Dr. Ammar Haider
Assistant Professor
School of Computing

CS3002 Information Security

Security Design Principles and Security Planning

Source: Stallings chap. 1

Security Design Principles

Principles of ….

1. Least Privilege
2. Separation of privilege
3. Fail-safe defaults
4. Complete mediation
5. Open design
6. Economy of mechanism
7. Least Common Mechanism
8. Psychological acceptability

Least privilege

- Provide bare minimum privileges to a program or user to function properly
- Temporary elevation should be relinquished immediately

Advantage

- Abuse of privileges is restricted
- Damage caused by the compromised user or application is reduced

Separation of Privilege

- Access should not be granted based on single condition
- Multiple conditions should be required to achieve access to restricted resources

Examples:

- Two persons to sign checks
- Password login + OTC to perform financial transactions

Fail-safe defaults

- The default configuration of a system should have a conservative approach…
  - Default access to an object is none
  - Explicit access to an object should be given

Examples

- Access Control Lists
- Firewall rules

Complete mediation

- Instead of one-time check, every access to a resource must be checked for compliance with a protection scheme
- Do not rely on caching of access information
- Security vs performance dilemma

Open design

- Design of a security mechanism should be open rather than secret
- Open design can be reviewed by many experts, their feedback helps in improving it.

Economy of mechanism

- Simplicity in design and implementation of security measures

- A simple secure framework provides…
  - Fewer errors
  - Development, testing and verification of security measures is easy
  - Less assumptions

Psychological acceptability

- Security mechanism should not make the resources difficult to access
- User interface should be well designed and intuitive
- Security related setting should consider the expectation of ordinary users

Least common mechanism

- Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.
- Shared mechanisms create possibilities of
  - Transmitting secret data (covert channels)
  - Limiting availability (attack on one service impacts others)
- This principle recommends "isolation" (e.g. virtual machines, sandboxes)

Security Policies, Planning and Architecture

Whitman, chap 4

Security Policies and Planning

The process of creating information security program includes:

- Creating policies and practices
- Design of information security architecture
- Use of a detailed information security mechanism
- Creation of contingency planning consisting of incident response planning, disaster recovery planning, and business continuity plans

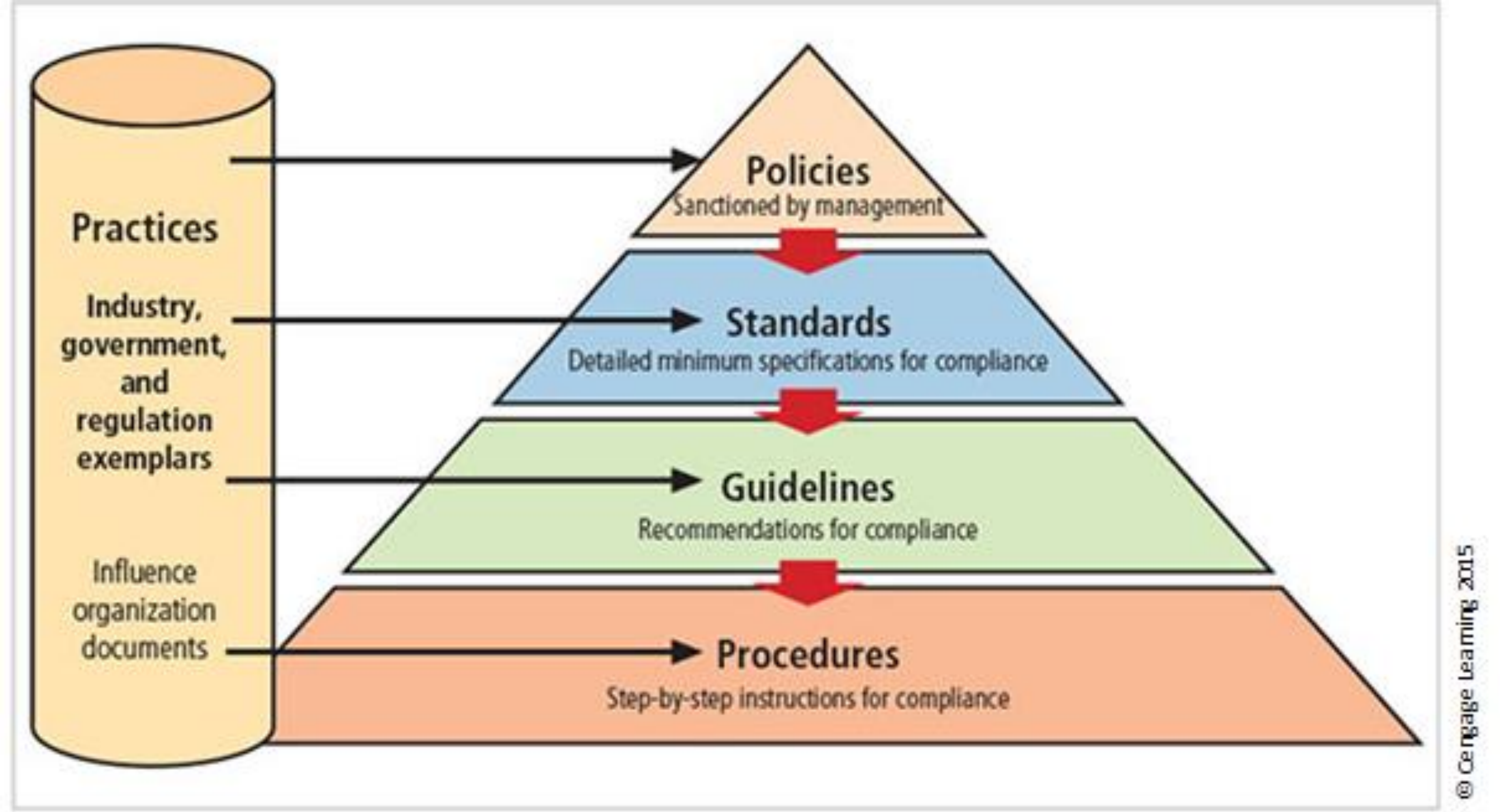
Security Policies

Policies direct how issues should be addressed and technologies used

- Security plan and associated course of action
- Convey instructions to ensure security and privacy
- Create organizational laws
- Dictate acceptable and unacceptable behavior
- Define penalties for violating policy

For a policy to be effective, it must be properly disseminated, read, understood and agreed to by all members of an organization.

Policies, standards, guidelines, and procedures


Practices
Industry, government, and regulation exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance

© Cengage Learning 2015

Figure 4-2

Policies, standards, guidelines, and procedures

Example

Policy

Employees must use strong passwords on their accounts. Passwords must be changed regularly and protected against disclosure.

Standard

Passwords must be at least 10 characters long and incorporate at least one lowercase letter, one uppercase letter, one numerical digit (0–9), and one special character (&%$#@!). Passwords must be changed every 90 days, and must not be written down or stored on insecure media.

Policies, standards, guidelines, and procedures

Example

Guidelines

In order to create strong yet easy-to-remember passwords, consider the following recommendations ….

Procedures

To change your log-in password on our system, perform the following steps: ….

Spheres of Security

How information is under attack, and layers of protection

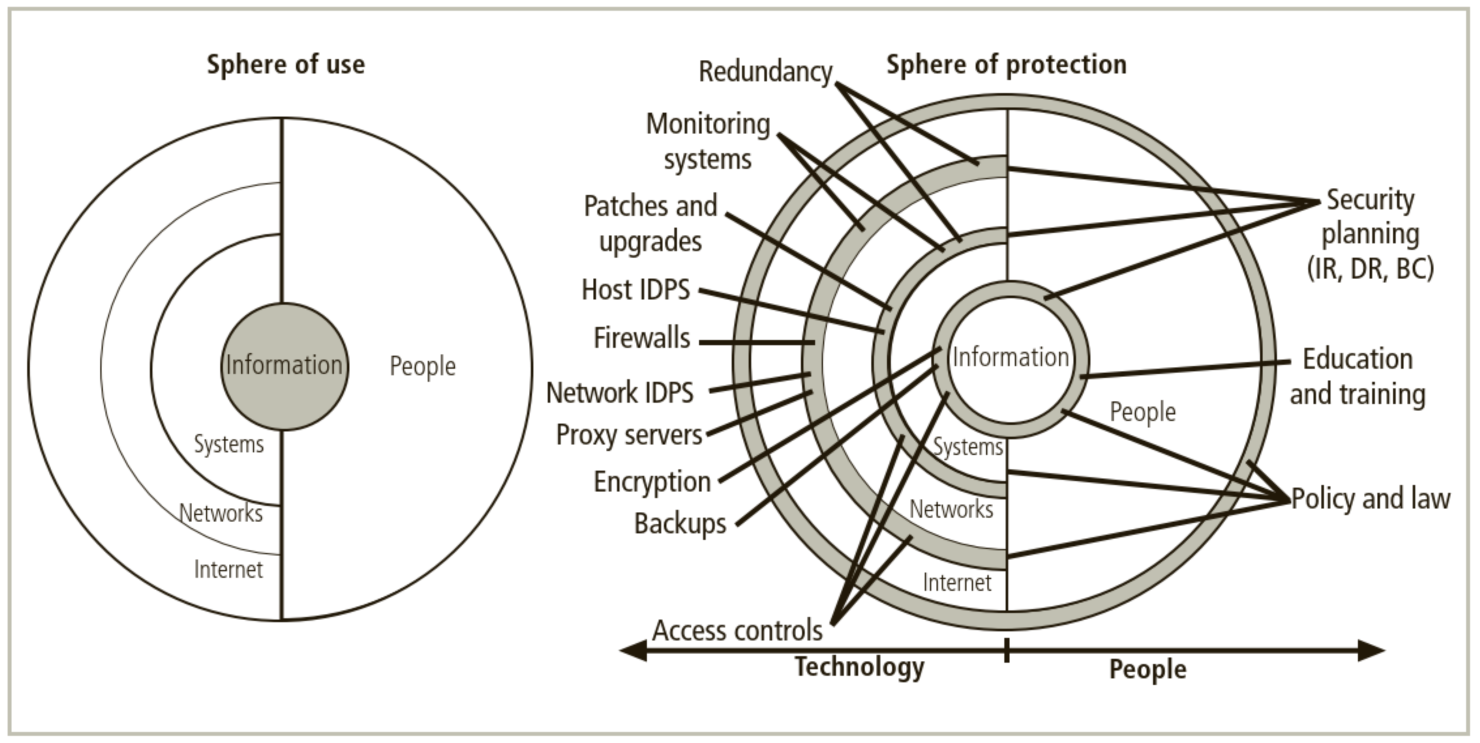


Figure 4-8

Classification of Controls

Managerial	Operational	Technical
• Cover design of security process • Implemented by security administrator • Set directions and scope • Address risk management & security control reviews • Necessity and scope of legal compliance	• Operational functionality of security • Disaster recovery and incident response planning • Address personnel and physical security and protection of production inputs and outputs • Development of education, training & awareness • Addresses maintenance of hardware and software and integrity of data	• Addresses the tactical & technical issues • Addresses identification, authentication, authorization, and accountability mechanisms • Covers cryptography • Addresses development and implementation of audits • Classification of assets and users

Design of Security Architecture

Defense in Depth

- Layered Implementation of Security
  - Policy
  - Training & education
  - Technology (in multiple layers)

Security Perimeter

- Border of security that protects internal systems from outside threats

Security Perimeters & Domains

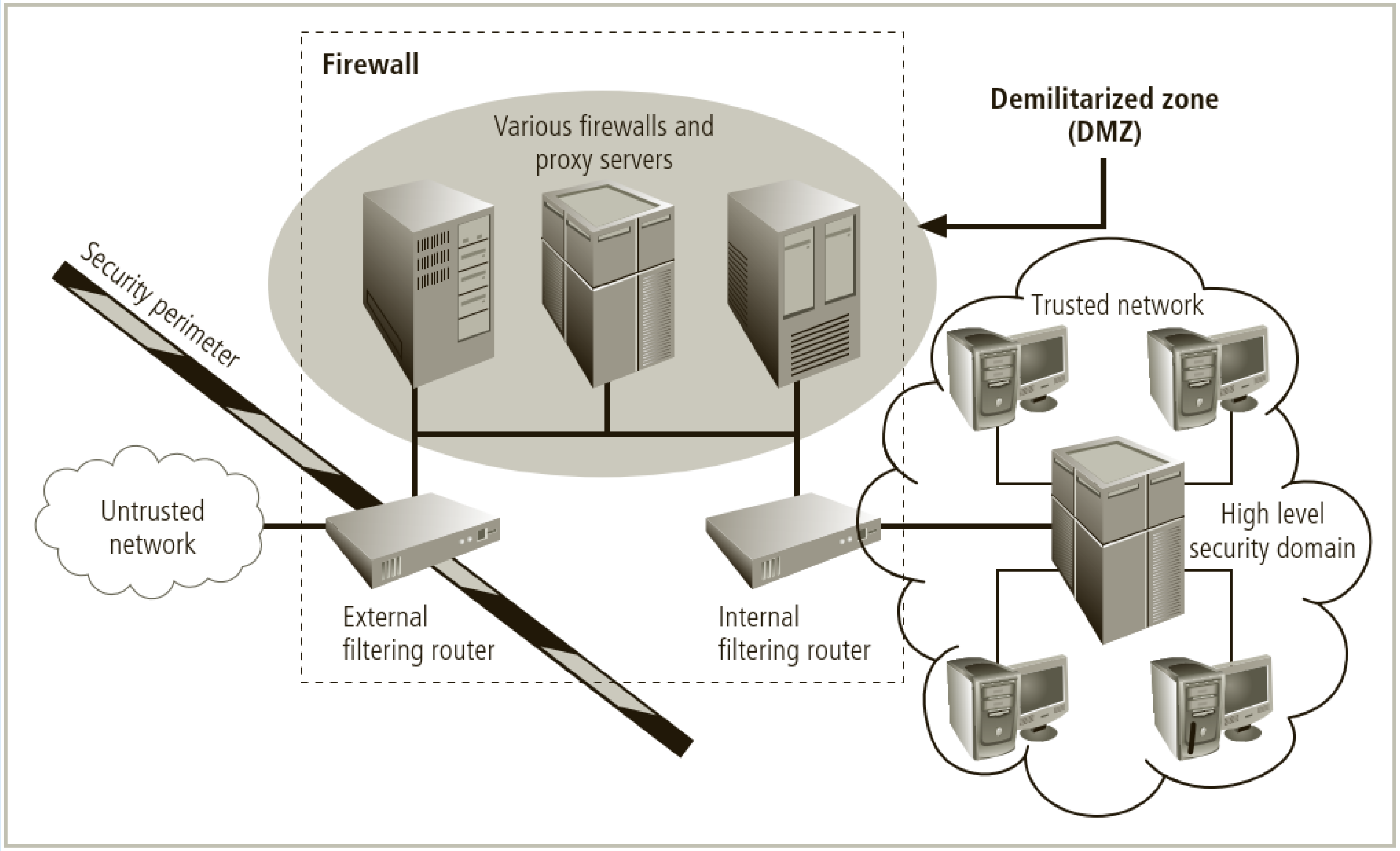

Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Security perimeter
Trusted network
Untrusted network
High level security domain
External filtering router
Internal filtering router

Figure 4-10