

Introduction to Networks System Security

#week1

#security

Security is about preserving the integrity, availability, and confidentiality of information. This is known as the CIA trio.

Integrity

Patient information stored in a database – **inaccurate** information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity. An example of a low-integrity requirement is an **anonymous** online poll

Availability

The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

An online telephone directory lookup application would be classified as a low-availability requirement

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

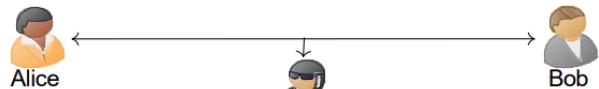
Regulated by the Family Educational Rights and Privacy Act (FERPA)

Basic Threat Scenarios

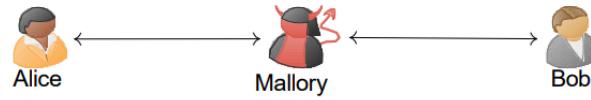
These are data in transit, data at rest, and data in use attacks.

Data in transit:

Eavesdropper: (passive)

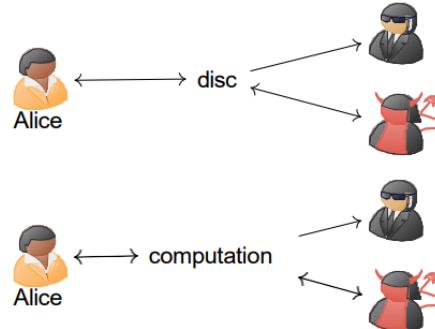


Middle-person attack: (active)

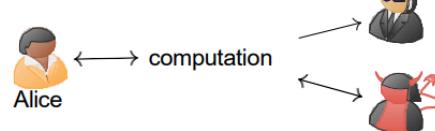


Data at rest:

Storage security:



Side channels / fault injection:



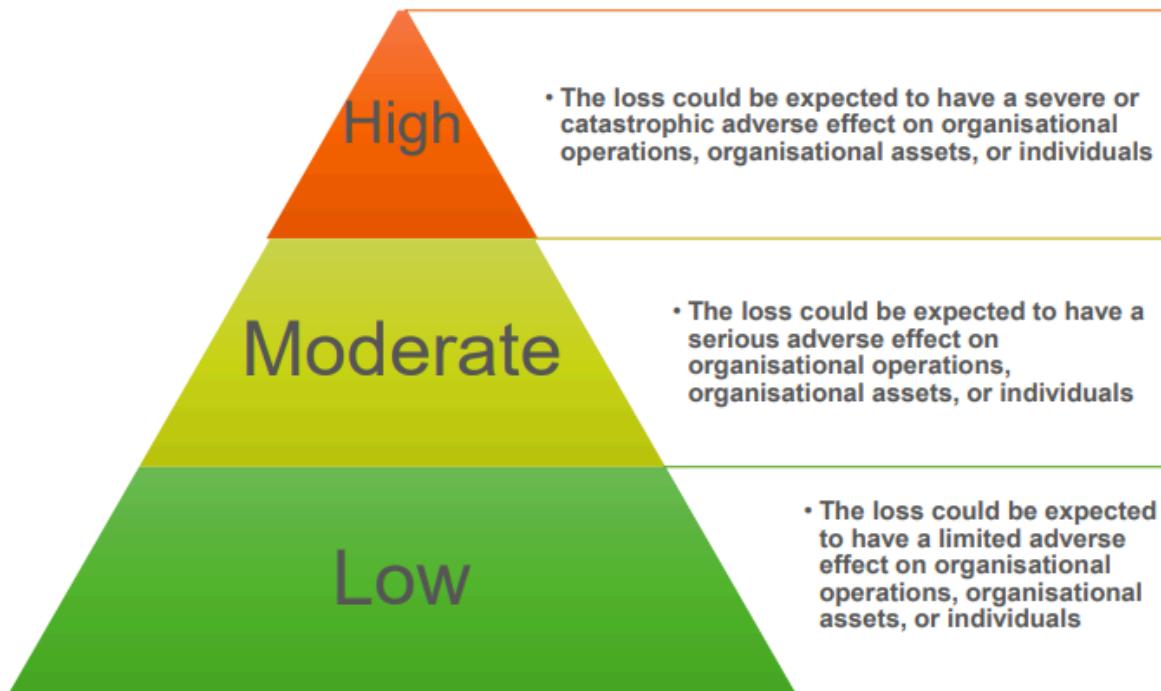
Aspects of integrity and availability protection

- Rollback, the ability to return to an earlier state
- Authenticity, verification of identity of communication partner
- Non-repudiation, origin and/or reception of message can't be denied in front of third party
- Audit, monitoring of user initiated events
- Intrusion detection

This is referred to as "optimistic security"

Security Attacks Levels by Impact

Not all security attacks are equal, some could be devastating and some could be of minimal impact



OSI Security Architecture

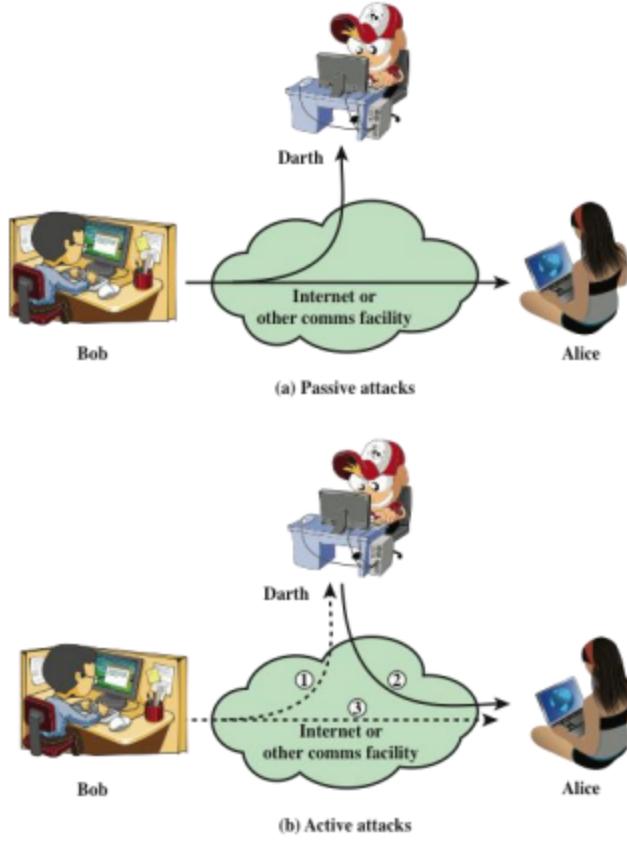
Security attack Any action that compromises the security of information owned by an organisation

Security mechanism A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack

Security service A processing or communication service that enhances the security of the data processing systems and the information transfers of an organisation. Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Attacks can be classified into two parts: passive and active. Passive attacks attempt to learn from a system without interacting with system resources. Active attacks attempt to alter system

resources.



Passive Attacks

Essentially eavesdropping on transmissions, the goal for the opponent is to obtain the information that's being transmitted. There are two types of passive attacks: The release of message contents, and traffic analysis

Active Attacks

These involve some form of modification of the data stream or creation of a false stream. These can be difficult to completely prevent due to variety of potential vulnerabilities.

The goal of defense is to detect attacks and recover from any harm they caused

Cyber Assessment Framework

A framework used for judging the security level of an organisation