E. G. S. Pillay Engineering College, Nagapattinam
Computer Science and Engineering

Elective II **IT 2042 INFORMATION SECURITY** **VIII Sem CSE**

QUESTION BANK - UNIT-IV

1) What is a policy?

- A policy is

A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters

- Policies are organizational laws
- Standards, on the other hand, are more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy
- For a policy to be effective it must be properly disseminated, read, understood and agreed to by all members of the organization

2) **Explain how information security policy is implemented as procedure?**

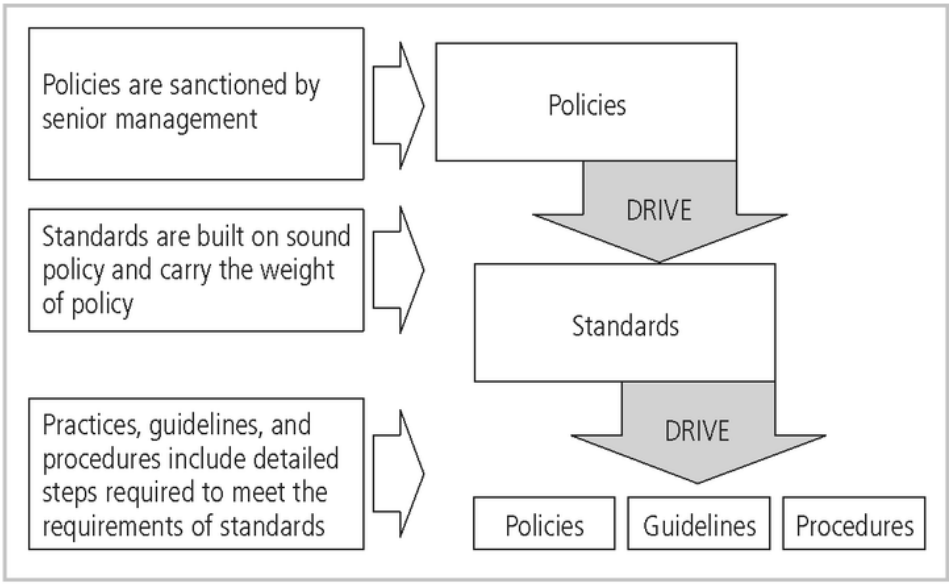

FIGURE 6-1 Policies, Standards, and Practices

3) **What are the three types of security policies? Explain.**

Types of Policy

Management defines three types of security policy:

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

Security Program Policy

- A security program policy (SPP) is also known as
  - A general security policy
  - IT security policy
  - Information security policy
- Sets the strategic direction, scope, and tone for all security efforts within the organization
- An executive-level document, usually drafted by or with, the CIO of the organization and is usually 2 to 10 pages long

Issue-Specific Security Policy (ISSP)

- As various technologies and processes are implemented, certain guidelines are needed to use them properly
- The ISSP:
  - addresses specific areas of technology
  - requires frequent updates
  - contains an issue statement on the organization's position on an issue
- Three approaches:
  - Create a number of independent ISSP documents
  - Create a single comprehensive ISSP document
  - Create a modular ISSP document

Systems-Specific Policy (SysSP)

- *SysSPs are frequently codified as standards and procedures used when configuring or maintaining systems*
- *Systems-specific policies fall into two groups:*
- *Access control lists (ACLs) consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system*
- *Configuration rules comprise the specific configuration codes entered into security systems to guide the execution of the system*

4) ***What are ACL Policies?***

ACL Policies

- Both Microsoft Windows NT/2000 and Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ACLs allow configuration to restrict access from anyone and anywhere
- ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

4) What is Information Security Blueprint?

The Security Blue Print is the basis for Design,Selection and Implementation of Security Policies,education and training programs,and technology controls.

The security blueprint is a more detailed version of the Security Framework,which is an outline of the overall information security strategy for the organization and a road map for the planned changes to the information security environment of the organization.

The blueprint should specify the tasks to be accomplished and the order in which they are to be realized.

It should serve as a scaleable,upgradable,and comprehensive paln for the information security needs for coming years.

One approach to selecting methodology to develop an information security bluepring is to adapt or adopt a published model or framework for information security.

5) Define ISO 17799/BS 7799 Standards and their drawbacks

ISO 17799/BS 7799

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- This Code of Practice was adopted as an international standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799 in 2000 as a framework for information security

Drawbacks of ISO 17799/BS 7799

- Several countries have not adopted 17799 claiming there are fundamental problems:
  - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
  - 17799 lacks "the necessary measurement precision of a technical standard"
  - There is no reason to believe that 17799 is more useful than any other approach currently available
  - 17799 is not as complete as other frameworks available
  - 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

6) What are the objectives of ISO 17799?

Organizational Security Policy is needed to provide management direction and support

Objectives:

a. Operational Security Policy
b. Organizational Security Infrastructure
c. Asset Classification and Control
d. Personnel Security

e. Physical and Environmental Security
f. Communications and Operations Management
g. System Access Control
h. System Development and Maintenance
i. Business Continuity Planning
j. Compliance

7) What is the alternate Security Models available other than ISO 17799/BS 7799?

- Another approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov) – Including:
- NIST SP 800-12 - The Computer Security Handbook
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing IT Systems
- NIST SP 800-18 - The Guide for Developing Security Plans for IT Systems

8) Explain NIST SP 800-14

- Generally accepted Principles and practices for Security Inf Tech Sys
- Provides **best practices** and security principles that can direct the security team in the development **of Security Blue Print**.as given below:

  - Security Supports the Mission of the Organization
  - Security is an Integral Element of Sound Management
  - Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations
  - Security Responsibilities and Accountability Should Be Made Explicit
  - Security Requires a Comprehensive and Integrated Approach
  - Security Should Be Periodically Reassessed
  - Security is Constrained by Societal Factors
  - 33 Principles enumerated

9) Explain NIST SP 800-26

It serves as a Security Self Assesment Guide comprising of

Management Controls

- Risk Management
- Review of Security Controls
- Life Cycle Maintenance
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

Operational Controls

- Personnel Security
- Physical Security
- Production, Input/Output Controls
- Contingency Planning

- Hardware and Systems Software
- Data Integrity
- Documentation
- Security Awareness, Training**, and Education**
- **Incident Response Capability**

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

10) What is Sphere of protection?

Sphere of Protection

- The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
- The people must become a layer of security, a human firewall that protects the information from unauthorized access and use
- Information security is therefore designed and implemented in three layers
  - policies
  - people (education, training, and awareness programs)
  - technology

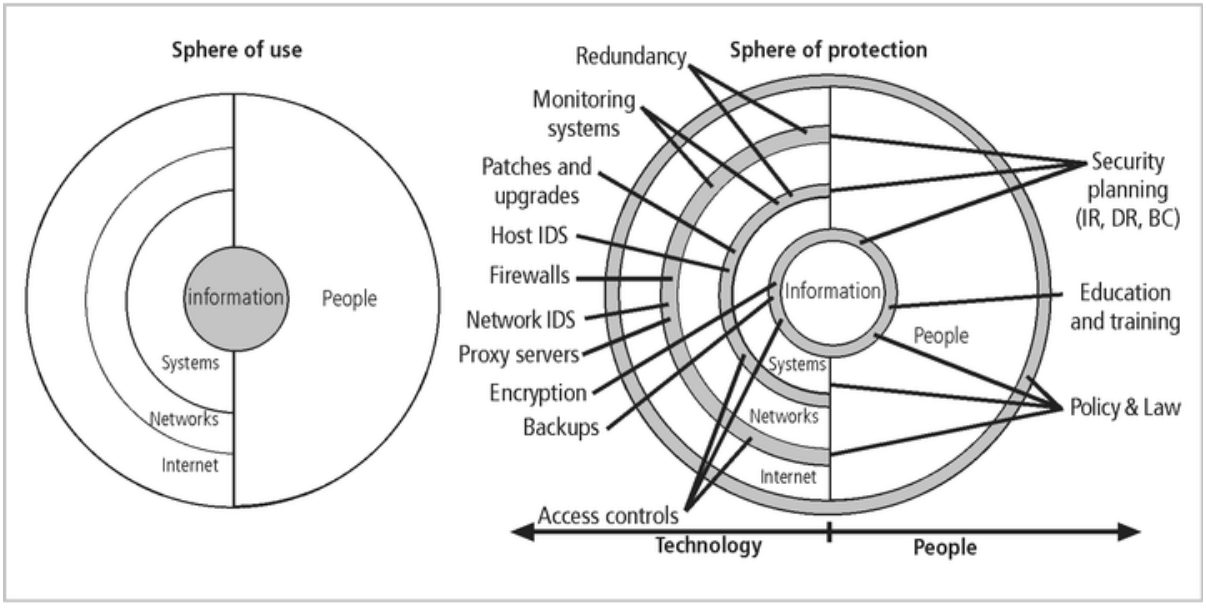

FIGURE 6-16 Spheres of Security

11) What is Defense in Depth?

Defense in Depth

a. One of the foundations of security architectures is the requirement to implement security in layers
b. Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls

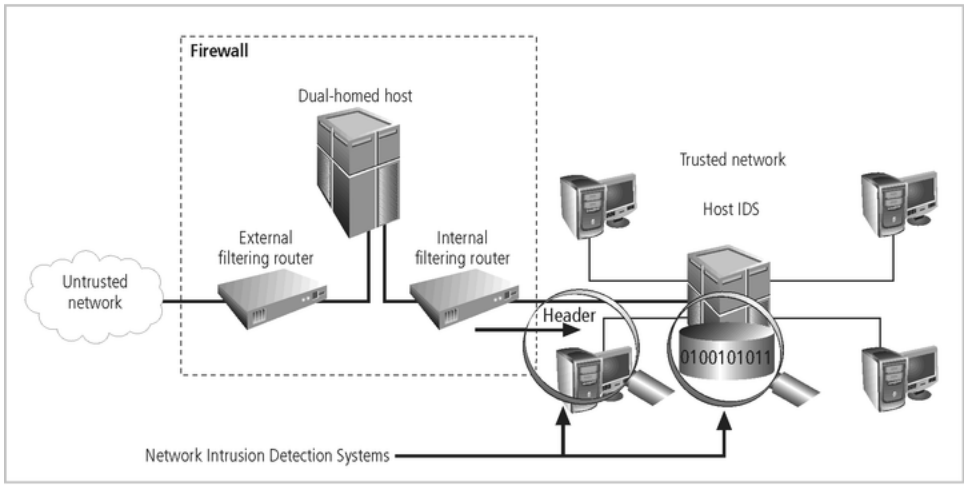

FIGURE 6-18 Defense in Depth

12) What is Security perimeter?

Security Perimeter

– The point at which an organization's security protection ends, and the outside world begins
– Referred to as the security perimeter
– Unfortunately the perimeter does not apply to internal attacks from employee threats, or on-site physical threats

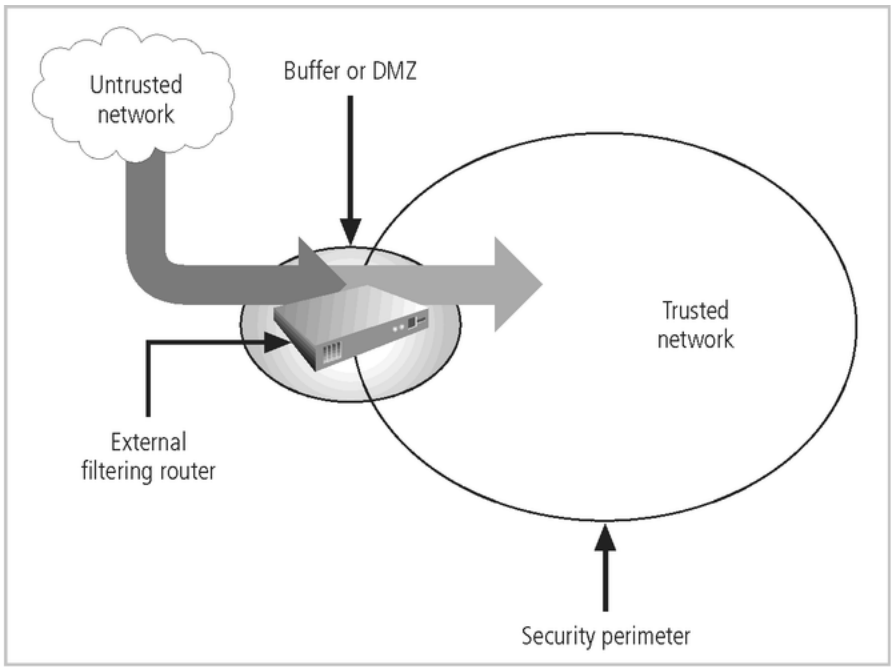

FIGURE 6-19 Security Perimeters and Domains

13) What are the key technological components used for security implementation?

Key Technology Components

- Other key technology components
  - A firewall is a device that selectively discriminates against information flowing into or out of the organization
  - The DMZ (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers
  - In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement Intrusion Detection Systems or IDS

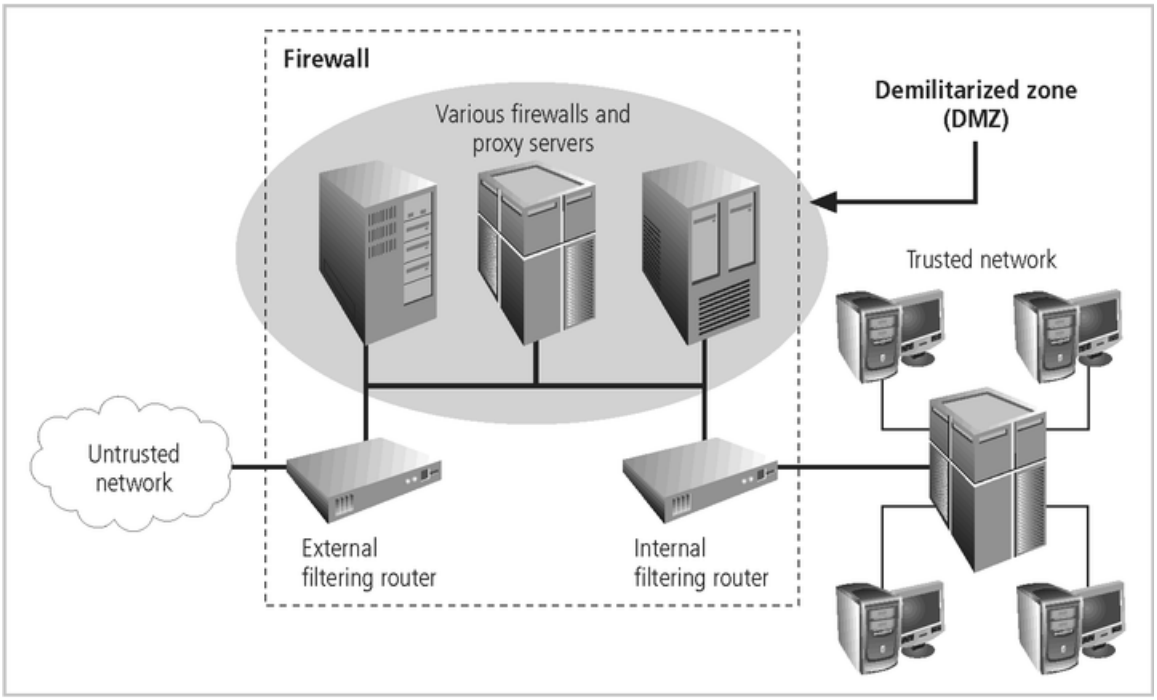

FIGURE 6-20 Firewalls, Proxy Servers, and DMZs

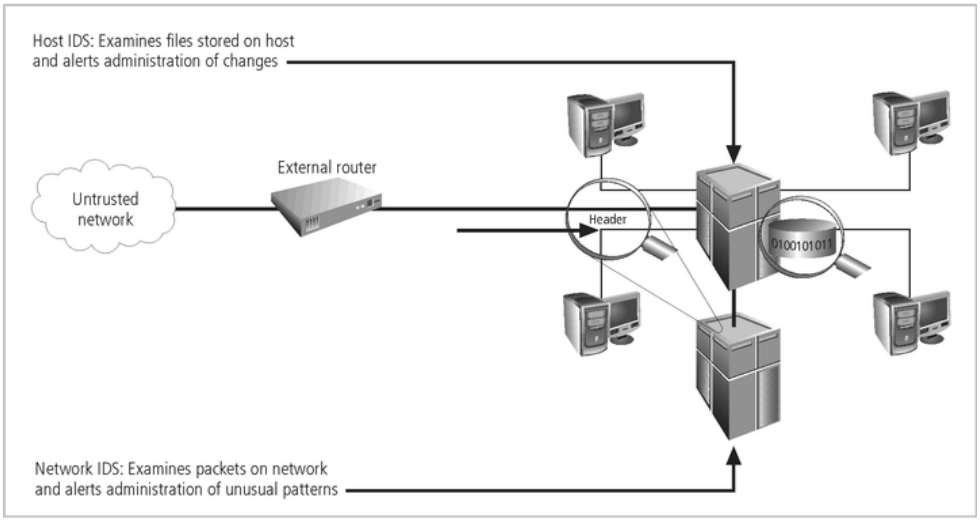

FIGURE 6-21 Intrusion Detection Systems