Introducing Computer and Network Security

Chapter 1

Computer Security Basics

- What is computer security?
  - Answer depends upon the perspective of the person you're asking
  - Network administrator has a different perspective than an end user or a security professional
  - "A computer is secure if you can depend on it and its software to behave as you expect" [Garfinkel,Spafford]

Computer Security Basics (continued)

- 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

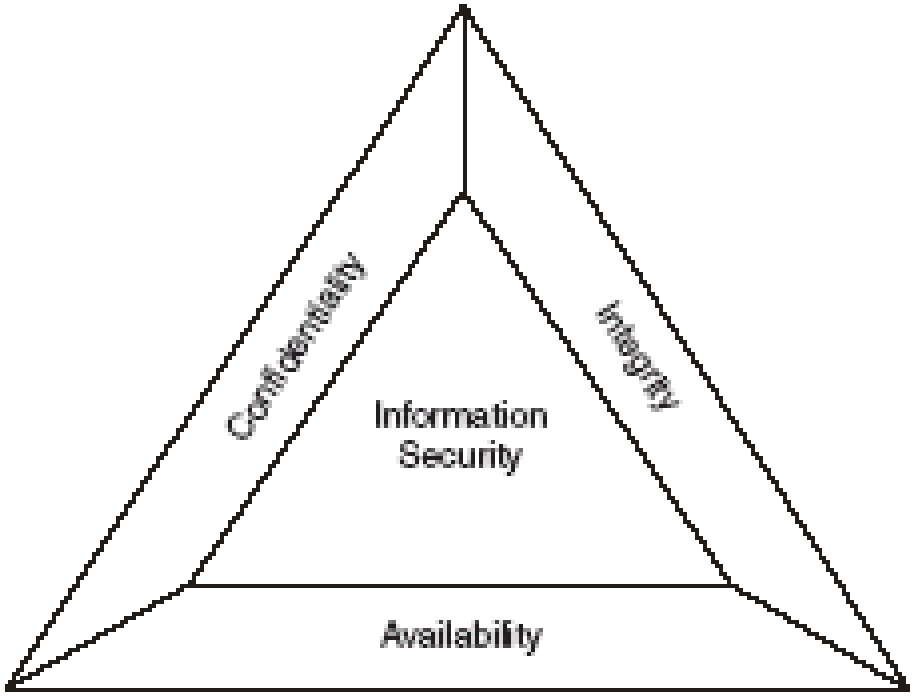

Figure 1.1
CIA triad

CIA Triad (continued)

- Confidentiality
  - Confidential information should not be accessible to unauthorized users
  - Prevent unauthorized reading of information
- Integrity
  - Data may only be modified through an authorized mechanism
  - Prevent unauthorized writing of information
- Availability
  - Authorized users should be able to access data for legitimate purposes as necessary

DAD Triad

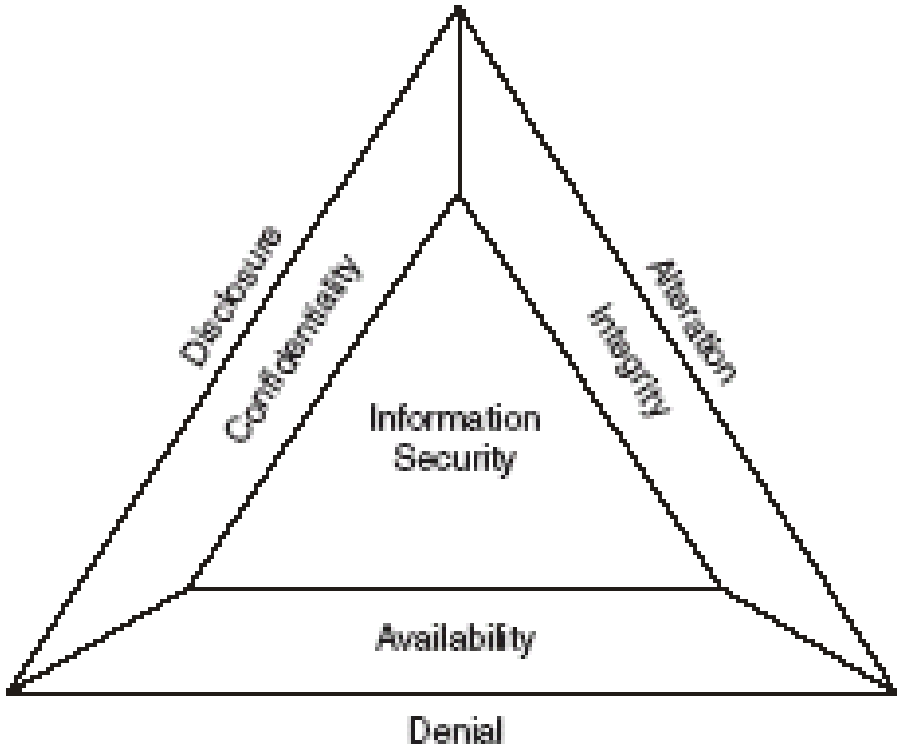

Figure 1.2
DAD triad

DAD Triad (continued)

- 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

Introducing Networks

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

Threats to Security

- Hacker
  - Anyone who attempts to penetrate the security of an information system, regardless of intent
  - Early definition included anyone very proficient in computer use

- Malicious code object
  - Virus, worm, Trojan horse
  - A computer program that carries out malicious actions when run on a system

Threats to Security (continued)

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

Risk Analysis

- Actions involved in risk analysis:
  - Determine which assets are most valuable
  - Identify risks to assets
  - Determine the likelihood of each risk occurring
  - Take action to manage the risk
- Security professionals formalize the risk analysis process

Identifying and Valuing Assets

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

Identifying and Valuing Assets (continued)

- 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

Identifying and Assessing Risks

- Second step in risk analysis process
- Two major classifications of risk assessment techniques
  - Qualitative
  - Quantitative
- Vulnerability
  - An internal weakness in a system that may potentially be exploited
  - Not having antivirus software is an example

Identifying and Assessing Risks (continued)

- Threat
  - A set of external circumstances that may allow a vulnerability to be exploited
  - The existence of a particular virus for example
- Risk
  - occurs when a threat and a corresponding vulnerability both exist

Identifying and Assessing Risks (continued)

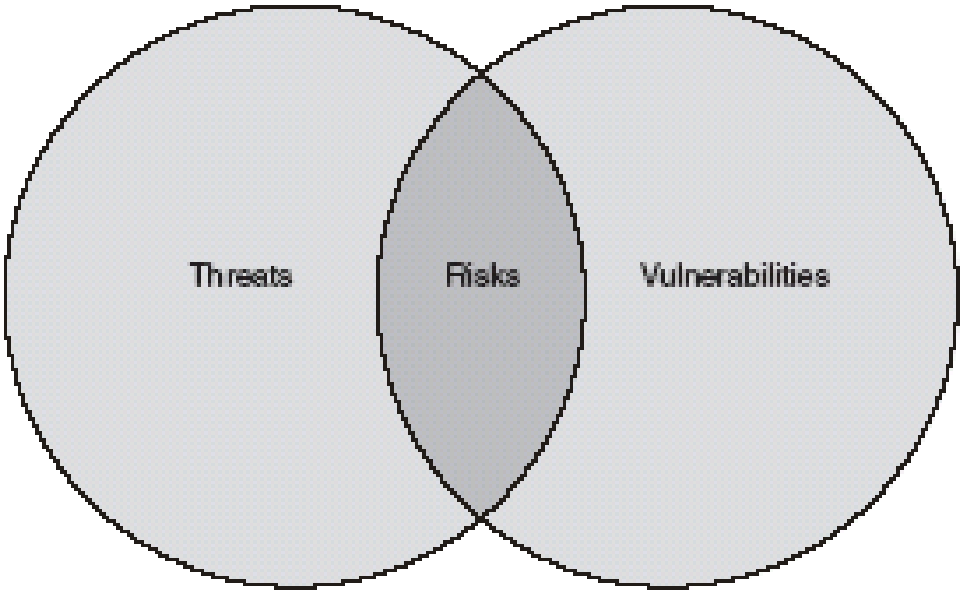

Figure 1.3
Identifying risks

Identifying and Assessing Risk (continued)

- 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

Identifying and Assessing Risk (continued)

- 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

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
  - Disabling e-mail is an example of risk avoidance
- Risk Mitigation
  - Used when a threat poses a great risk to a system
  - Takes preventative measures to reduce the risk
  - A firewall is an example of risk mitigation

Managing Risk (continued)

- Risk Acceptance
  - Do nothing to prevent or avoid the risk
  - Useful when risk or potential damage is small
- Risk Transference
  - Ensure that someone else is liable if damage occurs
  - Buy insurance for example
- 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 the security mechanism and the amount of damage it may prevent
- Tradeoff considerations are security, user convenience, business goals, and expenses

Considering Security Tradeoffs (continued)

- 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

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

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 (continued)

- 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 and potential costs of risks
  - Determining how to manage risks given this information
- Setting effective policies and educating users about policies is key