

# SECURITY ARCHITECTURE

.....

*Shih planned to make a great wall by extending and enlarging preexisting walls made by previous rulers. This ‘great’ wall would serve as a barricade to keep out all tribes that wanted to invade China. It also served to separate the civilized acts of the farmers in China to the barbaric acts of the nomadic tribes.*  
— **Anonymous essay**

## INTRODUCTION

.....

Creating a secure environment for computing takes planning and careful consideration. The security models previously discussed (Bell-LaPadula, Biba, and Clark-Wilson) can be implemented on any scale required. From configuring a single stand-alone system, to designing an enterprise network, the models are designed to be scalable. Security models can be applied to any network or system architecture. It is not necessary to use the model in its pure form, but it is desirable to take pieces that fit into the overall design from various models and theories. Securing a network begins with internal system security. A high percentage of all loss to businesses is from internal threats. Securing the network from external intruders will mitigate only a percentage of internal risks. If systems are secure and audited frequently, internal risks can be minimized. The security architecture of a network is partly based on the security of each system attached to it. Security architecture also applies to network devices, such as routers, switches, gateways, and wiring.

### Objectives

- 1 Discuss security architecture theory.
- 2 Explain system security architecture.
- 3 Describe secure network architecture.

## Key Terms

**Access Control List (ACL):** a set of data that informs a computer's operating system which permissions (or access rights) users or groups have to specific system Objects

**Content Filtering:** intercepts and evaluates network traffic based on payload content; frequently used for HTTP and SMTP traffic

**Reference Monitor:** abstract machine, mediates all access subjects have to objects

**Reference Validation Mechanism:** validates each reference to data or programs by any user (program), against a list of authorized types of reference for that user

**Resource Isolation:** enforces access controls, and separates resources from one another

**Restriction:** prevents unauthorized access to logical segments of a network and system

**Security Architecture:** a principle that describes security services as a system

**Security Kernel:** includes hardware, firmware, and software, and is the central component of the TCB mechanism(s)

**Segmentation:** provides a method for collaboration between coworkers, and prevents access by others in an organization

**State-Machine:** a security model that says if a system begins in a secure state and all transactions are secure, the system will remain in a secure state

**System Security:** actions required to reduce an individual system's vulnerability to acceptable levels

**Trusted Computing Base (TCB):** level of trust assigned to a complete system

**Virus Filtering:** reviews incoming and outgoing packets for malicious code

## SECURITY ARCHITECTURE THEORY

A variety of models have been created for security architecture. **Security architecture** is a principle describing security services a computer system is required to provide to meet the needs of its users, system elements required to implement the services, and performance levels required to deal with threats. These security models are the baselines for implementing and developing security in a networking and systems environment. The models can apply to technical, administrative, and physical controls, but are generally associated with logical system access.

### State Machine

The **state-machine** model says if a system begins in a secure state and all transactions are secure, the system will remain in a secure state. Subjects must access objects securely, and maintain consistency with the security policy. If all activities are processed in a secure fashion, the system will execute securely.

### Trusted Computing Base

As stated in the Department of Defense publication “Trusted Computer System Evaluation Criteria”, also called the Orange Book, the **Trusted Computing Base (TCB)** refers to “the reference validation mechanism, be it a Security Kernel, front-end security filter, or the entire trusted computer system.”

The heart of a trusted computer system is the TCB, containing all elements of the system responsible for supporting a security policy. The TCB also supports the isolation of objects on which protection is based. A TCB should be as simple as possible, consistent with the functions it is required to perform. The TCB includes the following:

- hardware
- firmware
- operating systems
- applications
- components

The TCB is an evaluation method for assigning the level of trust placed on a system. The Orange Book uses four classifications of trust, starting with the lowest level, D, to the highest level, A. The general TCB categorization is:

- A — Verified access, highest level of Trust in a system
- B — Mandatory Access Controls
- C — Discretionary Access Controls
- D — Untrusted, or not evaluated

A detailed list of TCB categories is available in the Orange Book. Products are tested, using a standard methodology, against the evaluation criteria. Once testing is completed, a rating is given to the product for a specific environment.

The TCB is critical to protection, and must be designed and implemented so system elements excluded from the TCB need not be trusted to maintain protection. Identification of the interface and elements of the TCB, along with their correct functionality, forms the basis for evaluation.

## Reference Monitor and Security Kernel

In 1972, the Computer Security Technology Planning Study produced the Anderson report for the United States Air Force. In this report, the concept of a **reference monitor** that “enforces the authorized access relationships between subjects and objects of a system” was introduced. The reference monitor concept is an essential element of any system, providing multilevel secure computing. All transactions passing from a subject to an object must be authorized by the reference monitor.

The Anderson report defines the **reference validation mechanism** as an implementation of the reference monitor concept, “that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user.” A reference validation mechanism:

- must be tamperproof
- must always be invoked
- must be small enough to be subject to analysis and tests, the completeness of which is assured

The **security kernel** includes hardware, firmware, and software, and is the central component of the TCB. The security kernel is the implementation of the reference monitor, used to enforce the reference monitor concept.

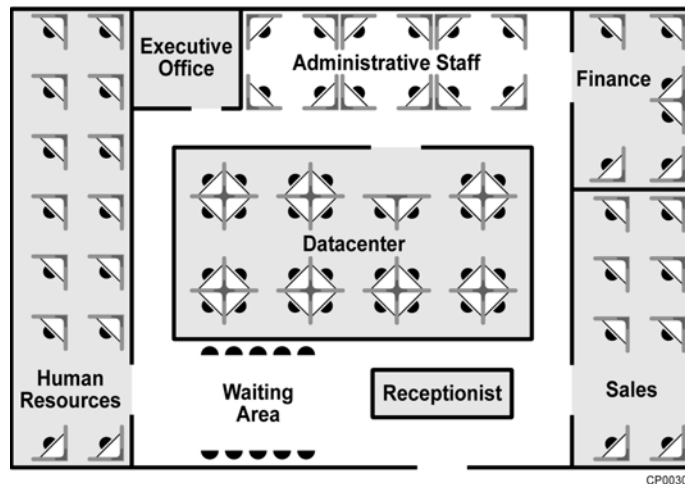
## Resource Isolation

The objective of **resource isolation** is to enforce access controls, and to clearly separate resources from one another. Segmenting resources allows a high degree of modularity, enabling:

- activity tracking
- enforcement of accountability
- unique identification of each subject and object
- independently assigned permissions and rights for subjects

Isolating resources on a network includes physical and logical separation of user populations and server areas. For workstations, resource isolation can include separating low-level processes from reading or writing to memory segments of higher-level processes.

When planning to separate resources on a network, organizational layout and business processes must be well defined, otherwise, employees could suffer work interruptions, and automated transactions might experience interference. As with any security initiative, upper-level management should drive support for a plan that either creates resource isolation for a new network, or restructures an existing network.



Physical Isolation in an Office

## SYSTEM SECURITY ARCHITECTURE

.....

A network cannot be secure if individual systems themselves are not secure. If one system is compromised, the remainder of the network is in peril.

### System Security

Providing **system security** begins with an appropriate operating system. The operating system requires users to log in, using an individual user name and password or other authentication mechanism. Operating systems provide directory and file-level access controls, providing users granular read, write, and execute privileges. An OS is thus installed in a secure manner, which means only authorized personnel install operating systems and applications on workstations and servers. Operating systems are installed from original media, or from a trusted networked system.

#### DEFINING GROUPS

Groups are defined on systems to ease administration issues. As users are added to a system, they are given the same rights and privileges as other users who perform similar job functions. Assigning rights to each individual user would create administrative chaos, making it nearly impossible to determine which users have access to available resources. Using groups to manage user privileges assists in preventing access creep, where users collect access privileges over a period of time.

#### DEFINING USERS

Users, including security administrators, should have individual accounts on systems. Using a generic user name and password for all users, or even just security administrators, provides users with anonymity that prevents useful logging and auditing. If each person who accesses a system uses his individual login name and password, his actions can be traced. Account and password sharing should be discouraged through security awareness training.

#### MONITORING SHARED DIRECTORIES

With most modern operating systems, sharing files and directories is a relatively trivial task. Shared files and directories need monitoring periodically, to ensure only appropriate personnel have access, inappropriate material is not available, and sharing is accomplished by following strict guidelines. There have been cases where employees find it easier to share an entire drive, rather than sharing a particular file or directory. This can lead to exposure of sensitive or classified materials, and should be monitored and prevented.

**PHYSICAL SECURITY**

The level of physical security for a particular system is evaluated on a per-system basis. For instance, workstations do not need to be physically secured for the average employee. If the employee is in a sensitive area of a company (such as the Human Resources department), it may be desirable to place the employee in a separate room that either has badge access, or can be locked.

Servers and other network-related systems are placed where only IT staff can access them. The area can be large, like a data center, or smaller, such as a server room or wiring closet. Access to these areas is restricted to required personnel, and logged and audited when possible.

Physical security prevents direct access to systems. If physical access is possible, systems can be damaged, stolen, or modified in an undesirable way.

**DEDICATED SYSTEMS FOR DEDICATED SERVICES**

Computing systems should not have excessive services or applications installed. Each operating system comes with many services installed and running by default. These services provide multiple entry points into a system if they are not disabled. There is little need for most workstations to have FTP, Web, telnet, or SMTP services running. The more services running on a system, the more vulnerabilities that are available for threats to gain access to computing resources. Only services required for operation of a system should remain enabled. This is particularly true for servers and gateways. If applications are not needed, they are removed from a system. This assists security administrators with software-licensing issues, and removes possible problems caused by conflicting services and applications.

Server systems, in particular, need to adhere to this guideline. A server typically has a single purpose, which can include serving as a(an):

- file server
- FTP server
- Web server
- application server
- database server
- authentication server
- access-control gateway

Each service is placed on a separate system. If there are multiple services running on a server, it creates vulnerabilities for risks to become realized. More services require more open ports on a system, to receive legitimate traffic. These open ports provide more opportunities for exploits. Ports also cause issues if applications and services need to use the same port for communication. With more services and applications, more patches need installation on each system. This has the probability of causing conflicts between installed software, and additional administrative effort to keep patch levels current.

This distribution of server systems creates additional hardware administration, however security and network integrity are more easily maintained. The software administration is no different than if multiple services are placed on the same system. The number of applications and services does not change, simply the number of systems in place.

#### **Multiple Services on a Firewall**

If services such as FTP or HTTP are running on a system acting as a network's firewall, it can lead to a compromise of the host. The firewall system should not accept any inbound connections itself, but may act as a proxy, or application gateway, for network traffic.

If FTP or HTTP services are installed, inbound connections must be allowed for these services. If there is an exploitable vulnerability in these additional services, the firewall host can be compromised, leading to further confidentiality and integrity issues deeper inside the network. This defeats the purpose of having the firewall host.

Workstations may be multipurpose, with various applications installed to facilitate a job function. The number of applications and services installed on workstations is normally dictated by business needs, and management decisions. Using the least privilege principle, ensure that if an employee changes job functions, his installed applications are reviewed to verify they are required for the new job function. Besides making application licenses available for use elsewhere, applications could be used to access data employees no longer need to do their jobs. A loss of data confidentiality and integrity is possible.

## OS Hardening

OS hardening is the process of making a computer's operating system as secure as possible. Many operating systems load with a variety of services enabled by default. They may also have known vulnerabilities. Before a machine is placed in a production environment, appropriate measures should be taken to remove unnecessary services and correct known vulnerabilities. The suggestions provided here are not exhaustive. Operating system manufacturers and user groups are good places to begin looking for additional information on OS hardening.

### INSTALLATION

The best place to start securing the OS is during installation. If the computer's purpose is to provide services, install a server-class operating system. Place the system in an isolated environment. During the configuration process, systems should not be connected to a live network or the Internet, to reduce the risk of exploitation. When loading service packs and hot fixes, download the software to another system, then burn a CD-ROM. Most operating systems have options that allow you to 'customize' the installation. Do not use default installation settings. Use an installation option that allows you to select which services will be installed, and know what you are choosing to install.

### CONFIGURATION

After installation is complete, determine which services are running and which ports are open. You should be able to identify every service or process listed. Following the installation, install the latest service pack and hot fixes. Staying current with the latest exploits is critical for a secure system. After installing service packs and hot fixes, check the system again, to make sure only the services and process you want running, are running. Remove or disable all unnecessary services. Test the system to confirm it responds only to the type of communication it is supposed to receive.

### USERS AND GROUPS

Change the user name and password for default administration accounts. Each system user, including administrators, should have his or her own account. Remove or disable unnecessary default users and groups. Check for inappropriate associations, and disable any that are not needed for the system to function. For example, a firewall should not be a member of a Windows domain.

## Patches

Patches are software modification utilities. Patches are usually provided by the software vendor, though they may be available from other sources. Patches can include new product features, code changes to make software more robust or efficient, and corrections for security problems. The names used for patches vary, but you may encounter patches under the names:

- patch
- hot fix
- service pack
- feature pack

All patches should include release notes, a document describing what the patch does. Never install a patch without reading the release notes and understanding *exactly* what the patch will do to your system.

### **ACQUIRING PATCHES**

Patches should always be acquired from a trusted source. As mentioned previously, patches are usually provided by the software vendor. However, patches may be available from other sources. When acquiring a patch, consider the source's integrity. If you are downloading patches from the Internet, confirm the MD5 checksum on the patch you acquired matches the checksum provided by the distributor. If the distributor does not provide MD5 checksums, ask them to start doing so, for their protection and yours.

### **INSTALLING PATCHES**

Do not install untested patches on production systems. Even if you trust the patch distributor's integrity, you cannot be certain how your system will react to the patch. Test patches on a development machine whose hardware and software matches the production target as closely as possible. Use the test machine to determine if the patch affects production or security in a negative way. Some patches will reinstall or enable services you removed or disabled when hardening the OS. Other times, a patch may require software you removed when hardening the OS. After installing a patch, test the test machine to confirm on the services and processes that should be running are running. Test the machine to confirm the machine only responds to appropriate communications. Once the patch is validated in a test environment, plan production installation. Include testing the production machine in your installation plan.

## SECURE NETWORK ARCHITECTURE

Ideally, a secure network architecture is designed before any systems are in place. Realistically, security professionals are more likely to find themselves attempting to make existing networks more secure. Networks tend to evolve in an organic fashion. Only after individual systems and policies are in place, does work usually begin on designing the network security infrastructure. When possible, design the network security architecture while designing the network.

### Isolating User Populations and Servers

The logical separation of user populations from one another plays an important role in establishing a secure network. Segmenting user populations allows users to be logically grouped by job function, role, or department. **Segmentation** provides a method for collaboration between coworkers, and prevents access by others in an organization. Need-to-know access is used within a departmental network segment. Least privilege is enforced using a network device, such as a router with an **Access Control List (ACL)**, between network segments. An ACL is a set of data that informs a computer's operating system which permissions, or access rights, users or groups have to specific system objects.

Placing network servers on a separate logical network segment allows access-control devices to enforce access, as defined by an organization's security policy. This helps establish layered security within a network. If a particular server is compromised, it can be used as a launching point for further attacks or intrusions. However, if a network is segmented, access to other server areas or user populations can be limited by effective ACL or firewall use.

Placing user and server populations on different segments allows the generation of audit trails from the gateway devices. Most devices used to segment networks are able to log access and traffic, which is later audited and used to verify security policies are being enforced.

### Restricting Access

Access **restrictions** are placed on gateway devices connecting network segments. Restrictions can also be placed on individual systems, and for access to networks. These restrictions assist in increasing security for networks, by preventing unauthorized access to logical segments of networks and systems. (This topic is discussed in the Access Control Models chapter of this book.)

**SYSTEMS**

Most operating systems require user names and passwords for access. Some operating systems have methods to prevent user access from the local console, allowing only network access to files and applications. For server systems, only security administrators should have local console access. Users are required to authenticate themselves, using their individual user names and passwords. Access restrictions for workstations are enabled to prevent snooping, manipulation of data, and unintentional deletion or modification of data. If a workstation is operated by a single user, no other users, except Security Administrators, should not have access rights. If a system is shared among several users, file separation is enforced, as with NTFS partitions in Windows NT/2000, to enforce data confidentiality and integrity, by preventing users from viewing each others' files, unless they are deliberately shared.

**CONNECTIVITY DEVICES**

Restricting access to network connectivity devices is a critical aspect of secure network architecture. Network connectivity devices, such as routers, switches, and hubs, provide and control access for many users. Like servers, the failure of a network connectivity device restricts the availability of information assets for many users. Default passwords should never be used for network connectivity devices. Only trained personnel should be allowed to modify configurations. A well-meaning, but poorly trained, junior network administrator can cause as much damage to the security of network connectivity devices as an army of malicious crackers. Physically securing network connectivity devices is also a priority. Disconnecting cables is a very effective denial of service technique.

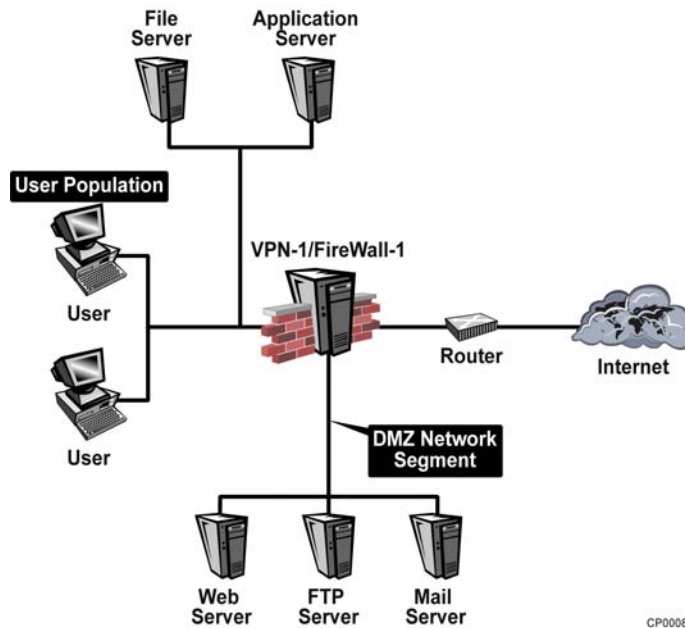
<b>Bad Locations for Network Connectivity Devices</b>	
To save money, organizations will often compromise their security by placing network connectivity devices in insecure locations. All of the (real, actually seen) locations in the list below put network connectivity devices at risk:	
broom closets (where any member of housekeeping has a key)	machine rooms (in a facility that uses steam and chilled water for climate control)
under the desk of the (non-technical) IT manager	lobbies, break areas, and conference rooms
next to EMP-emitting machines on a factory floor	on the HVAC units in warehouses

Place network connectivity devices in secure areas only accessible by IT staff.



**NETWORK SEGMENTS**

In some cases, one user segment must be prevented from sending network traffic to another. This can be accomplished by placing ACLs on a separating router or gateway device. Traffic can be filtered by the IP address of the source, or prompted for authentication before allowing the traffic to pass.



Logically Segmented Network

<b>Research versus Production</b>
<p>An example of why network separation is important is illustrated in the following situation between the research-and-development (R&amp;D) staff, and production staff in Company XYZ. Company XYZ produces desktop computers, and writes its own code for the BIOS firmware.</p> <p>The production staff accidentally begins using beta BIOS code it pulled from an R&amp;D server on the production line, before it is fully tested and ready for release. There are still bugs in the code that prevent XYZ systems from starting successfully. This will create an unfortunate consequence for the production staff, once the systems begin their testing and burn-in phase.</p>

**PHYSICAL SECURITY**

Physical access to network devices and corporate servers should be severely controlled. Only appropriate IT personnel should have access to network hardware and wiring. Allowing access to any employee could cause theft, denial of service, loss of data Integrity, or a loss of data confidentiality.

Using keyed locks to secure areas where network-related equipment and wiring is located, is the simplest form of physical security. This prevents most opportunistic compromises. Using smart cards is an alternative that provides logging and auditing capabilities. Biometric authentication and authorization can also be used. Of course, a combination of these methods provides a higher level of security than does a single security mechanism.

Drop ceilings should be examined when determining physical security of a server or network-device area. In some office buildings, walls are built as simple partitions, segmenting rooms to reduce noise and provide physical separation of departments. These walls frequently do not rise to the actual ceiling, but rise to a drop ceiling. Drop ceilings provide wiring and environmental space, and are easy to identify by ceiling tiles. If the walls around a network area do not rise to the ceiling, individuals can violate the area, by climbing through the crawl space over the partition walls from an adjacent space. This type of intrusion can defeat any keyed lock used on the area door.

**Gateway Security**

Security of an organization's gateway to external networks, internal networks, or the Internet is a concern for maintaining confidentiality and integrity of data. Availability of an organization's gateway is critical, when Web and other services are delivered to customers. If the services are not available, customers cannot access the data they require to do business with the organization. Generally, the gateway system is the most secure system on the network.

**VIRUS FILTERING**

**Virus filtering** can be performed on some gateway systems, and controls access to a network by analyzing incoming and outgoing packets. Viruses can be filtered from downloaded files, and from harmful ActiveX, Java or other applets. To perform virus filtering, network traffic is passed to a virus-scanning server that reviews the payload of a packet to determine if a virus exists. If not, the packet continues to its destination. If a virus is located, the packet terminates at the virus-scanning server, preventing it from infecting the network.



**CONTENT FILTERING**

**Content filtering** helps reduce exposure of an organization to unwanted materials available on the Internet. Content filtering can filter e-mail, HTTP, and FTP traffic, for materials defined as undesirable in an organization's security policy. Content filtering servers use a method similar to virus-scanning servers, where network traffic is intercepted and evaluated before being passed to a destination system.

## EXERCISES

---

### Activities

- 1 Design a small, secure network. Include a gateway to the Internet, Web server, FTP server, and user workstations. Include appropriate security techniques for securing each level and device on the network.
- 2 Consider a facility you use regularly. Suggestions include classrooms, offices, and libraries. Design a network to address the security needs of the facility you selected. Defend your conclusions.

### Ethical Dilemma

You are taking a class on network security at your local community college. Your instructor demonstrates a technique to exploit an operating system vulnerability. At work, you discover the file and print server is running the vulnerable operating system. You would like to test the file and print server to see if it is vulnerable. You think the test will do no harm, and you intend to report the results to your supervisor.

- What should you do?
- What if you are the network administrator?
- Does that change your course of action?

## Review Questions

- 1 What is the security kernel?
- 2 What is the objective of resource isolation?
- 3 Why should each system user, including administrators, have an individual account?
- 4 List several reasons for segmenting user populations.

## Answers to Review Questions

### 1 What is the security kernel?

*The security kernel includes hardware, firmware, and software, and is the central component of the TCB. The security kernel is the implementation of the reference monitor, used to enforce the reference monitor concept.*

### 2 What is the objective of resource isolation?

*The objective of resource isolation is to enforce access controls, and clearly separate resources from one another.*

### 3 Why should each system user, including administrators, have an individual account?

*Using a generic user name and password for all users, or even just security administrators, provides users with anonymity that prevents useful logging and auditing. If each person who accesses a system uses his individual login name and password, his actions can be traced.*

### 4 List several reasons for segmenting user populations.

*Segmenting user populations allows users to be logically grouped by job function, role, or department. Segmentation provides a method for collaboration between coworkers, and prevents access by others in an organization. Need-to-know access is used within a departmental network segment. Least privilege is enforced using a network device, such as a router with an Access Control List (ACL), between network segments.*

**Suggested Reading/Resources**

- “Department of Defense Trusted Computer System Evaluation Criteria.” DOD 5200.28-S; Library No.S225,711 August 15, 1983:<http://www.radium.ncsc.mil/tpep/library/rainbow/index.html>
- Anderson, J. P. “Computer Security Technology Planning Study.” ESD-TR-73-51. Volume I, October 1972, NTIS AD-758 206.
- Bell, D. E., and L. J. LaPadula. “Secure Computer Systems: Unified Exposition and Multics Interpretation.” Revision 1, March 1976, MTR-2997.

