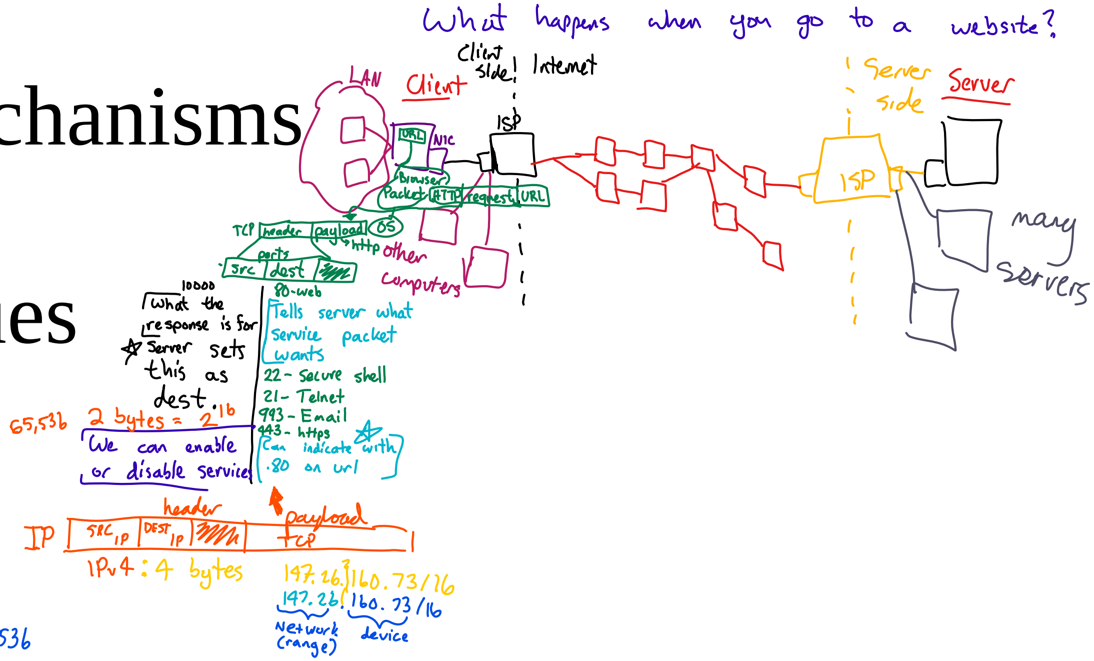
Introduction to Security

- Chapter 1
- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Operational Issues
- Human Issues

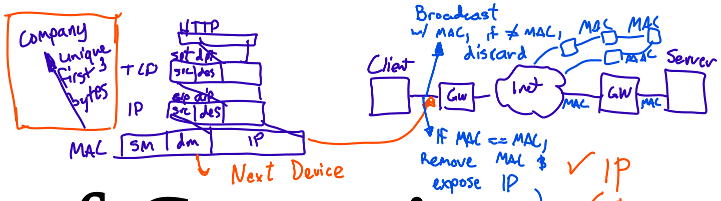


ifconfig

Class A: /8
B: /16
C: /24

$2^{16} = 65536$

192.168.x.x /16
10.x.x.x /24



Goals of Security

✓ IP /16
Gateway
✓ Network Mask – 255.255.0.0 = /16
255.255.255.0/24

If IP, ≠ $_{my}$IP, send back out, forwarding/routing
If IP in not, remake MAC → Add MAC
Routing Protocal → Next Internet Router

- Prevention
  - – Prevent attackers from violating security policy
- Detection
  - – Detect attackers’ violation of security policy
- Recovery
  - – Stop attack, and assess and repair damage
- Retaliation
  - – Stop and capture attackers

logs

revert system

Basic Components

- Confidentiality
  - Keeping data and resources hidden (access and encryption)
  - Existence of data (privacy)
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability ≠ reliability
  - Enabling access to data and resources
- Examples : file systems, networks

No read does not mean it can't be changed

redundancy does not always help

Confidentiality

- To protect classified and private data in government, business and users.
  - Secrecy of data
  - Existence and origin of data
- Mechanisms
  - Access control : controlling programs , permissions
  - Cryptography (encryption) : keys

Integrity

- Prevent improper or unauthorized change of data and provide credibility.
  - Integrity of data
  - Origin of data
- Mechanisms
  - Prevention : block unauthorized attempts
  - Detection : check if data is trustworthy

Availability

Benign Behavior

- Refer to reliability in the context of security.
  - Reliability : usable when components fail
    - Fault tolerant
  - Availability : accessible when attacks happen
    - Attack resilient
- Denial of service attacks
- Mechanisms ? attack or benign?

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Operational Issues
- Human Issues

Threats

techniques behind attacks

- Threats : potential violation of security
- Attacks : actions that violate the security
- Classes of threats
  - Violation of confidentiality, integrity, availability
  - Disclosure : unauthorized access to information
  - Deception : provision of false data
  - Disruption : interruption of correct operation
  - Usurpation : unauthorized control of system } integrity

Threats

- Snooping
  - Unauthorized interception of information
  - Sniffing, eavesdropping
  - Wiretapping attack
- Modification
  - Unauthorized change of information
  - Alteration
  - Man-in-the-middle attack

Threats

- Spoofing
  - Impersonation of another entity
  - Masquerading
  - Phishing
- Repudiation of origin
  - Denial of sending information

Threats

- Denial of receipt
  - Denial of receiving information
- Delay
  - Temporary inhibition of service
- Denial of service
  - Long-term inhibition of service

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Operational Issues
- Human Issues

Policies and Mechanisms

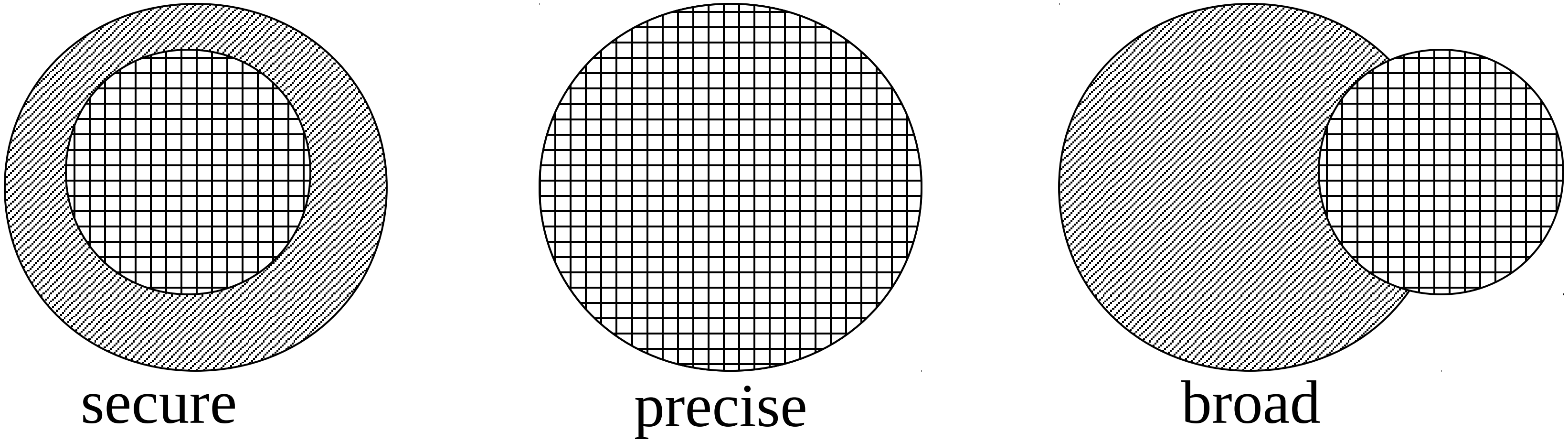
- Policy
  - Statements of what is, and is not, allowed
  - If policies conflict or miss, discrepancies may create security vulnerabilities.
- Mechanism
  - Methods, tools, procedures that enforce policies
  - If mechanisms are flawed, policies can be violated.

Example

- Policy
  - A student cannot copy another student's homework.
- Mechanism
  - Set permissions on files
- Alice fails to set permissions.
- Bob copies Alice's homework.
- Whose fault? (violation of policy)
- Is policy or mechanism flawed?
- How to improve/secure?

Types of Mechanisms

- P : reachable states defined by the system
- Q : secure states defined by security policy
- R : restricted states defined by security mechanism



▦ R: set of restricted states

▨ Q: set of secure states

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Operational Issues
- Human Issues

Trust

- Trust is the assumption a secure system relies on.
  - – Opening a door requires a key
    - The door is sturdy enough.
    - The lock is secure against lock picking and thus is trustworthy.
  - – Login requires a password
    - The login process has no flaw and thus is trustworthy.

Trust

- Trustworthy of policies
  - Unambiguously partition system states into secure and insecure
  - Correctly capture security requirements
- Trustworthy of mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

Trust of Mechanism

- Each mechanism is designed to implement one or more parts of the security policy.
- The union of the mechanisms implements all aspects of the security policy.
- The mechanisms are implemented correctly.
- The mechanisms are installed and administered correctly.

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Operational Issues
- Human Issues

Non-technical Issues

- Non-technical issues that affect the security
- Operational issues
  - Balance between the benefits of the protection and the cost of designing, implementing, and using the protection.
- Human issues
  - Designers, implementers, maintainers, users

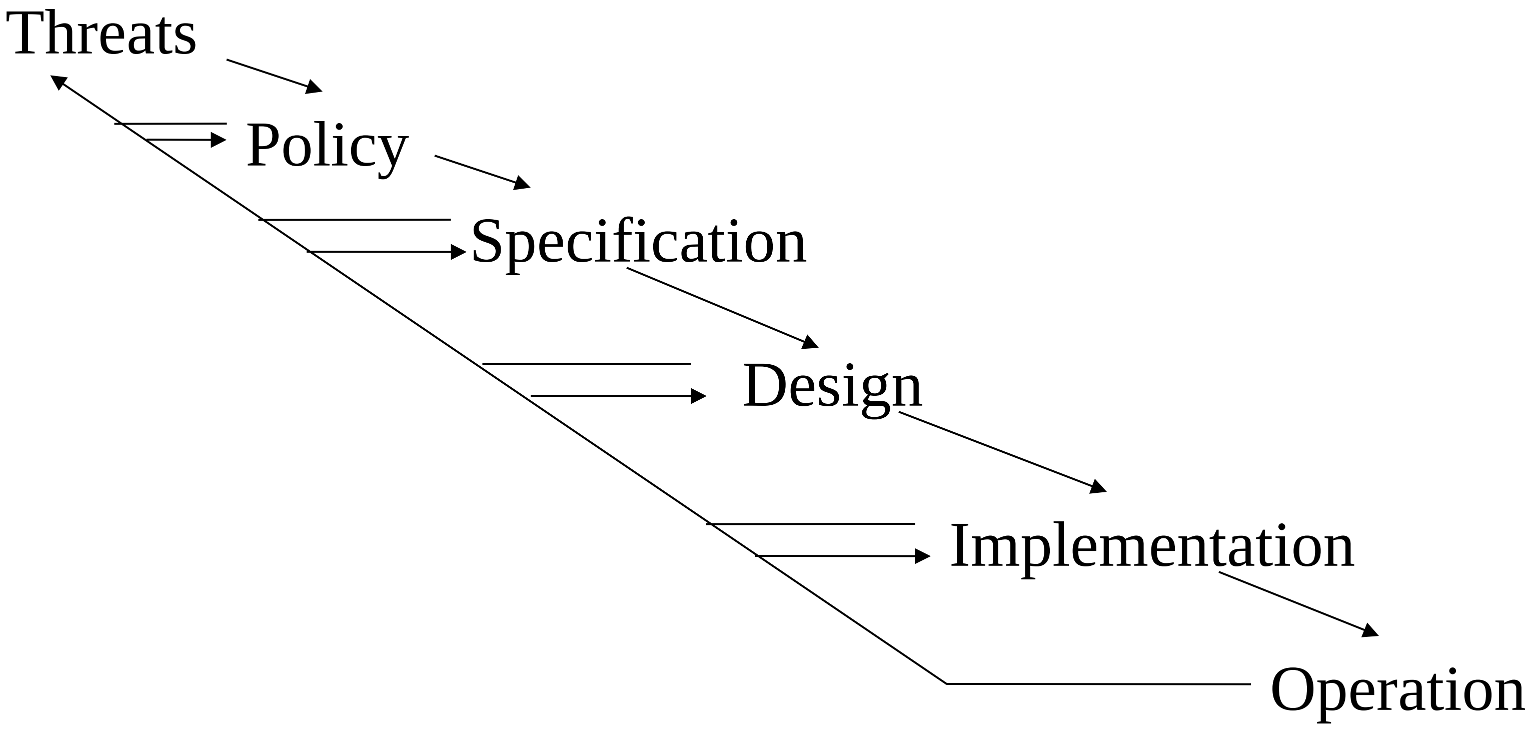
Operational Issues

- Cost-Benefit Analysis
  - Is it worth to protect?
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Is an asset likely to be attacked?
- Laws and Customs
  - Are desired security measures illegal?
  - Examples: exportation of cryptographic technologies

Human Issues

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

Tying Together



Threats

Policy

Specification

Design

Implementation

Operation