Introducing Computer and Network Security

Chapter 1

Lecturer: Pei-yih Ting

Overview

- What is security?
- Risk Analysis

Computer Security Basics

- What is *computer security* ?
  - Answer depends upon who you're asking
    - End user
    - Network administrator
    - Manager
    - Security professional
  - "A computer is secure if you can depend on it and its software to behave as you expect."
  - "Security is all about trust, trust in protection, authenticity, and usability."

[Garfinkel&Spafford]

Computer Security Basics (cont'd)

- CIA Triad
  - Goals for implementing security practices
  - Confidentiality, Integrity, and Availability
- DAD Triad
  - Goals for defeating the security of an organization
  - Disclosure, Alteration, and Denial

CIA Triad

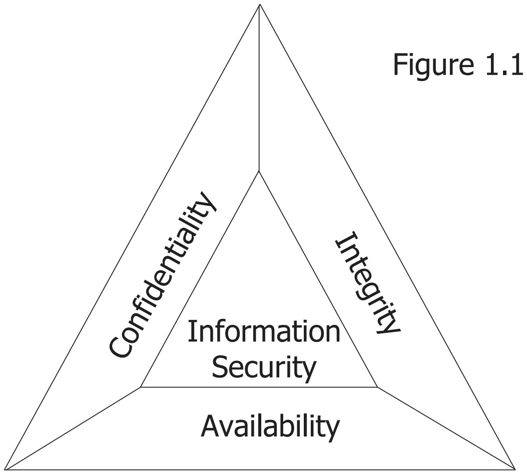

Figure 1.1 CIA triad

CIA Triad (cont'd)

- Confidentiality
  - Confidential information (in storage or during communication) should not be accessible to unauthorized users
- Integrity
  - Data may only be modified through an authorized mechanism
- Availability
  - Authorized users should be able to access data for legitimate purposes as necessary

There is still one other important goal of information security: non-repudiation.

DAD Triad

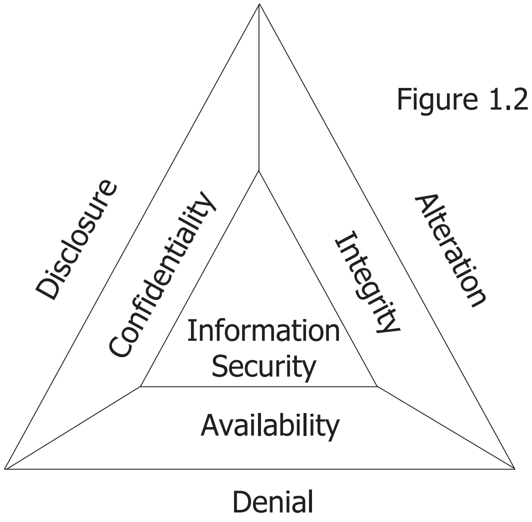

Figure 1.2 DAD triad

DAD Triad (cont'd)

- Disclosure
  - Unauthorized individuals gain access to confidential information
- Alteration
  - Data is modified through some unauthorized mechanism
- Denial
  - Authorized users cannot gain access to a system for legitimate purposes
- DAD activities may be malicious or accidental

Network Security

- In early days, computer security focused on protecting individual systems
- Advent of Local Area Networks (LANS) and Internet in the 80’s make the job much more difficult
- Security considerations include:
  - Protecting TCP/IP protocol suite and services based upon it.
  - Firewalls
  - Intrusion detection systems

goal: *protect networked computers*

Threats to Security

- Hacker
  - Anyone who attempts to penetrate the security of an information system, regardless of intent (cracker)
  - Early definition included anyone very proficient in computer use
- Malicious code object
  - Virus, worm, Trojan horse
  - A computer program that carries some type of payload, the specific portion of the program that carries out malicious actions when run on a system

Threats to Security (cont’d)

- Malicious insider
  - Someone from within the organization that attempts to go beyond the rights and permissions that they legitimately hold
  - Former employees
  - Security professionals and system administrators are particularly dangerous

Risk Analysis

- Security professionals formalize the risk analysis process to determine and mitigate the impact of the risks to security in their organization.
- Actions involved in risk analysis:
  - Determine which assets are most valuable
  - Identify potential risks to assets
  - Determine the likelihood of each risk occurring
  - Take action to manage the risk

Identify and Value Assets

- First step
- Identify the information assets in the organization
  - Hardware, software, data, and business continuation process
- Assign value to those assets using a valuation method
- Assigning value to assets is the foundation for decisions about cost/benefit tradeoffs

Identify and Value Assets (cont’d)

- Common valuation methods
  - Replacement cost valuation
    - Uses the replacement cost as the value of an asset
  - Original cost valuation
    - Uses the original purchase price as the value of an asset
  - Depreciated valuation
    - Uses the original cost less an allowance for value deterioration
  - Qualitative valuation
    - Assigns priorities to assets without using dollar values
    - Especially for intangible properties of assets

Identify and Assess Risks (1/5)

- Second step

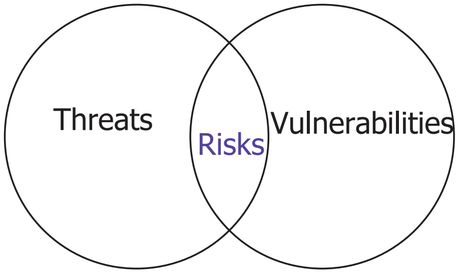

Figure 1.3 Identifying risks

Identify and Assess Risks (2/5)

- Vulnerability
  - An internal weakness in a system that may potentially be exploited
  - Ex. Not having antivirus software
- Threat
  - A set of external circumstances that may allow a vulnerability to be exploited
  - Ex. The existence of a particular virus
- Risk
  - Occurs when a threat and a corresponding vulnerability both exist

Identify and Assess Risks (3/5)

- Two major classifications of risk assessment techniques
  - Qualitative
  - Quantitative
- Qualitative Risk Assessment
  - Focuses on analyzing intangible properties of an asset rather than monetary value
  - Prioritizes risks to aid in the assignment of security resources
  - Relatively easy to conduct
  - Ex. Customer's good will / good impression

Identify and Assess Risks (4/5)

- Quantitative Risk Assessment
  - Assigns dollar values to each risk based on measures such as *asset value*, *exposure factor*, *annualized rate of occurrence*, *single loss expectancy*, and *annualized loss expectancy*
  - Uses potential loss amount to decide if it is worth implementing a security measure
- Asset value (AV): The value of the asset as determined by the 1st step of risk analysis.
  - Ex. A computer might have an AV of $1,000.
- Exposure factor (EF): The expected portion of an asset that would be destroyed by a given risk.
  - Ex. If the value of the power supply is 10% of the value of the computer, the EF of the computer to a power surge is 10%.

Identify and Assess Risks (5/5)

- Annualized rate of occurrence (ARO): The number of times you expect a risk to occur each year.
  - Ex. 2 times a year
- Single loss expectancy (SLE): The amount of damage the asset would incur each time the risk occurs.
  - Ex. $1,000 × 10% = $100
- Annualized loss expectancy (ALE): The amount of damage the asset would incur each year from a given risk.
  - Ex. 2 × $100 = $200
- Benefit = (ALE × life of measure) - cost of measure

Managing Risks

- Risk Avoidance
  - Used when a risk overwhelms the benefits gained from having a particular mechanism available
  - Avoid any possibility of risk by disabling the mechanism that is vulnerable
  - Ex. Disabling e-mail
- Risk Mitigation
  - Used when a threat poses a great risk to a system
  - Takes preventative measures to reduce the risk
  - Ex. Implementing a firewall

Managing Risk (cont'd)

- Risk Acceptance
  - Useful when risk is small or potential damage is trivial
  - Do nothing to prevent or avoid the risk
  - Ex. Risk is a meteor hitting a data center
- Risk Transference
  - Ensure that someone else is liable if damage occurs
  - Ex. Buy insurance
- Combinations of the above techniques are often used

Considering Security Tradeoffs

- Security can be looked at as a tradeoff between risks and benefits
  - Cost of implementing and maintaining the security mechanism
  - The amount of damage it may prevent
- Tradeoff considerations are security, user convenience, business goals, and expenses

Security Tradeoffs (cont'd)

- An important tradeoff involves user convenience
  - Between difficulty of use and willingness of users
  - If users won't use a system because of cumbersome security mechanisms, there is no benefit to having security
  - If users go out of their way to circumvent security, the system may be even more vulnerable
- Human is always the weakest link in chains of security protection mechanisms
  - Human's mistakes
  - Human's willingness to trust, to simplify things

Security Policy and Education

- Cornerstone of a security effort is to
  - Implement proper policies
  - Educate users about those policies
- Information security policies should be
  - Flexible enough not to require frequent rewrites
  - Comprehensive enough to ensure coverage of situations
  - Available to all members of the organization
  - Readable and understandable

Policy And Education (cont’d)

- Example policy:
  - Never tell anybody (even your supervisor) your account password
  - Use at least 8 characters including to special characters in your password
  - Never use the same password in any two computers
  - Change your passwords every 3 months
  - …

Summary

- CIA Triad summarizes the goals of security professionals (confidentiality, integrity, and availability)
- DAD Triad summarizes the goals of those who seek to evade security measures (disclosure, alteration, and denial)
- The explosion of networking has shifted focus from protecting individual computers to protecting interconnected computers

Summary (cont’d)

- Threats to security include hackers, malicious code objects, malicious insiders
- Risk analysis is used to determine the cost/benefit tradeoffs of implementing specific security measures
  - Valuation of assets
  - Identifying and assessing risks
  - Determining the likelihood & potential costs of risks
  - Determining how to manage risks given this information
- Setting effective policies and educating users about policies is key

Discussions

- Why is computer security more and more important?
- Why is it harder to protect than it has been in the past?
- Many people hack other’s computer for fun claming that they did not do anything harmful, do you think this is positive or negative?
- Has your computer been infected by any virus or worm? What is its behavior? What is it? How do you overcome the incident?

Assignments

- Reading: Chapter 1
- Practice 1.9 Challenge Questions

- Turn in Challenge Exercise 1.1 next week