CSCE 465 Computer & Network Security

Instructor: Abner Mendoza

http://people.tamu.edu/~abmendoza/csce465/spring2019.html

Security Overview

Roadmap

- Security definition, components/objectives
- Security threats and attacks
- Achieving security: Security Policy, Mechanism, Assurance

What is Security?

- [Informally] Security is the *prevention* of certain types of *intentional* actions from occurring
  - Weaknesses are **Vulnerabilities**
  - Potential actions are **Threats**
  - Threats that are carried out are **Attacks/Exploits**
  - Intentional attacks are carried out by an **Attacker**
  - Objects of attacks are **Assets**

Security: Definition

- *Security* is a ***state of well-being*** of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is ***kept low or tolerable***

- Security rests on confidentiality, authenticity, integrity, and availability

Goals of Security

Prevention

- Prevent attackers from violating security policy

Detection

- Detect attackers' violation of security policy

Response & Recovery

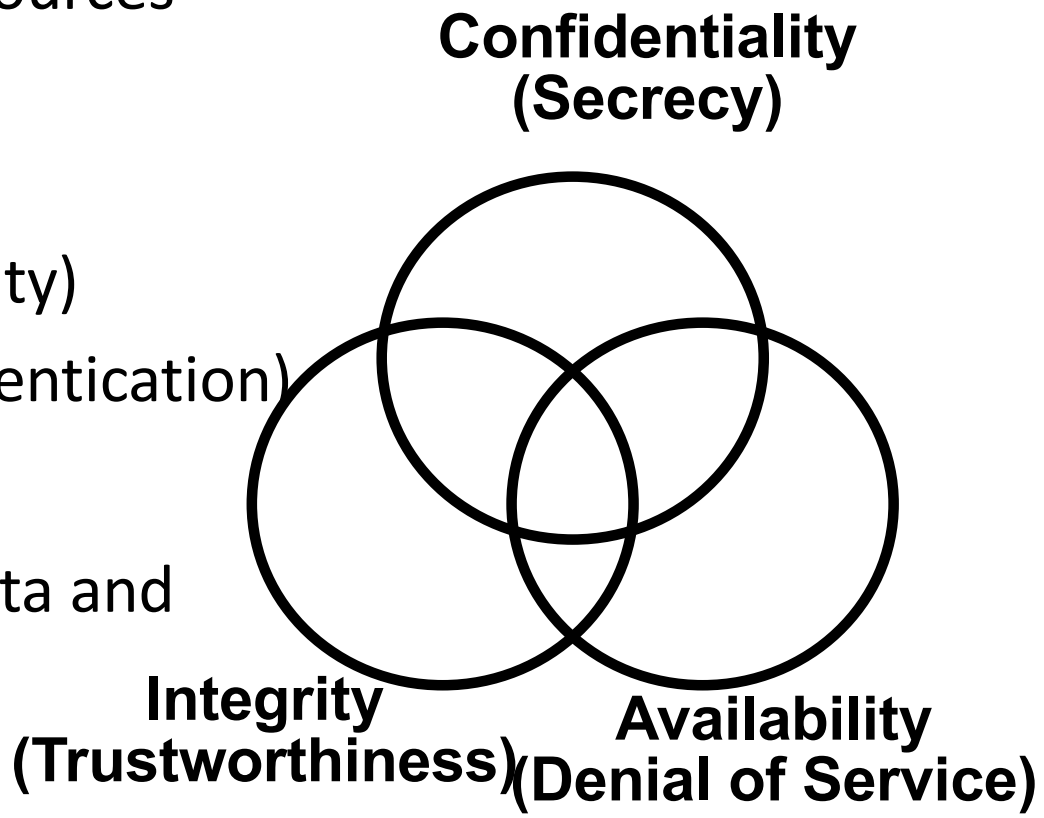
- Stop attack, assess and repair damage

Survivability

- Continue to function correctly even if attack succeeds

Basic Components (Security Objectives)

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources



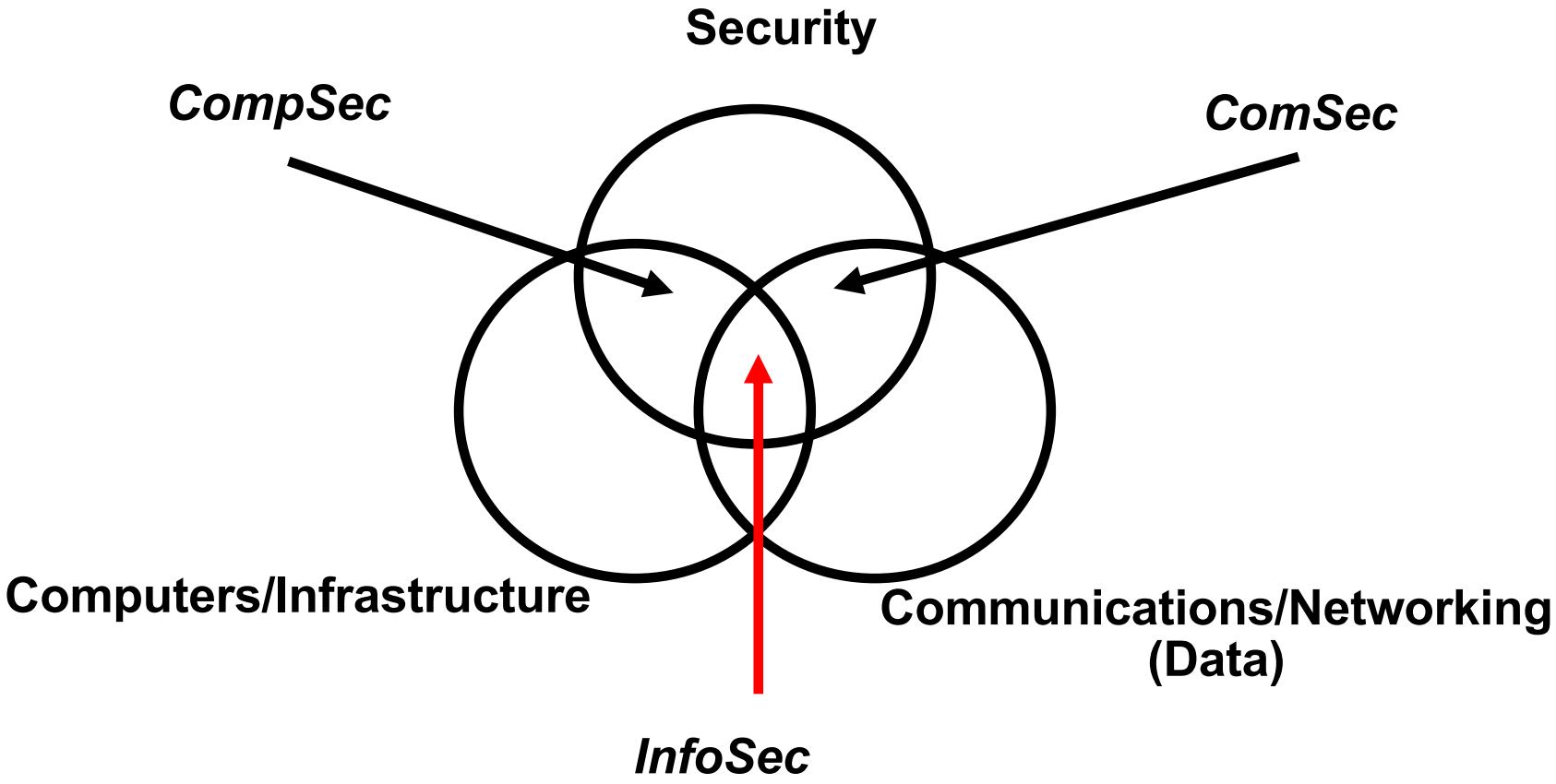
Commercial Example

- Confidentiality — An employee should not come to know the salary of his manager
- Integrity — An employee should not be able to modify the employee's own salary
- Availability — Paychecks should be printed on time as stipulated by law

Military Example

- Confidentiality — The target coordinates of a missile should not be improperly disclosed
- Integrity — The target coordinates of a missile should not be improperly modified
- Availability — When the proper command is issued the missile should fire

Information Security (CompSec+ComSec):



Why is Security Important

- Computers and networks are the nerves of the basic services and critical infrastructures in our society
  - Financial services and commerce
  - Transportation
  - Power grids
  - Etc.
- Computers and networks are targets of attacks by our adversaries.

Why Is Security Hard (and Harder)

- **Lack of awareness** of threats and risks of information systems
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
  - The situation is getting better, but …
- (Historical) **Reluctance** to invest in security mechanisms (defense is inherently more expensive)
  - The situation is improving
    - Example: Windows 95 → Windows 2000 → Windows XP → Windows XP SP2 → Windows Vista → Windows 7 → Windows 10
  - But there exists ***legacy software***

Why Is Security Hard (and Harder)

- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of security management and administration
  - Security is not just encryption and authentication
- Software vulnerabilities
  - Example: buffer overflow vulnerabilities
  - We need techniques and tools to better software security

Why Is Security Hard (and Harder)

- The complexity of computers and networks
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access
- Hacker skills keep improving
  - It's a business…
- User ignorance
  - Social engineering
- Defense is inherently more expensive
  - Offense only needs the weakest link

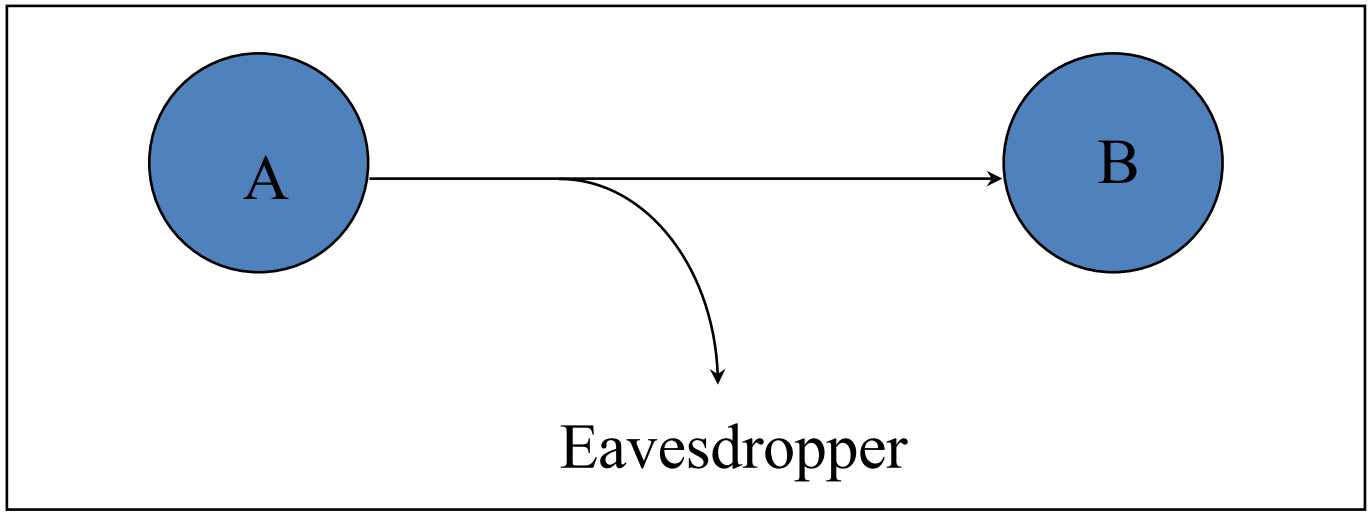
Security Threats and Attacks

- A threat is a *potential* violation of security
  - Flaws in design, implementation, and operation
- An attack is any *action* that violates security
  - Active vs. passive attacks

ATTACK EXAMPLES

Eavesdropping - Message Interception (Attack on Confidentiality)

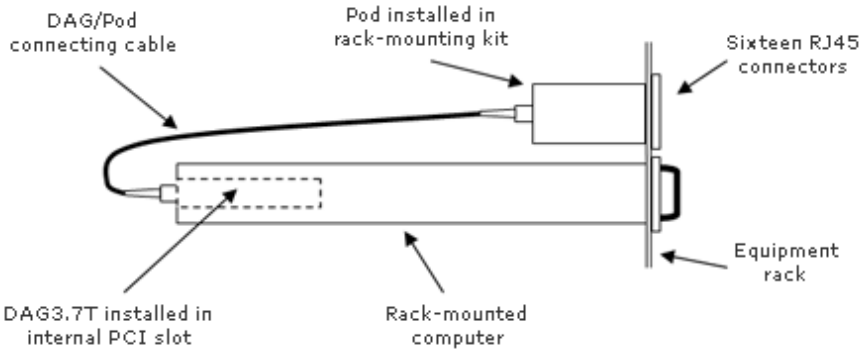
- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs

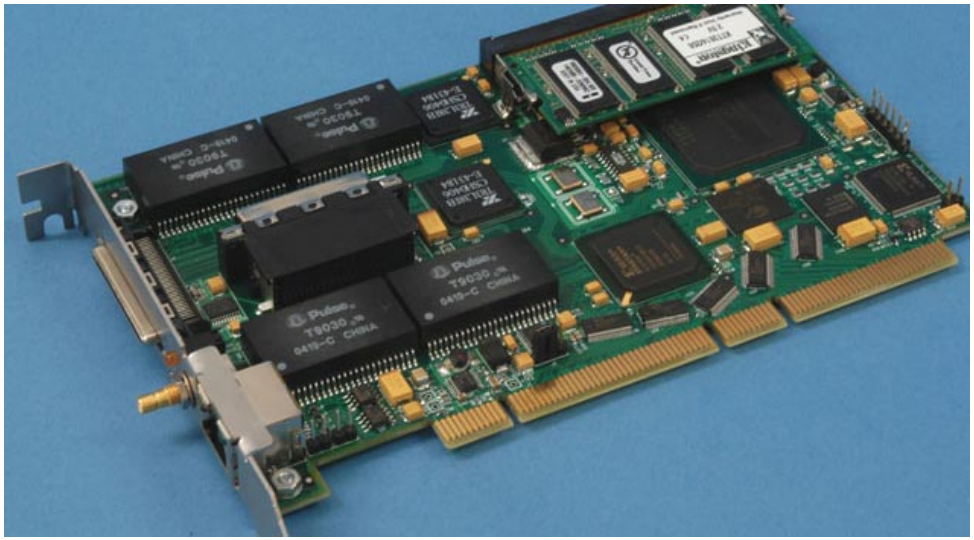


Full Packet Capture (Passive)

Example: OC3Mon

- Rack-mounted PC
- Optical splitter
- Data Acquisition and Generation (DAG) card





Source: endace.com

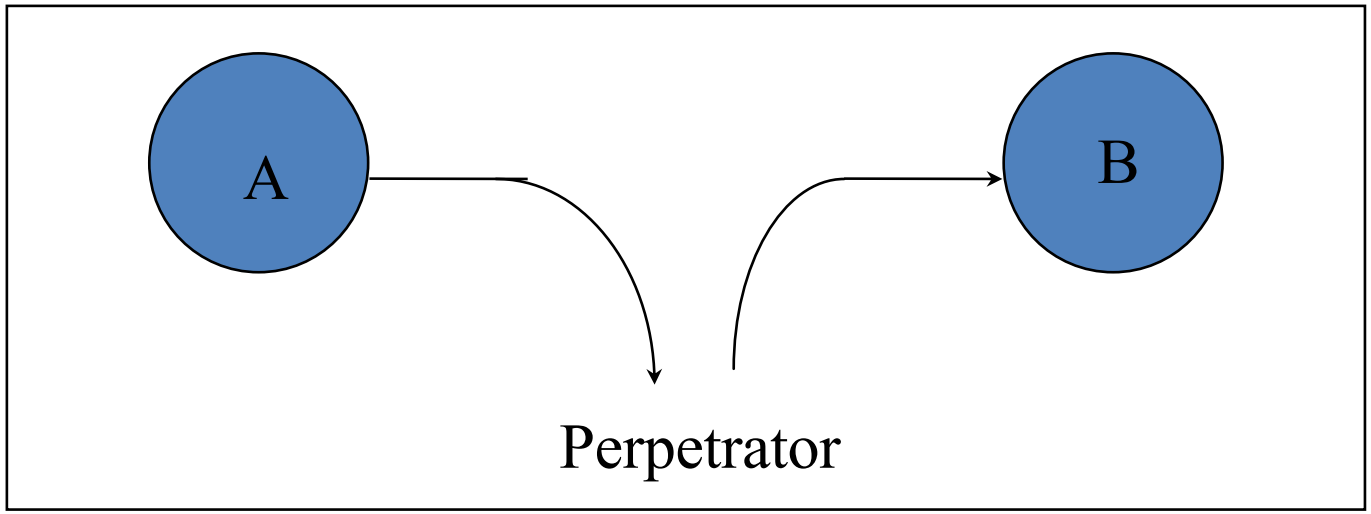
Eavesdropping Attack: Example

- tcpdump with promiscuous network interface
  - On a switched network, what can you see?

- What might the following traffic types reveal about communications?
  - DNS lookups (and replies)
  - IP packets without payloads (headers only)
  - Payloads

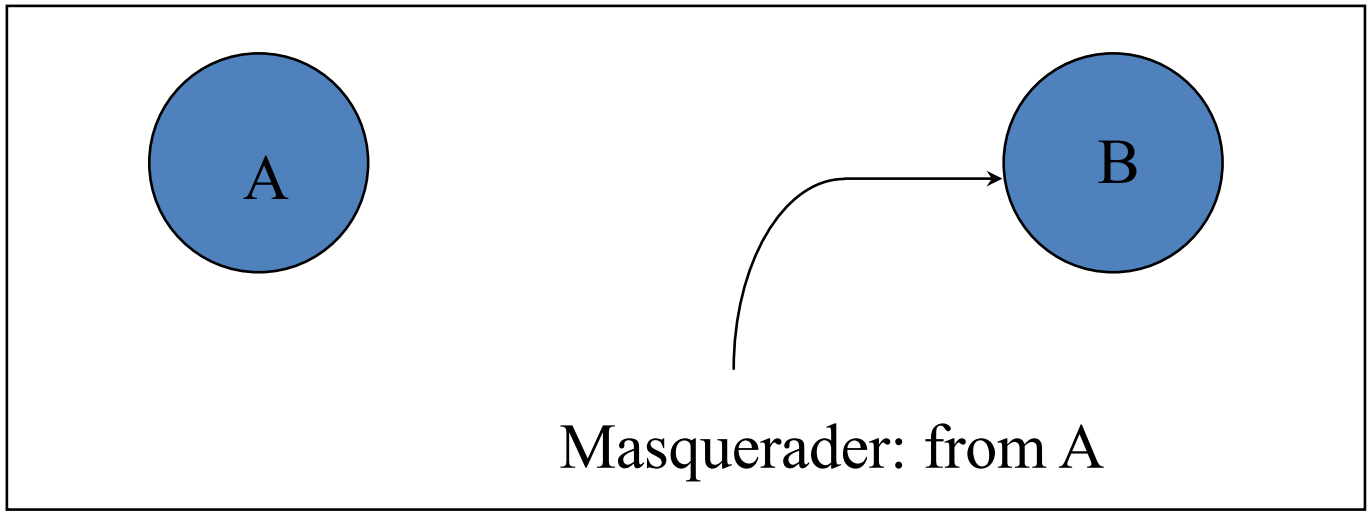
Integrity Attack - Tampering

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



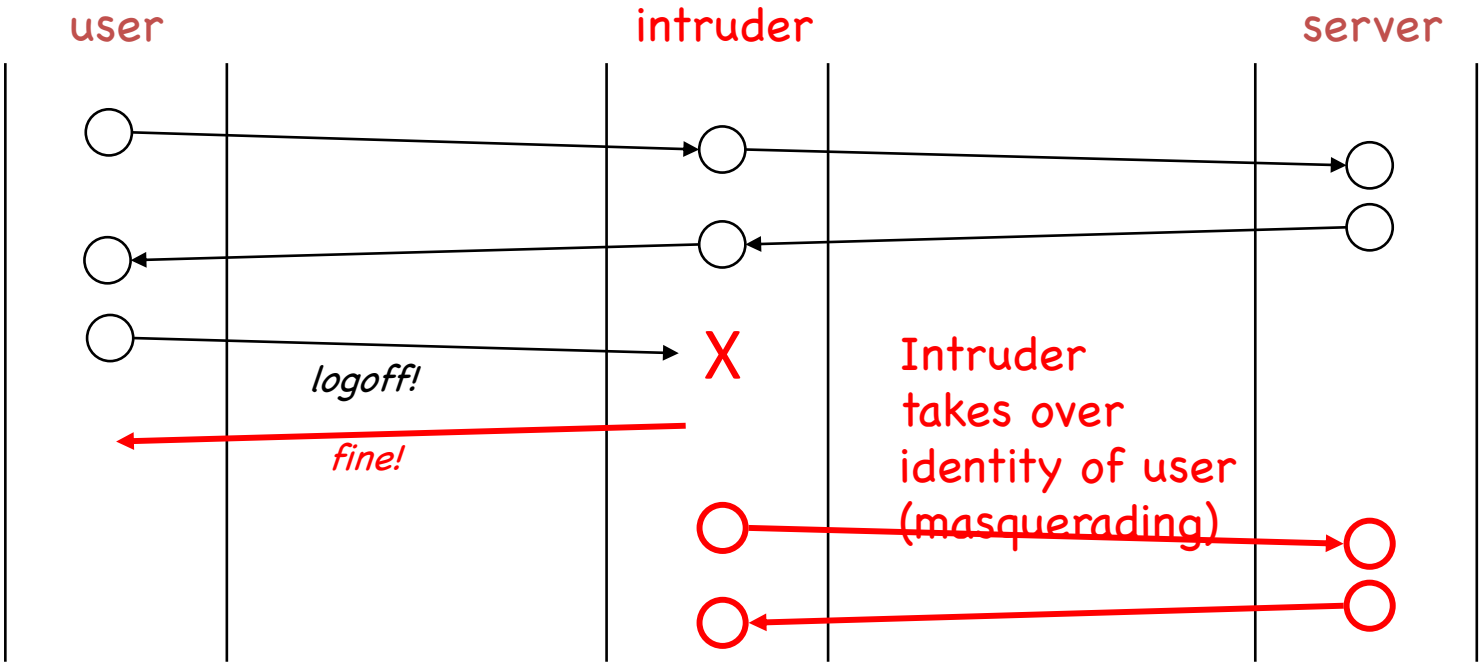
Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



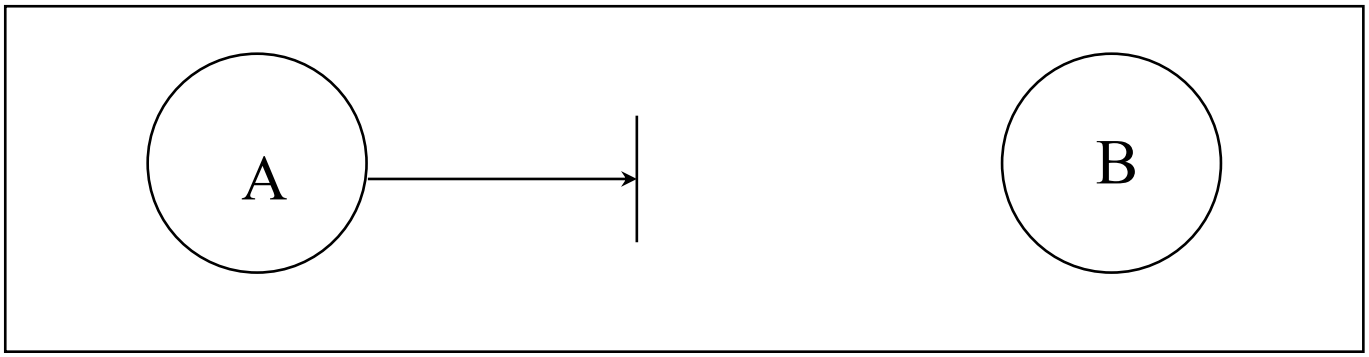
Man-In-The-Middle: Example

- **Passive tapping**
  - Listen to communication without altering contents.
- **Active wire tapping**
  - Modify data being transmitted
  - Example:



Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit



- Blatant *denial of service* (DoS):
  - Crashing the server
  - Overwhelm the server (use up its resource)

Impact of Attacks

- Theft of confidential information
- Unauthorized use of
  - Network bandwidth
  - Computing resource
- Spread of false information
- Disruption of legitimate services

All attacks can be related and are dangerous!

Achieving Security

How do we achieve security?

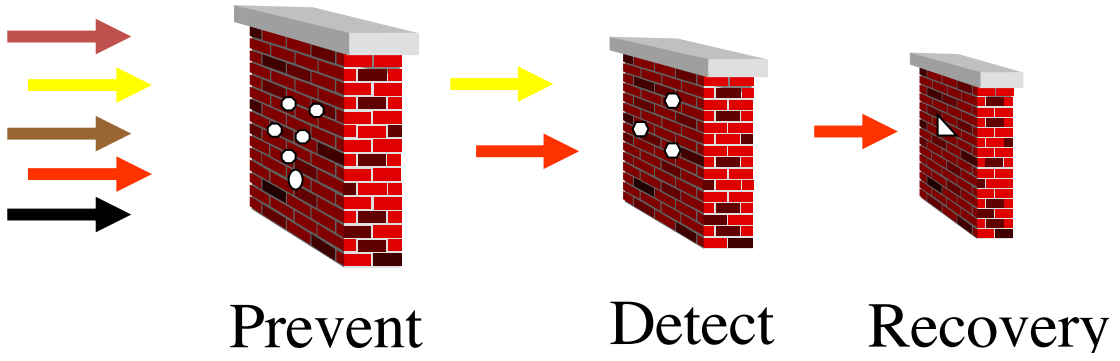
- Security policy — What?
- Security mechanism — How?
- Security assurance — How well?

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines “security” for the site/system/*etc*.
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

General Types of Security Mechanisms (Goals)

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds



Security Mechanisms

- Prevention is more fundamental
  - Detection requires that the audit trail be protected from alteration
- Sometime detection is the only option, e.g.,
  - Accountability in proper use of authorized privileges
  - Modification of messages in a network
- Security functions are typically made available to users as a set of ***security services***
- Cryptography underlies many security mechanisms

Security Services

- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces

- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

Security Services (Cont'd)

- Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
- Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

BASIC SECURITY PRINCIPLES

Some Basic Security Principles

- Domain Separation
- Process isolation
- Resource Encapsulation
- Least Privilege
- Layering/Abstraction/Data Hiding
- Modularity/Minimization

Security by Obscurity?

- Security by obscurity
  - If we hide the inner workings of a system it will be secure

- Less and less applicable in the emerging world of vendor-independent open standards.
- Less and less applicable in a world of widespread computer knowledge and expertise.

Security by Legislation?

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder

- User awareness and cooperation is important, but cannot be the principal focus for achieving security

Trust and Assumptions

- Underlie *all* aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support infrastructure work correctly

Security Assurance

- How well your security mechanisms guarantee your security policy
- Everyone wants high assurance
- High assurance implies high cost
  - May not be feasible
- Trade-off is needed
  - Security vs Functionality vs Usability, etc.

Security Assurance

- Specification
  - Arise from Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

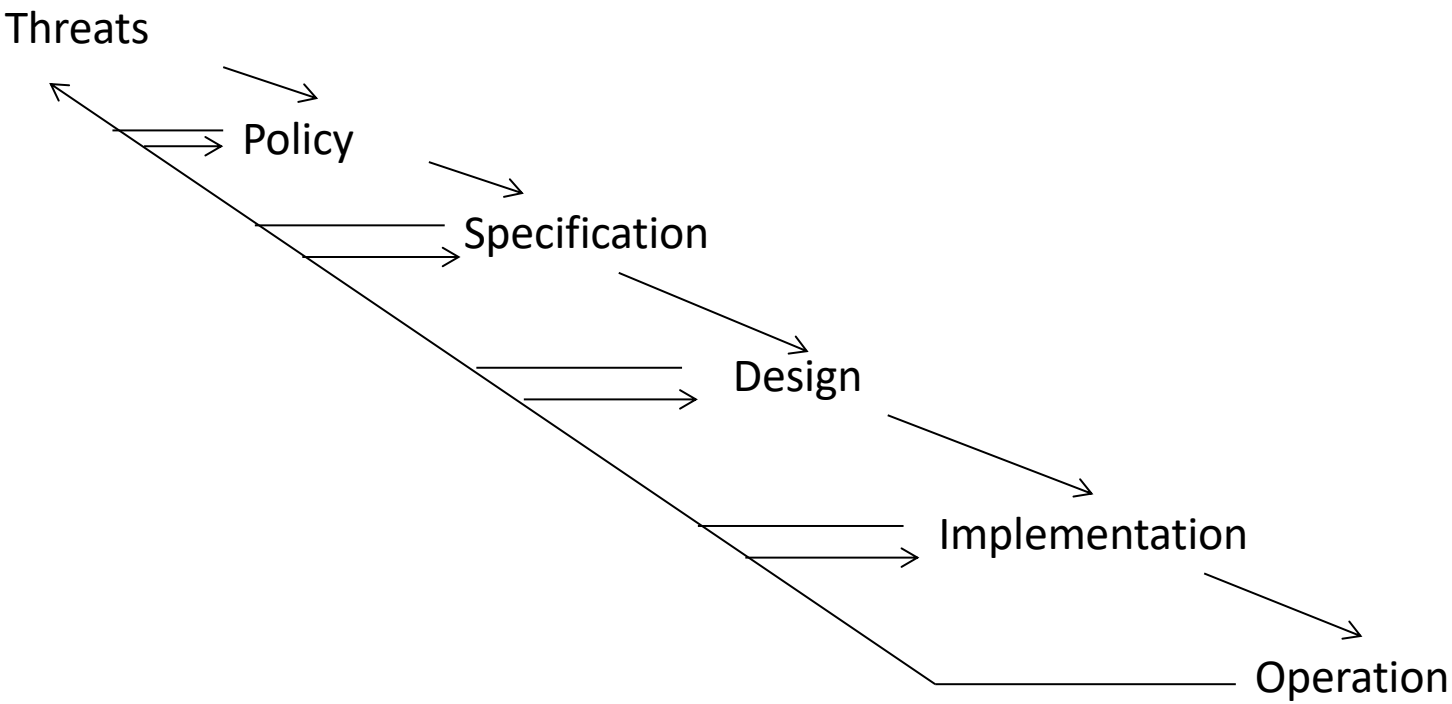
Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Tying Together: The Security Life-Cycle



Next Week

- Homework 1 released
- Kevin as Instructor
- Lab basics (TCR demo)
- Intro to Network Security