Chapter 4

The JES Security Model

The purpose of this chapter is to introduce and define the various layers of the JES Security Model. We'll also look at how the layers work together to provide a secure processing environment. In the chapters that follow, we'll take a more detailed look at the physical, technical, and administrative areas in each of the model layers.

Upon completion of this chapter, you'll be able to discuss:

1. The importance of a *layered approach* to protecting information resources
2. The layers of the *JES Model* and how they work together to provide a secure processing environment
3. How the JES model meets *confidentiality, integrity*, and *availability* requirements

Just Enough Security

The Just Enough Security (JES) model is based on the premise that it takes *layers* of controls to effectively protect information assets. Also known as "defense-in-depth", layered security can take on a variety of forms. The JES model is my take on a model for planning, implementing, and managing an organization's Information Security effort. Figure 4-1 depicts the JES approach.

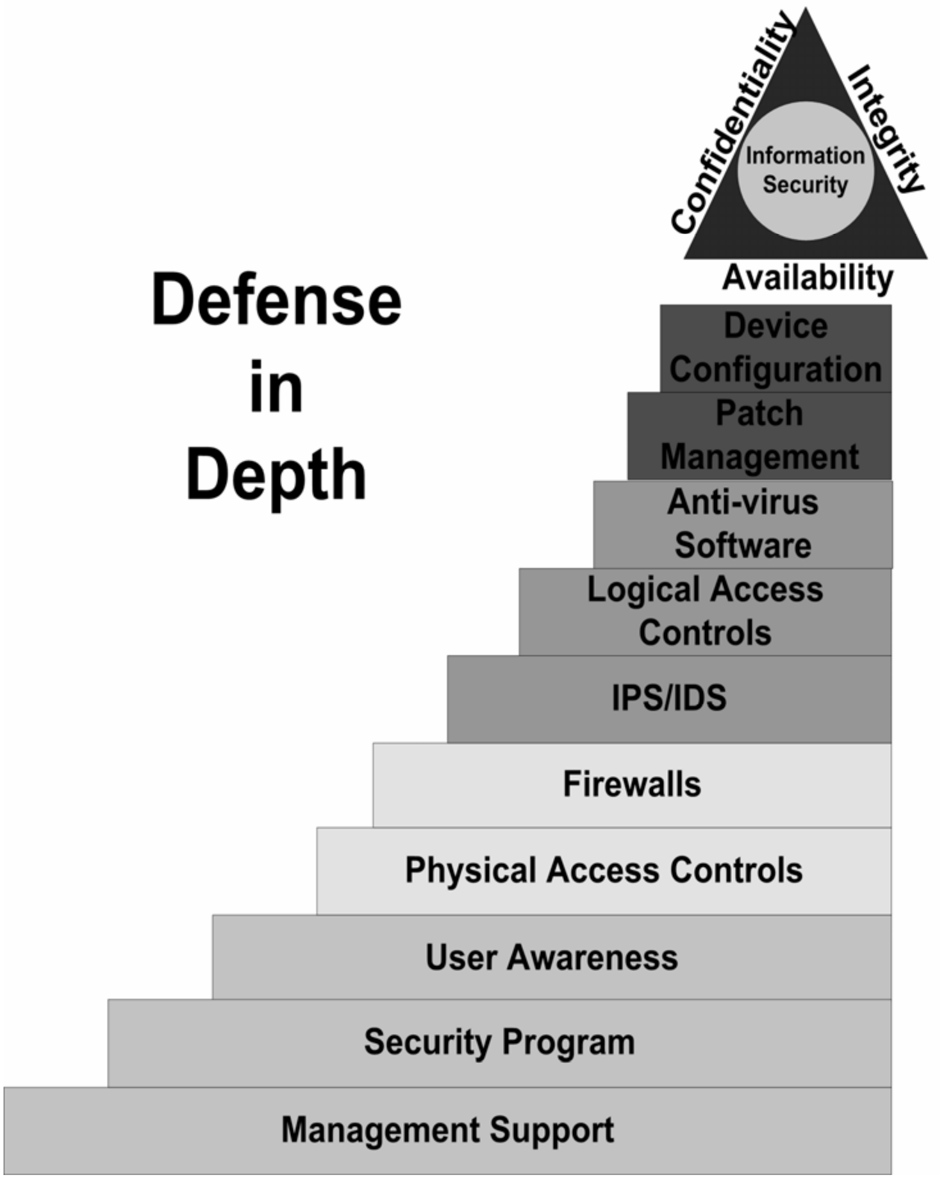

Figure 4 - 1: JES Model

The objective of layered security is to implement a variety of controls that work in concert to neutralize the efforts of a threat agent. A threat agent attempting to compromise the confidentiality, integrity, or availability of a system protected by a layered security environment must pass through several different tests before reaching its target. These layers comprise administrative, physical, and technical safeguards. To be truly effective, this model must extend to all company owned devices, whether located on the company network, at home, or at a customer site.

Is it necessary to implement all layers to ensure security? Not necessarily. That's the point of JES. Which layers to implement, and to what extent, is a risk management decision. Chapter 3 defined a risk management process designed to help make informed decisions about the layers, and the controls at those layers, on which to focus security resources. In the following sections and chapters, we'll look at each layer and how it fits into an overall security effort.

Management support

The foundation of any security program is management support. This support should be comprised, at a minimum, of effective policies, adequate budgets, and consistent enforcement. Efforts to change user behavior and to implement security measures carry no weight unless there is visible executive support from all levels of management. Visible support isn't just the hanging of a few posters around the lunch room. Effective support is evident in the project approval process, in the presence of a meaningful awareness program, and in how management deals with violations of security policy. It's reinforced in management and employee meetings, memos, and if appropriate, the annual report. In other words, management support of information security should be manifested as a part of the organization's culture.

Security program

An organization's security program defines and facilitates the security objectives of management. It consists of policies, procedures, standards, and guidelines. Policies are high level statements of management's goals and objectives. They don't provide step-by-step directions to reach those goals and objectives; such directions are provided by procedures. A policy should consist of at least three elements:

1. Purpose
2. Scope
3. Compliance

The purpose of the policy clearly explains the objectives it's intended to achieve. It should also reflect management's commitment to a secure enterprise. Scope describes all enterprise technology and activities affected by the policy. Finally, compliance defines consequences if the policy is not followed. It's the compliance piece – necessary to strongly encourage implementation – that's often missing from security policies.

Procedures are the administrative, physical, and technical recipes for producing a secure enterprise. They're derived from and support management policies. The step-by-step nature of procedures helps to ensure consistent compliance with security policy.

Along with procedures that support security policies, standards and guidelines form the security handbook of an organization. Standards are mandatory configurations and approaches to technology implementation. Guidelines assist implementers and managers with issues that are not specifically covered by standards; they aren't mandatory.

User awareness

Unless fully engaged in the company's security efforts, end-users can be an organization's greatest threat. Continuous awareness training is the best way to obtain end-user participation in a security program. Training should include:

1. Review of policies, standards, and guidelines
2. Implementation and configuration procedures
3. Password protection
4. How to deal with social engineering attacks
5. Proper protection of workstations
    a. Logging off before walking away from a device
    b. Use of systems by unauthorized users
    c. Elimination of potential **shoulder surfing** opportunities
6. Proper handling of PDAs, laptops, cell phones, etc.
7. Proper handling and disposition of media
    a. Backup tapes
    b. CD-ROM
    c. Floppy disks
    d. Other types of storage devices

Key Terms

Shoulder Surfing – *When a person looks over another's shoulder to see what keys she presses to enter her password, that's shoulder surfing. Shoulder surfing is a term used to describe any activity whereby a person watches a user perform some action that may result in the unauthorized and unintentional revelation of confidential information.*

User awareness should begin with new hire orientation. Existing employees should receive training at least annually. In addition to formal training, daily reminders should be everywhere in the workplace; posters and login messages are two good vehicles for reminder distribution. Managers should talk about security whenever appropriate during daily interaction with staff. Finally, first line managers must ensure that attention to security compliance is part of every operational task.

Physical access controls

The effectiveness of the security program is directly proportional to the effectiveness of the physical access controls surrounding information assets. Strong passwords, biometrics, and other logical access methods will not prevent the financial loss associated with the theft or physical destruction of critical business systems. Further, the level of effort applied to extracting information from secure devices within the normal business environment will probably fall far short of the effort applied in a cracker's basement.

Physical access controls include locked doors, cable locks, and security personnel. Only IS personnel whose day-to-day duties require it should have physical access to your data center. Also, educating users on the proper physical control of laptops, PDAs, and other mobile devices is an important factor in the prevention of information loss or compromise. This includes immediate notification of the appropriate manager if a portable device is lost or stolen.

Firewalls

The term "firewall" was traditionally used to describe a barrier that prevented fires from spreading. In a network, a firewall serves a similar purpose; it protects an organization's network from malware and other threat agents seeking to enter through connections to the Internet or other external networks. These connections are usually your network's weakest points. You can also place a firewall at the entry point into each subnet containing your most critical information. This helps prevent threat agents already on your network from spreading to your mission critical systems. So what is a network firewall?

A network firewall is a collection of programs that protect the resources of a private network. These programs can reside on a device designed to act as a firewall or on a server configured to act as a firewall. In either configuration, the firewall performs the same basic function; it inspects packets to determine if their content matches the criteria required to pass through to your internal or protected network. The types of packet inspection are covered in more detail in Chapter 6.

IPS/IDS

There are two primary types of Intrusion Protection Systems (IPS) -- network and host. Network-based IPS systems protect the entire network or a network segment.

Host-based IPS systems reside on and protect individual systems. The same is true of Intrusion Detection Systems (IDS). The primary difference between IPS and IDS is how each reacts to a potential attack. An IDS device reports the attack so that a human can react. Once an IPS device detects an attack, however, it can react automatically based on rules you set up. Most devices today combine IPS and IDS.

In an ideal environment, malicious code and unauthorized users are always denied access to critical systems. The protections in an ideal environment prevent authorized users from destabilizing their systems as well as the network. But who works in an ideal environment?

Host-based IPS is a layer of protection that attempts to "catch" activities not blocked by the layers lower in the JES model. These activities include, but are not limited to:

1. Deleting files
2. Moving files
3. Copying files
4. Installing executable files
5. Registry modifications
6. Denial of service processes

Network IPS looks at network traffic, attempting to recognize attack patterns and behavior. Once a potential attack is identified, the IPS device can block traffic, shut down one or more services, or a number of other actions you define. This topic is covered in Chapter 7.

Logical access controls

Logical (technical) access controls include hardware or software components that prevent either unauthorized users from gaining access to information resources or authorized users from gaining access to information for which they have no data owner authorization. Logical controls include passwords, biometrics, and tokens. Regardless of the controls used, they should:

1. Have minimal impact on end-user productivity
2. Be reliable
3. Be effective with a ROI resulting from their initial and ongoing deployment costs

How logical controls are implemented is just as important as which controls are selected. The following is a list of guidelines.

1. Relying on strong, easy to forget passwords may be a mistake for your organization. Strong passwords consist of upper case and lower case letters, numbers, and one or more special characters. Users often post strong

passwords on their monitors or in other office locations that are less conspicuous but just as accessible. If you choose not to use strong passwords, make sure you look at a **compensating control**.

2. Establishing an effective account policy is crucial to a logical access control implementation. The policy should include
   a. Automatic password expiration, usually 60 to 90 days
   b. A minimum password length, typically 6 to 8 characters
   c. Password history to ensure that a password is not reused when it expires
   d. A threshold of login attempts that when exceeded locks the user account, usually set at 3
   e. An effective lockout duration that will deter **brute force attacks**

Finally, it is a good idea to combine password controls with another access control, such as biometrics. This is known as **two factor authentication**. If a password is compromised, the second control will help stop unauthorized use of system resources.

Key Terms

Compensating Control – *A compensating control is a process or technology that helps to make up for the lack of a primary control. For example, if your organization insists on assigning weak passwords to the local administrator accounts on your servers, a compensating control might be to implement much stricter controls on physical access to the data center. Since local accounts are used by someone actually standing at the server keyboard, imposing strong physical access restrictions can help reduce risk.*

Brute Force Attack – *There are two types of password attacks: dictionary and brute force. In a dictionary attack, a cracker compares a list of dictionary words to each password. This is the fastest method, since most users invariably use common words found in the dictionary for their passwords. If a dictionary attack fails, a cracker will often try a brute force attack. In this type of attack, every letter, number, and special character combination is compared against the list of passwords. If given enough time, a brute force attack can crack almost any password.*

Two Factor Authentication – *There are three principle approaches to*

authenticating a user to a system or network. These approaches include the use of something you know, something you are, or something you have. An example of something you know is your password. Your fingerprint is an example of something you are. A ***token*** *is an example of something you have. The use of any two of the three approaches is called two factor authentication.*
Token – *A token is a physical object, usually about the size of a credit card, that identifies the person carrying it to a system or network. A token is typically used with a PIN.*

Antivirus software

Malicious code attacks are the most common type of penetration into a company's internal network. According to the CSI/FBI 2005 Computer Crime and Security Survey (www.gocsi.com), almost 33% of business losses related to security incidents are from virus attacks.

Why, when 96% of the nearly 700 respondents to the survey have an antivirus solution in place, did virus attacks retain the number one position? One explanation is the theory that target organizations often incorrectly report denial of service attacks as virus attacks. Another cause may be the failure on the part of many organizations to maintain current virus signature files. Hundreds of new worms and viruses are released each month. Without a consistent effort to keep antivirus solutions current and operational, every end user device in your network is a potential open door into your network. This is especially true of email systems.

Email has become one of the primary tools used by propagators of malware. Unsuspecting users opening attachments or distributing apparently harmless chain email can cause internal infections even on networks with a perfectly configured firewall perimeter. Make sure you're aware of the types of attachments allowed to pass through your email system. For example, any type of executable file is a threat and should be stripped from a message before it's delivered.

Another point of entry may be home devices connecting to your network. Unless you implement a remote access solution that checks for the presence of an operational and up to date antivirus package, you are opening a gaping hole in your security perimeter. New technologies, such as **SSL VPN**, provide the means to check for **personal firewalls** and antivirus applications before allowing a device access to internal resources.

But no matter how up to date you keep your antivirus solution, there is always a delay between the time new malicious code is identified and when your software vendor provides an update.

Key Terms

SSL VPN – *A VPN, or Virtual Private Network, is a secure connection between two points, usually at distant locations across the Internet. A VPN connection is often more secure than one with a device on the same internal network. The common method of implementing VPN is with IPSec (Internet Protocol Security). However, a new VPN technology is emerging based on SSL (Secure Sockets Layer). SSL uses certificates and public and private key encryption technology. SSL VPN brings more functionality to the network administrator and is usually much easier to implement than a traditional IPSec VPN implementation.*

Personal Firewall – *A personal firewall is an application that resides on and protects an end-user device from external threat agents. It operates in much the same way as a network class firewall.*

Patch management

Unless a system is properly **patched**, an attacker can take advantage of one or more of the many publicly known vulnerabilities. Organizations that delay the implementation of an effective patch management process may face increasing costs associated with attacks that exploit these weaknesses.

Patch management, as referenced in our model, is a set of policies, processes, and tools employed to ensure that all systems are at the proper patch level. Processes include:

1. Checking vendor resources for new patches
2. Checking systems for current patch level
3. Regularly testing and applying patches to operating systems, **firmware**, and business applications

These processes can be very time consuming and expensive if done manually. Many larger organizations are prime candidates for one of the many automated patch management solutions available today. Patch management is covered in further detail in Chapter 7.

Key Terms

Patch – *A patch is a small fix to a program that corrects a problem. Security patches are regularly released by software and hardware vendors to eliminate newly discovered vulnerabilities in their products.*

Firmware – *Put simply, firmware is a program on an integrated circuit or "chip". Many hardware devices contain firmware that performs tasks ranging from boot up activities to fundamental operating and housekeeping tasks.*

Device configuration

Device configuration vulnerabilities are prime targets for malicious attacks. There are two primary paths to secure device configurations. First, we must continue to apply pressure on software vendors to distribute applications in "secure mode". In other words, when I install an application it should install in a secure state. All **services** and add-ons that allow potential network or malicious code access to my system should be disabled by default.

The second path relies on the secure deployment of systems that may not yet support a secure state installation. This is known as "system hardening." System hardening includes:

1. Keeping business applications and operating systems at the most current version. This provides not only the ability to take advantage of new security features; it also ensures the availability of security patches.
2. Ensuring that all systems require appropriate authentication.
3. Ensuring that remote access for the purpose of administration or support is controlled by strong authentication methods.
4. Disabling any service or port that isn't required for the intended function of the system
5. Controlling device configurations through the use of standard system images that are locked to prevent modification.
6. Using the security features included in the operating system to restrict access to information.
7. Ensuring systems are properly configured to perform backups.

Device configuration is one of the layers over which you have a great deal of control. Make sure you take advantage of it. A detailed look at configuration management is located in Chapter 7.

Putting It All Together

Each of the layers in the JES Model supports the layers below it. Let's take a quick walk up the model to get a better idea of the relationships.

Strong *management support* is necessary to create a business culture in which information security is integrated into each daily task. Guidance on how to apply security is contained in the *security program***.** It's through the use of the security program that technical and non-technical employees are given the tools - in the form of policies, standards, guidelines, and procedures - necessary to protect information throughout the enterprise. Employees are trained on and continuously reminded of their roles and responsibilities in the protection of information assets through a strong *user awareness* program. These first three layers form the administrative foundation of a secure environment.

Physical access controls prevent intruders from performing unauthorized tasks, as defined by policies, standards, and guidelines in the security program, that require actual physical contact with a system. These tasks may include the theft or destruction of one or more components of a system, laptop, PDA, etc. *Firewalls* are placed at entry points in the network perimeter as well as into subnets containing sensitive data. They allow only the traffic defined in the policies and standards of the security program to pass. Together, physical access controls and firewalls work to prevent unauthorized access to critical areas of the network. However, if an intruder cracks a network firewall, he still has no direct access to information resources.

Logical access controls begin their work once the firewalls and physical controls allow general access. In order to directly access information resources on servers and workstations, an intruder must authenticate to the target system. Authentication may include entering a user ID and password, using a biometric device, a token, or a combination these. *IPS/IDS* devices or software help detect and prevent the activities of threat agents that have gained unauthorized access to the network or to a specific resource. They can also help prevent the installation of malware onto servers and end-user devices. Finally, IPS/IDS solutions can detect and react to attempts to circumvent logical access controls by, for example, dictionary or brute force attacks. *Anti-virus (AV) software* supports the IPS/IDS layer by detecting trojans, viruses, worms, and non-viral intrusions such as spyware that may have circumvented its controls. AV and IPS/IDS software protect against attempts by intruders to gain access to information or resources that either assist in cracking logical access controls or in bypassing them altogether. All the layers up to this point are designed to prevent threat agents from reaching an information resource or detecting and removing a threat agent from the network.

Patch management and *device configuration* form the last line of defense against threats. It's the hardening of systems, through the timely application of patches and the careful configuration of system components that removes the most fundamental security vulnerabilities. Most of the layers below these two serve to protect systems from delayed patch release or implementation as well as weak or nonexistent system security standards and guidelines for secure system configuration.

Chapter Summary

The JES model is just one way of looking at defense in depth. It allows us to visualize the various methods required to fully protect critical or sensitive information assets.

The controls included in the model begin with administrative support and preparation, followed by general access controls. The upper layers help to defend assets from intruders who make it past the controls implemented in the first five layers. Finally, the last two layers form the fundamental last line of defense through due diligence in patching and configuring system components.

This chapter is a summary of how each layer works and interfaces with the other layers. The rest of this book explores these concepts in more detail.