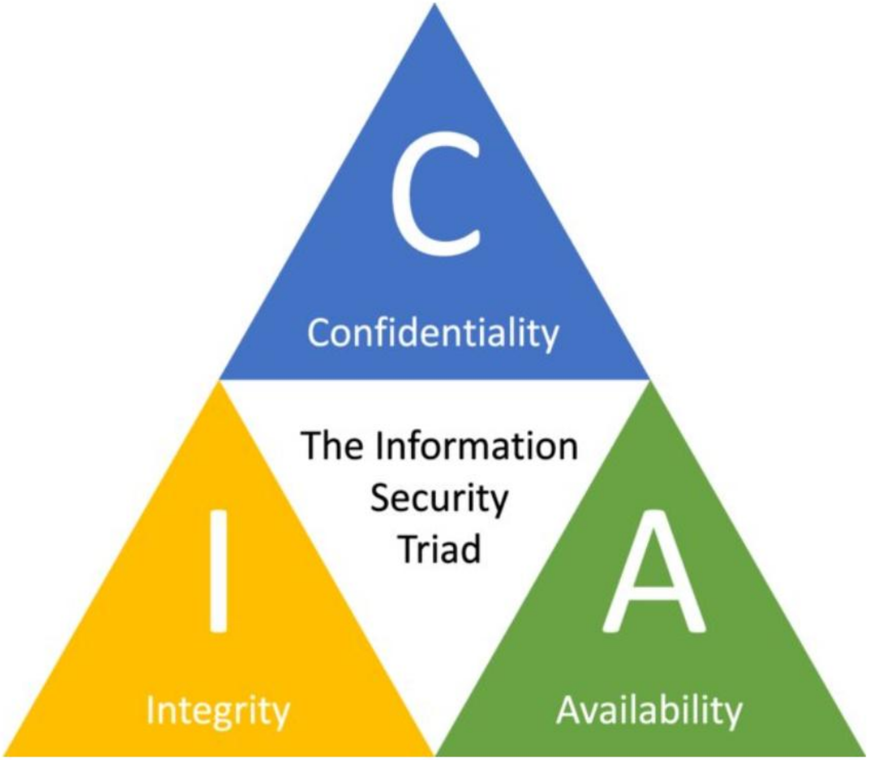
Basic Types of Information Security



CIA Triad

Confidentiality

- Information is not made available to unauthorized individuals
- Restrict access to the information
- Restrict what can be done with this information, e.g. Deletion of information, forward of information my emails
- Classify the information: Sensitive, personal, secret and public information.



CIA Triad

Integrity

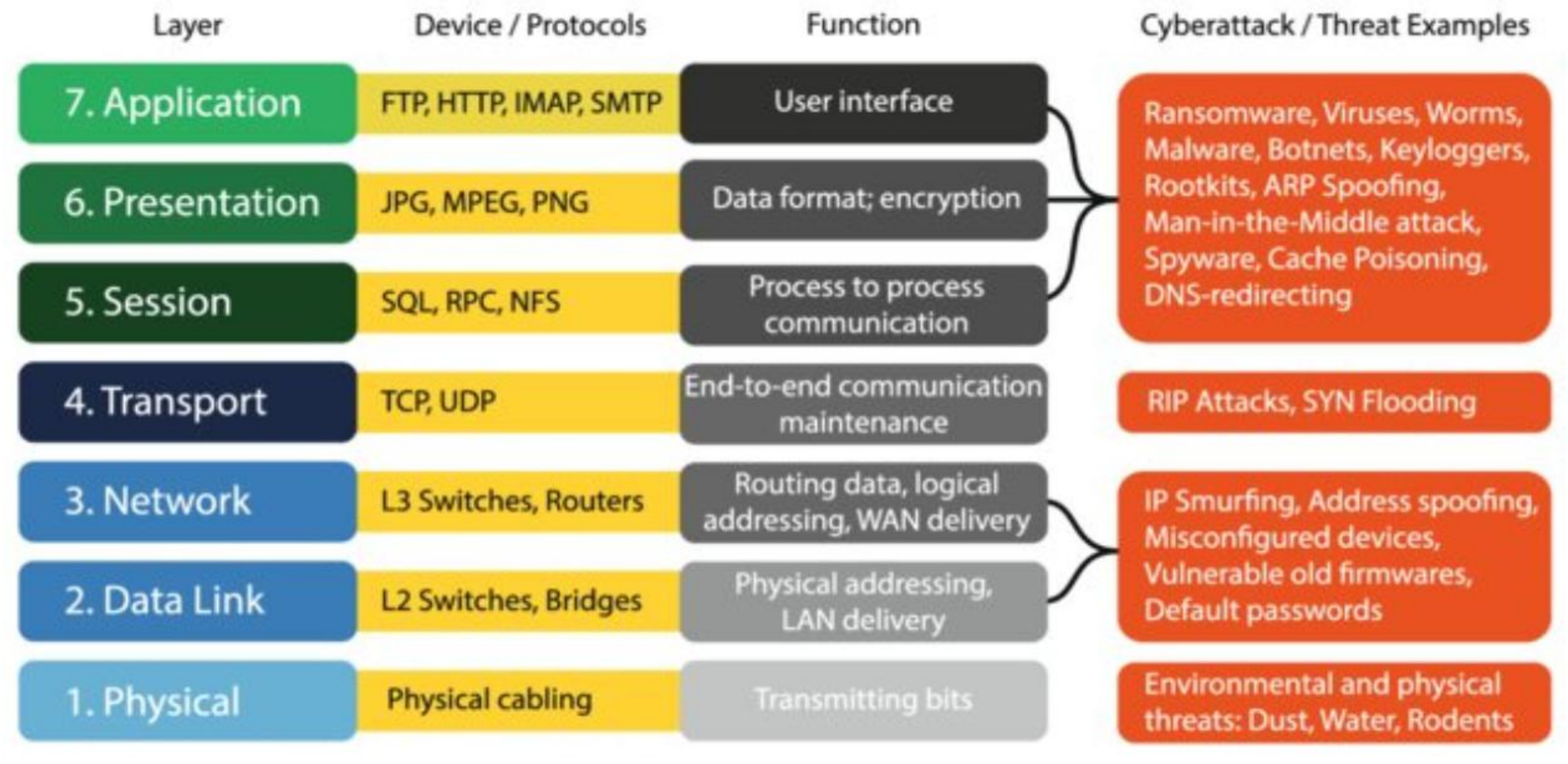
- Information security professionals require to ensure:
- Accuracy of information
- Completeness of information
- Information verified
- Who created the information (source)
- Who can update or delete the information (editors)
- Information age

CIA Triad

Availability

- Access to information when required (exact right time)
- Need to know (who need to know the information at particular time)
- Response times
- Back-up and recovery times

The OSI Model & Cyber Attack E.G.



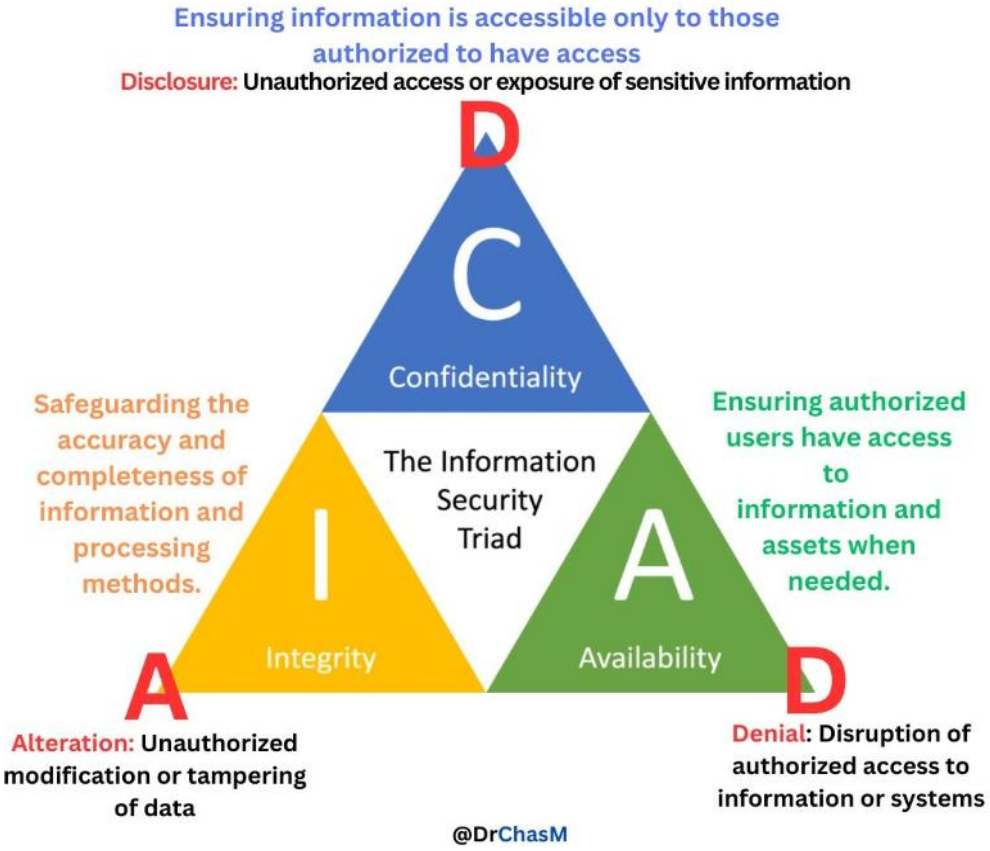
Layer	Device / Protocols	Function	Cyberattack / Threat Examples
7. Application	FTP, HTTP, IMAP, SMTP	User interface	Ransomware, Viruses, Worms, Malware, Botnets, Keyloggers, Rootkits, ARP Spoofing, Man-in-the-Middle attack, Spyware, Cache Poisoning, DNS-redirecting
6. Presentation	JPG, MPEG, PNG	Data format; encryption	
5. Session	SQL, RPC, NFS	Process to process communication	
4. Transport	TCP, UDP	End-to-end communication maintenance	RIP Attacks, SYN Flooding
3. Network	L3 Switches, Routers	Routing data, logical addressing, WAN delivery	IP Smurfing, Address spoofing, Misconfigured devices, Vulnerable old firmwares, Default passwords
2. Data Link	L2 Switches, Bridges	Physical addressing, LAN delivery	
1. Physical	Physical cabling	Transmitting bits	Environmental and physical threats: Dust, Water, Rodents

DAD Triad

The **DAD triad** is a threat model used to describe types of attacks against information assets.

It is the **inverse of the CIA triad** in IS.

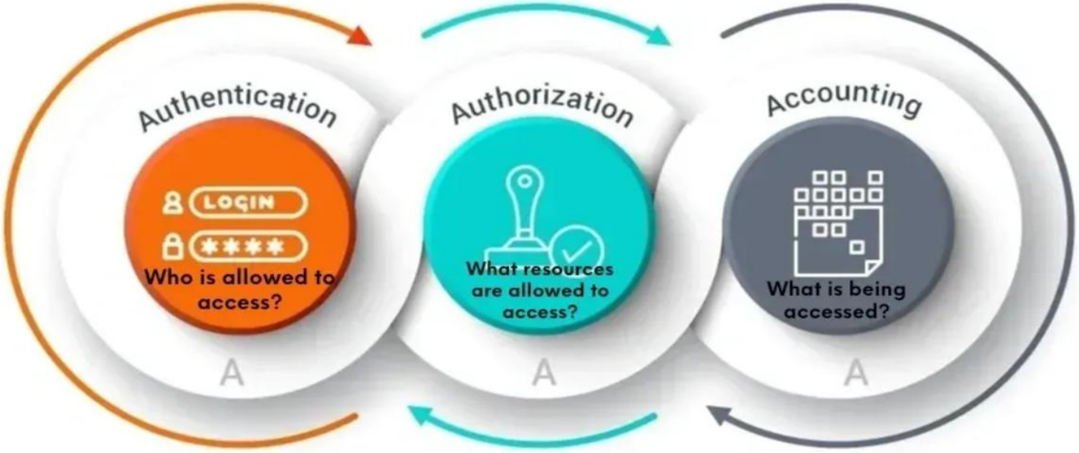
It shows what **DAD actors** want to do when they try to break security.


Ensuring information is accessible only to those authorized to have access
Disclosure: Unauthorized access or exposure of sensitive information
D
C
Confidentiality
Safeguarding the accuracy and completeness of information and processing methods.
The Information Security Triad
Ensuring authorized users have access to information and assets when needed.
I
A
Integrity
Availability
A
D
Alteration: Unauthorized modification or tampering of data
Denial: Disruption of authorized access to information or systems
@DrChasM

Authentication, Authorization, and Accounting (AAA)

AAA is a security framework for controlling access to computer resources.
Commonly used in: Network security, Remote access, Cloud computing

- Authentication – Who are you?
- Authorization – What are you allowed to do?
- Accounting – What did you do?



Authentication, Authorization, and Accounting (AAA)

- **Identity Proofing:** The process of verifying that a person is who they claim to be before granting them access.
- **Least Privilege:** Users should be given only the minimum access needed to perform their job.
- **Non-Repudiation:** Ensures that a person cannot deny having performed an action.
- **Legal and Regulatory Issues:** Organizations must follow laws and standards when handling data and security.

Authentication, Authorization, and Accounting (AAA)

- **Modern Password Guidelines:** New password best practices to enhance security and usability

- **Code of Ethics:** A formal set of rules that guide ethical behavior in a profession.

- **Education and Training:** Teaching users and staff about cybersecurity best practices and policies.

Recommended Books

Books

1. **Information Security Management Handbook** (6th Edition), Harold et al.
2. **Information Security and IT Risk Management**, Manish et al.
3. Random online resources