University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

PSIT302 & PSIT3P2 – Information Security Management (ISM)

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

Unit II – Security Management of IT Systems

- Network Security Management

- Firewalls, IDS and IPS Configuration Management
- Web and Wireless Security Management
- **General Server Configuration guidelines and maintenance**
- ISM Classification
- Access control Models
- Linux and Windows Case Study
- Technical Controls
- Password Management and Key Management for USers

Topics

- Introduction
- Background
- Server Security Planning
- Securing the Server Operating system
- Securing the Server Software
- Maintaining the Security of the Server

Server

- Is a host that provides one or more services for other hosts over a network as a primary function.

- A file server provides file sharing services so that users can access, modify, store, and delete files.
- A database server that provides database services for Web applications on Web servers.
- The Web servers provide Web content services to users' Web browsers.
- There are many other types of servers, such as application, authentication, directory services, email, infrastructure management, logging, name/address resolution services (e.g., Domain Name Server [DNS]), print, and remote access.

Server Vulnerabilities, Threats, and Environments

- To secure a server, it is essential to first define the threats that must be mitigated.
- Knowledge of potential threats is important to understanding the reasons behind the various baseline technical security practices presented in this document.
- Many threats against data and resources are possible because of mistakes—either bugs in operating system and server software that create exploitable vulnerabilities, or errors made by end users and administrators.
- Threats may involve intentional actors (e.g., attacker who wants to access information on a server) or unintentional actors (e.g., administrator who forgets to disable user accounts of a former employee.)
- Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another geographical area.
- Organizations should conduct risk assessments to identify the specific threats against their servers and determine the effectiveness of existing security controls in counteracting the threats; they then should perform risk mitigation to decide what additional measures (if any) should be implemented,

Security Categorization of Information and Information Systems

- Three security categories—low, moderate, and high
- As per the above, security weaknesses in the system need to be resolved
- The system should offer only the required functionality to each authorized user, so that no one can use functions that are not necessary. This principle is known as least privilege.
- Using multiple layers of security—defense in depth.

Basic Server Security Steps

Taking the following steps for server security within the context of the organization's security policy should prove effective:

1. Plan the installation and deployment of the operating system (OS) and other components for the server.
2. Install, configure, and secure the underlying OS.
3. Install, configure, and secure the server software.
4. For servers that host content, such as Web servers (Web pages), database servers (databases), and directory servers (directories), ensure that the content is properly secured.
5. Employ appropriate network protection mechanisms
6. Employ secure administration and maintenance processes, including application of patches and upgrades, monitoring of logs, backups of data and OS, and periodic security testing.

Server Security Principles

- General information security principles:
- Simplicity—Security mechanisms (and information systems in general) should be as simple as possible. Complexity is at the root of many security issues.
- Fail-Safe—If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.
- Complete Mediation—Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples of mediators include file system permissions, proxies, firewalls, and mail gateways.
- Open Design—System security should not depend on the secrecy of the implementation or its components.
- Separation of Privilege—Functions, to the degree possible, should be separate and provide as much granularity as possible.
- Least Privilege—This principle dictates that each task, process, or user is granted the minimum rights required to perform its job.

Server Security Principles

- Psychological Acceptability—Users should understand the necessity of security. This can be provided through training and education.
- Least Common Mechanism—When providing a feature for the system, it is best to have a single process or service gain some function without granting that same function to other parts of the system.
- Defense-in-Depth—Organizations should understand that a single security mechanism is generally insufficient.
- Work Factor—Organizations should understand what it would take to break the system or network's security features.
- Compromise Recording—Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the organization.

Server Security Planning

- The most critical aspect of deploying a secure server is careful planning before installation, configuration, and deployment.
- Careful planning will ensure that the server is as secure as possible and in compliance with all relevant organizational policies.
- Many server security and performance problems can be traced to a lack of planning or management controls.

Installation and Deployment Planning

In the planning stages of a server, the following items should be considered:

1. Identify the purpose(s) of the server.

- What information categories will be stored on the server?
- What information categories will be processed on or transmitted through the server?
- What are the security requirements for this information?
- Will any information be retrieved from or stored on another host (e.g., database server, directory server, Web server, Network Attached Storage (NAS) server, Storage Area Network (SAN) server)?
- What are the security requirements for any other hosts involved?
- What other service(s) will be provided by the server (in general, dedicating the host to only one service is the most secure option)?
- What are the security requirements for these additional services?
- What are the requirements for continuity of services provided by the server, such as those specified in continuity of operations plans and disaster recovery plans?
- Where on the network will the server be located?

Installation and Deployment Planning

In the planning stages of a server, the following items should be considered:

2. Identify the network services that will be provided on the server, such as (HTTP), (FTP), (SMTP), (NFS), or database services (e.g., Open Database Connectivity [ODBC]). The network protocols to be used for each service (e.g., IPv4, IPv6) should also be identified.

- Identify any network service software, both client and server, to be installed on the server and any other support servers.
- Identify the users or categories of users of the server and any support hosts.
- Determine the privileges that each category of user will have on the server and support hosts.
- Determine how the server will be managed (e.g., locally, remotely from the internal network, remotely from external networks).
- Decide if and how users will be authenticated and how authentication data will be protected.
- Determine how appropriate access to information resources will be enforced.

Installation and Deployment Planning

In the planning stages of a server, the following items should be considered:

2. Identify the network services that will be provided on the server, such as (HTTP), (FTP), (SMTP), (NFS), or database services (e.g., Open Database Connectivity [ODBC]). The network protocols to be used for each service (e.g., IPv4, IPv6) should also be identified.

- Determine which server applications meet the organization's requirements. Consider servers that may offer greater security, albeit with less functionality in some instances. Some issues to consider include—
  - Cost
  - Compatibility with existing infrastructure
  - Knowledge of existing employees
  - Existing manufacturer relationship
  - Past vulnerability history
  - Functionality.
- Work closely with manufacturer(s) in the planning stage.

Installation and Deployment Planning

The choice of server application may determine the choice of OS. However, to the degree possible, server administrators should choose an OS that provides the following:

- Ability to granularly restrict administrative or root level activities to authorized users only
- Ability to granularly control access to data on the server
- Ability to disable unnecessary network services that may be built into the OS or server software
- Ability to control access to various forms of executable programs, such as Common Gateway
- Interface (CGI) scripts and server plug-ins for Web servers, if applicable
- Ability to log appropriate server activities to detect intrusions and attempted intrusions
- Provision of a host-based firewall capability torestrict both incoming and outgoing traffic
- Support for strong authentication protocols and encryption algorithms

Installation and Deployment Planning

- When planning the location of a server, the following issues should be considered:
- Are the appropriate physical security protection mechanisms in place for the server and its networking components (e.g., routers, switches)? Examples include—
  - Locks
  - Card reader access
  - Security guards
  - Physical intrusion detection systems (e.g., motion sensors, cameras).
- Are there appropriate environmental controls so that the necessary humidity and temperature are maintained? If high availability is required, are there redundant environmental controls?
- Is there a backup power source? For how long will it provide power?
- Is there appropriate fire containment equipment? Does it minimize damage to equipment that would otherwise not be impacted by the fire?
- If high availability is required, are there redundant network connections? (For Internet-facing servers, this generally means Internet connections from at least two different Internet service providers [ISP].)
- Is there another data center that can be used to host servers in the event of a catastrophe at the original data center?
- If the location is subject to known natural disasters, is it hardened against those disasters and/or is there a contingency site outside the potential disaster area?

Security Management Staff

- Chief Information Officer : The Chief Information Officer (CIO) ensures that the organization's security posture is adequate.
  - Coordinating the development and maintenance of the organization's information security policies, standards, and procedures
  - Coordinating the development and maintenance of the organization's change control and management procedures
  - Ensuring the establishment of, and compliance with, consistent IT security policies for departments throughout the organization.

Security Management Staff

- Information Systems Security Program Managers: The Information Systems Security Program Managers (ISSPM) oversee the implementation of and compliance with the standards, rules, and regulations specified in the organization's security policy.
  - Ensuring that security procedures are developed and implemented
  - Ensuring that security policies, standards, and requirements are followed
  - Ensuring that all critical systems are identified and that contingency planning, disaster recovery plans, and continuity of operations plans exist for these critical systems
  - Ensuring that critical systems are identified and scheduled for periodic security testing according to the security policy requirements of each respective system.

Security Management Staff

- Information Systems Security Officers :Information Systems Security Officers (ISSO) are responsible for overseeing all aspects of information security within a specific organizational entity.
- They ensure that the organization's information security practices comply with organizational and departmental policies, standards, and procedures. ISSOs are responsible for the following activities associated with servers:
  - Developing internal security standards and procedures for the servers and supporting network infrastructure
  - Cooperating in the development and implementation of security tools, mechanisms, and mitigation techniques
  - Maintaining standard configuration profiles for the servers and supporting network infrastructure controlled by the organization, including, but not limited to, OSs, firewalls, routers, and server applications
  - Maintaining operational integrity of systems by conducting security tests and ensuring that designated IT professionals are conducting scheduled testing on critical systems.

Security Management Staff

- Server, Network, and Security Administrators: are system architects responsible for the overall design, implementation, and maintenance of a server. Network administrators are responsible for the overall design, implementation, and maintenance of a network.
- The administrators are responsible for the following activities associated with servers:
  - Installing and configuring systems in compliance with the organizational security policies and standard system and network configurations
  - Maintaining systems in a secure manner, including frequent backups and timely application of patches
  - Monitoring system integrity, protection levels, and security-related events
  - Following up on detected security anomalies associated with their information system resources
  - Conducting security tests as required.

Management Practices

- To ensure the security of a server and the supporting network infrastructure, organizations should implement the following practices:
- Organizational Information System Security Policy—
  - A security policy should specify the basic information system security tenets and rules, and their intended internal purpose.
  - The policy should also outline who in the organization is responsible for particular areas of information security (e.g., implementation, enforcement, audit, review).
  - The policy must be enforced consistently throughout the organization to be effective. Generally, the CIO is responsible for drafting the organization's security policy.
- Configuration/Change Control and Management—
  - The process of controlling modification to a system's design, hardware, firmware, and software provides sufficient assurance that the system is protected against the introduction of an improper modification before, during, and after system implementation.
  - Configuration control leads to consistency with the organization's information system security policy. Configuration control is traditionally overseen by a configuration control board that is the final authority on all proposed changes to an information system.
  - If resources allow, consider the use of development, quality assurance, and/or test environments so that changes can be vetted and tested before deployment in production.

Management Practices

- Risk Assessment and Management—
  - Risk assessment is the process of analyzing and interpreting risk.
  - It involves determining an assessment's scope and methodology, collecting and analyzing risk related data, and interpreting the risk analysis results.
  - Collecting and analyzing risk data requires identifying assets, threats, vulnerabilities, safeguards, consequences, and the probability of a successful attack.
  - Risk management is the process of selecting and implementing controls to reduce risk to a level acceptable to the organization.
- Standardized Configurations—
  - Organizations should develop standardized secure configurations for widely used OSs and server software.
  - This will provide recommendations to server and network administrators on how to configure their systems securely and ensure consistency and compliance with the organizational security policy.
  - Because it only takes one insecurely configured host to compromise a network, organizations with a significant number of hosts are especially encouraged to apply this recommendation.

Management Practices

- Secure Programming Practices—Organizations should adopt secure application development guidelines to ensure that they develop their applications for servers in a sufficiently secure manner.
- Security Awareness and Training—
  - A security training program is critical to the overall security posture of an organization. Making users and administrators aware of their security responsibilities and teaching the correct practices helps them change their behavior to conform to security best practices.
  - Training also supports individual accountability, which is an important method for improving information system security. If the user community includes members of the general public, providing security awareness specifically targeting them might also be appropriate.
- Contingency, Continuity of Operations, and Disaster Recovery Planning—
  - Contingency plans, continuity of operations plans, and disaster recovery plans are established in advance to allow an organization or facility to maintain operations in the event of a disruption.
- Certification and Accreditation—
  - Certification in the context of information system security means that a system has been analyzed to determine how well it meets all of the security requirements of the organization.
  - Accreditation occurs when the organization's management accepts that the system meets the organization's security requirements.