## Chapter 1:

Three basic components of computer security:

*Confidentiality*: The concealment of information or resources.

*Integrity*: The trustworthiness of data or resources, preventing unauthorized changes.

*Availability:* The ability to use information or resources (reliability).

Threat Model:

Classifications: Deception (fake news), Disruption (prevent operation), Usurpation (unauthorized control), Disclosure.

Characterizations: Alteration, Spoofing, Repudiation, Denial of Receipt, Delay, Denial of Service.

Policy and Mechanism:

*Security Policy*: A statement of what is, and what is not allowed.

*Security Mechanism*: A method, tool or procedure for enforcing a security policy.

Assumptions and Trust:

*Trust*: Your belief the system is trustworthy.

*Assurance*: Level at which the security mechanism implements the policy.

Let P be the set of all possible states, Q be the set of secure states, R be the set of states restricted by the security system.

A security mechanism is *secure* if R in Q, *precise* if R = Q, and *broad* if there are some states r not in Q.

*Specification*: A statement of the desired functioning of the system.

A system is said to *satisfy* a specification if the specification correctly states how the system will function.

*Design*: Translates the specifications into components that will implement them.

*Implementation*: Creates a system that satisfies the design.

A program is *correct* if its implementation performs as specified.

## Chapter 2:

Protection State:

*State*: The collection of the current valu

## Chapter 3:

## Chapter 4:

## Chapter 5:

## Chapter 6: