Lecture 1 "Information Security"

Content to be covered

The meaning of computer security

Importance and some terms

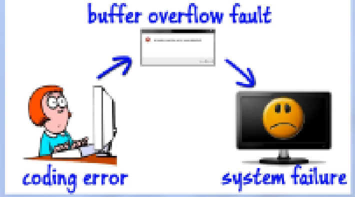
Data Security Goals

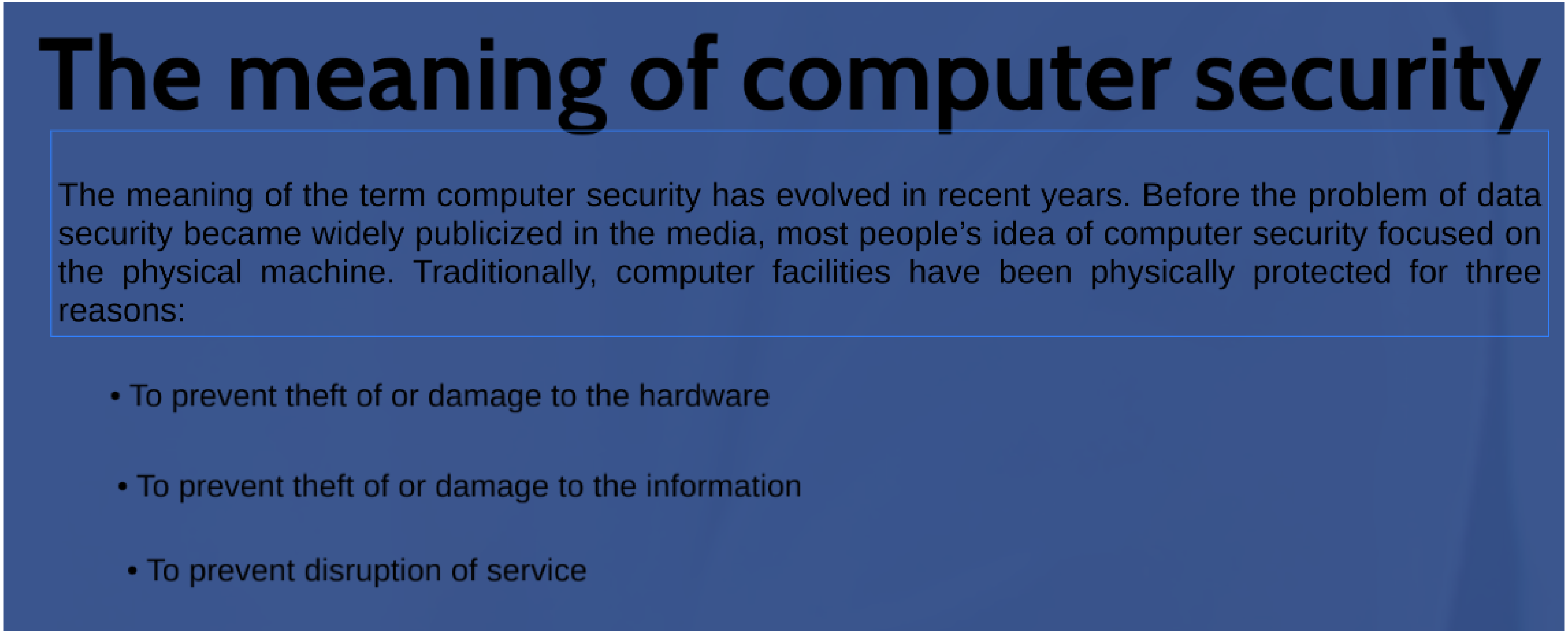
Thanks

Information Security by Engr. Darakhshan Syed

The core content of this course comprises of the following 4 modules:

Module I The Security Problem in Computing.
Module II Program Security.
Module III Data base Security.
Module IV Administering Security.

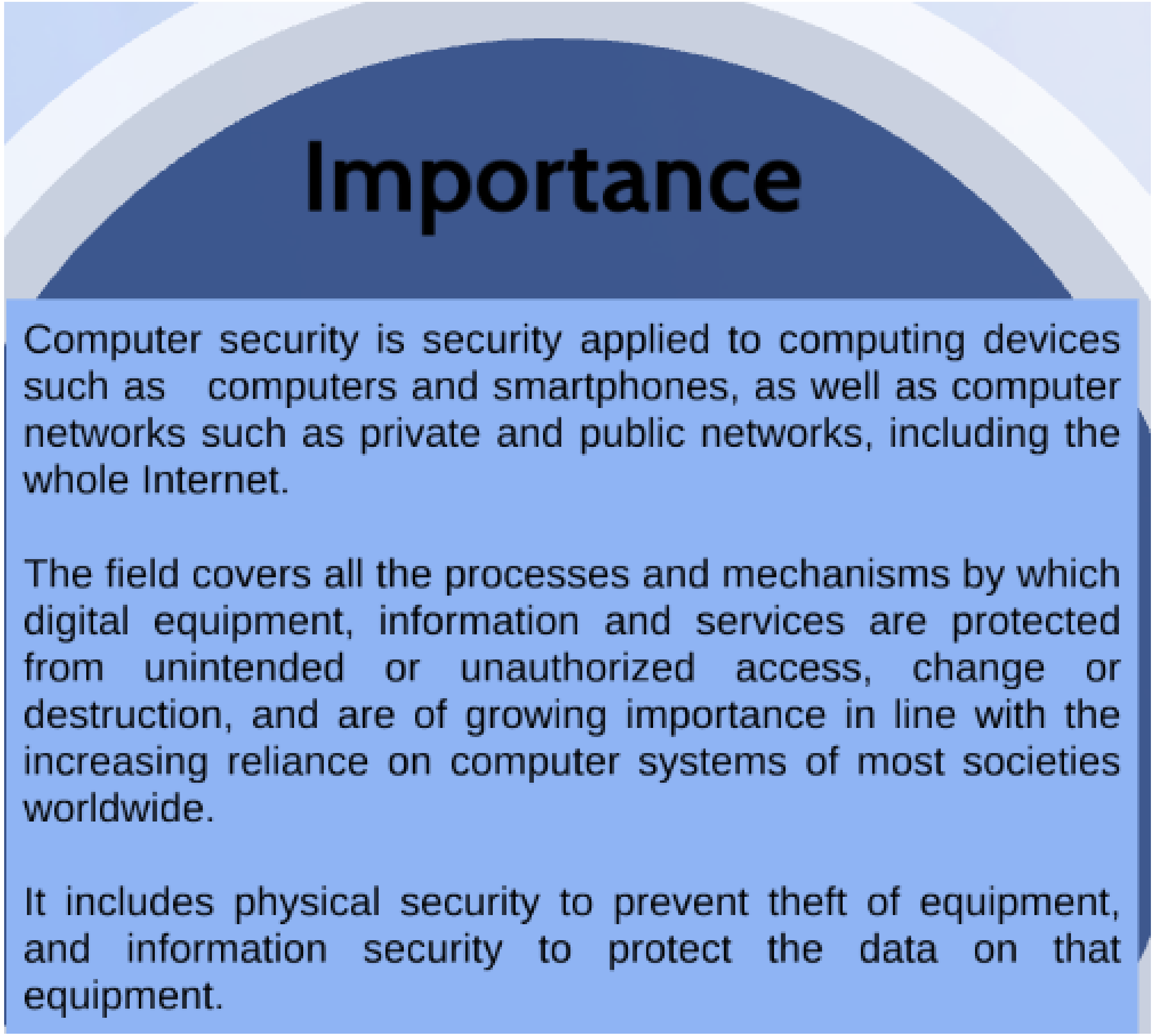




The meaning of computer security

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service



Importance

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet.

The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide.

It includes physical security to prevent theft of equipment, and information security to protect the data on that equipment.

Some important terms used in computer security are:

Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Backdoors

A backdoor in a computer system, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.

Denial-of-service attack

Denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims.These types of attack are, in practice, very hard to prevent, because the behaviour of whole networks needs to be analyzed, not only the behaviour of small pieces of code.

Direct-access attacks

An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions, install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way.

Eavesdropping

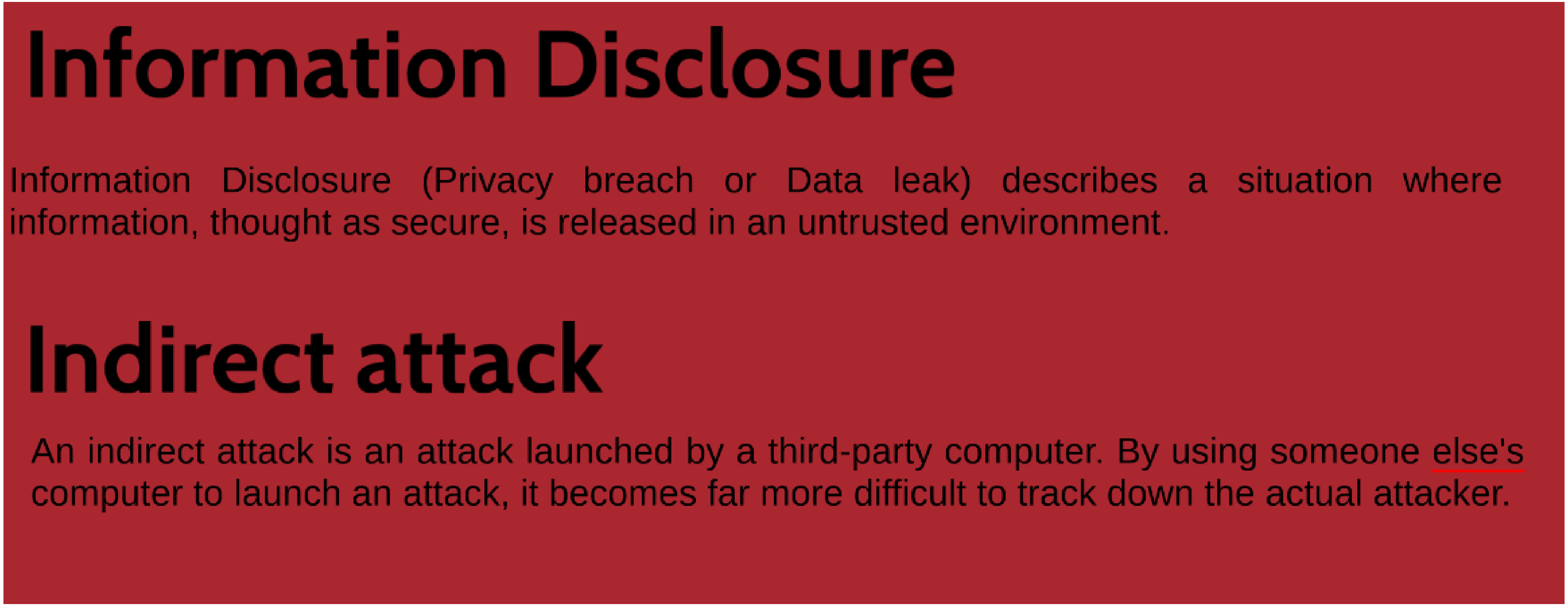
Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Tampering

Tampering describes an intentional modification of products in a way that would make them harmful to the consumer.



Information Disclosure

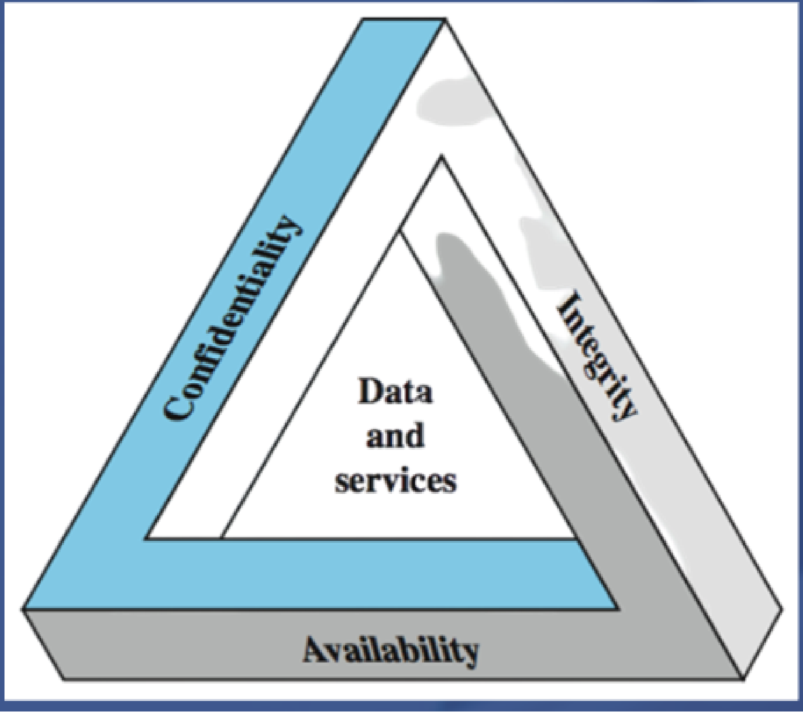
Information Disclosure (Privacy breach or Data leak) describes a situation where information, thought as secure, is released in an untrusted environment.

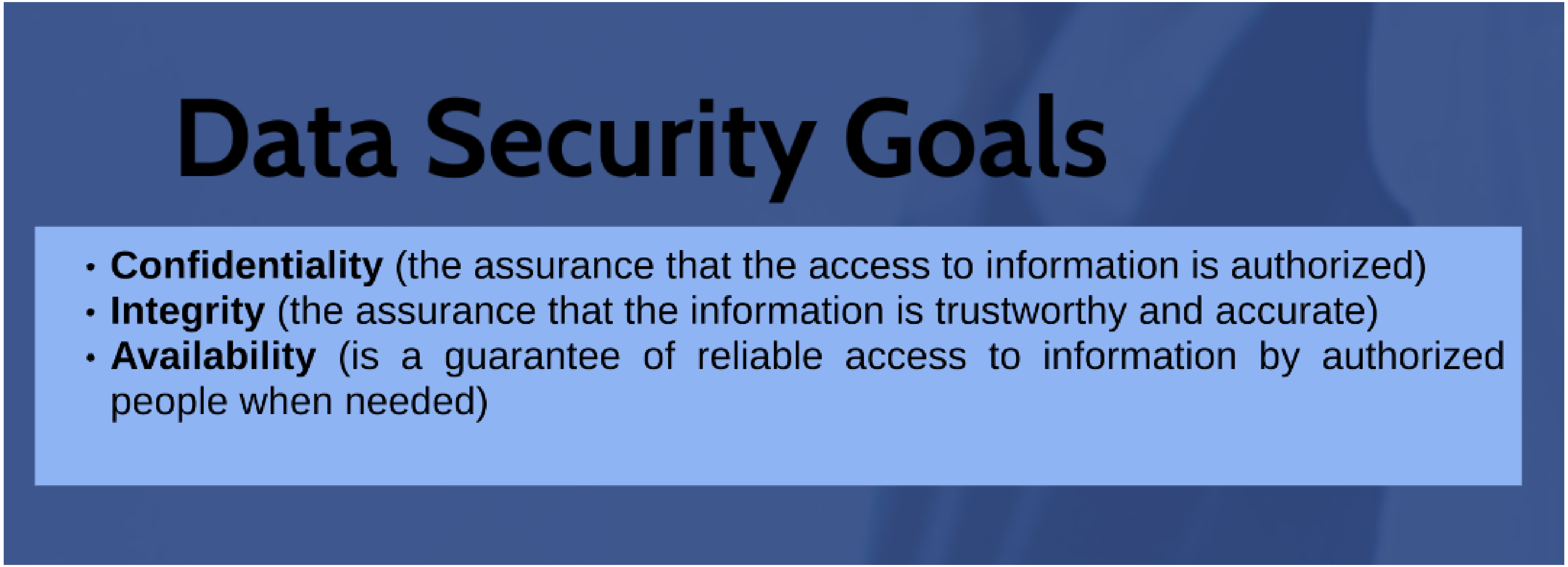
Indirect attack

An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker.

Data Security Goals

- Data security goals are three-fold.
- It is known as CIA triad





Data Security Goals

- **Confidentiality** (the assurance that the access to information is authorized)
- **Integrity** (the assurance that the information is trustworthy and accurate)
- **Availability** (is a guarantee of reliable access to information by authorized people when needed)

Confidentiality

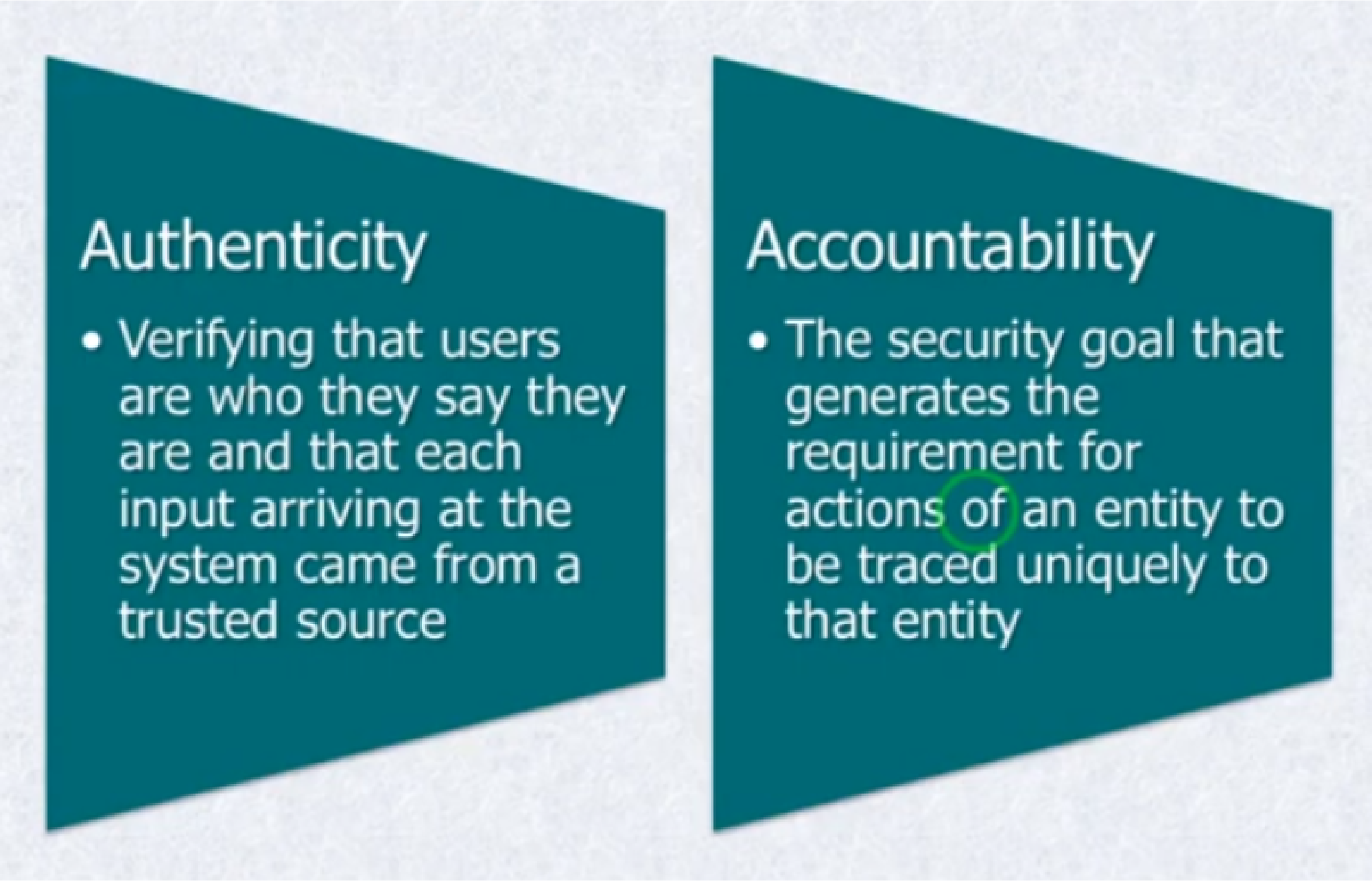
- Confidentiality is roughly equivalent to **privacy.**
- **Data encryption** is a common method of ensuring confidentiality.
- User IDs and passwords, two-factor authentication, biometric verification, OTP, security tokens etc. are common examples of achieving confidentiality.
- Extra measures might be disconnected storage devices or, for highly sensitive information, in hard copy form only.

Integrity

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data.
- Data must not be changed in transit.
- Version control may be used to prevent erroneous changes or accidental deletion by authorized users.
- Backups or redundancies must be available to restore the affected data to its correct state.

Availability

- Availability is best ensured by keeping all necessary system upgrades all the time.
- Providing adequate communication bandwidth and preventing the bottlenecks.
- Redundancy, failover, RAID can mitigate serious consequences.
- Comprehensive disaster recovery plan (DRP).
- Safeguards against natural disasters and fire. A backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe.
- Extra security such as firewalls and proxy servers can guard against downtime and unreachable data due to denial-of-service (DoS) attacks and network intrusions.



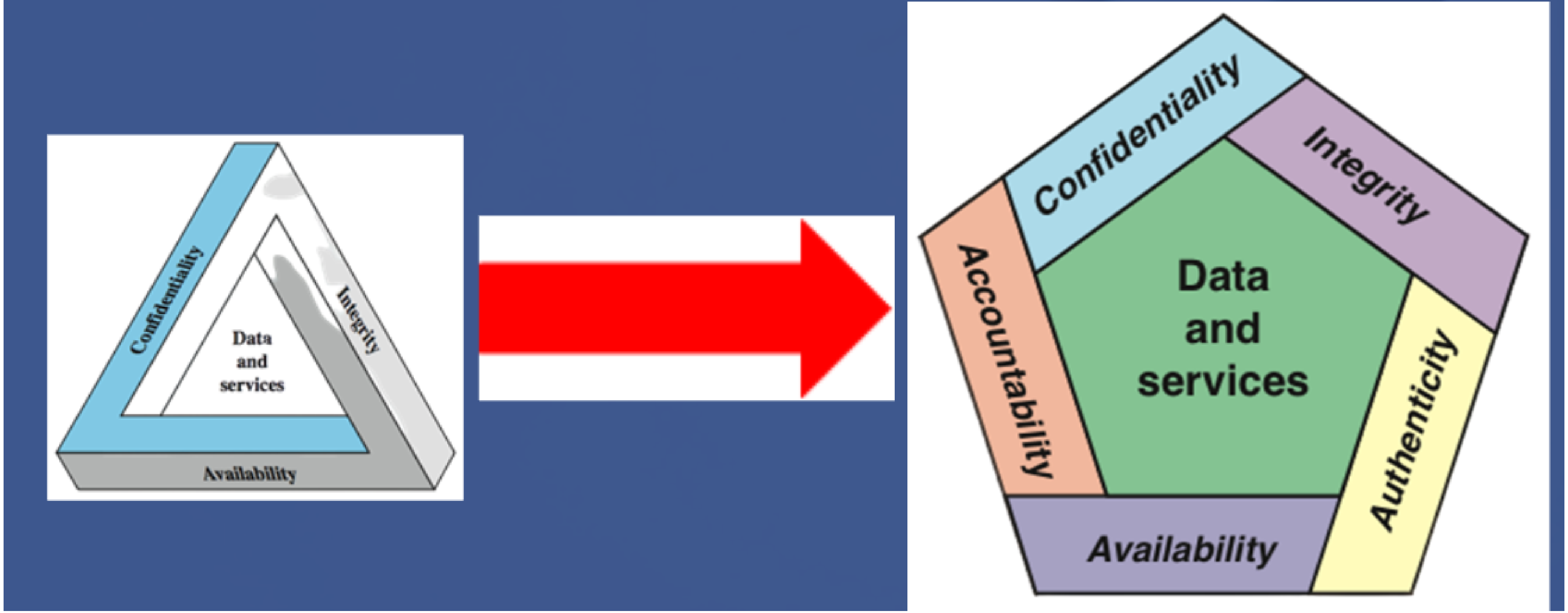
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

CIAAA (5 Principles of Security)



Thanks