CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Introduction to the course:
  - Objective: After completion of this course a student should have a background of security and privacy issues in different aspects of computing including security issues and solutions in programs, operating systems, networks, and applications.

- What is Security?
  - Relative or Absolute measure?

Schedule

- Mon 3-4PM → 12-1PM or 10-11AM
- Tue: 4-5PM
- Wed: 5-6PM

This Class

- Computer Security
  - Few Definitions
  - Basic Security Services and Tools\ Techniques
  - Threat consequences
  - Security Functional Requirements

Defining Security

- Security : *Ability to avoid being harmed by any risk, danger or threat* (Cambridge dictionary)

- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities

- Security is achieving some goals in presence of Adversary

Computer Security Terminology

- **Threat**
  - A potential for violation of security, which exists 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.

Computer Security Terminology

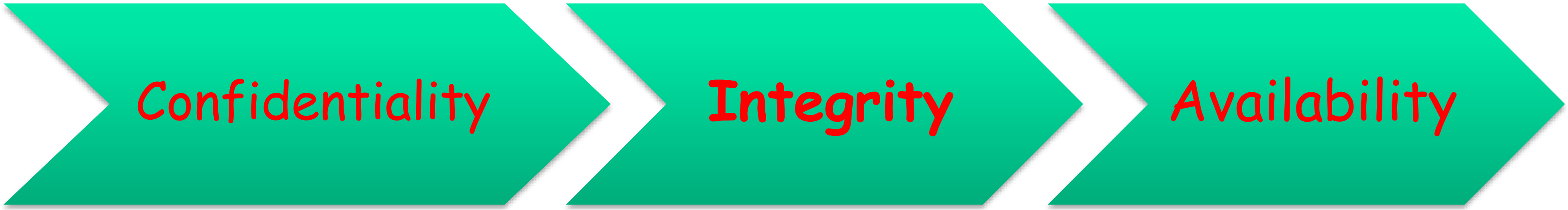
- **Adversary** (threat agent)
  - An entity that attacks, or is a threat to, a system.
- **Attack**
  - A deliberate attempt to evade security services and violate security policy of a system.
- **Countermeasure**
  - An action, device, procedure, or technique that reduces a threat, a vulnerability, 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

- **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.

Security Goals

Basic Security Services
Key Security Concepts (FIPS PUB 199)



Confidentiality

- preserving authorized restrictions on information access and disclosure.

Integrity

- guarding against improper information modification or destruction,

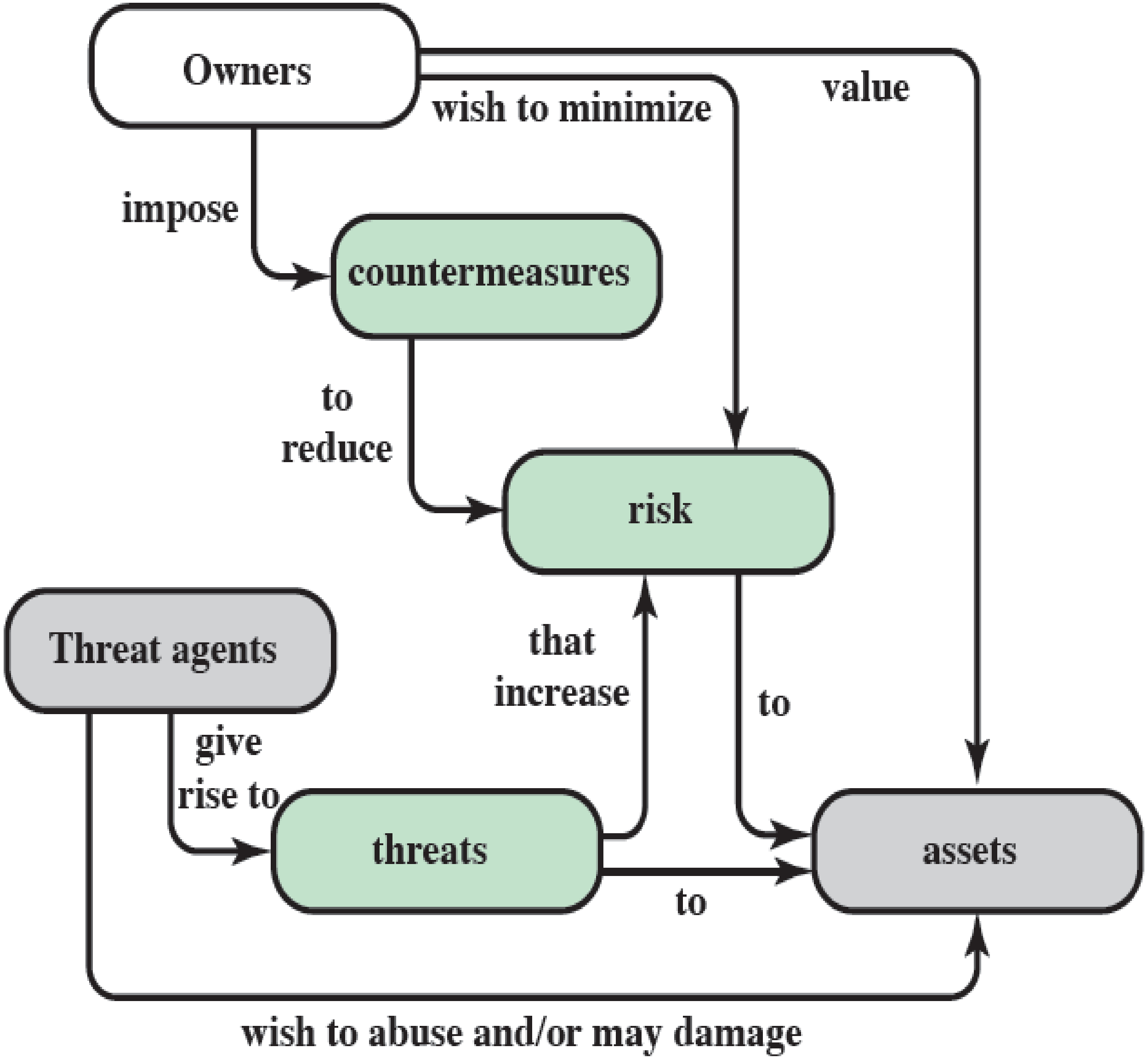
Availability

- ensuring timely and reliable access to and use of information

Computer and Network Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Security Concepts and Relationships



Owners

wish to minimize

value

impose

countermeasures

to reduce

risk

Threat agents

that increase

to

give rise to

threats

to

assets

wish to abuse and/or may damage

Security Plan

- Threat model: What an adversary can do
- Policy: Goal you want to achieve
- Common goal: CIA
- Mechanism: Techniques that your system provides to up-hold the policy
- Why Security is hard?
- Need to guarantee policy, assuming the threat model
  - To consider all aspects of adversary
- Weakest link maters
- Security is a process

Problems with Threat model

- Consider a system uses DES 56-bit key at present
  - Computational assumption changes over time
- User gets email asking to send credential, transfer money etc.
  - Phishing attack, human factor not accounted
- In 2011 CA were issued fake certificates
  - two certificate authority (CA) compromised
  - Assumed CA are fully trusted
- More explicit threat models to understand possible weakness

Problems with the policy

- Yahoo mail has user name password and security Qs
  - Adversary could guess/ know the answers to Security Qs and login to email unauthorisedly

- Think hard about policy statements

Problems with the mechanism

- No of password attempts in login system
- Small IV in WEP
- Missing access control in Citibank credit card website
- Proper mechanism needs to be incorporated

Countermeasures

means used to deal with security attacks

- prevent
- detect
- recover

may introduce new vulnerabilities

Residual vulnerabilities may remain

goal is to minimize residual level of risk to the assets