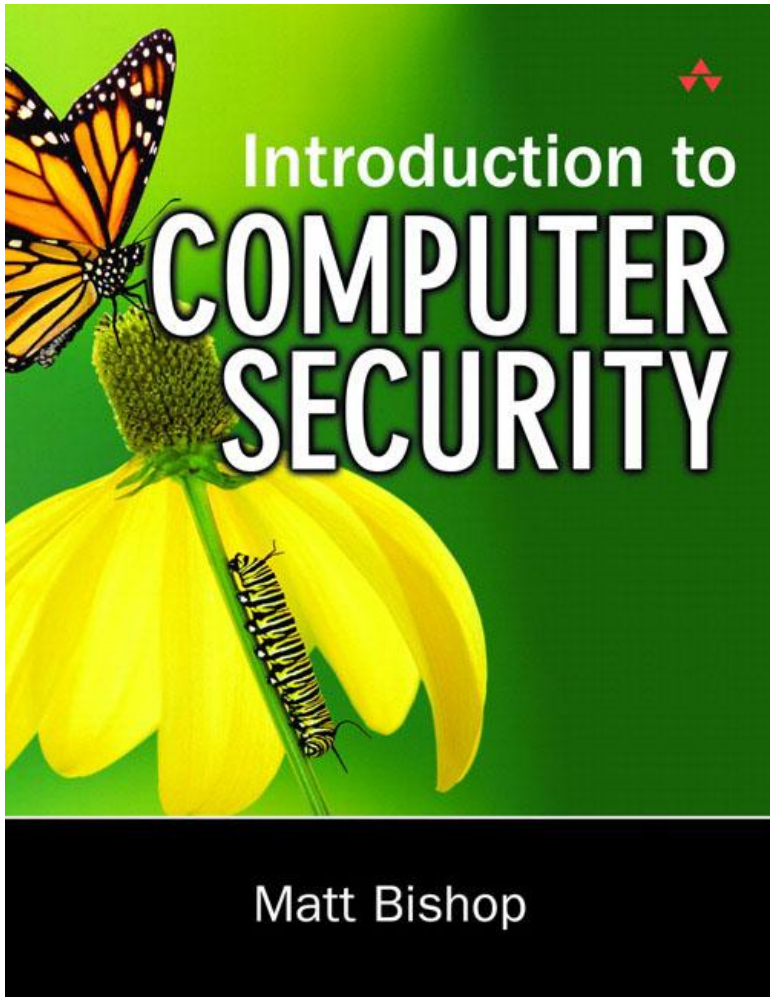
These Slides are prepared from
Matt Bishop slides and book "Introduction to Computer Security"
Benefiting from the Slides posted by Ahmad Al-Mulhem

An Overview of Computer Security



Adnan Gutub

Computer Engineering Department
King Fahd University of Petroleum & Minerals
Dhahran, Saudi Arabia

Network Security

- What is network security?
  - Protection of networks and their services from unauthorized modification, destruction, or disclosure.
- Why is it important?
  - Computer networks are important in our life (mission-critical, business, banks, . . . etc).
  - Information is power and money.
- Why is it difficult?
  - Computer networks are growing in complexity and size.
  - People make mistakes!

Course Goals

- Both theory and practice are important!
- Computer security ≠ Cryptography
- Computer security is a science and art

Ethics

Is hacking . . .

- legal?
  - NO!
- ethical?
  - NO!
- cool?
  - NO!

How about studying attacks for . .

- education?
  - YES
- awareness?
  - YES
- learning to build more secure systems?
  - YES

Outline

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

Basic Components

- Confidentiality
  - Keeping data and resources hidden
  - Supported by: Access control
- Integrity
  - Preventing unauthorized modification
  - Data integrity - integrity
  - Origin integrity - authentication
  - Integrity mechanisms: Prevention vs. Detection
- Availability
  - Enabling access to data and resources
    - Denial of service attacks

Attacks Examples

- Malwares: viruses/worms, Trojans/backdoors, keyloggers/spywares. . etc.
- Intrusions: Compromises.
- Denial of Service Attacks: flooding. . . etc.
- Theft
- Spamming and Phishing
- Social engineering

Threats

Threat - Definition

- A threat is a potential violation of security

Attack – Definition

- An attack is a threat executed by an attacker

- confidentiality
- integrity
- availability

} used to counter threats & attacks

Classes of Threats

- Disclosure - unauthorized access to information
  - snooping, sniffing, wiretapping
  - **Confidentiality** services counter this threat
- Deception - acceptance of false data
  - Modification, spoofing, repudiation of origin, denial of receipt
  - **Integrity** services counter this threat
- Disruption - interruption or prevention of correct operation
  - Modification
  - **Integrity** services counter this threat
- Usurpation - unauthorized control of some part of a system
  - Modification, spoofing, delay, denial of service
  - **Availability** services counter this threat

Policies and Mechanisms

Security ***policy*** - Definition

- A security policy is a statement of what is, and what is not, allowed
  - Policy says: formal or informal --- legal or illegal
  - This defines "security" for the site/system/etc.

Security ***mechanism*** - Definition

- A security mechanism is a method, tool, or procedure for enforcing a security policy.
  - Mechanisms enforce policies – can be non technical (ID proof)
  - Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

Policies & Mechanisms Example

- Copying HWs files Prohibited
  - System provide security mechanism to prevent others from reading users files.
- Ali does not use the secure method.
- Omar copies Ali's files.
- Does Ali's failure to protect his files authorize Omar to copy them?
- If Omar looks into Ali's files without copying, is it a security violation?

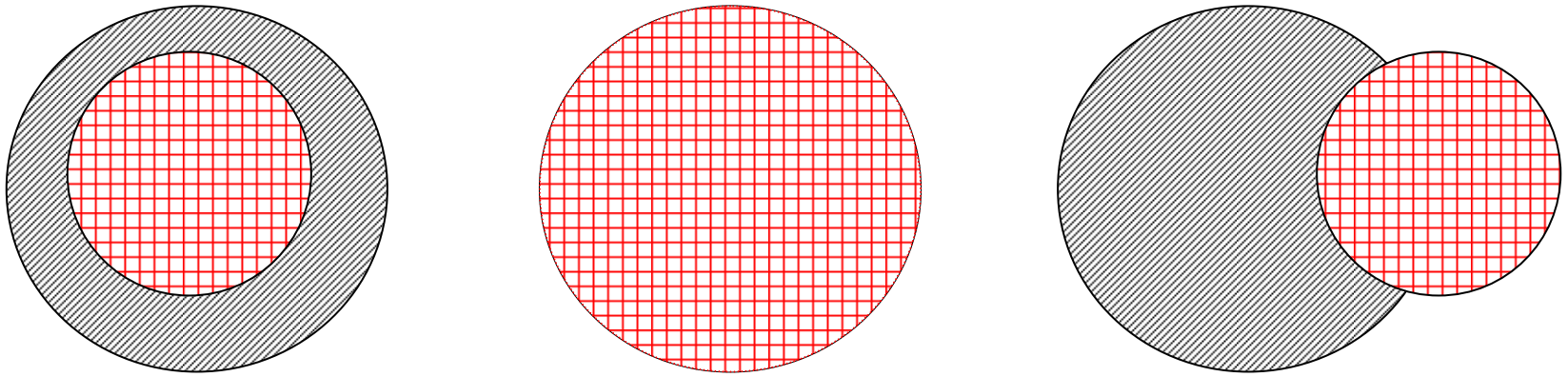
Goals of Security

- Prevention
  - stop attackers from violating security policy
- Detection
  - discover attackers' violation of security policy
- Recovery
  - Prevent or end attack, assess and repair damage
  - continue to function correctly even if attack succeeds

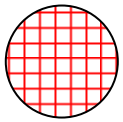
Assumptions & Trust

- Underlie *all* aspects of security
  - example: Opening a door lock requires a key?
- Policies
  - Unambiguously & clearly partition system states into "secure & non-secure" states.
  - Correctly capture security requirements not allowing the system to enter in "non-secure" state.
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

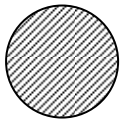
Types of Mechanisms



secure precise broad



set of reachable states



set of secure states

Assurance

Assurance - Definition

- A basis of "how much" one can trust a system
  - Specification
    - Requirements analysis
    - Statement of desired functionality
  - Design
    - How system will meet specification
  - Implementation
    - Programs/systems that carry out design

Medication Example….

Operational Issues

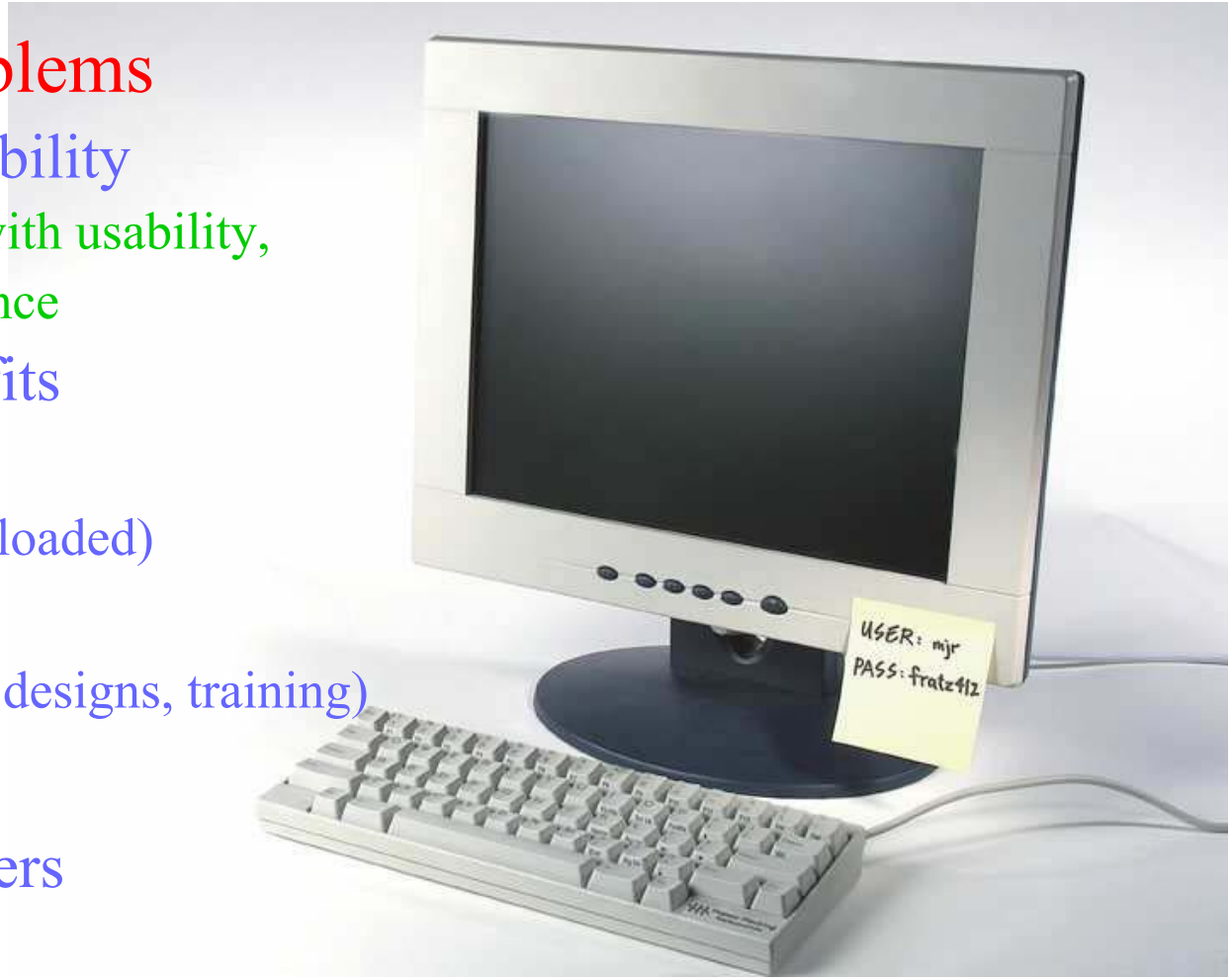
- Policies and mechanisms must consider factors other than protection
- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis - Attack trees
  - Should we protect something? - potential threats
  - How much should we protect this thing? – level of protection
- Laws and Customs
  - Are desired security measures illegal? - legal
  - Will people do them? – acceptable

Unused mechanisms ?

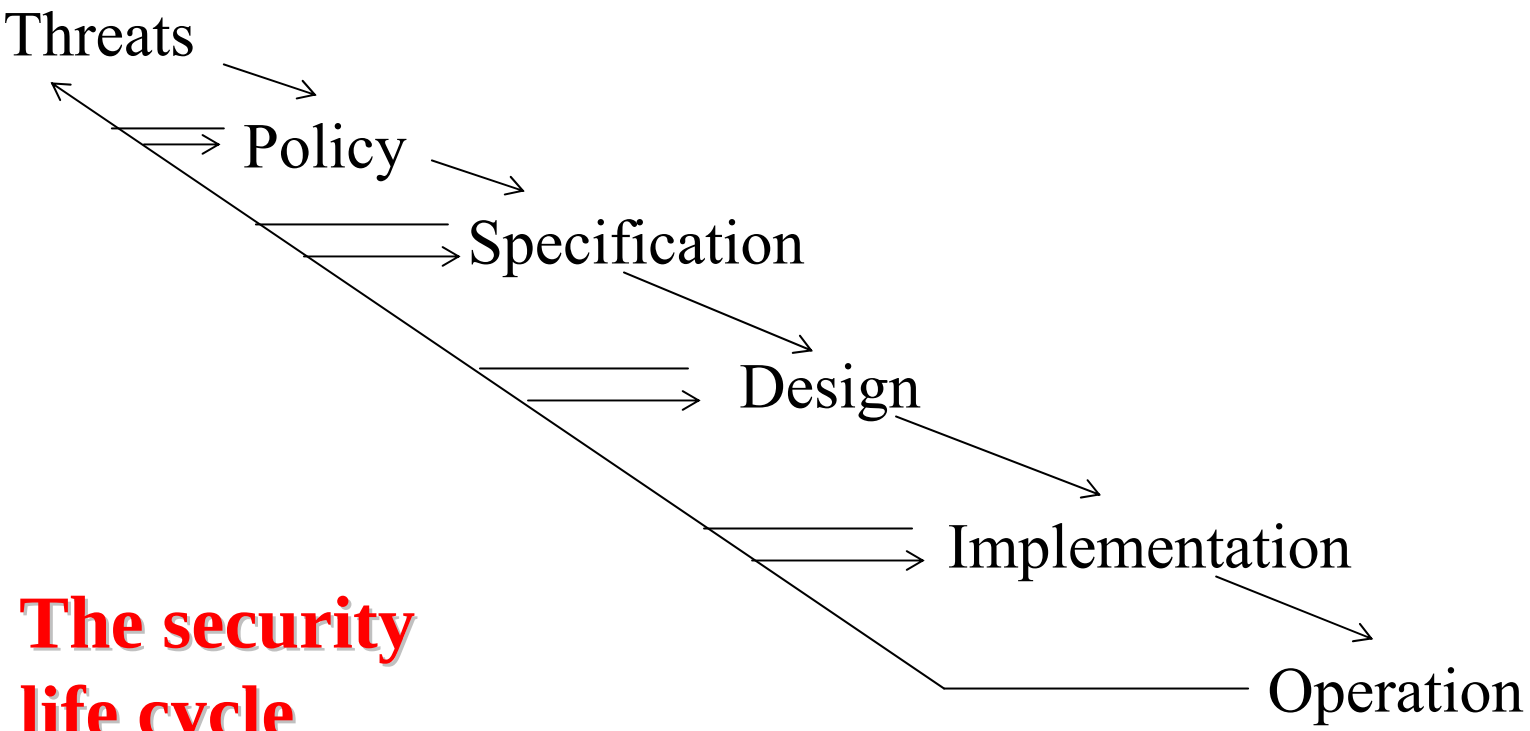
- Better not to have a mechanism than unused one
- give false security impression – users may rely on them without knowing!!

Human Issues

- Organizational Problems
  - Power and responsibility
    - Security conflicts with usability, free access, performance
  - NO Financial benefits
  - Human limitation (non-knowledgeable, overloaded)
  - Lack of resources (work time, technology & designs, training)
- People problems
  - Outsiders and insiders
  - Social engineering



Tying Together



The security life cycle

Key Points

- Policy defines security
- Mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions
- Importance of assurance
- The human factor