General Security Principles and Practices

Chapter 4

Common Security Principles

- Information security is not new, many principles come from military and commercial fields
- Separation of Privileges Principle
  - No single person should have enough authority to cause a critical event to happen
  - Many examples from outside of computing, e.g., two keys needed to launch a missile
  - Tradeoff between security gained and manpower required to achieve it

Common Security Principles (continued)

- Least Privilege Principle
  - An individual should have only the minimum level of access controls necessary to carry out job functions
  - A common violation of this principle occurs because of administrator inattention
    - Users are placed in groups that are too broad
  - Another common violation occurs because of privilege creep
    - Users are granted new privileges when they change roles without reviewing existing privileges

Common Security Principles (continued)

- Defense in Depth Principle
  - Defenses should be layered
  - Layers begin with points of access to a network and continue with cascading security at bottleneck points
- Security through Obscurity
  - In early days of computing, administrators depended upon secrecy about the security that was in place
  - No longer very effective in most cases because so much information is freely available

Defense in Depth

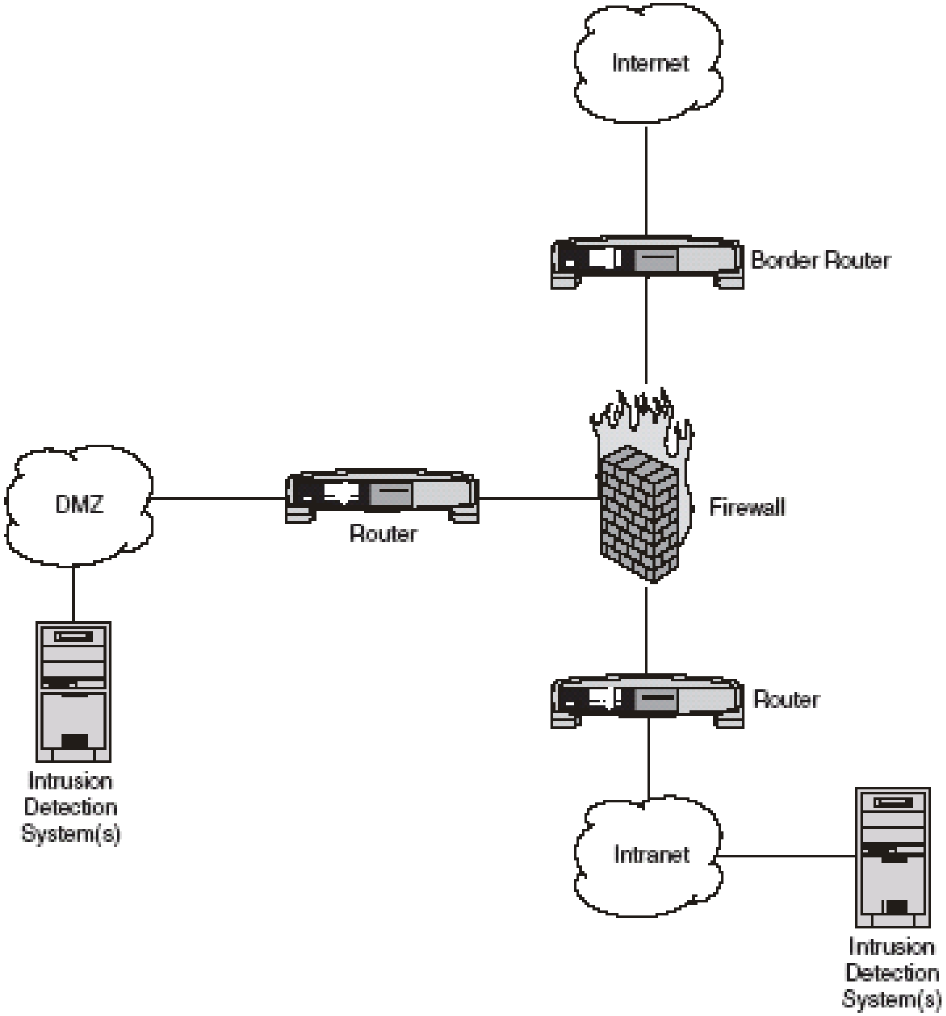


Figure 3.1
Example of defense in depth

Security Policies

- Goal is to have clearly defined security objectives to
  - Design specific controls
  - Keep users informed of expected behavior
- A security policy should be a written document
  - Available to all users of an organizational information system
- Security policies range from single documents to multiple documents for specialized use or for specific groups of users

Acceptable Use Policy (AUP)

- Defines allowable uses of an organization's information resources
- Must be specific enough to guide user activity but flexible enough to cover unanticipated situations
- Should answer key questions
  - What activities are acceptable?
  - What activities are not acceptable?
  - Where can users get more information as needed?
  - What to do if violations are suspected or have occurred?

Backup Policy

- Data backups protect against corruption and loss of data
  - To support the integrity and availability goals of security
- Backup policy should answer key questions
  - What data should be backed up and how?
  - Where should backups be stored?
  - Who should have access?
  - How long should backups be retained?
  - How often can backup media be reused?

Confidentiality Policy

- Outlines procedures used to safeguard sensitive information
- Should cover all means of information dissemination including telephone, print, verbal, and computer
- Questions include
  - What data is confidential and how should it be handled?
  - How is confidential information released?
  - What happens if information is released in violation of the policy?
- Employees may be asked to sign nondisclosure agreements

Data Retention Policy

- Defines categories of data
  - Different categories may have different protections under the policy
- For each category, defines minimum retention time
  - Time may be mandated by law, regulation, or business needs, e.g., financial information related to taxes must be retained for 7 years
- For each category, defines maximum retention time
  - This time may also be mandated by law, regulation, or business needs
  - Common in personal privacy areas

Wireless Device Policy

- Includes mobile phones, PDAs, palm computers
- Users often bring personal devices to the workplace
- Policy should define
  - Types of equipment that can be purchased by the organization
  - Type of personal equipment that may be brought into the facility
  - Permissible activities
  - Approval authorities for exceptions

Implementing Policy

- A major challenge for information security professionals
- Includes processes of developing and maintaining the policies themselves as well as ensuring their acceptance and use within the organization
- Activities related to policy implementation are often ongoing within an organization

Developing Policies

- In any but the smallest organization, a team approach should be employed
  - Include members from different departments or functional elements within the organization
- Commonly, a high-level list of business objectives is first developed
- The second step is to determine the documents that must be written to achieve objectives
- These steps are followed by documents drafts until consensus is achieved

Building Consensus

- Once consensus is reached among the development committee, consensus must be spread throughout the organization (“selling” the policies)
- Important because employees who are not on board may bypass the security policies, leaving the information system vulnerable
- Often the policies are promoted and advertised by senior management

Education

- Includes education and training programs for affected employees
- Users should be aware of their responsibilities with regard to policies
- Two types of training
  - Initial training is a one-time program early in an employee’s tenure with company
  - Refresher training should be done periodically to
    - Remind employees of their responsibilities
    - Provide employees with updates of policies and technologies that affect their responsibilities

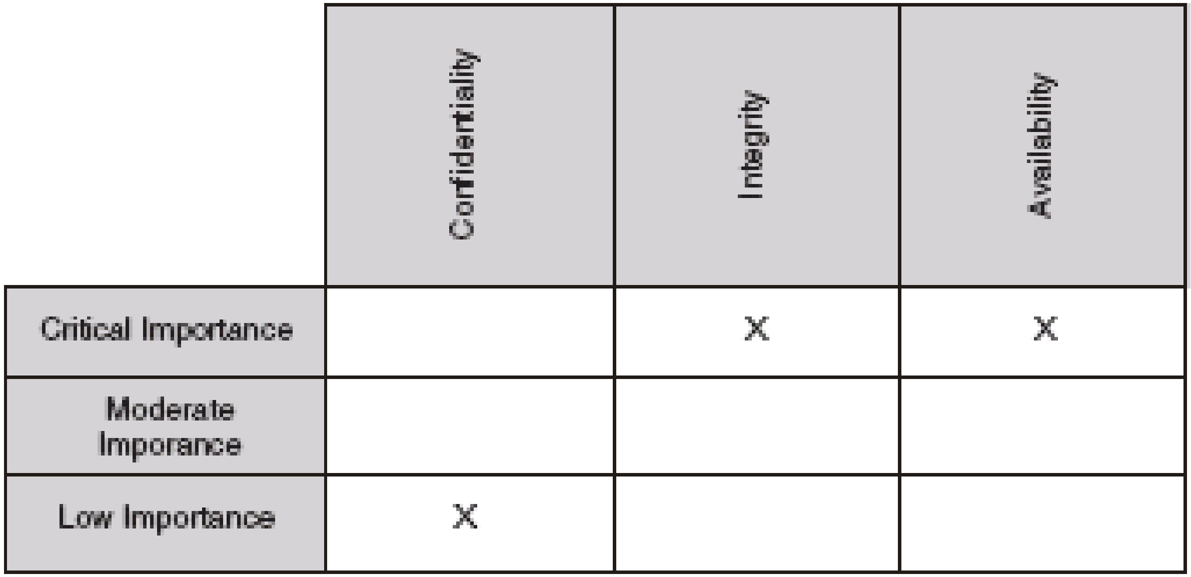
Enforcement and Maintenance

- Policies should define responsibilities for
  - Reporting violations
  - Procedures when violations occur
- Policies should be strictly enforced
- Policy changes occur as companies and technologies change
- Policies should contain provisions for modification through maintenance procedures
  - Common to have periodic reviews mandated

Security Administration Tools

- Tools that help with consistent application and enforcement of security policy
- Security checklists
  - Security professionals should review all checklists used in an organization for compliance with security procedures
  - Security professionals may develop their own checklists for security-specific tasks
- Security matrices
  - Used in development of security policies and implementation of particular procedures
  - Helps focus amount of attention paid to particular goals

Security Matrices



	Confidentiality	Integrity	Availability
Critical Importance		X	X
Moderate Imporance			
Low Importance	X		

Figure 3.2

Sample security matrix

Physical Security

- Ensures that people cannot gain physical access to a facility where they can manipulate information resources
- Ensures that data resources are protected from natural disasters such as fires and floods
- Many large organizations have separate professionals for physical security
- Three common categories of physical security issues
  - Perimeter protection
  - Electronic emanations
  - Fire protection

Perimeter Protection/Access Controls

- On the perimeter of a facility you can use
  - Fences
  - Lighting
  - Motion detectors
  - Dogs
  - Patrols
- Remember the defense in depth principle
  - For example, use fences around the facility and biometrics for specific offices within a facility

Electronic Emanations and Fire Protection

- Electronic devices emit electromagnetic radiation
  - Emanations can be picked up and interpreted outside facility
  - Equipment is available to block interception but it is costly and bulky, sometimes used by government facilities
- Fire protection requires detection and suppression systems
  - Often dictated by building codes
  - Suppression systems include sprinklers, chemicals, and fire extinguishers

Personnel Security

- People are the weakest link in a security system
- Perform background investigations
  - Can include criminal record checks, reference evaluations
- Monitor employee activity
  - Can include monitoring Internet activity, surveillance cameras, telephone recording
- Mandatory vacations
- Exit procedures for employees leaving the company
  - Remind employees of any nondisclosure agreements

Summary

- Many common security principles date from pre-computer times
- The Separation of Privileges Principle ensures that no one person has control of major decisions
- The Least Privilege Principle states that an individual should have only the access really required by the tasks he or she is assigned
- The Defense in Depth principle recognizes the value of having layered defense systems

Summary

- The Security through Obscurity Principle has a weakness that can be fatal in today's information age
- Security Policies are written documents protecting an organization's information resources
  - May include Acceptable Use, Backup, Confidentiality, Data Retention, and Wireless Device Policies
- Policy implementation includes
  - Developing a policy, building consensus, educating users, and enforcing and maintaining the policy

Summary

- Administration tools include
  - Security checklists
  - Security matrices
- Physical security includes
  - Perimeter protection
  - Electronic emanations
  - Fire protection
- Personnel security includes
  - Background checks
  - Ongoing monitoring
  - Exit policies