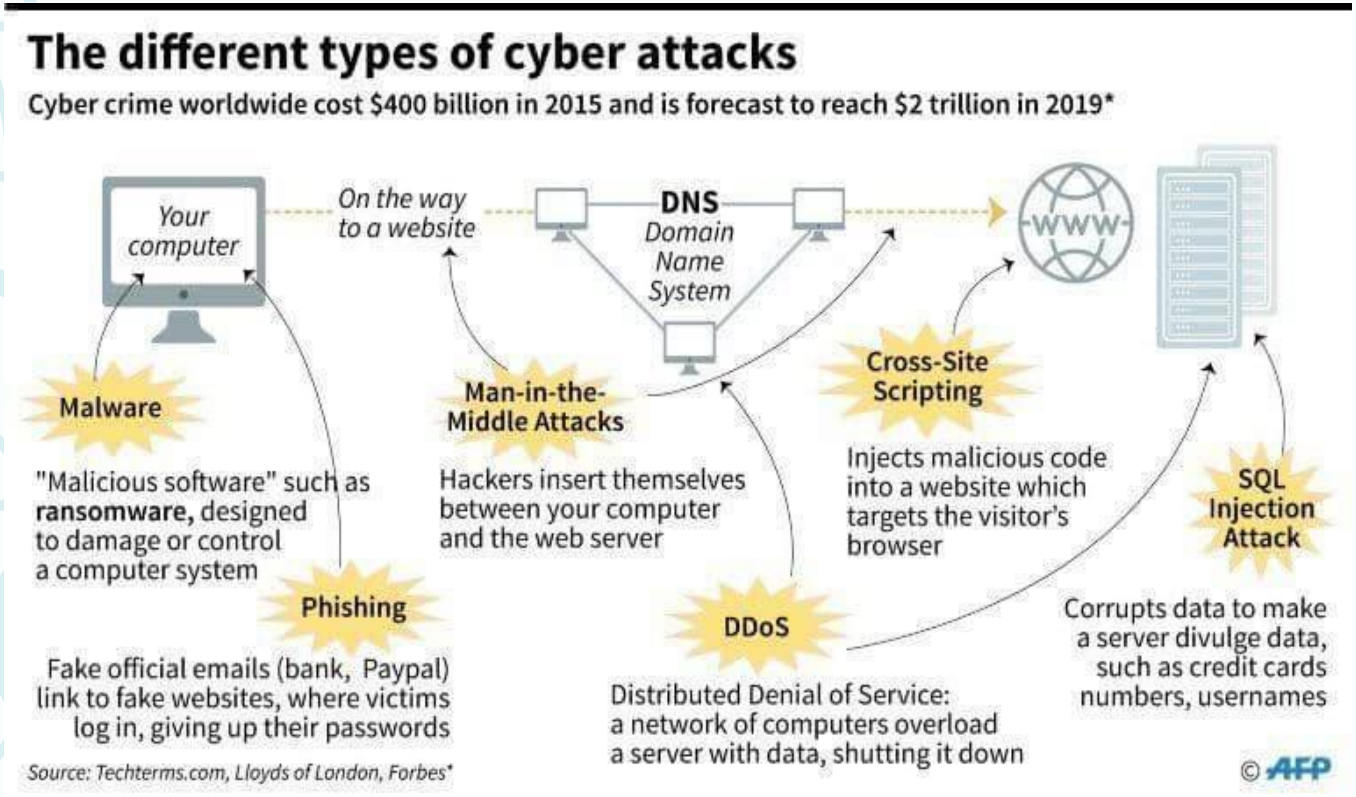
Information Security
CO362

Introduction

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

Present Scenario



The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*

Malware: "Malicious software" such as **ransomware,** designed to damage or control a computer system

Phishing: Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Man-in-the-Middle Attacks: Hackers insert themselves between your computer and the web server

DDoS: Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Cross-Site Scripting: Injects malicious code into a website which targets the visitor's browser

SQL Injection Attack: Corrupts data to make a server divulge data, such as credit cards numbers, usernames

Source: Techterms.com, Lloyds of London, Forbes*

© AFP

Components of Security

Three main components

- Confidentiality
- Integrity
- Availability

Confidentiality

- It hides/conceals information or resources.
- Need arises from the use of computer in sensitive fields such as financial institution, Defense, Health care, etc.
- It also hides the existence of information.
- Information should not be disclosed to unauthorized users.

For example, a student should not be allowed to examine other students’ grades.

Integrity

- It refers to the trustworthiness of information/data or resources.
- It includes data integrity and origin integrity (the source of data, often called authentication)
- Only authorized users should be allowed to modify data.

For example, students may be allowed to see their grades, yet not allowed to modify them.

Integrity Mechanisms Classes

Prevention Mechanism:

It blocks any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.

Detection Mechanism:

It only detects the violations of integrity.

Integrity Differs from Confidentiality

Confidentiality:

It conveys whether the data is compromised or not.

Integrity:

It conveys

- how and from data was received.
- how well the data was protected before it arrived at the current machine.
- how well the data is protected on the current machine.

Availability

- It refers to the ability to use data or resources desired.
- Authorized users should not be denied access.

For example, an instructor who wishes to change a grade should be allowed to do so.

Threat

- It is a potential violation of security.
- The violation need not actually occur for there to be threat.
- Those actions that could cause it to occur are guarded against.
- Three security services counter threats to the security of a system.

Classes of Threats

- Disclosure (unauthorized access to information)
  - Snooping
- Deception (acceptance of false data)
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption (interruption or prevention of correct operation)
  - Modification
- Usurpation (unauthorized control of some part of a system)
  - Modification, spoofing, delay, denial of service

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.

Goals of Security

- Prevention
  - Prevent attackers from violating security policy.
- Detection
  - Detect attackers’ violation of security policy.
  - Useful when attack cannot be prevented.
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds.

Assumptions and Trust

Question: How do we determine the policy correctly describes the required level and type of security for the site?

– Security rests on assumptions specific to the type of security required and the environment in which it is to be employed.

Example:

– Opening a door lock requires a key.

Assumptions and Trust

- – The assumption is that the lock is secure against lock picking.
- – This assumption is treated as an axiom and is made because most people would require a key to open a door lock.
- – A good lock picker, however, can open a lock without a key.

Assumptions and Trust

- If the lock picker is trustworthy, the assumption is valid.
- The term “trustworthy” implies that the lock picker will not pick a lock unless the owner of the lock authorizes the lock picking.
- “back door” through which the security mechanism (the locks) can be bypassed.
- The trust resides in the belief that this back door will not be used except as specified by the policy.

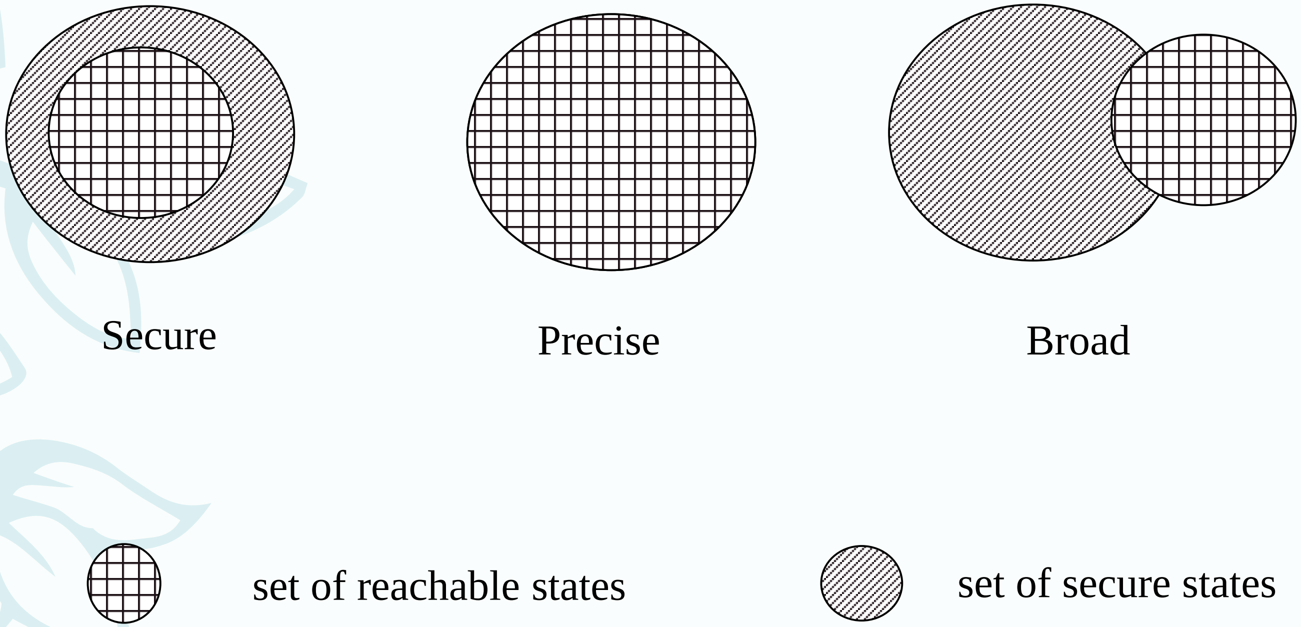
Assumptions and Trust

- A policy consists of a set of axioms that the policy makers believe can be enforced.
- Designers of policies always make two assumptions.
- First, the policy correctly and unambiguously partitions the set of system states into “secure” and “nonsecure” states.
- Second, the security mechanisms prevent the system from entering a “nonsecure” state.
- If either assumption is erroneous, the system will be nonsecure.

Assumptions and Trust

- The first assumption asserts that the policy is a correct description of what constitutes a “secure” system.
- The second assumption says that the security policy can be enforced by security mechanisms.
- These mechanisms are either *secure*, *precise*, or *broad.*

Types of Mechanisms



Secure

Precise

Broad

▦ set of reachable states

▨ set of secure states

Assurance

- Trust cannot be quantified precisely. System specification, design, and implementation can provide a basis for determining “how much” to trust a system.
- This aspect of trust is called *assurance*.

Assurance in the computer world is similar.

- It requires specific steps to ensure that the computer will function properly.
- The sequence of steps includes detailed

Assurance

- – Specifications of the desired (or undesirable) behaviour.
- – An analysis of the design of the hardware, software, and other components to show that the system will not violate the specifications.
- – Arguments or proofs that the implementation, operating procedures, and maintenance procedures will produce the desired behavior.
- – A system is said to *satisfy* a specification if the specification correctly states how the system will function.

Assurance

– Specification

A *specification* is a (formal or informal) statement of the desired functioning of the system.

- – Requirements analysis
- – Statement of desired functionality

Assurance

Design

- The *design* of a system translates the specifications into components that will implement them.
  - How system will meet specification

Implementation

- Given a design, the *implementation* creates a system that satisfies that design. If the design also satisfies the specifications, then by transitivity the implementation will also satisfy the specifications.
  - Programs/systems that carry out design

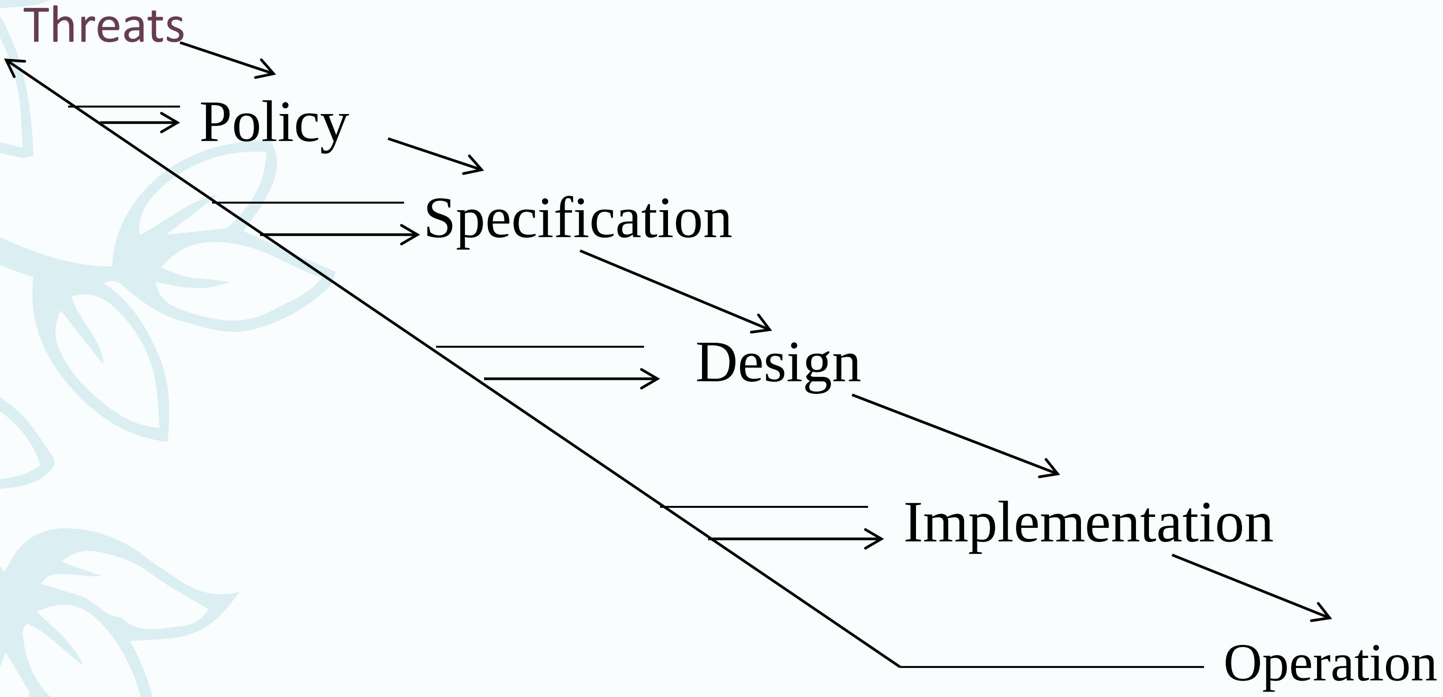
Operational Issues

- 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



Threats

Policy

Specification

Design

Implementation

Operation

Key Points

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