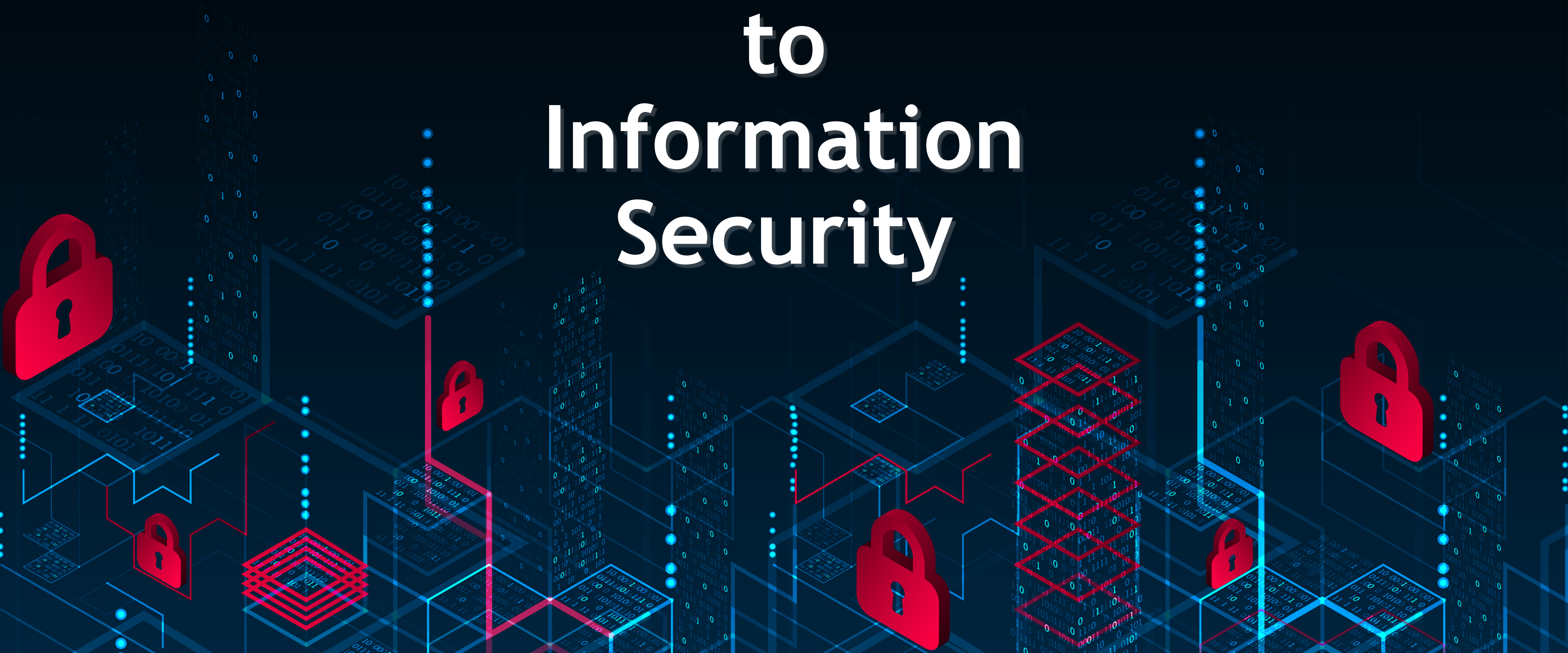
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Information Security



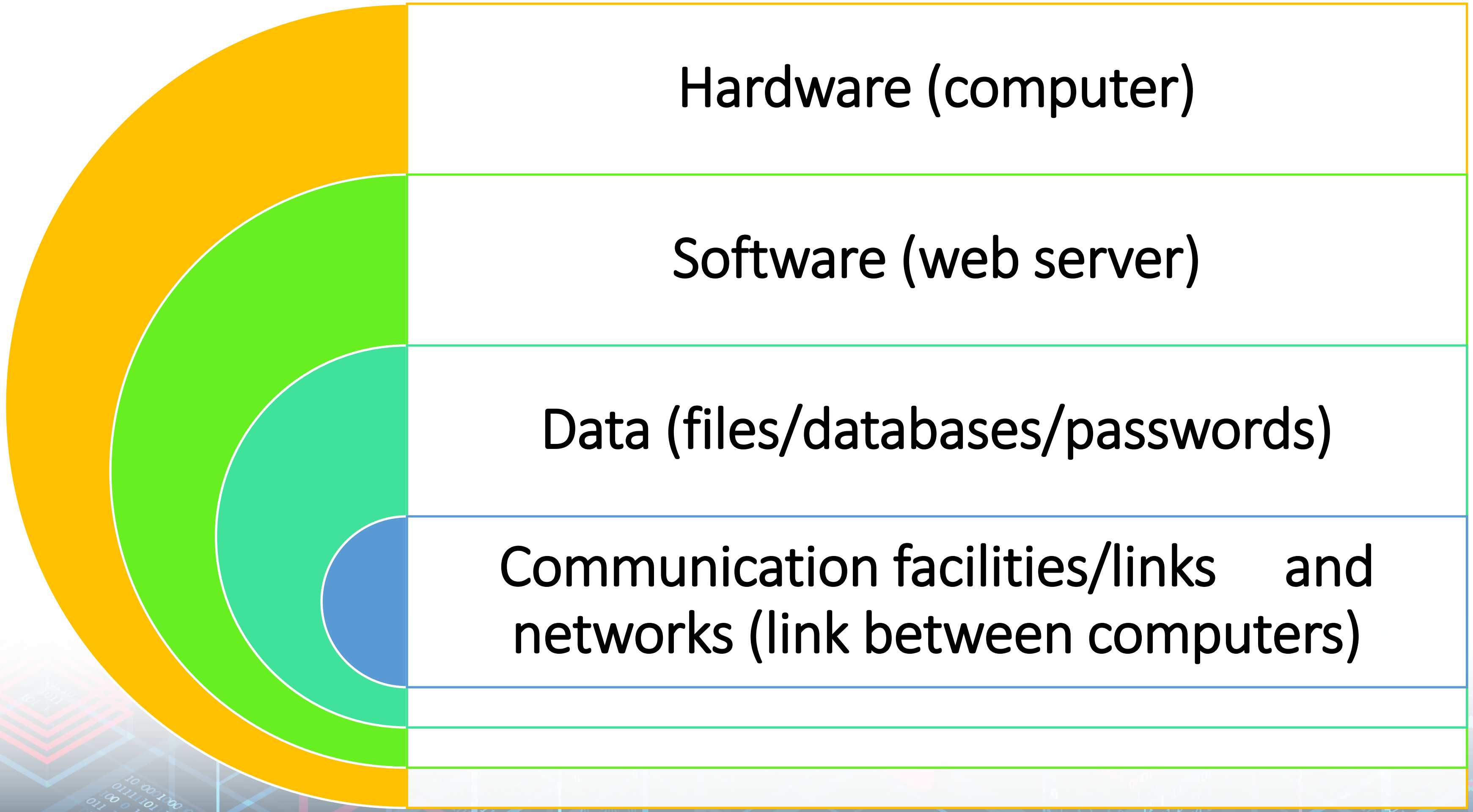
Module:

- Introduction to Information Security
  - By the end of this module you will be able to:
    - Differentiate between Confidentiality, Integrity, and Availability
    - Understand technical areas that must underpin any effective security strategy
    - Differentiate between threats, attacks and assets

Computer Security Concepts

- Assets
- Vulnerabilities
- Security Policies
- Threats
- Attacks
- Countermeasure

Assets of a Computer System
(things that we want to protect)



Hardware (computer)

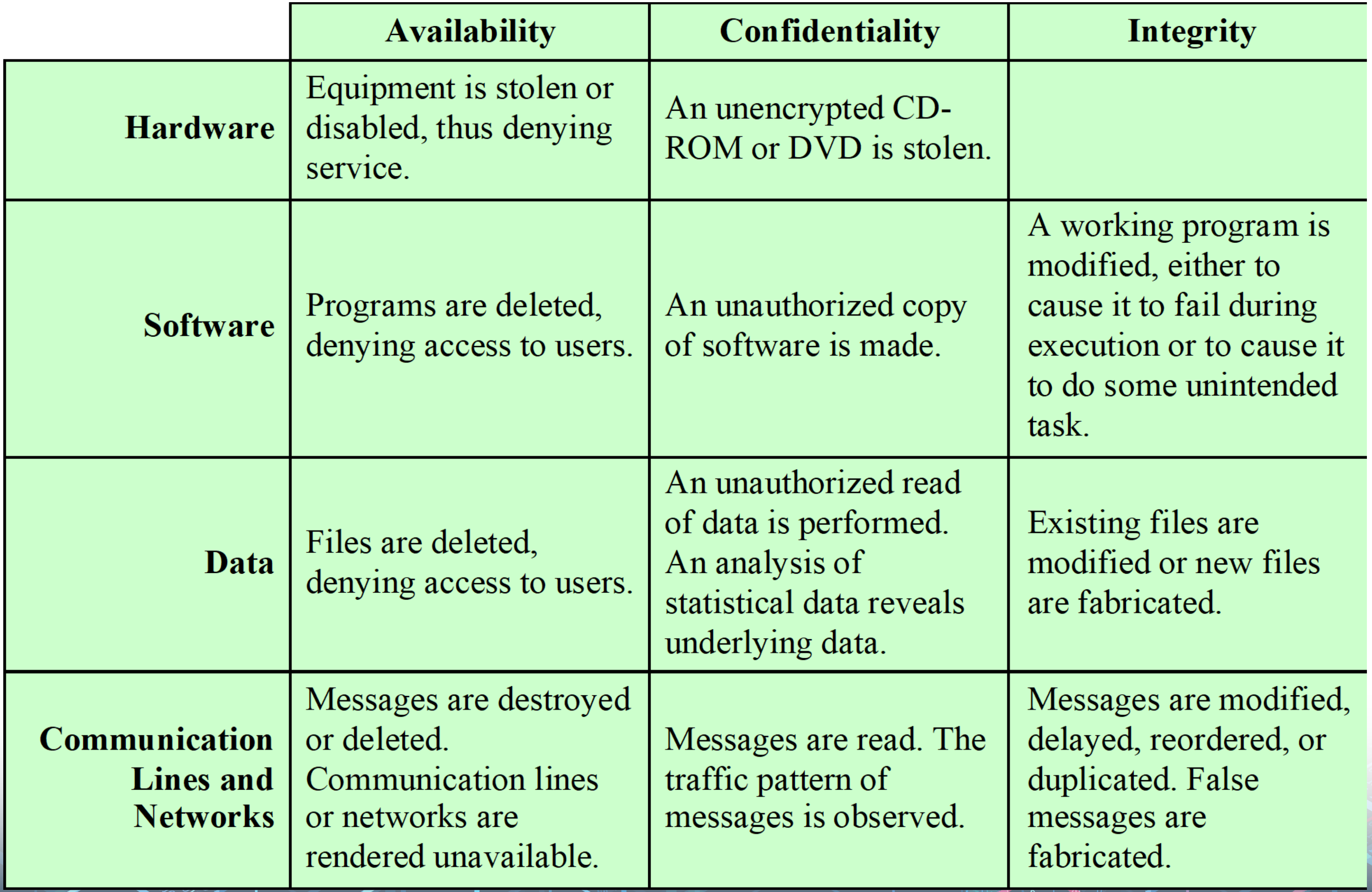
Software (web server)

Data (files/databases/passwords)

Communication facilities/links and networks (link between computers)

Table 1.3

Computer and Network Assets, with Examples of Threats



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity – ex: asset doesn't do its function)
  - Leaky (loss of confidentiality – ex: leaks out information)
  - Unavailable or very slow (loss of availability - ex: users can't access the asset)

- Note that it is complex to write a software without a bug
- it is complex to build a hardware without flaws,
- and it is complex to keep track of data

There are often vulnerabilities… try to avoid them

Vulnerabilities, Threats and Attacks

- Security Policy
  - Set of rules and practices that specifies how a certain organization/company provides security services to protect assets
  - Example in the university there is a policy for who can access student’s data (Confidentiality).
  - Can I access your grades in another course?
  - The organization must implement certain techniques to implement those policies

Computer Security Concepts

- Assets
- Vulnerabilities
- Security Policies
- Threats
- Attacks
- Countermeasure