Security Principles

COMP620

Information Privacy and Security

Goals for Today

- Review some of the major principles of computer security

Sources for today's lecture include:

- Textbook , *"Computer Security"* by Matt Bishop
- *"Information Security, Principles and Practices"* by Merkow and Breithaupt

Nothing is Absolutely Secure

- There is no such thing as absolutely secure
- Attackers may be willing to spend considerable resources
- Previously unknown (and unprotected) vulnerabilities will be discovered
- You **can** secure a system to make it very difficult to attack

Major Security Goals

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

- Sometimes referred to as **CIA**

Confidentiality

- Prevent unauthorized release of information
- Authentication and authorization are necessary to maintain confidentiality
- Encryption can often be used to provide confidentiality

Hiding

- A useful way to keep data and resources confidential is to hide them
- Firewalls and Network Address Translation (NAT) can be used to hide the existence of systems in a network
- Hiding must be done in a sound way. Do not just *"hope they won't find it"*

Integrity

- Prevent unauthorized users from making modifications to data or programs
- Prevent authorized users from making improper modifications
- The *"principle of least privilege"* states that users should only be given enough privileges to perform their duties and no more
- Maintain consistency of data and programs
- Digital signatures can detect violations of integrity, but not prevent them
- Trustworthiness of data and origin affects integrity

Availability

- Prevent Denial of Service (DoS) attacks
- Prevent loss of information or capabilities due to natural disasters or human actions
- Minimize the impact of equipment failures during normal use

Threats to System Security

Threats to network security typically come in any of four forms:

1. **Interception** – sniffing, wiretapping, eavesdropping
2. **Modification** – unauthorized access/tampering
3. **Fabrication** – impersonation or fabrication of data or objects to gain access to services/information.
4. **Interruption** – Denial of Service

Methods of Attack

- Eavesdropping
  - Viewing data or passwords on the network.
  - Easy to do on broadcast networks.
- Message Tampering
  - Changing messages as they travel the network.
- Masquerading
  - Sending messages and programs with invalid sender identification.
- Invalid Input
  - Entering data that exploits a flaw in the program

Methods of Attack (cont.)

- Replay
  - Interception and duplication of transmissions at a later time.
- Denial of Service
  - Crashing the system or flooding it with messages or tasks.
- False Identification
  - Password Guessing
- Malicious Software
  - Viruses, Worms, Trojan Horses, etc.

Defense in Depth

- You need multiple, overlapping defenses
- Defenses should include:
  - Prevention – develop systems that avoid common vulnerabilities
  - Detection– recognize when suspicious activity is occurring
  - Response – be capable of taking measures to stop or limit damage.
- If an attacker defeats one security defense, other defenses should block them

People, Process and Technology

- Be sure that the people are trained
- It may be useful to require two people to do something
- Processes should be documented to ensure that proper procedures are carried out

Users Often Make Bad Decisions

- Many naive users will OK anything
- Many users have insecure passwords
- Most users do not know how to protect their computer

Computer users are often the greatest threat to their own system security.

Phishing

- Phishing is the practice of enticing users to access a website that is not what they expect
- Common scenario
  - User clicks on a link in an “official looking” email
  - The phishing website asks for personal information
  - The information is used to attack or impersonate the user

Safe Computing Rules

- Form a group of 3-4 students
- Write some rules for safe computing
- The rules should apply to the average computer user
- Be prepared to tell the class your rules
- Each team should have a unique rule

Functional and Assurance Requirements

- Functional requirements describe what a system should do
- Assurance requirements describe what a systems should not do

Security Through Obscurity

- Some people think they can secure their system by guarding the software source
- This provides a false sense of security
- It is easy to change a password, difficult to change the “secret” software
- Cryptography should work because the algorithm is strong and carefully analyzed

Risk Management

- **Risk** is defined as the effect of uncertainty on objectives (whether positive or negative)
- **Risk management** can be considered the identification, assessment, and prioritization of risks followed by efforts to minimize, monitor, and control the probability and/or impact of unfortunate events

Risk Strategies

- Strategies to manage risk include
  - avoiding the risk
  - reducing the negative effect of the risk
  - transferring the risk to another party
  - accepting some or all of the consequences of a particular risk

Risk Management Methodology

- Identify, characterize, and assess threats
- Assess the vulnerability of critical assets to specific threats
- Determine the risk (i.e. the expected consequences of specific types of attacks on specific assets)
- Identify ways to reduce those risks
- Prioritize risk reduction measures based on a strategy

Consequence / Likelihood Matrix

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Moderate	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

- Extreme risk: Immediate action required
- High risk: Senior management attention needed
- Moderate risk: Management responsibility must be specified
- Low risk: Manage by routine procedures

Cost Effectiveness

- The level of security must correspond to the value of the assets
- It is pointless to spend more on security than the value of the assets

Complexity

- The more complex a system is, the harder it is to secure
- While a certain level of complexity is required, you should attempt to keep things simple
- It is difficult to secure a system that nobody understands

Honest Assessment for Management

- Fear, uncertainty and doubt would once prod management to invest in security
- The field has matured so you now need to provide an honest assessment of the risks and costs

Open Disclosure of Vulnerabilities

- When security vulnerabilities are announced
  - System managers can take steps to reduce the threat
  - Hackers can use the information to generate exploits

What Do You Think?

- Should security vulnerabilities be announced when they are discovered?

Review of Security Principles

- No absolute security
- Goals are confidentiality, integrity and availability
- Use defense in depth
- Users often make bad security decisions
- Security need functional and assurance requirements
- Security through obscurity is not the answer

Review of Security Principles

- Security = risk management
- Controls are preventative, detective and responsive
- Complexity is the enemy of security
- Give honest assessment of security risks
- People, process and technology are all needed
- Open disclosure of vulnerabilities