Security and Privacy

Prof. Jingsha He
Faculty of Information Technology
Beijing University of Technology

Overview

Objectives

Security Issues

Reading Material

- Matt Bishop
  - Chapter 1

Fact of the Lecture

- The art of war teaches us that
  - we could not rely on the chance that the enemy doesn’t exist, but rely on making sure that we are ready to confront any threat
  - we could not rely on the chance that the enemy won’t launch an attack, but should rely on making sure that our defense is strong enough to protect us

Overview

Objectives

Course Objectives

- To better understand the importance of security and privacy in the context of information technology
- To learn general knowledge of information security and privacy
- To establish an insight view on the effects of security and privacy on information systems

Course Objectives

- To appreciate the effort required to integrate security and privacy solutions and practices into information systems
- To realize security challenges facing today’s information systems

Security in General

- Safety
  - To stay away from risk or danger
- Means or ways of ensuring safety
  - a group of guards
  - measures adopted by the government to prevent espionage, sabotage or attack
  - measures adopted by businesses or homeowners to prevent crimes such as burglary or assault
  - measures adopted for preventing escape
- Confidence
  - To overcome doubt, fear or anxiety

Security in General

- Pledge
  - Something that is provided to ensure the fulfillment of an obligation
- Surety
  - Someone who fulfills the obligation of another
- Stock or bond certificate
  - A document that ensures ownership or creditorship

Computer/Information Security

- A generic name
  - The collection of mechanisms and tools for protecting data and for countering malicious attacks
- A blend of science, art, technology, engineering and human factors
  - Theory
  - Algorithm and method
  - Implementation
  - Deployment
  - Execution

Computer/Information Security

- The security of a system is as strong as the weakest point or link in the whole process
  - Individual points
  - Connections between points

Information System

- Computer system
  - A box with CPU, memory, disk, I/O, etc.
- Information system
  - A collection of computer systems
  - A network
  - Data/information
- Computer/information security
  - Terms that are used interchangeably

Information Assets

- Physical assets
  - Hardware
  - Software
- Intangible assets
  - Data (sensitive/private)
  - Intellectual properties
  - Rights for access to other assets that need to be protected

Security

- Security is about the protection of assets from loss or damage
  - Prevention
    - ◆To prevent assets from loss or damage
    - ◆Examples: locks, bars, walls, laws, etc.
  - Avoidance
    - ◆To avoid assets from loss or damage
    - ◆Examples: guards, weapons, etc.

Security

- Security is about the protection of assets from loss or damage
  - Detection
    - To determine when/how/what assets have got lost or damaged
    - Examples: alarms, cameras, detectives, audit trail, etc.
  - Recovery
    - To recover assets from loss or damage
    - Examples: courts, insurance, replacement, etc.

Common Security Threats

- Errors and faults
- Fraud and theft
- Employee sabotage
- Loss of physical or infrastructural support
- Malicious attacks
- Malicious code
- Industrial espionage
- Foreign government espionage
- Threats to personal privacy

Security Goals

- V: value of information assets
  - Subjective or objective
- C: cost of providing security measures
  - Total cost of all the measures
- P: price to pay for getting the assets through illegitimate means
  - Total effort required to gain access to the assets
  - Potential risk or punishment for trying to get the assets
- Goals
  - $C \leq V$
  - $P \geq V$

Overview

Security Issues

Goal of Information Security

- Protection of information assets
  - Prevent, avoid, detect and recover from the loss or damage to information assets
- No real solid universal definition
- Relative
  - Based on security requirements or policies
  - A value proposition
    - Value vs. cost
    - Value vs. price

Properties of Security

- Security is about dealing with a chain of vulnerable points, not just a single point
- Security is about a process, not just individual mechanisms
- Security measures must be enforced along the chain or throughout the whole process, not just at selected points

Dilemma

- Stronger security requires more resources
  - More costly development
  - Slower execution time
  - Less friendly user interface
  - More complicated procedures for administration and management
  - Lower productivity
- Easy is better
  - The KISS (keep it simple, stupid) rule
- Stronger security implies higher cost
  - Justification of security requires risk analysis

Sources of Vulnerability

- Physical
- Natural
- Hardware
- Software
- Communication media
- Protocol
- Human

Security Threats

- Environmental
  - Break-in, physical damage, natural disaster, etc.
- Unintentional
  - Human error, poor training, insufficient documentation, etc.
- Intentional
  - Internal
    - Staff
  - External
    - Intelligence agencies, hackers, terrorists, crackers, criminals, industrial intelligence, etc.

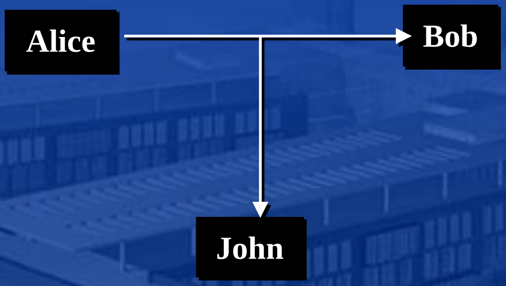
Common Forms of Security Threats

- Snooping
  - Unauthorized reading or interception of information
- Modification
  - Unauthorized change of information
- Masquerading or spoofing
  - Impersonation of one entity by another

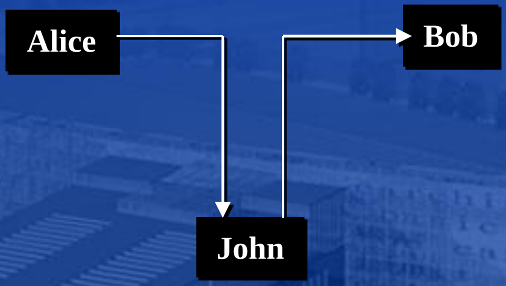
Common Forms of Security Threats

- Repudiation
  - False denial of sending or creating information
- Denial of receipt
  - False denial of receiving information
- Delay
  - Temporary inhibition of access to services or information
- Denial of service
  - Long-term or permanent inhibition of access to services or information

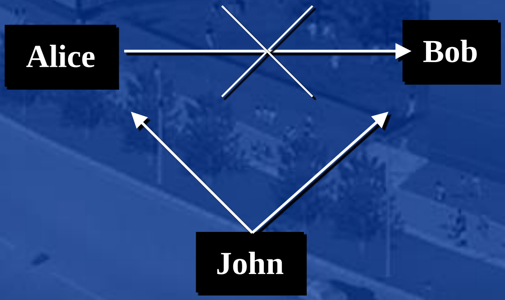
Illustration of Some Common Threats



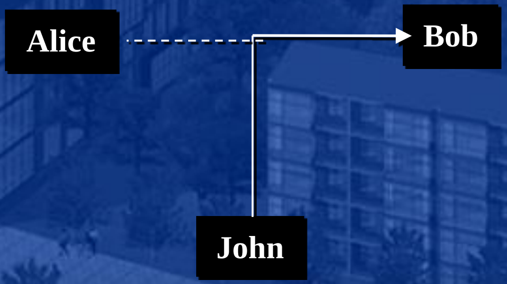
Snooping



Modification



Denial of service



Spoofing

Data vs. Information

- Data
  - Representation of information
  - Precursor to information
  - May have little or no meaning on its own
- Information
  - Interpretation of data
  - Converted form of data
  - Used for decision-making

Main Security Issues

- Confidentiality
  - Unauthorized disclosure of information
  - Secrets, classified documents, etc.
- Integrity
  - Unauthorized modification of information
  - Financial records, evidential data, etc.
- Availability
  - Unauthorized denial of access to information from authorized users
  - Shared resources, etc.

Confidentiality

- Historically closely related to secrecy and privacy
- Concerned with unauthorized reading of information
  - In general, unauthorized learning of information
- Organizational information
  - Secrecy
- Personal information
  - Privacy

Integrity

- Concerned with unauthorized modification of information
  - Usually closely associated with confidentiality
- Independent from confidentiality
  - Enforced without respecting confidentiality
  - Require different access privileges or rights from those for confidentiality

Availability

- Concerned with unauthorized inhibition of access to information
- Denial of service (DoS)
  - Threat to the property that services are accessible upon request by an authorized entity
  - Threat to the property that services are accessible when needed without undue delay
- Consequence of DoS
  - Unavailability of information or services to authorized users

Accountability

- Part of the control of access to information
  - An authorized action may be a violation
    - Security flaws may allow undesirable access, resulting in unpredictable consequences
  - Users must be held accountable for their actions
- Require identification, authentication, authorization, audit trail, etc.
- Audit information must be selectively kept and properly protected so that actions that violate security can be traced to the responsible party

Examples

- Damage to information
  - Integrity
- Disruption of service
  - Availability
- Theft of money
  - Integrity
- Theft of information
  - Confidentiality
- Loss of privacy
  - Confidentiality

Policy vs. Mechanism

- Security policy
  - A statement about what is/is not allowed to happen with respect to security requirements
  - Usually associated with abstract, model, requirement, etc.
  - Example
    - No access is allowed without authentication

Policy vs. Mechanism

- Security mechanism
  - A method, tool, process, procedure, etc. that enforces a security policy
  - Usually associated with algorithm, design, implementation, deployment, execution, etc.
  - Example
    - Identification and authentication method

Correctness of Security

- Security policy must be correct in terms of describing security concerns or requirements
  - It unambiguously distinguishes between secure states and insecure states
- Security mechanism can be correct in terms of enforcing the security policy
  - Could be more restrictive

Summary

- Aspects of computer/information security
- Security goals
- Main security issues
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- Policy vs. mechanism
- Correctness of security

Thoughts of the Lecture

- Do you trust the information in this course?
- What would make you trust it?
- How could you verify whether the information can be trusted?
- Do you trust the identity and the authenticity of the source?
- How do you verify that I am whom I say I am?
- How much proof do you need?

Q & A