NETWORK ADMINISTRATION AND SECURITY

DEVELOPING NETWORK SECURITY STRATEGIES

Developing security strategies that can protect all parts of a complicated network while having a limited effect on ease of use and performance is one of the most important and difficult tasks related to network design.

Security design is challenged by the complexity and porous nature of modern networks that include public servers for electronic commerce, extranet connections for business partners, and remote access services for users reaching the network from home, customer sites, hotel rooms, Internet cafes, and so on.

To help handle the difficulties inherent in designing network security for complex networks, this chapter teaches a systematic, top-down approach that focuses on planning and policy development before the selection of security products.

Network Security Design

To effectively plan and execute a security strategy, the security design process consists of the following steps:-

1. Identification of network assets
2. Analysis of security risks
3. Analysis of security requirements and tradeoffs
4. Development of a security plan
5. Defining a security policy
6. Developing procedures for applying security policies
7. Developing a technical implementation strategy
8. Achieving buy-in from users, managers, and technical staff
9. Training users, managers, and technical staff

10. Implementing the technical strategy and security procedures
11. Testing the security and update it if any problems are found
12. Maintaining security

1. *Identification of network assets*

- Network assets can include:-
- Network hosts (including the hosts' operating systems, applications, and data),
- Internetworking devices (such as routers and switches), and
- Network data that traverses the network
- Less obvious assets include intellectual property, trade secrets, and a company's reputation.

2. *Analysis of security risks*

Risks can range from

- hostile intruders
- untrained users
- Hostile intruders can
- steal data, change data, and
- Cause service to be denied to legitimate users.

3. *Analysis of security requirements and tradeoffs*

Security requirements boil down to the following:-

- The confidentiality of data, so that only authorized users can view sensitive information
- The integrity of data, so that only authorized users can change sensitive information

- System and data availability, so that users have uninterrupted access to important computing resources

Principle of least protection

- The cost of protecting against a threat should be less than the cost of recovering if the threat were to strike.
- Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures.

Tradeoffs

Achieving security goals means making tradeoffs.

- Tradeoffs must be made between security goals and goals for affordability, usability, performance, and availability. Also, security ads to the amount of management work because user login IDs, passwords, and audit logs must be maintained.
- Security also affects network performance: consuming CPU power and memory on hosts, routers, and servers.
- Delay that packets experience while being encrypted or decrypted

4. Development of a security plan

- One of the first steps in security design is developing a security plan.
- A security plan is a high-level document that proposes what an organization is going to do to meet security requirements.
- The plan specifies the time, people, and other resources that will be required to develop a security policy and achieve technical implementation of the policy.
- The plan should be practical and pertinent. And based on the customer's goals and the analysis of network assets and risks

Topology, services, access, administration

The plan should reference the network topology and include a list of network services that will be provided (eg. FTP, web, email).

This list should specify who provides the services, who has access to the services, how access is provided, and who administers the services.

Minimal complexity

Complicated security strategies are hard to implement correctly without introducing unexpected security holes

Responsibility

One important aspect of the security plan is a specification of the people who must be involved in implementing network security:-

- Will specialized security administrators be hired?
- How will end users and their managers get involved?
- How will end users, managers, and technical staff be trained on security policies and procedures?
- For a security plan to be useful, it needs to have the support of all levels of employees within the organization.

5. Defining a security policy

Security policy: a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

A security policy informs users, managers, and technical staff of their obligations for protecting technology and information assets.

The policy specifies the mechanisms by which these obligations can be met.

The security policy should have buy-in from employees, managers, executives, and technical personnel. Developing a security policy is the job of senior management, with help from security and network administrators.

The administrators get input from managers, users, network designers and engineers, and possibly legal counsel. The role of network designer is to work closely with the security administrators to understand how policies might affect the network design.

A security policy is a living document. And because organizations constantly change, security policies should be regularly updated to reflect new business directions and technological shifts. Risks change over time also and affect the security policy.

COMPONENTS OF A SECURITY POLICY:

- An *access policy:-* It defines access rights and privileges: - The access policy should provide guidelines for connecting external networks, connecting devices to a network, and adding new software to systems. An access policy might also address how data is categorized (for example, confidential, internal, and top secret).
- An *accountability policy:* - It defines the responsibilities of users, operations staff, and management. The accountability policy should specify an audit capability and provide incident-handling guidelines that specify what to do and whom to contact if a possible intrusion is detected.
- An *authentication policy:* - *it* establishes trust through an effective password policy and sets up guidelines for remote-location authentication.

- A *privacy policy: -* it defines reasonable expectations of privacy regarding the monitoring of electronic mail, logging of keystrokes, and access to users' files.
- *Computer-technology purchasing guidelines: - it* specifies the requirements for acquiring, configuring, and auditing computer systems and networks for compliance with the policy.

Developing procedures for applying security policies

Security procedures implement security policies. Procedures

- Define configuration, login, audit, and maintenance processes.

It is Written for:-

End users, network administrators, and security administrators.

It is Specifies

How to handle incidents (that is, what to do and who to contact if an intrusion is detected).

Maintaining Security

Security maintained by:-

Scheduling periodic independent audits,

- Reading audit logs,
- Responding to incidents,
- Reading current literature and agency alerts,
- Performing security testing,
- Training security administrators and updating the security plan and policy

Security wheel: illustrates that implementing, monitoring, testing, and improving security is a never-ending process.

Security Mechanisms

i) Physical Security

Physical security: using physical control to protect key network resources. It can protect a network from misuse or abuse by:-

- Untrained employees and contractors (inadvertent)
- Hackers, competitors, and terrorists walking in off the street and changing equipment configurations
- From natural disasters such as floods, fires, storms, and earthquakes should be installed to protect

Core routers, demarcation points, cabling, modems, servers, hosts, backup storage, and so on should be placed in computer rooms that have card key access and/or security guards.

Computer rooms should also be equipped with uninterruptible power supplies, fire alarms, fire-abatement mechanisms, and water removal systems.

To protect equipment from earthquakes and high winds during storms, equipment should be installed in racks that attach to the floor or wall.

Planning for physical security should start during the early phases of the top-down design process in case there are lead times to build or install security mechanisms

ii) Authentication

Authentication identifies who is requesting network services and it can refer to human users, devices or software processes. Forms of authentication include:-

Re-usable password scheme: most common

One-time (dynamic) passwords scheme:

Smartcard based implementation: - User enters a PIN, card provides a onetime password that is used to access the corporate network for a limited time. Typically used by telecommuters and mobile users.

Authentication is traditionally based on one of three proofs:

i) *Something the user knows:* This usually involves knowledge of a unique secret that is shared by the authenticating parties. To a user, this secret appears as a classic password, a PIN, or a private cryptographic key.

ii) *Something the user has:* This usually involves physical possession of an item that is unique to the user. Examples include password token cards, security cards, and hardware keys.

iii) *Something the user is:* This involves verification of a unique physical characteristic of the user, such as a fingerprint, retina pattern, voice, or face. Many systems use two-factor authentication, which requires a user to have two proofs of identity. E.g., accesses control system that requires a security card and a password.

With two-factor authentication, a compromise of one factor does not lead to a compromise of the system. An attacker could learn a password, but the password is useless without the security card. Conversely, if the security card is stolen, it cannot be used without the password.

iii) Authorization

Authorization says what user can do after authentication. i.e. Authorization grants privileges to processes and users. Authorization lets a security administrator control parts of a network (for example, directories and files on servers).

Authorization varies from user to user, partly depending on a user's department or job function. For example, a policy might state that only Human Resources employees should see salary records for people they do not manage.

Security experts recommend use of the principle of least privilege in the implementation of authorization. It is based on the idea that each user should be given only the minimal necessary rights to perform a certain task. Therefore, an authorization mechanism should give a user only the minimum access permissions that are necessary.

iv) Accounting (Auditing)

Accounting or auditing: collecting network activity data for purposes of effectively analyze the security of a network and to respond to security incidents such as:-

- Ensure audit data include time-stamped
- Attempts to achieve authentication and authorization
- Log "anonymous" or "guest" access to public servers
- Attempts by users to change their access right

A further extension of auditing is security assessment

- The network is periodically examined from within by professionals, trained in the vulnerabilities exploited by network invaders.
- Output of assessment: specific plan for correcting any deficiencies

v) Data Encryption

It is the process for scrambling data to protect it from being read by an un-intended party

A router, server, end system, or dedicated device can be encryption or decryption device. Encryption should be used when a customer has analyzed security risks and identified severe consequences if data is not kept confidential and/or the identity of senders of data is not guaranteed.

On internal networks and networks that use the Internet simply for web browsing, email, and file transfer, encryption may not necessary. For connection of private

sites via the Internet, using virtual private networking (VPN), encryption is recommended to protect the confidentiality authentication and integrity

vi) Packet Filters

Packet filter: forward or discard packets based on defined filtering rules. Can be set up on routers, firewalls, and servers to accept or deny packets from particular addresses or services

Broad security policies:

- Permissive: Deny specific types of packets, accept all else
- Prudent: Accept specific types of packets, deny all else

The first policy requires a thorough understanding of specific security threats and can be hard to implement. While the second policy is easier to implement and more secure because the security administrator does not have to predict future attacks for which packets should be denied.

The second policy is also easier to test because there is a finite set of accepted uses of the network. To do a good job implementing the second policy requires a good understanding of network requirements. The network designer should work with the security administrator to determine what types of packets should be accepted.

Packet filters usually use access control lists (ACL) for specifying rules. ACLs control whether network traffic is forwarded or blocked at interfaces on a router or switch. Typical criteria are: source address, destination address, or the upper-layer protocol in the packet.

vii) Firewalls

It is a device that enforces security policies at the boundary between two or more networks. It can be a router with ACLs, a dedicated hardware appliance, or software running on a PC or UNIX system. It applies a set of rules that specifies which traffic should be allowed or denied

- A static-stateless-packet-filter firewall looks at individual packets and is optimized for speed and configuration simplicity.
- A stateful firewall can track communication sessions and more intelligently allow or deny traffic

Example

Proxy firewall: It acts as an intermediary between hosts, intercepting some or all application traffic between local clients and outside servers. Proxy firewalls examine packets and support stateful tracking of sessions. These types of firewalls can block malicious traffic and content that is deemed unacceptable.

viii) Intrusion Detection and Prevention Systems

An IDS detects malicious events and notifies an administrator of the occurrence. They can also perform statistical and anomaly analysis. Some IDS devices can report to a central database that correlates information from multiple sensors to give an administrator an overall view of the real-time security of a network.

An intrusion prevention system (IPS) can dynamically block traffic by adding rules to a firewall. An IPS can detect and prevent attacks. There are two types of IDS devices:-

- *Host IDS:* Resides on an individual host and monitors that hos
- *Network IDS:* Monitors all network traffic watching for predefined signatures of malicious events

A network IDS is often placed on a subnet that is directly connected to a firewall so that it can monitor the traffic that has been allowed and look for suspicious activity. A major concern with both IDS and IPS was: volume of false alarms. This problem has been ameliorated by sophisticated software and services.

Modern IPS solutions: include anomaly detection that learns about typical actual network traffic on a customer's network and alarms only upon deviation. It also

supports reputation filtering and global correlation services so that an IPS can keep up-to-date on global security trends and more accurately deny traffic from flagged networks known to be currently associated with spam, and other malware.

NETWORK MANAGEMENT PROCESSES

ISO defines five types of network management processes referred to as FCAPS:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

a) Fault Management

Consists of faults

- detection
- isolation
- diagnosis
- correction

It also includes

- Reporting problems (to end users and managers)
- Tracking trends (related to problems)
- Developing workarounds (until a problem can be fixed)

Fault Management Tools

A variety of tools include:-

- monitoring tools that alert managers to problems,
- Protocol analyzers for fault resolution, and

- Help-desk software for documenting problems and alerting users of problems

Monitoring tools often based on the standards:

- *SNMP*: (Simple Network Management Protocol) standard
- *RMON:* (Remote Monitoring) standard
- OS mechanisms: most operating systems provide a means for the system and its

Cisco devices produce syslog messages as a result of network events. A syslog message contains a *time stamp*, *leve*l, and *facility*

Syslog levels:

- Emergency (level 0, the most severe level)
- Alert (level 1)
- Critical (level 2)
- Error (level 3)
- Warning (level 4)
- Notice (level 5)
- Informational (level 6)
- Debugging (level 7)

Syslog messages can be sent to:-

- Cisco router or switch console.
- A network management station or a remote network host on which a syslog analyzer is installed

A syslog analyzer applies filters and sends only a predefined subset of all syslog messages. This saves bandwidth and also reduces the amount of information a network administrator must analyze.

b) Configuration Management

This helps a network manager to:-

Keep track of network devices and maintain information on how devices are configured.

A network manager can

- define and save a default configuration for similar devices,
- modify the default configuration for specific devices,
- Load the configuration on devices.
- maintain an inventory of network asset
- Do version-logging: - *Which is keeping track of the version of operating systems, applications running on network devices.*

The inventory also includes information on the hardware configuration of devices, such as RAM size, flash memory, and the type of cabling the devices use.

CM facilitates change management.

c) Accounting Management

It facilitates usage-based billing, for charging departments, projects for network services. Even if no monetary charging, accounting can be useful to catch “abuse” in form of:-

- Un-authorized/undesirable activities which cause excessive traffic
- track unexpected traffic growth is so that the traffic can be considered during the next capacity-planning phase

d) Performance Management

The measurement of network behavior and effectiveness including

- examining network application and protocol behavior
- analyzing reachability
- measuring response time
- recording network route changes

It also facilitates the following:-

- Optimizing a network,
- Meeting service-level agreements (SLAs)
- Planning for expansion

Monitoring performance involves the following:-

- Collecting data
- Processing the data
- Displaying the data
- Archiving some or all of the data

Types of performance monitored:-

- ***End-to-end performance:*** This is performance across an internetwork. It includes availability, capacity, utilization, delay, delay variation, throughput, reachability, response time, errors, and the burstiness of traffic.
- ***Component performance***: This is performance of individual links or devices

TOOLS

- They are used for surveying remote parts of the network to test reachability and measure response times.
- Response-time: use ***ping*** and measuring the round-trip time (RTT).
- On large networks, reachability and RTT studies can be impractical. E.g. on a network with 10,000 devices polling can take hours and can cause significant network traffic.
- Use protocol analyzers or SNMP tools to record traffic loads between important sources and destinations.
- Another less reliable tool is *Traceroute*

Objective: document the mbps between pairs of autonomous systems, networks, hosts, or applications.

Source/destination traffic-load documentation is useful for capacity planning, troubleshooting, and figuring out which routing protocols to use on the routers.

e) Security Management

It involves:-

- Maintaining and distributing passwords and other authentication and authorization information.
- Processes for generating, distributing, and storing encryption keys
- Includes tools and reports to analyze router and switch configurations for compliance with site security standards.
- Collecting, storing, and examining security audit logs. Problem with audit logs: large amount of data

Efficiency requirements (storage can be minimized by):

- keeping data for a short period of time

- Summarizing data.

Drawback to keeping less data:-

- harder to investigate security incidents
- Other solution: data compression

Tools

A variety of tools for maintaining security logs:

- *Event Viewer* on Windows systems
- *syslog* on UNIX and Cisco IOS devices

Most contemporary operating systems support audit event logging because of requirements in the Common Criteria for Information Technology Security Evaluation, an international standard for computer security certification

.