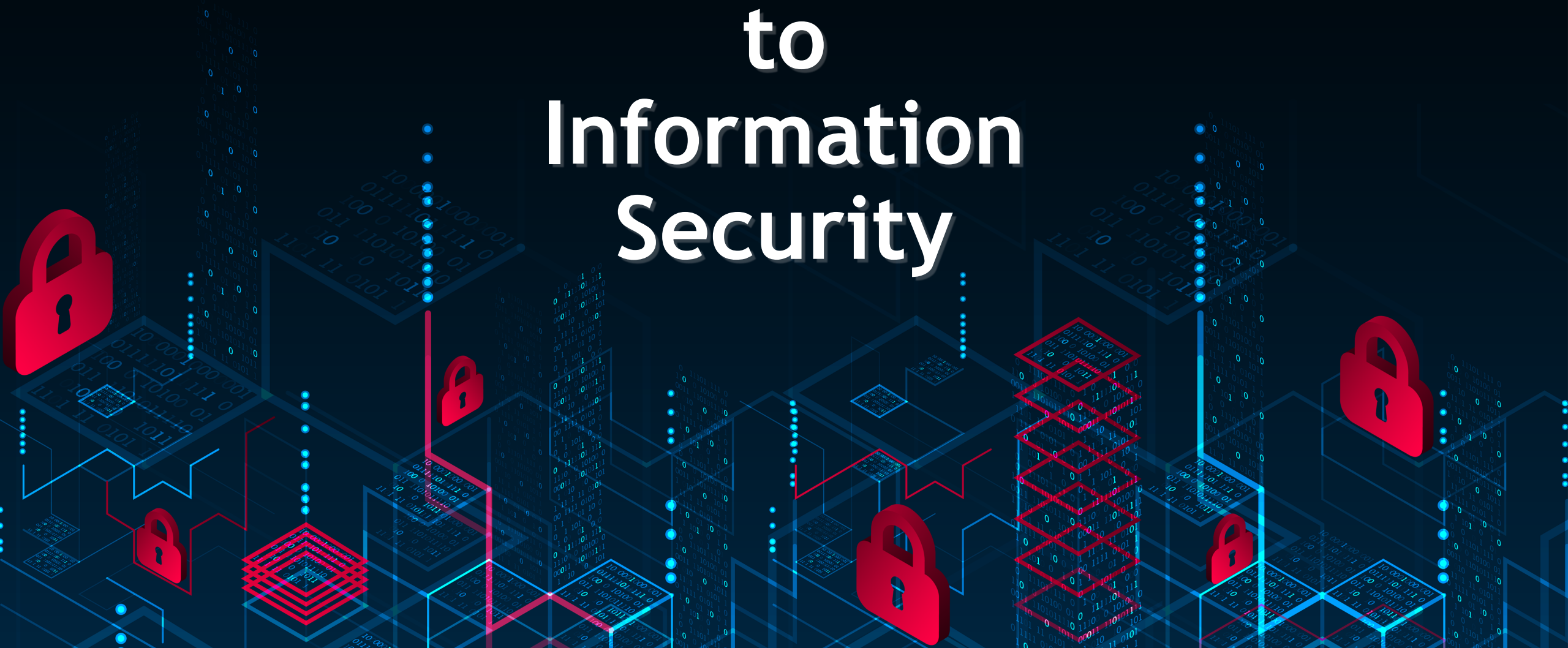
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

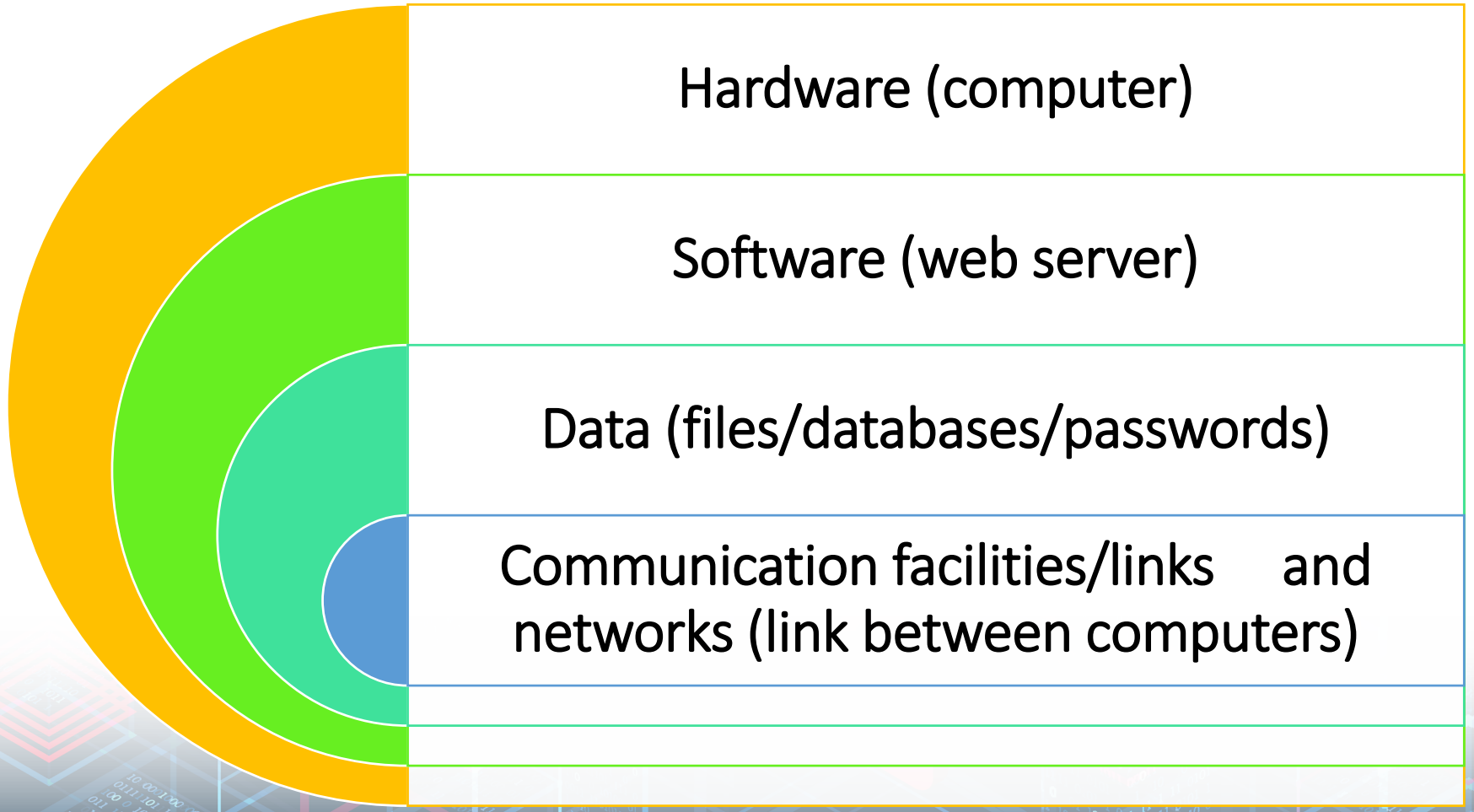
Introduction to Information Security



Computer Security Concepts

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

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



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

Vulnerabilities, Threats and Attacks

- Threats
  - Potential violation of security policy by exploiting a vulnerability
  - Represent potential security harm to an asset
  - If we have a policy that a student can't access the grades of another student. Threat is if something allow a student to potential access another student's grades.

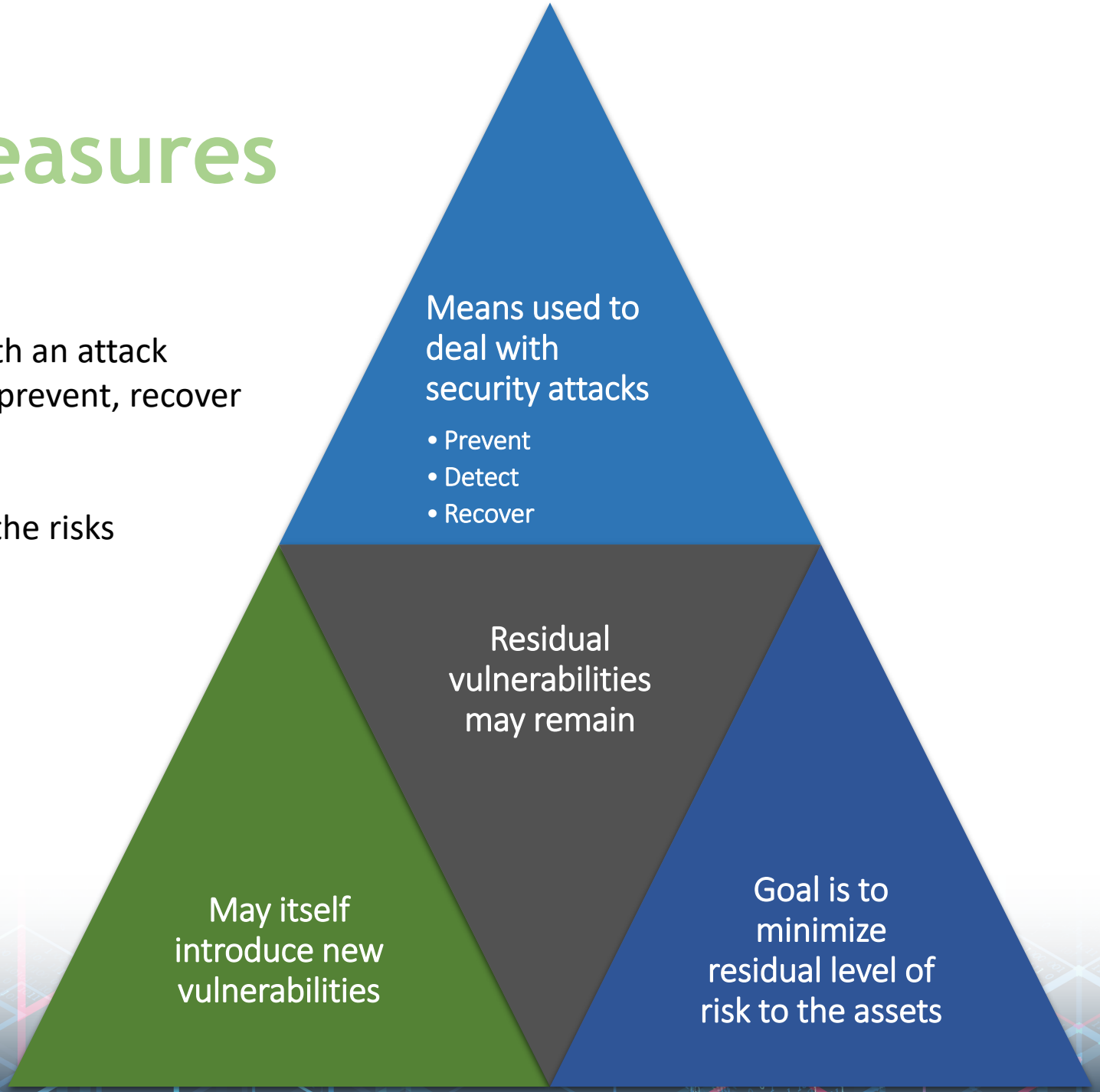
Vulnerabilities, Threats and Attacks

- Attacks
  - A threat that is carried out; a successful attack leads to violation of security policy
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Countermeasures

A way to deal with an attack
Detect, respond, prevent, recover

Aim to minimize the risks



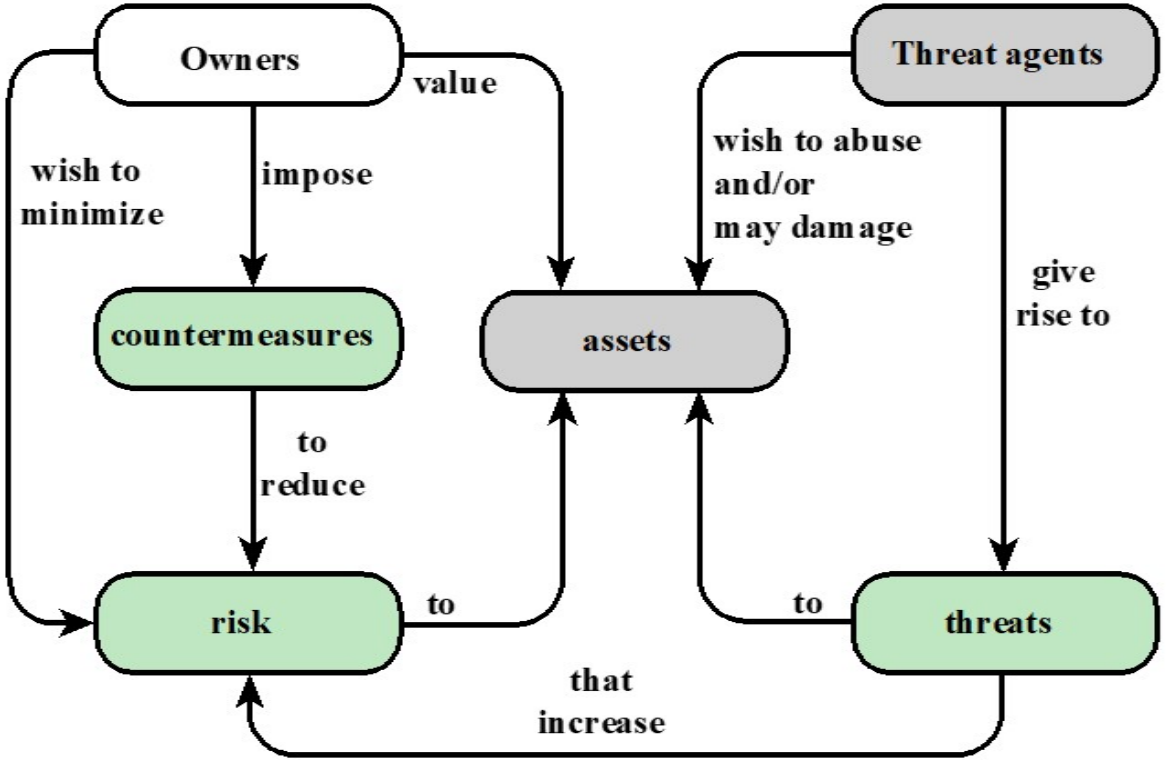


Figure 1.2 Security Concepts and Relationships

Threat Consequences and Attacks

- Threat Action: an attack
- Threat Agent: Entity that attacks, or is threat to system (hacker, attacker (don't have to be bad - law enforcement), malicious user)
- Threat Consequence: A security violation that results from threat action

Computer Security Concepts

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