CHITKARA UNIVERSITY

Introduction to Security

Key Security Concepts

CHITKARA UNIVERSITY

Confidentiality

- preserving authorized restrictions on information access and disclosure.
- including means for protecting personal privacy and proprietary information

Integrity

- guarding against improper information modification or destruction,
- including ensuring information nonrepudiation and authenticity

Availability

- ensuring timely and reliable access to and use of information

Computer Security Terminology

CHITKARA UNIVERSITY

- **Adversary** (threat agent) - An entity that attacks, or is a threat to, a system.
- **Attack** - An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.
- **Countermeasure** - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Computer Security Terminology

CHITKARA UNIVERSITY

- **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Security Policy** - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.
- **System Resource (Asset)** - Data; a service provided by a system; a system capability; an item of system equipment; a facility that houses system operations and equipment.

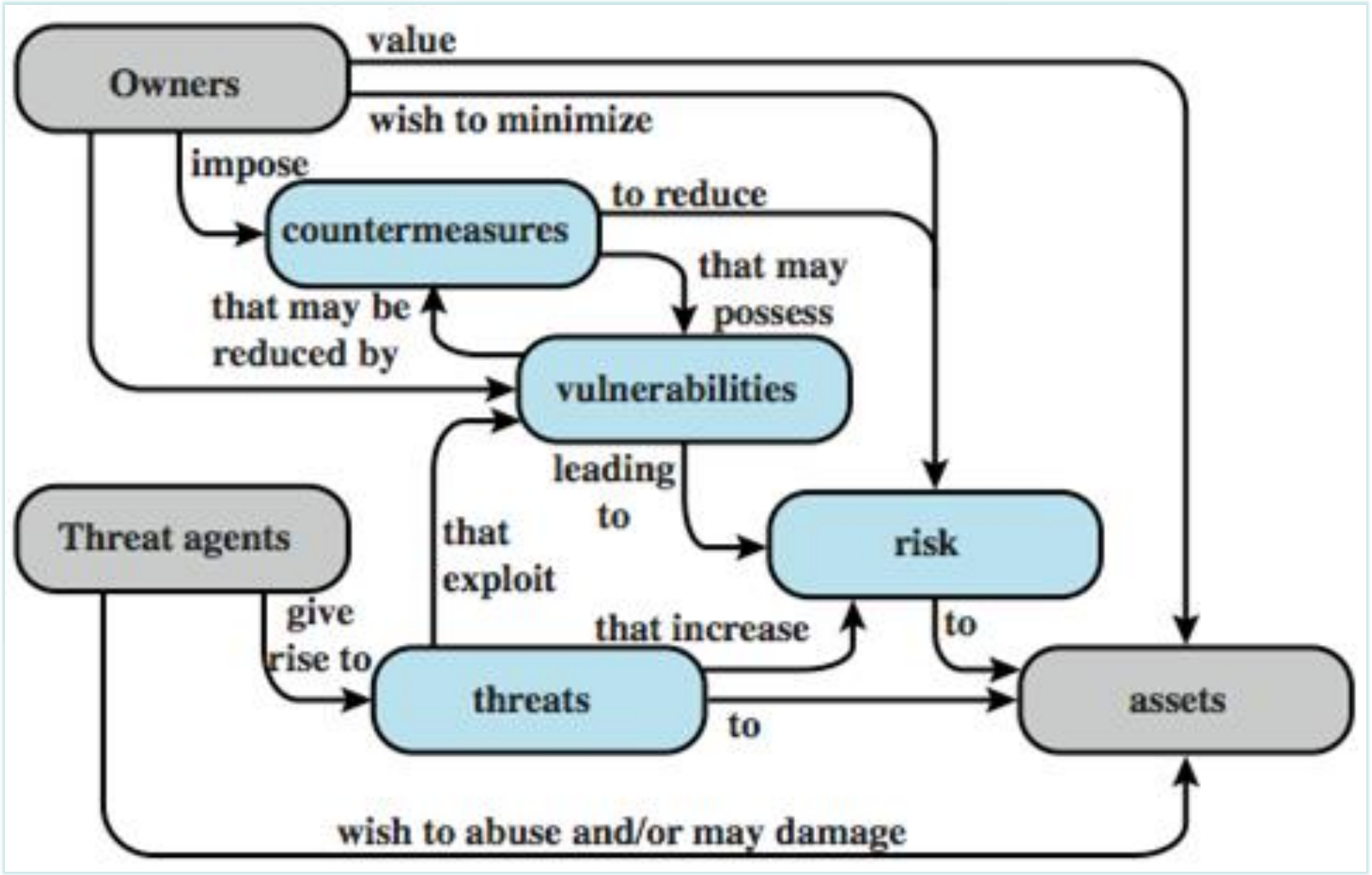
- **Threat** - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

- **Vulnerability** - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Threat - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

- **Vulnerability** - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Security Concepts and Relationships



Threat Consequences

CHITKARA UNIVERSITY

- **Unauthorized disclosure** is a threat to *confidentiality*
- ***Exposure***: This can be deliberate or be the result of a human, hardware, or software error
- ***Interception***: unauthorized access to data
- ***Inference***: e.g., traffic analysis or use of limited access to get detailed information
- ***Intrusion***: unauthorized access to sensitive data

- **Deception** is a threat to either system or data *integrity*
- ***Masquerade***: e.g., Trojan horse; or an attempt by an unauthorized user to gain access to a system by posing as an authorized user
- ***Falsification***: altering or replacing of valid data or the introduction of false data
- ***Repudiation***: denial of sending, receiving or possessing the data.

Passive and Active Attacks

CHITKARA UNIVERSITY

- **Passive attacks** attempt to learn or make use of information from the system but does not affect system resources
  - eavesdropping/monitoring transmissions
  - difficult to detect
  - emphasis is on prevention rather than detection
  - two types:
    - message contents
    - traffic analysis
- **Active attacks** involve modification of the data stream
  - goal is to detect them and then recover
  - four categories:
    - masquerade
    - replay
    - modification of messages
    - denial of service

CHITKARA UNIVERSITY

Thanks