Chapter 5

Securing Hosts and Data

CompTIA Security+ objectives covered in this chapter:

1.6 Explain the impact associated with types of vulnerabilities.

- Vulnerabilities due to: (End-of-life systems, Embedded systems, Lack of vendor support), Misconfiguration/weak configuration

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- DLP (USB blocking, Cloud-based, Email), Hardware security module

2.3 Given a scenario, troubleshoot common security issues.

- Permission issues, Access violations, Data exfiltration, Weak security configurations, Unauthorized software, Baseline deviation, License compliance violation (availability/ integrity)

2.4 Given a scenario, analyze and interpret output from security technologies.

- Application whitelisting, Removable media control, Patch management tools, DLP

2.5 Given a scenario, deploy mobile devices securely.

- Connection methods (Cellular, WiFi, SATCOM, Bluetooth, NFC, ANT, Infrared, USB), Mobile device management concepts (Application management, Content management, Remote wipe, Geofencing, Geolocation, Screen locks, Push notification services, Passwords and pins, Biometrics, Context-aware authentication, Containerization, Storage segmentation, Full device encryption), Enforcement and monitoring for: (Third-party app stores, Rooting/jailbreaking, Sideloading, Custom firmware, Carrier unlocking, Firmware OTA updates, Camera use, SMS/MMS, External media, USB OTG, Recording microphone, GPS tagging, WiFi direct/ad hoc, Tethering, Payment methods), Deployment models (BYOD, COPE, CYOD, Corporate-owned, VDI)

3.3 Given a scenario, implement secure systems design.

- Hardware/firmware security (FDE/SED, TPM, HSM, UEFI/BIOS, Secure boot and attestation, Supply chain, Hardware root of trust, EMI/EMP), Operating systems (Types, Network, Server, Workstation, Appliance, Kiosk, Mobile OS, Patch management, Least functionality, Secure configurations, Trusted operating system, Application whitelisting/ blacklisting), Peripherals (Wireless keyboards, Wireless mice, Displays, WiFi-enabled MicroSD cards, Printers/MFDs, External storage devices, Digital cameras)

3.4 Explain the importance of secure staging deployment concepts.

- Sandboxing, Environment (Development, Test, Staging, Production), Secure baseline, Integrity measurement

3.5 Explain the security implications of embedded systems.

- SCADA/ICS, Smart devices/IoT (Wearable technology, Home automation), HVAC, SoC, RTOS, Printers/MFDs, Camera systems, Special purpose (Medical devices, Vehicles, Aircraft/UAV)

3.7 Summarize cloud and virtualization concepts.

- Cloud storage, Cloud deployment models (SaaS, PaaS, IaaS, Private, Public, Hybrid, Community), On-premise vs. hosted vs. cloud, Cloud access security broker, Security as a Service

3.8 Explain how resiliency and automation strategies reduce risk.

- Automation/scripting (Automated courses of action), Templates, Master image, Non-persistence (Live boot media)

4.3 Given a scenario, implement identity and access management controls.

- File system security, Database security

5.3 Explain risk management processes and concepts.

- Change management

**

In this chapter, you'll learn about different methods used to implement a secure systems design. This includes the use of different operating systems, peripherals, and hardware and firmware security. More and more organizations are using cloud resources and this chapter summarizes the important cloud concepts. Additionally, the use of mobile devices has exploded in the last few years with more and more organizations allowing employees to connect mobile devices to the network. This results in many challenges for an organization, but mobile device management tools help administrators handle these challenges. This chapter also covers the security implications of embedded systems that are now in printers, vehicles, smart devices, and more. Last, you’ll learn many different methods used to protect data.

Implementing Secure Systems

Secure systems design concepts help ensure that computing systems are deployed and maintained in a secure state. In this context, a system is any host such as a server, workstation, laptop, network device, or mobile device. In an ideal world, systems start in a secure state. Unfortunately, it’s not an ideal world, and administrators need to be proactive to secure systems before deployment and keep them secure after deployment. This section outlines several steps used to secure hosts.

Hardening is the practice of making an operating system (OS) or application more secure from its default installation. It helps eliminate vulnerabilities from default configurations, misconfigurations, and weak configurations.

A core principle associated with secure systems design is ***least functionality***. Systems should be deployed with only the applications, services, and protocols they need to meet their purpose. If a service or protocol is not running on a system, attackers cannot attack it. As a simple example, a system is not vulnerable to any File Transfer Protocol (FTP) attacks if FTP is not running and available on the system.

In addition to disabling unnecessary services to reduce vulnerabilities, it’s important to uninstall unneeded software. Software frequently has bugs and vulnerabilities. Although patching software frequently closes these vulnerabilities, you can eliminate these vulnerabilities by simply eliminating unneeded applications.

Years ago, I was working at a small training company. One of the servers had a default configuration for Windows that resulted in a significant vulnerability. We were using the server as a file server, but because it wasn’t hardened from the default configuration, it was also running Internet Information Services (IIS), the Microsoft web server.

At some point, attackers released the Nimda virus, which exploited a vulnerability with IIS. Microsoft released a patch for IIS, but because IIS was installed by default and we weren’t using it, we also weren’t managing it. Ultimately, the Nimda virus found our server, and the worm component of Nimda quickly infected our network. If the IIS software hadn’t been installed, the server would not have been vulnerable to the attack.

It’s also important to disable unnecessary accounts. For example, the Guest account is disabled by default in current Windows systems and it should remain disabled unless there is a specific need for it.

Some applications also include backdoor accounts. A backdoor is an access point to an application or service that bypasses normal security mechanisms. Developers use backdoors for legitimate purposes to view the internal workings of an application or for ease of administration. However, the use of backdoors is strongly discouraged in the final released version. If a backdoor exists, you can expect attackers to locate and exploit it. Similarly, if a system or application has a default account with a default password, the password should be changed.

Remember this

Least functionality is a core security principle stating that systems should be deployed with the least amount of applications, services, and protocols.

Operating Systems

There are three primary types of computer operating systems (OSs): Windows, Apple’s operating systems, and Linux- or Unix-based systems. Chapter 1, “Mastering Security Basics,” introduces Linux and Unix. For simplicity, instead of stating “Linux or Unix” throughout this book, I’m just stating it as Linux.

Within these types, there are many different versions. For example, the Windows operating system includes versions for desktop workstations (including laptops) and other versions for servers. Additionally, these versions are regularly updated such as Windows 8 and Windows 10, and Windows Server 2012 and Windows Server 2016. Windows operating systems are closed source software, meaning that the underlying code is not freely available to the public. Microsoft developed these OSs and updates them.

Apple also uses closed source OSs—macOS for its Macintosh computers and iOS as a mobile OS for mobile devices such as iPhones and iPads. Because they are closed source, only Apple updates or modifies these OSs.

Linux is derived from Unix and is open source, meaning that it is freely available to anyone. Developers have access to the code and can modify, improve, and, at times, freely redistribute it. Because of this, there is an almost endless assortment of Linux versions. As an example, the Android OS is open source software, and it was derived from the open source Linux OS. Additionally, many mobile device manufacturers modify the Android OS and use it as a mobile OS for their devices. It's worth noting that the use of Linux in many systems has steadily increased. More, CompTIA has been adding additional Linux-based objectives in their exams, including the Security+ exam.

While you primarily see OSs operating on desktops, laptops, and servers, they are also operating in other locations, including:

- **Kiosks.** A kiosk is a small structure in an open area used to sell something, provide information, or display advertisements. For example, an organization can create a touch-screen application installed on a computer and place it in a kiosk. This could be in a mall or store (designed to advertise something), in a medical center (designed to share information), or anywhere an organization thinks it might be useful.
- **Network.** Many network devices such as switches, routers, and firewalls include an operating system used to manage the device. These are often a version of Linux. Some Cisco network devices use the Cisco IOS (originally called the Internetwork Operating System).
- **Appliance.** A network appliance is a dedicated hardware device that bundles several features within it. As an example, Chapter 3, "Exploring Network Technologies and Tools," discusses a unified threat management (UTM) device that includes multiple layers of protection. Many appliances run on a Linux version.

It's also possible to use live boot media to create a non-persistent operating system on a computer. As an example, the Defense Information Systems Agency (DISA) uses Bootable Media (BootMe), which is a CD that authorized Department of Defense (DoD) users can use to run an operating system on almost any computer. It provides users with an operating system to perform specific functions, such as accessing DoD resources via remote access. It's called a non-persistent operating system because it disappears when users turn off the computer.

Secure Operating System Configurations

Most operating systems aren’t secure out of the box. Instead, administrators must take specific steps to secure them. A common method of deploying systems is to create a master image with a secure configuration, and then deploy the image to multiple systems.

A ***trusted operating system*** meets a set of predetermined requirements with a heavy emphasis on authentication and authorization. The overall goal of a trusted operating system is to ensure that only authorized personnel can access data based on their permissions. Additionally, a trusted operating system prevents any modifications or movement of data by unauthorized entities. A trusted OS helps prevent malicious software (malware) infections because it prevents malicious or suspicious code from executing.

A trusted OS meets a high level of security requirements imposed by a third party. For example, the Common Criteria for Information Technology Security Evaluation (or simply Common Criteria) includes requirements for a trusted OS. Operating systems that meet these requirements can be certified as trusted operating systems. Also, a trusted OS typically uses the mandatory access control (MAC) model, discussed in Chapter 2, “Understanding Identity and Access Management.”

Remember this

A trusted operating system meets a set of predetermined requirements, such as those identified in the Common Criteria. It uses the mandatory access control (MAC) model.

Using Master Images

One of the most common methods of deploying systems is with images starting with a master image. An image is a snapshot of a single system that administrators deploy to multiple other systems. Imaging has become an important practice for many organizations because it streamlines deployments while also ensuring they are deployed in a secure manner.

Figure 5.1 and the following text identify the overall process of capturing and deploying an image:

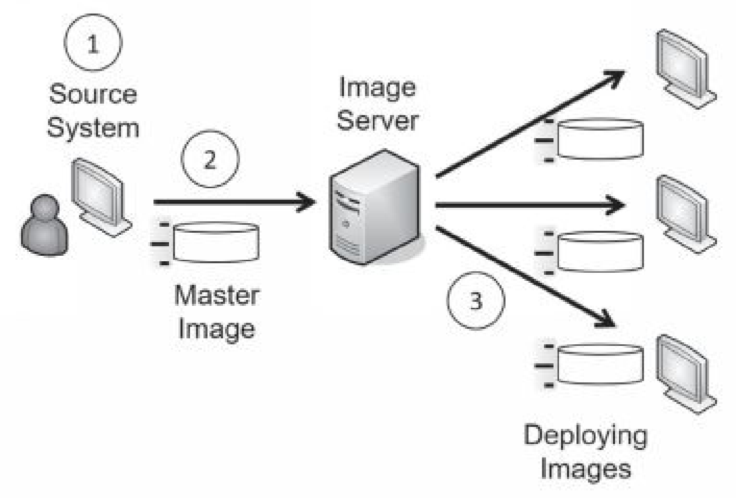


Figure 5.1: Capturing and deploying images

1. Administrators start with a blank source system. They install and configure the operating system, install and configure any desired applications, and modify security settings. Administrators perform extensive testing to ensure the system works as desired and that it is secure before going to the next step.
2. Next, administrators capture the image, which becomes their master image. Symantec Ghost is a popular imaging application, and Windows Server versions include free tools many organizations use to capture and deploy images. The captured image is simply a file that can be stored on a server or copied to external media, such as a DVD or external USB drive.
3. In step 3, administrators deploy the image to multiple systems. When used within a network, administrators can deploy the same image to dozens of systems during an initial deployment, or to just a single system to rebuild it. The image installs the same configuration on the target systems as the original source system created in step 1.

Administrators will often take a significant amount of time to configure and test the source system. They follow the same hardening practices discussed earlier and often use security and configuration baselines. If they're deploying the image to just a few systems such as in a classroom setting, they may create the image in just a few hours. However, if they're deploying it to thousands of systems within an organization, they may take weeks or months to create and test the image. Once they've created the image, they can deploy it relatively quickly with very little administrative effort.

Imaging provides two important benefits:

- **Secure starting point.** The image includes mandated security configurations for the system. Personnel who deploy the system don't need to remember or follow extensive checklists to ensure that new systems are set up with all the detailed configuration and security settings. The deployed image retains all the settings of the original image. Administrators will still configure some settings, such as the computer name, after deploying the image.
- **Reduced costs.** Deploying imaged systems reduces the overall maintenance costs and improves reliability. Support personnel don't need to learn several different end-user system environments to assist end users. Instead, they learn just one. When troubleshooting, support personnel spend their time focused on helping the end user rather than trying to learn the system configuration. Managers understand this as reducing the total cost of ownership (TCO) for systems.

Many virtualization tools include the ability to convert an image to a virtual system. In other words, once you create the image, you can deploy it to either a physical system or a virtual system. From a security perspective, there is no difference how you deploy it. If you've locked down the image for deployment to a physical system, you've locked it down for deployment to a virtual system.

Imaging isn't limited to only desktop computers. You can image any system, including servers. For example, consider an organization that maintains 50 database servers in a large data center. The organization can use imaging to deploy new servers or as part of its disaster recovery plan to restore failed servers. It is much quicker to deploy an image to rebuild a failed server than it is to rebuild a server from scratch. If administrators keep the images up to date, this also helps ensure the recovered server starts in a secure state.

Resiliency and Automation Strategies

Resiliency and automation strategies include automation, scripting, and templates and they can help deploy systems securely, and keep them in a secure state. As an example, administrators often use Group Policy in Microsoft domains to automatically check and configure systems. Chapter 2 discusses the use of Group Policy in more depth. It provides automated courses of action by applying security and other settings.

Additionally, Microsoft has created several security templates with various levels of security. Administrators can modify these templates to fit their needs, import them into a Group Policy Object (GPO), and then apply them to systems within the domain. Some organizations deploy a master image to all systems, and then use the security templates to automatically apply different security settings to different groups of systems based on their security needs.

Secure Baseline and Integrity Measurements

A baseline is a known starting point and organizations commonly use secure baselines to provide known starting points for systems. One of the primary benefits of secure baselines is that they improve the overall security posture of systems. Weak security configuration is a common security issue, but secure baselines help eliminate this.

The use of baselines works in three steps:

1. **Initial baseline configuration.** Administrators use various tools to deploy systems consistently in a secure state.
2. **Integrity measurements for baseline deviation.** Automated tools monitor the systems for any baseline changes, which is a common security issue. Some tools such as vulnerability scanners monitor the systems and report any changes they detect. Other tools such as Group Policy automatically reconfigure the systems to the baseline settings when they detect changes.
3. **Remediation.** Chapter 4, “Securing Your Network,” covers network access control (NAC). NAC methods can detect some changes to baseline settings and automatically isolate or quarantine systems in a remediation network. Typically, administrators need to correct the problems in these systems manually.

Remember this

A master image provides a secure starting point for systems. Administrators sometimes create them with templates or with other tools to create a secure baseline. They then use integrity measurements to discover when a system deviates from the baseline.

Patch Management

Software is not secure. There. I said it. As someone who has written a few programs over the years, that’s not easy to say. In a perfect world, extensive testing would discover all the bugs, exploits, and vulnerabilities that cause so many problems.

However, because operating systems and applications include millions of lines of code, testing simply doesn’t find all the problems. Instead, most companies make a best effort to test software before releasing it. Later, as problems crop up, companies write and release patches or updates. Administrators must apply these patches to keep their systems up to date and protected against known vulnerabilities.

Patch management ensures that systems and applications stay up to date with current patches. This is one of the most efficient ways to reduce operating system and application vulnerabilities because it protects systems from known vulnerabilities. Patch management includes a group of methodologies and includes the process of identifying, downloading, testing, deploying, and verifying patches.

After testing the patches, administrators deploy them. They don’t deploy the patches manually though. Instead, they use systems management tools to deploy the patches in a controlled manner. For example, Microsoft System Center Configuration Manager (SCCM, also known as ConfigMgr) is a systems management tool used for many purposes, including patch management.

In addition to deploying patches, systems management tools also include a verification component that verifies patch deployment. They periodically query the systems and retrieve a list of installed patches and updates. They then compare the retrieved list with the list of deployed patches and updates, providing reports for any discrepancies. In some networks, administrators combine this with network access control (NAC) technologies and isolate unpatched systems in quarantined networks until they are patched.

WannaCry Ransomware Attacked Unpatched Systems

(Sidebar)

In May 2017, attackers launched an attack infecting more than 200,000 computers in over 150 countries in just a few days. When users logged on, they saw the WannaCry ransomware message: “Ooops, your files have been encrypted!” The message demanded a payment of $300 within three days, doubled the ransom after six days, and threatened to delete the files after seven days if users didn’t pay.

However, this was 100 percent preventable if users followed one simple security practice—keep systems up to date with current patches. The WannaCry ransomware exploited a known vulnerability in Microsoft Windows systems, but Microsoft released an update to this vulnerability two months before the attack. Patched systems were not vulnerable to the attack. Unpatched systems were vulnerable.

Change Management Policy

The worst enemies of many networks have been unrestrained administrators. A well- meaning administrator can make what appears to be a minor change to fix one problem, only to cause a major problem somewhere else. A misconfiguration can take down a server, disable a network, stop email communications, and even stop all network traffic for an entire enterprise.

For example, I once saw a major outage occur when an administrator was troubleshooting a printer problem. After modifying the printer’s Internet Protocol (IP) address, the printer began to work. Sounds like a success, doesn’t it? Unfortunately, the new IP address was the same IP address assigned to a Domain Name System (DNS) server, and it created an IP address conflict. The conflict prevented the DNS server from resolving names to IP addresses. This resulted in a major network outage until another administrator discovered and corrected the problem.

These self-inflicted disasters were relatively common in the early days of IT. They still occur today, but organizations with mature change management processes in place have fewer of these problems. ***Change management*** defines the process for any type of system modifications or upgrades, including changes to applications. It provides two key goals:

- To ensure changes to IT systems do not result in unintended outages
- To provide an accounting structure or method to document all changes

When a change management program is in place, administrators are discouraged from making configuration changes without submitting the change for review and approval. In other words, they don’t immediately make a change as soon as they identify a potential need for the change. This includes making any type of configuration changes to systems, applications, patches, or any other change. Instead, they follow the change management process before making a change.

Experts from different areas of an organization examine change requests and can either approve or postpone them. The process usually approves simple changes quickly. A formal change review board regularly reviews postponed requests and can approve, modify, or reject the change. This entire process provides documentation for approved changes. For example, some automated change management systems create accounting logs for all change requests. The system tracks the request from its beginning until implementation. Administrators use this documentation for configuration management and disaster recovery. If a modified system fails, change and configuration management documentation identifies how to return the system to
its prefailure state.

Remember this

Patch management procedures ensure that operating systems and applications are up to date with current patches. This protects systems against known vulnerabilities. Change management defines the process and accounting structure for handling modifications and upgrades. The goals are to reduce risks related to unintended outages and provide documentation for all changes.

Unauthorized Software and Compliance Violations

A common security issue is the use of unauthorized software, which can cause many different problems. The most common problem is that unauthorized software often includes malware. When users install the software, they are also installing malware.

Another problem is related to support. Users who install unauthorized software typically want the IT department to help them with it when they have problems. However, the IT department personnel can't be experts on everything, so this takes them away from other tasks. Another common security issue related to the use of unauthorized software is license compliance violations. As an example, imagine an organization purchases 10 licenses for an application. Nine users have this installed and have activated it on their systems. Bart discovers the key and decides to install the software on his computer, even though he doesn't need it for his job.

Later, the organization hires Maggie. IT personnel set her up with a new computer and try to activate the application, but it fails because the tenth license is already in use. This results in a loss of availability of the application for Maggie.

Some applications verify the key is valid, but they don't necessarily check to see if the key is already in use. If IT personnel successfully install and activate the software on Maggie's computer, it results in a loss of integrity for the organization's license compliance. The organization can be susceptible to fines and penalties if the application developer discovers that the organization is violating the license requirements.

Application Whitelisting and Blacklisting

Whitelisting and blacklisting are two additional methods used to protect hosts, including workstations, servers, and mobile devices. An ***application whitelist*** is a list of applications authorized to run on a system. An ***application blacklist*** is a list of applications the system blocks.

You can use Software Restriction Policies in Microsoft Group Policy for both whitelisting and blacklisting for computers within a domain. For a whitelist, you identify the applications that can run on the system, and Group Policy blocks all other applications. For a blacklist, you identify the applications that cannot run on the system, and Group Policy allows any other applications.

Similarly, many mobile device management (MDM) applications use application whitelists and blacklists to allow or block applications on mobile devices. MDM applications are discussed later in this chapter.

Messages that users see when they can't install an application due to whitelisting or blacklisting are sometimes cryptic. When users try to install an application that isn’t on the whitelist, it will often report a permission issue or sometimes just fail with a vague error. However, application logs will typically include details on why the installation failed.

Remember this

An application whitelist is a list of authorized software and it prevents users from installing or running software that isn’t on the list. An application blacklist is a list of unauthorized software and prevents users from installing or running software on the list.

Secure Staging and Deployment

Another concept within secure systems design is secure staging and deployment concepts. These include sandboxing, controlling the environment, using secure baselines, and performing integrity measurements.

Sandboxing with VMs

Sandboxing is the use of an isolated area on a system and it is often used for testing. Chapter 1 covers the use of virtual machines (VMs) and you can create them so that they are isolated in a sandbox environment. Chapter 7, “Protecting Against Advanced Attacks,” discusses how sandboxing is often used for testing applications.

Administrators and security professionals also use sandboxing to test various security controls before deploying them to a live production network. Virtualization provides a high level of flexibility when testing security controls because the environments are easy to re-create. For example, they can test the effectiveness of antivirus software to detect malware released within a sandbox. If the antivirus software doesn’t detect the malware and the malware causes problems, it is easy to revert the system to a previous state. Also, the isolation within the sandbox prevents the malware from spreading.

Similarly, virtualized sandboxes are useful for testing patches. For example, software vendors typically develop software updates and patches, but they need to test them in various environments before releasing them. They could create VMs for multiple operating systems. When they’re ready to test, they turn on one of the VMs, take a snapshot, and then apply and test the patch. If the patch causes a problem, they can easily revert the VM.

Sandboxing with Chroot

Another method of sandboxing is with the Linux-based ***chroot*** command. It is used to change the root directory for an application, effectively isolating it. Normally, the root of Linux is designated as / and all other directories can be accessed from here. Users often have their own home directories within the /home directory. For example, Lisa's root directory on a Linux system might be /home/lisa. Regular users won't have access to the root directory, but only to files within their directory. In contrast, a root user (or administrator) has root access and can access all files and folders on the drive.

Imagine Lisa is a root user and wants to test an application within an isolated area. She could create a directory named testing in her environment. It would be /home/lisa/testing. She would copy her application files and copy any other required directories such as the /bin and /lib directories into the sandbox directory. She would then use chroot to create the isolated sandbox in the testing directory. This sandbox is often referred to as a chroot jail.

At this point, any commands she enters can only access files within the /home/lisa/testing directory. Additionally, her application can only access files with the same path. If the application is malicious or buggy, it cannot access any system files.

Secure Staging Environment

A secure staging environment includes multiple environments, and typically includes different systems used for each stage. As an example, imagine a software development team is creating an application that will be used to sell products via the Internet. The different environments are:

- **Development.** Software developers use a development environment to create the application. This typically includes version control and change management controls to track the application development.
- **Test.** Testers put the application through its paces and attempt to discover any bugs or errors. The testing environment typically doesn't simulate a full production environment, but instead includes enough hardware and software to test software modules.

- **Staging.** The staging environment simulates the production environment and is used for late stage testing. It provides a complete but independent copy of the production environment.
- **Production.** The production environment is the final product. It includes everything needed to support the application and allow customers and others to use it. In this example, it would include the live web server, possibly a back-end database server, and Internet access.

Secure systems design includes secure staging and deployment.

Remember this

Sandboxing is the use of an isolated area and it is often used for testing. You can create a sandbox with a virtual machine (VM) and on Linux systems with the chroot command. A secure deployment environment includes development, testing, staging, and production elements.

Peripherals

When implementing secure systems design, organizations should consider the use of various computer peripherals, including the following:

- **Wireless keyboards and wireless mice.** Wireless transmissions can sometimes be intercepted. If these devices are used with systems processing sensitive data, it might be prudent to use wired devices instead.
- **Displays.** If displays show sensitive or private data, their view should be limited. For example, they shouldn’t be viewable from windows. Additionally, privacy screens can be placed over displays to limit the view of the information unless someone is looking straight at the display.
- **External storage devices.** External storage devices include any external device that has memory capabilities. It typically refers to external USB drives, but also includes other devices such as smartphones, tablets, MP3 players, and digital cameras. Users can plug them into a system and easily copy data to and from a system. They can transport malware without the user’s knowledge and can be a source of data leakage. Malicious users can copy and steal a significant

amount of information using an easily concealable thumb drive. Also, users can misplace these drives and the data can easily fall into the wrong hands. Many organizations block the use of any external devices using technical policies.

- **Digital cameras.** Digital cameras typically include built-in storage and support additional storage by plugging in a memory card. These include the same risks as any external storage device.
- **Wi-Fi-enabled MicroSD cards.** Traditional Micro Secure Digital (SD) cards need to be plugged into a port to read the data. They are typically used in digital cameras. However, newer MicroSD cards include wireless capabilities. As with any wireless devices, the risk is that wireless transmissions can be intercepted, so if these are necessary, they should be configured with strong wireless security.
- **Printers and other multi-function devices (MFDs).** ***MFDs*** often have extra features that should be considered when purchasing them, especially if they will process sensitive information. These typically have embedded systems with their own risks discussed later in this chapter. Additionally, they often have internal storage that might retain documents that they process. For example, if the device is used to copy or scan a document, a copy of the document might remain in the system's internal memory.

Hardware and Firmware Security

When implementing secure systems design, it's also important to evaluate several hardware elements, including those covered in this section. Additionally, an organization should evaluate the supply chain. A supply chain includes all the elements required to produce a product. In secure systems design, the product is a secure system.

There have been many incidents where new computers were shipped with malware. As an example, Microsoft researchers purchased several new computers in China and found them infected with the Nitol virus. These computers were also running counterfeit versions of Windows. This helps illustrate the importance of purchasing computers from reputable sources.

EMI and EMP

When designing systems, it's important to consider electromagnetic interference (EMI) and electromagnetic pulse (EMP). ***EMI*** comes from sources such as motors, power lines, and fluorescent lights and it can interfere with signals transmitted over wires. Chapter 9, “Implementing Controls to Protect Assets,” discusses shielding that helps prevent EMI from causing problems. It’s easier to include shielding during the design process rather than add shielding later.

EMP is a short burst of electromagnetic energy. EMP can come from a wide assortment of sources and some sources can cause damage to computing equipment. Some sources include:

- **Electrostatic discharge (ESD).** Basic ESD prevention practices, such as using ESD wrist straps, help prevent ESD damage.
- **Lightning.** Lightning pulses can go through electrical wires and damage unprotected systems. Surge protection methods, such as surge protection strips, protect electrical systems.
- **Military weapons.** Nuclear explosions create a large EMP that can damage electronic equipment (including embedded systems) over a large area. Some non-nuclear weapons have been designed to mimic the nuclear EMP, but without the nuclear explosion. Non- nuclear EMP has a smaller range than nuclear EMP, but can still damage equipment. The best publicly known protection is to turn equipment off, but you’re unlikely to know when one of these explosions will occur.

Remember this

Secure systems design considers electromagnetic interference(EMI) and electromagnetic pulse (EMP). EMI comes from sources such as motors, power lines, and fluorescent lights and can be prevented with shielding. Systems can be protected from mild forms of EMP (a short burst of electromagnetic energy) such as electrostatic discharge and lightning.

FDE and SED

Full disk encryption (***FDE***) encrypts an entire disk. Several applications are available to do this. For example, VeraCrypt is an open source utility that can encrypt partitions or the entire storage device.

Many hardware vendors now manufacture hardware-based FDE drives. These are sometimes referred to as self-encrypting drives (SEDs). An ***SED*** includes the hardware and software to encrypt all data on the drive and securely store the encryption keys. These typically allow users to enter credentials when they set up the drive. When users power up the system, they enter their credentials again to decrypt the drive and boot the system.

UEFI and BIOS

The Basic Input/Output System (***BIOS***) includes software that provides a computer with basic instructions on how to start. It runs some basic checks, locates the operating system, and starts. The BIOS is often referred to as firmware. It is a hardware chip that you can physically see and touch and it includes software that executes code on the computer. The combination of hardware and software is firmware.

Newer systems use Unified Extensible Firmware Interface (***UEFI***) instead of BIOS. UEFI performs many of the same functions as BIOS, but provides some enhancements. As an example, it can boot from larger disks and it is designed to be CPU-independent.

Both BIOS and UEFI can be upgraded using a process called flashing. Flashing overwrites the software within the chip with newer software.

Trusted Platform Module

A Trusted Platform Module (***TPM***) is a hardware chip on the computer's motherboard that stores cryptographic keys used for encryption. Many laptop computers include a TPM and you may see them on many mobile devices, too. However, if the system doesn't include a TPM, it is not feasible to add one. Once enabled, the TPM provides full disk encryption capabilities. It keeps hard drives locked, or sealed, until the system completes a system verification and authentication process.

A TPM supports secure boot and attestation processes. When the TPM is configured, it captures signatures of key files used to boot the computer and stores a report of the signatures securely within the TPM. When the system boots, the ***secure boot*** process checks the files against the stored signatures to ensure they haven't changed. If it detects that the files have been modified, such as from malware, it blocks the boot process to protect the data on the drive.

A remote ***attestation*** process works like the secure boot process. However, instead of checking the boot files against the report stored in the

TPM, it uses a separate system. Again, when the TPM is configured, it captures the signatures of key files, but sends this report to a remote system. When the system boots, it checks the files and sends a current report to the remote system. The remote system verifies the files are the same and attests, or confirms, that the system is safe.

The TPM ships with a unique Rivest, Shamir, Adleman (RSA) private key burned into it, which is used for asymmetric encryption. This private key is matched with a public key and provides a ***hardware root of trust***, or a known secure starting point. The private key remains private and is matched with a public key. Additionally, the TPM can generate, store, and protect other keys used for encrypting and decrypting disks. Chapter 10, “Understanding Cryptography and PKI,” discusses asymmetric encryption and public and private keys in more depth.

If the system includes a TPM, you use an application within the operating system to enable it. For example, many Microsoft systems include BitLocker, which you can enable for systems that include the TPM.

BitLocker uses the TPM to detect tampering of any critical operating system files or processes as part of a platform verification process. Additionally, users provide authentication, such as with a smart card, a password, or a personal identification number (PIN). The drive remains locked until the platform verification and user authentication processes are complete.

If a thief steals the system, the drive remains locked and protected. An attacker wouldn’t have authentication credentials, so he can’t access the drive using a normal boot process. If the attacker tries to modify the operating system to bypass security controls, the TPM detects the tampering and keeps the drive locked. If a thief moves the drive to another system, the drive remains locked because the TPM isn’t available.

Remember this

A Trusted Platform Module (TPM) is a hardware chip included on many laptops and mobile devices. It provides full disk encryption and supports a secure boot process and remote attestation. A TPM includes a unique RSA asymmetric key burned into the chip that provides a hardware root of trust.

Hardware Security Module

A hardware security module (***HSM***) is a security device you can add to a system to manage, generate, and securely store cryptographic keys. High-performance HSMs are external devices connected to a network using TCP/IP. Smaller HSMs come as expansion cards you install within a server, or as devices you plug into computer ports.

HSMs support the security methods as a TPM. They provide a hardware root of trust, secure boot, and can be configured for remote attestation.

One of the noteworthy differences between an HSM and a TPM is that HSMs are removable or external devices. In comparison, a TPM is a chip embedded into the motherboard. You can easily add an HSM to a system or a network, but if a system didn't ship with a TPM, it's not feasible to add one later. Both HSMs and TPMs provide secure encryption capabilities by storing and using RSA keys. Many high-performance servers use HSMs to store and protect keys.

Remember this

A hardware security module (HSM) is a removable or external device that can generate, store, and manage RSA keys used in asymmetric encryption. Many server-based applications use an HSM to protect keys.

Additional Vulnerabilities

Two issues that organizations need to avoid are vulnerabilities associated with end-of-life systems and a lack of vendor support. When systems reach the end of their life, you need to ensure that they don't have any valuable data on them before disposing of them. Chapter 11, "Implementing Policies to Mitigate Risks," discusses several methods of sanitization.

Also, when a vendor stops supporting a system, an operating system, or an application, it is time to start using something else. As an example, consider Windows XP. It was a solid operating system for 12 years and it probably still runs fine on many computers. However, Microsoft stopped supporting it on April 8, 2014. This means that they no longer provide security updates or technical support for it. Any new vulnerabilities discovered after April 8, 2014, remain unpatched.

Summarizing Cloud Concepts

Cloud computing refers to accessing computing resources via a different location than your local computer. In most scenarios, you’re accessing these resources through the Internet.

As an example, if you use web-based email such as Gmail, you’re using cloud computing. More specifically, the web-based mail is a Software as a Service cloud computing service. You know that you’re accessing your email via the Internet, but you really don’t know where the physical server hosting your account is located. It could be in a data center in the middle of Virginia, tucked away in Utah, or just about anywhere else in the world.

Cloud storage has become very popular for both individuals and organizations. For example, Apple offers iCloud storage, Microsoft offers OneDrive, and Google offers Google Drive. You can typically get some storage for free or pay nominal fees for more storage. Their prices continue to drop as they continue to offer more storage space.

Heavily utilized systems and networks often depend on cloud computing resources to handle increased loads. As an example, consider the biggest shopping day in the United States— Black Friday, the day after Thanksgiving, when retailers hope to go into the black. Several years ago, Amazon.com had so much traffic during the Thanksgiving weekend that its servers could barely handle it. The company learned its lesson, though. The next year, it used cloud computing to rent access to servers specifically for the Thanksgiving weekend, and, despite increased sales, it didn’t have any problems.

As many great innovators do, Amazon didn’t look on this situation as a problem, but rather an opportunity. If it needed cloud computing for its heavily utilized system, other companies probably had the same need. Amazon now hosts cloud services to other organizations via its Amazon Elastic Compute Cloud (Amazon EC2) service. Amazon EC2 combines virtualization with cloud computing and they currently provide a wide variety of services via Amazon EC2.

As a comparison, organizations can also use on-premise or hosted services:

- **On-premise.** All resources are owned, operated, and maintained within the organization’s building or buildings.

- **Hosted.** Organizations can rent access to resources from a specific organization. Note that the line is blurred between hosted and cloud services. In some cases, you know exactly where the services are hosted. However, in most cases, hosted services are somewhere within the cloud.

Software as a Service

Software as a Service (***SaaS***) includes any software or application provided to users over a network such as the Internet. Internet users access the SaaS applications with a web browser. It usually doesn't matter which web browser or operating system a SaaS customer uses. They could be using Microsoft Edge, Chrome, Firefox, or just about any web browser.

As mentioned previously, web-based email is an example of SaaS. This includes Gmail, Yahoo! Mail, and others. The service provides all the components of email to users via a simple web browser.

If you have a Gmail account, you can also use Google Docs, another example of SaaS. Google Docs provides access to several SaaS applications, allowing users to open text documents, spreadsheets, presentations, drawings, and PDF files through a web browser.

A talented developer and I teamed up to work on a project a while ago. He's an Apple guy running a macOS while I'm a Microsoft guy running Windows, and we live in different states. However, we post and share documents through Google Docs and despite different locations and different applications running on our individual systems, we're able to easily collaborate. One risk is that our data is hosted on Google Docs, and if attackers hack into Google Docs, our data may be compromised.

Platform as a Service

Platform as a Service (***PaaS***) provides customers with a preconfigured computing platform they can use as needed. It provides the customer with an easy-to-configure operating system, combined with appropriate applications and on-demand computing.

Many cloud providers refer to this as a managed hardware solution. For example, I host *http://gcgapremium.com/* on a virtual server through Liquid Web (*http://www.liquidweb.com/*) using one of their "Fully Managed" offerings.

Liquid Web provides several features in their fully managed solutions, including an installed operating system, a core software package used for web servers, Apache as a web server, antivirus software, spam protection, and more. Additionally, they keep the operating system up to date with relevant updates and patches. I manage the software used for the web site, including software changes and updates. However, I don’t need to worry about managing the server itself. The couple of times when the server developed a problem, they fixed it before I was even aware of the problem.

Infrastructure as a Service

Infrastructure as a Service (***IaaS***) allows an organization to outsource its equipment requirements, including the hardware and all support operations. The IaaS service provider owns the equipment, houses it in its data center, and performs all the required hardware maintenance. The customer essentially rents access to the equipment and often pays on a per-use basis.

Many cloud providers refer to this as a self-managed solution. They provide access to a server with a default operating system installation, but customers must configure it and install additional software based on their needs. Additionally, customers are responsible for all operating system updates and patches.

IaaS can also be useful if an organization is finding it difficult to manage and maintain servers in its own data center. By outsourcing its requirements, the company limits its hardware footprint. It can do this instead of, or in addition to, virtualizing some of its servers. With IaaS, it needs fewer servers in its data center and fewer resources, such as power, HVAC, and personnel to manage the servers.

Remember this

Applications such as web-based email provided over the Internet are Software as a Service (SaaS) cloud-based technologies. Platform as a Service (PaaS) provides customers with a fully managed platform, which the vendor keeps up to date with current patches. Infrastructure as a Service (IaaS) provides customers with access to hardware in a self- managed platform.

Security Responsibilities with Cloud Models

One important consideration with cloud service models is the difference in security responsibilities assigned to the cloud service provider (CSP) and the customer. Figure 5.2 (derived from Figure 1 in the U.S. Department of Defense (DoD) “Cloud Computing Security Requirements Guide”) shows the difference in the amount of responsibilities for a SaaS, PaaS, and IaaS. This includes both maintenance responsibilities and security responsibilities.

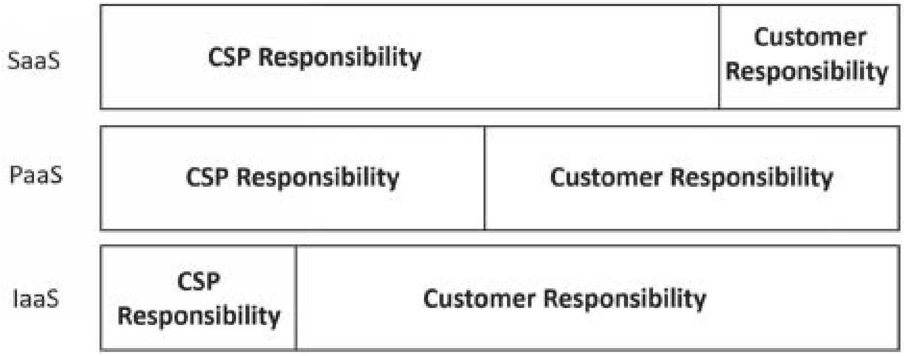


Figure 5.2: Security responsibilities with cloud models

As an example, for SaaS, consider Gmail. Google has the primary responsibility for maintaining the app and ensuring it is available. Additionally, Google has the primary responsibility of ensuring the security for Gmail. If you use it, you still have some responsibility, such as ensuring you use a strong password that is different from other online accounts.

With a PaaS solution, the CSP has the responsibility to provide you with the platform and ensure it remains available. Many CSPs provide additional security protection, such as firewalls, malware content filters, and intrusion detection systems. Still, the customer has a much greater responsibility for the operation, configuration, and security of the platform.

The CSP has the least responsibility for an IaaS solution and the customer has the most responsibility when compared with both PaaS and SaaS.

Security as a Service

Another entry into cloud computing is Security as a Service. It includes any services provided via the cloud that provide security services, and is commonly viewed as a subset of the Software as a Service (SaaS) model.

A common example of a Security as a Service application is antivirus software. Imagine radio station W-KOMA decides to purchase antivirus software for its eight employees. They purchase licenses to access the software from an antivirus company. Each employee then configures their system to use the software with their individual licenses. Once installed, the software automatically downloads virus definitions keeping each user's system up to date without relying on the user to do so.

A key benefit of Security as a Service is that it outsources the administrative tasks associated with implementing the service. Additionally, professionals are focused on the specific security services offered, eliminating the need for employees to be experts on everything.

Organizations that use cloud resources often add a ***cloud access security broker (CASB)*** for additional security. This is a software tool or service deployed between an organization's network and the cloud provider. It monitors all network traffic and can enforce security policies. As an example, it can ensure that all data stored in the cloud is encrypted.

Cloud Deployment Models

There are four categories of ***cloud deployment models***: public, private, community, and hybrid. These identify who has access to the cloud infrastructure.

Public cloud services are available from third-party companies, such as Amazon, Google, Microsoft, and Apple. They provide similar services to anyone willing to pay for them.

A private cloud is set up for specific organizations. For example, the Shelbyville Nuclear Power Plant might decide it wants to store data in the cloud, but does not want to use a third- party vendor. Instead, the plant chooses to host its own servers and make these servers available to internal employees through the Internet.

Communities with shared concerns (such as goals, security requirements, or compliance considerations) can share cloud resources within a community cloud. As an example, imagine that the Shelbyville Nuclear Power Plant and several schools within Springfield decided to share educational resources within a cloud. They could each provide resources for the cloud and only organizations within the community would have access to the resources.

Not all cloud implementations fit exactly into these definitions, though. A hybrid cloud is a combination of two or more clouds. They can be private, public, community, or a combination. These retain separate identities to help protect resources in private clouds. However, they are bridged together, often in such a way that it is transparent to the users.

Remember this

A cloud access security broker (CASB) is a software tool or service deployed between an organization's network and the cloud provider. It provides Security as a Service by monitoring traffic and enforcing security policies. Private clouds are only available for one organization. Public cloud services are provided by third-party companies and available to anyone. A community cloud is shared by multiple organizations. A hybrid cloud is a combination of two or more clouds.

Deploying Mobile Devices Securely

Mobile devices represent significant challenges for organizations today. Organizations need to determine if employees can connect mobile devices to the network. If so, organizations need to identify methods to manage the security related to the devices, and how to monitor the devices and enforce security policies.

What is a mobile device? Within the context of the CompTIA Security+ exam, you can think of a mobile device as a smartphone or tablet. Further, NIST SP 800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," mentions that mobile devices have additional characteristics, such as at least one wireless network interface, local data storage, an operating system (that isn't a full-fledged desktop or laptop operating system), and the ability to install additional applications.

Mobile devices typically have other optional features. This includes other networking options such as Bluetooth, near field communication, cellular access for voice communications, and Global Positioning System

(GPS) services. They typically include a digital camera, a video recorder, a microphone, and the ability to transfer data to another system such as a traditional computer or to other mobile devices.

The NIST definition excludes many devices. For example, a laptop is not considered a mobile device within this definition. Laptops have full operating systems and there are many security controls available for them, which aren't available in smartphones and tablets. Additionally, basic cell phones and digital cameras are not included in this definition because they cannot access networks and aren't susceptible to the same risks associated with smartphones and tablets.

Deployment Models

Any device connected to an organization's network represents a potential risk. As a simple example, if someone connects an infected device to a network, it might be able to infect other devices on the network. To limit this risk, organizations take steps to monitor and manage mobile devices.

If the organization owns all the devices connected to the network, it's a simple matter to monitor and manage them. However, if employees own these devices (such as their own smartphone), monitoring and managing the devices becomes more challenging. As an example, employees want to access the network resources with their own device, but they are sometimes resistant to allowing the organization to monitor and manage their personal device.

The following list identifies some common deployment models for mobile devices. Notice that in some models, the organization owns the device, but in other models, employees own the device:

- **Corporate-owned.** In this traditional deployment model, the organization purchases devices and issues them to employees.
- **COPE (corporate-owned, personally enabled).** ***COPE*** is similar to the traditional corporate-owned model, but the primary difference is that the employees are free to use the device as if it was their personally owned device. This allows employees to use the devices for personal activities in addition to connecting them to the organization's network. Because the organization owns the devices, it makes it easier to manage them.
- **BYOD (bring your own device).** Some organizations allow

employees to bring their own mobile devices to work and attach them to the network. Employees are responsible for selecting and supporting the device and they typically must comply with a ***BYOD*** policy when connecting their device to the network. While this is simple for the employees, it is sometimes referred to as *bring your own disaster* among IT professionals. Because employees can have any possible device, the IT department is now responsible for supporting, monitoring, and managing any possible device owned by employees.

- **CYOD (choose your own device).** To avoid some of the challenges related to supporting any possible mobile devices, some organizations create a list of acceptable devices along with a ***CYOD*** policy. Employees can purchase devices on the list and bring them to work. This gives the IT department a specific list of devices that they need to support, monitor, and manage.
- **VDI (virtual desktop infrastructure).** Chapter 1 discusses VDIs, which host a user's desktop operating system on a server. While these are typically accessed by traditional computers within a network, it's also possible to deploy a ***VDI*** that users can access with their mobile device. This allows users to access any applications installed on their desktop. When the organization hosts a remote access solution such as a virtual private network (VPN), users can access the mobile VDI from anywhere if they have Internet access.

Remember this

Corporate-owned, personally enabled (COPE) devices are owned by the organization, but employees can use them for personal reasons. A bring your own device (BYOD) policy allows employees to connect their own personal devices to the corporate network. A choose your own device (CYOD) policy includes a list of approved devices. Employees with a device on the list can connect them to the network. A virtual desktop infrastructure (VDI) is a virtual desktop and these can be created so that users can access them from a mobile device.

Connection Methods

There are several methods that mobile devices can use to connect to networks and other devices. They include:

- **Cellular.** Smartphones (and many tablets) include the ability to connect to a cellular network, such as a third generation (3G), long-term-evolution (LTE), fourth generation (4G), or 4G LTE network. The type of network you connect with is dependent on your cellular provider. Newer generations typically provide increased speed for digital transfers and improved voice communications.
- **Wi-Fi.** Mobile devices almost always have a wireless network interface that you can configure to connect to a wireless network. Chapter 4 discusses common wireless security methods and wireless protocols. Typical wireless networks require you to enter or select the service set identifier (***SSID***) and enter the pre-shared key or password to access the network. More secure networks use ***Enterprise mode*** with an 802.1x server.
- **SATCOM.** Some mobile devices support connections to networks using satellite communications (***SATCOM***). The most common usage of SATCOM is in mobile phones rather than tablets. However, you can purchase satellite hot spots. You can connect mobile devices to the hot spot, and the hot spot provides Internet and voice access via a satellite connection. Additionally, some vehicles include satellite communication technologies that can be used for phone calls and sometimes for shared Internet access.
- **Bluetooth.** Most mobile devices include Bluetooth support. Bluetooth is a wireless protocol commonly used with personal area networks. For example, most smartphones support the use of a Bluetooth headset for hands-free use of the phone. Additionally, some technologies use Bluetooth to connect two smartphones. For example, Apple’s AirDrop uses Bluetooth to create a peer-to-peer network. This makes it easy to exchange files such as photos or videos between two phones.
- **NFC (near field communication).** NFC is most commonly used as a payment gateway allowing you to make payments simply by waving your phone in front of an NFC reader at a retailer. You can also

create a peer-to-peer network between two devices with NFC. For example, Android Beam allows two users with Android devices to share data displayed on the screen by placing two devices back to back. Some applications use NFC to enable Bluetooth on the two devices, send the shared data via Bluetooth, and then disable Bluetooth.

- **ANT.** ***ANT*** and ANT+ are proprietary wireless protocols used by some mobile devices. While it looks like an acronym, it isn't spelled out on the ANT Wireless web site (*https://www.thisisant.com/*). Many sports and fitness sensors (such as Fitbit) collect data on users (such as heart rate, steps taken, and so on) and use ANT to send the data to a mobile device application.
- **Infrared.** Infrared is a line-of-sight wireless technology used by some mobile devices. This is the same technology used by most remote controls for TVs and other audiovisual equipment. Many people add apps to their smartphones and use them as a universal remote for their equipment. It's also possible to transfer files between smartphones using infrared, as long as both smartphones support infrared.
- **USB (Universal Serial Bus).** Mobile devices can typically be connected to a desktop PC or laptop via a USB cable. Most Apple devices have a Lightning port and can connect to PCs via a Lightning to USB cable. Many Android devices have a mini-USB cable and can connect to PCs via a mini-USB to standard USB cable.

Mobile Device Management

Mobile device management (***MDM***) includes the technologies to manage mobile devices.

The goal is to ensure these devices have security controls in place to keep them secure.

System management tools, such as Microsoft System Center Configuration Manager (SCCM, also known as ConfigMgr), ensure systems are kept up to date with current patches, have antivirus software installed with up-to-date definitions, and are secured using standard security practices. While these tools originally focused on desktop PCs and laptops, they have expanded to include many mobile devices. As an example, ConfigMgr includes support for many mobile devices, including Apple iOS-based devices and Android-based devices.

MDM applications help administrators manage mobile devices. The following bullets describe many of the MDM concepts that apply to mobile devices:

- **Application management.** MDM tools can restrict what applications can run on mobile devices. They often use application whitelists to control the applications and prevent unapproved applications from being installed.
- **Full device encryption.** Encryption protects against loss of confidentiality on multiple platforms, including workstations, servers, mobile devices, and data transmissions. Encryption methods such as full device encryption provide device security, application security, and data security. While an organization can ensure corporate-owned devices use full device encryption, this isn't always possible when employees use their own devices.
- **Storage segmentation.** In some mobile devices, it's possible to use ***storage segmentation*** to isolate data. For example, users might be required to use external storage for any corporate data to reduce the risk of data loss if the device is lost or stolen. It's also possible to create separate segments within the device. Users would store corporate data within an encrypted segment and personal data elsewhere on the device.
- **Content management.** After creating segmented storage spaces, it's important to ensure that appropriate content is stored there. An MDM system can ensure that all content retrieved from an organization source (such as a server) is stored in an encrypted segment. Also, content management can force the user to authenticate again when accessing data within this encrypted segment.
- **Containerization.** Chapter 1 discusses the use of application cell virtualization (also known as container virtualization). ***Containerization*** can also be implemented in mobile devices. By running an application in a container, it isolates and protects the application, including any of its data. This is very useful when an organization allows employees to use their own devices. It's possible to encrypt the container to protect it without encrypting the entire device.
- **Passwords and PINs.** Mobile devices commonly support the use

of passwords or personal identification numbers (PINs). MDM systems typically support password policies, similar to the password policies used in desktop systems. The only limitation is that some mobile devices only support PINs, while others support either passwords or PINs.

- **Biometrics.** Chapter 2 discusses biometrics as one of the authentication factors (something you are). Many mobile devices now support biometrics for authentication. For example, you can teach the device your fingerprint and then use your fingerprint to authenticate instead of entering a password or PIN.
- **Screen locks.** Most devices support the use of a passcode or password to lock the device. This is like a password-protected screen saver on desktop systems that automatically locks the device after a period of time. It prevents someone from easily accessing the device and the data it contains. This is often combined with an erase function. For example, if someone steals the phone and enters the incorrect passcode ten times, the smartphone will automatically erase all data on the phone.
- **Remote wipe.** ***Remote wipe*** capabilities are useful if the phone is lost. It sends a remote signal to the device to wipe or erase all the data. The owner can send a remote wipe signal to the phone to delete all the data on the phone. This also deletes any cached data, such as cached online banking passwords, and provides a complete sanitization of the device by removing all valuable data.

Remember this

Mobile device management (MDM) tools help enforce security policies on mobile devices. This includes the use of storage segmentation, containerization, and full device encryption to protect data. They also include enforcing strong authentication methods to prevent unauthorized access.

- **Geolocation.** Mobile devices commonly include Global Positioning System (***GPS***) capabilities that can be used for ***geolocation***. Applications commonly use GPS to identify the location of the device. This can also be used to locate a lost device.
- **Geofencing.** Organizations sometimes use GPS to create a virtual

fence or geographic boundary using ***geofencing*** technologies. Apps can respond when the device is within the virtual fence. As an example, an organization can configure mobile apps so that they will only run when the device is within the virtual fence. Similarly, an organization can configure a wireless network to only operate for mobile devices within the defined boundary.

- **GPS tagging. *GPS tagging*** (also called geotagging) adds geographical information to files such as pictures when posting them to social media web sites. For example, when you take a picture with a smartphone that has GPS features enabled, the picture application adds latitude and longitude coordinates to the picture. Thinking of friends and family, this is a neat feature. However, thinking of thieves and criminals, they can exploit this data. For example, if Lisa frequently posts pictures of friends and family at her house, these pictures identify her address. If she later starts posting pictures from a vacation location, thieves can realize she's gone and burglarize her home.
- **Context-aware authentication. *Context-aware authentication*** uses multiple elements to authenticate a user and a mobile device. It can include the user's identity, geolocation, verification that the device is within a geofence, time of day, and type of device. Combined, these elements help prevent unauthorized users from accessing apps or data.
- **Push notification services. *Push notification services*** send messages to mobile devices from apps. As an example, if Lisa installs the Facebook app on her smartphone and enables notifications, the Facebook app will send her notifications. Software developers can configure the notifications to appear even if the device is in screen lock mode and even if the app is not running. MDM apps can send notifications to remind users of security settings, or to let them know if their device is complying with security policy requirements.

Remember this

Remote wipe sends a signal to a lost or stolen device to erase all data. Geolocation uses Global Positioning System (GPS) and can help locate a lost or stolen device. Geofencing creates a virtual fence or geographic boundary and can be used to detect when a device is within an organization's property. GPS tagging adds geographical data to files such as pictures. Context-aware authentication uses multiple elements to authenticate a user and a mobile device.

Mobile Device Enforcement and Monitoring

MDM tools often manage devices differently depending on who owns them. If the organization owns the device, the MDM tool will typically download and install all required applications, and ensure they are kept up to date.

If the device is employee-owned, MDM tools will monitor them for compliance and block access to the network if the device doesn’t meet minimum requirements. For example, if the device isn’t patched or doesn’t have up-to-date antivirus software, the MDM software works with network access control (NAC) technologies to prevent the device from connecting to the network. The following paragraphs identify many common issues that an MDM can monitor and/or enforce.

Unauthorized Software

Organizations typically want users to only install apps obtained from approved sources. For example, all iPhone and iPad devices would only obtain apps from Apple’s App Store. Apple is aggressive in testing these apps for malware and any developer who attempts to distribute malware through the Apple store is often banned. Similarly, Google maintains the Google Play site for Android devices.

A ***third-party app store*** is something other than Apple’s App Store or Google Play. Apps obtained from these third-party app stores don’t undergo the same level of scrutiny as apps on the App Store or Google Play and represent a higher risk. Apple makes it very difficult to obtain apps from a third-party app store, but it is relatively easy to obtain apps from third-party stores for Android devices.

Jailbreaking refers to removing all software restrictions from an Apple device. After jailbreaking a device, users can install software from any third-party source. ***Rooting*** is the process of modifying an Android device to give the user root-level (or full administrator) access to the device. Both rooting and jailbreaking introduce risks and vulnerabilities to the device, so it’s common for an MDM to block all access to a network if it detects a device has either been rooted or jailbroken.

Mobile devices typically have the operating system stored in onboard memory such as flash memory, which retains data even without power. Because the operating system is the software and the memory is hardware, this is commonly called firmware. Updates to the operating system overwrite the firmware using over-the-air (OTA) techniques. ***Firmware OTA updates*** keep the device up to date.

It's also possible to overwrite the firmware with ***custom firmware***. Some people do this as another method of rooting Android devices. The process is typically complex and fraught with risks. However, some people find downloadable images and copy them onto their devices to overwrite the firmware.

It's also possible to install applications on Android devices by ***sideloading*** them. Sideloading is the process of copying an application package in the Application Packet Kit (APK) format to the device and then activating it. The device must be set to allow apps from Unknown Sources, which can significantly weaken security. Sideloading is useful for developers testing apps, but considered risky when installing apps from third parties.

Remember this

Jailbreaking removes all software restrictions from an Apple device. Rooting modifies an Android device, giving users root-level access to the device. Overwriting the firmware on an Android device with custom firmware is another way to root an Android device. Sideloading is the process of installing software on an Android device from a source other than an authorized store.

Many people use text messaging services such as Short Message Service (***SMS***) and Multimedia Messaging Service (***MMS***). SMS is a basic text messaging service supported on many telephone and mobile devices. MMS is an extension of SMS that allows users to include multimedia content such as a picture, a short video, audio, or even a slideshow of multiple images.

There are two primary risks with text messaging. First, both send text in plaintext, allowing the information to be intercepted and read by others. However, many apps such as iMessage offer encryption capabilities.

The second risk only applies to MMS because it can send media. Attackers have discovered ways to send an MMS message to a phone number and gain remote code execution privileges on the user's phone. For example, security researchers identified a vulnerability in Stagefright, a media library within the Android operating system that is susceptible to attacks. In 2015, experts indicated that 95 percent of Android devices were vulnerable. At this point, the vulnerability is patched on most devices.

Most smartphones can store credit card data and be used for payments. For example, NFC (described earlier in this chapter) is often used as a payment gateway with some mobile devices. When issuing phones to users, organizations need to consider if they want to put their own payment methods on the phone for some payments. If so, this typically needs to be monitored closely.

Hardware Control

An organization might want to control the use of some of the hardware on mobile devices and MDM tools can help. Mobile devices commonly include a camera and a recording microphone. These are useful for regular users, but can present significant risks for employees within an organization.

As an example, attackers have successfully inserted malicious code into some apps available on some third-party sites. When users install the apps, it allows an attacker to remotely connect to the phone, snap pictures, record audio, and much more.

To eliminate the risk, an organization can configure the MDM software to disable the camera and recording microphone. Ideally, the MDM tool will only disable the camera and microphone when it detects the device is within a previously configured geofence. Unfortunately, all MDM tools don't support disabling hardware based on geolocation. If the MDM tool doesn't support this feature, the organization may prohibit the possession of smartphones in certain areas.

MDM tools can also prevent the use of external media and Universal Serial Bus On-The-Go (***USB OTG***) cables. Mobile devices commonly have one or more ports where you can plug in a cable. Apple devices have a Lightning port and Android devices typically have a micro-USB or mini-USB. In some cases, it's possible to connect external media (such as an external drive) to the device. Organizations might want to prevent this because the media presents additional risks. It could contain malware. It might also allow a

malicious insider to copy a massive amount of data. USB OTG cables allow you to connect just about any device to your mobile device, including another mobile device. This includes a mouse, keyboard, Musical Instrument Digital Interface (MIDI) keyboard, and external media. Many people find this very useful to transfer photos from digital cameras to their mobile device. Again, though, because this allows connections to
external media, an organization might choose to disable the feature using MDM tools.

Unauthorized Connections

Management within an organization might want to limit a mobile device's connection. For example, if the mobile device can connect to the primary network, management might want to ensure that the mobile device cannot access the Internet using another connection. This section identifies other connections that can be modified and blocked with an MDM tool.

Most smartphones support ***tethering***, which allows you to share one device's Internet connection with other devices. As an example, you can connect your smartphone to the Internet and then use this Internet connection with a laptop, a tablet, or any device that has a wireless connection. If employees use tethering within the organization, it allows them to bypass security such as firewalls and proxy servers. Imagine Bart wants to visit a not safe for work (NSFW) site with his work laptop. The proxy server blocks his access. However, he can tether his laptop to his smartphone and visit the site. This direct connection will also bypass any content filters in the network, and possibly allow malware onto his laptop.

Many mobile devices also support ***Wi-Fi Direct***, which is a standard that allows devices to connect without a wireless access point, or wireless router. This is similar to a wireless ***ad hoc*** network, which allows devices to connect together without a wireless access point or wireless router. The difference is that Wi-Fi Direct uses single radio hop communication. In other words, none of the devices in a Wi-Fi Direct network can share an Internet connection. However, systems in a wireless ad hoc network use multihop wireless communications and can share an Internet connection.

Smartphones are typically locked into a specific carrier such as Verizon or AT&T. A subscriber identification module (SIM) card identifies what countries and/or networks the phone will use. In other words, if Lisa has a smartphone and a Verizon plan, the SIM card in her phone will connect her to a Verizon network instead of an AT&T network.

If Lisa purchased her phone under a two-year contract and fulfilled all the terms of her plan, she can unlock her phone (also called ***carrier unlocking***) and use it with another carrier. An organization might want to block this capability for all COPE devices.

Remember this

Tethering is the process of sharing a mobile device's Internet connection with other devices. Wi-Fi Direct is a standard that allows devices to connect without a wireless access point, or wireless router. MDM tools can block access to devices using tethering or Wi-Fi Direct to access the Internet.

Exploring Embedded Systems

An ***embedded system*** is any device that has a dedicated function and uses a computer system to perform that function. Desktop PCs, laptops, and servers all use central processing units (CPUs), operating systems, and applications to perform various functions. Similarly, embedded systems use CPUs, operating systems, and one or more applications to perform various functions. As a simple example, a wireless multi-function printer typically includes an embedded system. It runs a web site that you can access wirelessly to configure the printer. Of course, you can also send print jobs to it, scan documents, and copy documents with the printer. Many include faxing capabilities and sending documents via email.

Person of Interest (Sidebar)

Person of Interest, a science fiction TV show that includes a mix of fiction and facts, does give some realistic insight into how mobile devices can be compromised and used by attackers.

Some scenarios showed John Reese (and others on the show) using Bluetooth to pair with a device or send a message to a phone and then install malware. Once installed, Reese and others on the show have almost unlimited access to the phone. Some of their capabilities include:

- Monitoring all text messages
- Tracking the phone’s location
- Turning on the microphone to listen in on conversations
- Monitoring and recording all phone calls (including phone numbers)

While there aren’t any known ways to do this on current phones, these capabilities have existed in the past. For example, forced Bluetooth pairing was frequently possible in the early 2000s, but security measures have closed this security hole for most, if not all, smartphones today. Similarly, MMS vulnerabilities on Android smartphones allowed attackers to take over a phone just by sending an MMS message to it. Once an attacker takes over the phone, the other capabilities become almost trivial.

Other systems that include embedded systems are camera systems, medical devices, smart televisions, automobiles, and household appliances like refrigerators, microwave ovens, and burglar alarm systems. Each device can use a different CPU, operating system, and application depending on its function.

Security Implications and Vulnerabilities

The challenge with embedded systems is keeping them up to date with security fixes. Exploits are regularly discovered for desktop PC and server operating systems and applications. When vendors discover them, they release patches. When you apply the patch, the system is no longer vulnerable to the exploit. In contrast, vendors of embedded systems are not as aggressive in identifying vulnerabilities and creating patches to fix them.

Also, patch management is a routine function for IT administrators in most organizations. They regularly review patches, test them, and apply them when necessary. In contrast, how often does a regular user think about checking or applying patches to his refrigerator?

Another significant security concern is when embedded systems are deployed with default configurations. For example, imagine Homer creates a home security system using Internet- accessible security cameras, deployed with default username and passwords. If attackers discover the cameras, they can access them over the Internet.

Worse, if attackers discover a vulnerability within the cameras' embedded systems, they can exploit them. This is exactly what attackers did in the 2016 Dyn cyberattack that took down the Internet. Chapter 7 discusses this attack within the "DNS Attacks" section. Attackers infected cameras and other Internet-connected devices and joined them to a botnet. They then used these devices to launch attacks.

Comparing Embedded Systems

The CompTIA Security+ objectives include a long list of embedded systems. Some of these might be familiar to you, but others use acronyms that aren't familiar to many people. The following section describes many common embedded systems.

A smart television (TV) is one of many smart devices that you might have in your home. You can easily connect it to your home's wired or wireless network and use it to access the Internet. Many people use it to stream TV shows and movies to their TV. This is possible because these smart TVs have embedded systems giving them additional capabilities.

Other smart devices include wearable technology and home automation systems.

Combined, these smart devices are often referred to as the Internet of things (***IoT***).

Wearable technology has exploded in recent years. It includes any device you can wear or have implanted. These devices can then be used to interact with other devices, such as a smartphone. As an example, Fitbit has manufactured a range of products that you can wear to monitor your health and fitness. Combined with an app on their smartphone, people can gain insight into how well they're doing on their goals.

Most veterinarians recommend implanting microchips in pets. Animal shelters routinely look for these and if found, they can help return the pets to their owners. Some can even be used to open some pet doors. The company Dangerous Things sells a similar device for people that can reportedly be injected into your hand at the tattoo parlor. Once injected, you can program it to open some smart locks or control your cell phone. Be careful, though. Dangerous Things warns "Use of this device is strictly at your own risk."

Home automation includes Internet-connected devices, such as wireless thermostats, lighting, coffee makers, and more. These devices typically connect to the home's network, which gives them Internet access. This allows people to access or control these devices from the Internet, even when they aren't home.

Camera systems often include Internet-connected cameras. These cameras can be within a home automation system or supporting physical security goals for an organization.

A system on a chip (***SoC***) is an integrated circuit that includes all the functionality of a computing system within the hardware. It typically includes an application contained within onboard memory, such as read-only memory (ROM), electrically erasable programmable ROM (EEPROM), or flash memory. Many mobile computing devices include an SoC.

Remember this

An embedded system is any device that has a dedicated function and uses a computer system to perform that function. It includes any devices in the Internet of things (IoT) category, such as wearable technology and home automation systems. Some embedded systems use a system on a chip (SoC).

An industrial control system (***ICS***) typically refers to systems within large facilities such as power plants or water treatment facilities. An ICS is controlled by a supervisory control and data acquisition (***SCADA***) system. Ideally, these systems are contained within isolated networks, such as within a virtual local area network (VLAN), that do not have access to the Internet. If they are connected to the corporate network, they are often protected by a network intrusion prevention system (NIPS) to block unwanted traffic. Chapter 3 discusses VLANs and Chapter 4 discusses NIPS.

Understanding Stuxnet (Sidebar)

Stuxnet provides a great example of the need to protect embedded systems, such as SCADA systems. Stuxnet is a computer worm designed to attack a specific embedded system used in one of Iran's nuclear enrichment facilities. It caused centrifuges to spin fast enough to tear themselves apart and some reports indicated it destroyed as many as 20 percent of these centrifuges.

Security expert Roel Schouwenberg completed extensive research on Stuxnet and identified how it operated in six major steps:

1. **Infection.** Stuxnet first infected Windows systems through infected USB drives after someone plugged one into the system. One of the architects of Stuxnet reportedly said "...there is always an idiot around who doesn't think much about the thumb drive in their hand." Indeed, USB sticks have been the source of many infections.
2. **Search.** Stuxnet checks the network of the infected system looking for the targeted system.
3. **Update.** If it finds the targeted system, it downloads an updated version of the worm.
4. **Compromise.** It then attempts to compromise the targeted system. When first released, Stuxnet took advantage of four zero-day vulnerabilities. Zero-day vulnerabilities are either unknown to the vendor, or the vendor hasn't released a patch for them yet.
5. **Control.** It then sends signals to the systems. A late version of Stuxnet told the systems to spin the centrifuges uncontrollably.
6. **Deceive and destroy.** While it was causing the

> centrifuges to spin out of control, it was sending false data to engineers monitoring the system. Monitoring systems indicated everything was fine.

A real-time operating system (***RTOS***) is an operating system that reacts to input within a specific time. If it can’t respond within the specified time, it doesn’t process the data and typically reports an error. As an example, imagine an automated assembly line used to create donuts. Each location on the line receives materials from the previous location, adds additional materials or somehow processes the materials (such as mixing them), and passes the result to the next location. Each of these locations could include an embedded system with an RTOS to ensure it receives and processes the materials within a specified time. If it doesn’t, it can raise an error or alert and stop the assembly line.

Admittedly, an RTOS is probably overkill for a donut assembly line. There are simpler ways. However, some assembly lines are much quicker and require response times for each location in the millisecond or nanosecond range. An RTOS can be used reliably in these systems.

Heating, ventilation, and air conditioning (***HVAC***) systems keep computing systems at the proper temperature and with the proper humidity. Most have embedded systems to control them. If attackers can access these systems, they may be able to remotely turn off the HVAC system or trick it into keeping the temperature at 95 degrees within a data center. The resulting damage to systems within this data center could be catastrophic.

You can also find many embedded systems in special-purpose devices, such as medical devices, automotive vehicles, and unmanned aerial vehicles. Some control dedicated tasks, such as ensuring each engine cylinder fires at exactly the right time. Others control much more complex tasks, such as automatically parallel parking a car. Select the option and take your hands off the wheel. The car will park itself, within the space, and without hitting anything.

While these systems aren't necessarily accessible via the Internet, many autos now include Internet access via satellite communications. Manufacturers could decide to integrate all the embedded systems in an automobile, making them all accessible via the Internet.

Aircraft and unmanned aerial vehicles (***UAVs***) include embedded systems. Hobbyists use small UAVs to take pictures remotely. Other organizations such as the military include sophisticated embedded systems for reconnaissance and to deliver weapons.

Remember this

A supervisory control and data acquisition (SCADA) system has embedded systems that control an industrial control system (ICS), such as one used in a power plant or water treatment facility. Embedded systems are also used for many special purposes, such as medical devices, automotive vehicles, aircraft, and unmanned aerial vehicles (UAVs).

Protecting Data

Data is one of the most valuable resources any organization manages, second only to its people. If you ever tune into the news, you've likely heard about data breaches at organizations such as Arby's, Edmodo, OkCupid, St. Mark's Surgery Center, Uber, Verizon, Washington State University, and Yahoo!. Unfortunately, data breaches are frequent and they affect millions of people. In the worst-case scenarios, thieves use the stolen data to empty bank accounts, rack up fraudulent charges on credit cards, and steal individuals' identities.

Losing control of data directly affects the reputation, and often the bottom line, of an organization. The importance of taking steps to protect valuable data cannot be overstated.

Chapter 11 covers security policies that an organization can implement to protect data. The security policy helps an organization classify and label its data. This section presents many of the security controls an organization can use to protect data based on the requirements set within a data security policy.

Confidentiality is primarily protected through encryption and strong access controls. Chapter 2 focuses on access controls starting with strong authentication methods. This chapter discusses software-based and hardware-based encryption methods, and Chapter 10 covers specific encryption algorithms used to protect data.

Protecting Confidentiality with Encryption

As mentioned in Chapter 1, one of the primary ways you can prevent the loss of confidentiality is by encrypting data. This includes encrypting data-at-rest no matter what type of device it is stored on and encrypting data-in-transit no matter what type of transmission media is used. It is much more difficult for an attacker to view encrypted data than it is to view unencrypted data.

You can use other tools to restrict access to data, but this isn't always effective. For example, consider the Microsoft New Technology File System (NTFS), which allows you to configure permissions within access control lists (ACLs). You can use NTFS to set permissions on files and folders to restrict access. However, if a thief steals a laptop with NTFS-protected files, it's a simple matter to access them. The thief simply moves the drive to another system as an extra drive, logs on as the administrator, and takes ownership of the files. Encryption isn't as easy to bypass.

Database Security

Another form of software-based encryption is with databases. For example, many database applications such as Oracle Database or Microsoft SQL Server include the ability to encrypt data held within a database. Although it's possible to encrypt the entire database, it's more common to encrypt specific data elements.

As an example, imagine a database includes a table named Customers. Each record within the table has multiple columns, including customer number, last name, first name, credit card number, and security code. Instead of encrypting the entire table, administrators can choose to encrypt only the credit card number and security code fields within each record. This protects the sensitive data, but doesn't waste valuable processing power encrypting data that isn't sensitive.

Remember this

The primary methods of protecting the confidentiality of data are with encryption and strong access controls. Database column encryption protects individual fields within a database.

File System Security

Many operating systems support file- and folder-level encryption. Linux systems support GNU Privacy Guard (GnuPG or GPG), which is a command-line tool used to encrypt and decrypt files with a password. Microsoft NTFS includes the Encrypting File System (EFS), available in most Windows operating systems. An attacker will have a more difficult time accessing these encrypted files.

A benefit of file- and folder-level encryption is that you can encrypt individual files without encrypting an entire disk. For example, a server may store files accessed by users throughout the company. Access controls provide a first level of protection for these files, but administrators may be able to bypass the access controls. Imagine that a company stores payroll data on the server and wants to ensure that a malicious insider with administrative privileges can't access the data. Using file encryption provides an additional level of protection.

Permission Issues and Access Violations

A common security issue with permissions is giving users more permissions than they need. The principle of least privilege is a core security principle and mentioned several times in this book. In short, it means that users are given only the rights and permissions they need to do their job, and no more. When users have more permissions than they need, they can accidentally, or maliciously, cause problems.

An access violation occurs if users access materials that they shouldn't. As an example, imagine that Bart is a help-desk technician. During a review of logs, security administrators discover that Bart has accessed payroll data though he has no business looking at this data. This is an access violation and should be investigated. A primary objective of security investigators is to discover how Bart accessed the materials.

Linux Permissions

CompTIA has been increasingly adding questions about Linux so you should understand some basics about Linux permissions. There are three primary entities that you can assign permissions to within Linux. They are:

- **Owner.** This is a user who owns the file or directory and the owner is typically granted all permissions for the file or directory.
- **Group.** The file can also be owned by a named group. Members of this group are granted specific permissions for the file or directory. These permissions are typically less than the permissions applied to the owner.
- **Others.** You can think of this as everyone else. Permissions applied here do not override the Owner or Group permissions.

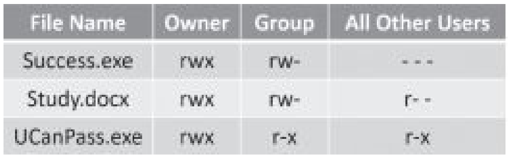
In addition to understanding who you can assign permissions to, it's also important to understand the basic Linux permissions. These may be represented as letters (*r*, *w*, and *x*) or as numbers. They are:

- **Read (r).** This allows you to view the file and is represented with the number **4**.
- **Write (w).** This allows you to modify the file and is represented with the number **2**.
- **Execute (x).** This allows you to run the file (assuming it is an application) and is represented with the number **1**.

If a permission is not assigned, you'll see it represented as a dash. It's also possible to assign multiple permissions, such as Read and Execute; Read and Write; and Read, Write, and Execute. The following bullets show the numbers used to represent combined permissions:

- **5** indicates Read (4) + Execute (1)
- **6** indicates Read (4) + Write (2)
- **7** indicates Read (4) + Write (2) + Execute (1)

Table 5.1 shows how these Linux permission types are often displayed in a file access control list (FACL). Each line represents the FACL for a different file.



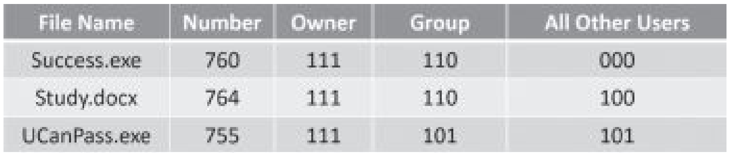
File Name	Owner	Group	All Other Users
Success.exe	rwx	rw-	- - -
Study.docx	rwx	rw-	r- -
UCanPass.exe	rwx	r-x	r-x

Table 5.1: Linux permissions

Looking at Table 5.1, you can see that the following permissions will be assigned to the different entities:

- **Success.exe.** Owner has read, write, and execute permissions (rwx), Group has read and write permissions (rw-), and other users have zero permissions (- - -).
- **Study.docx.** Owner has read, write, and execute permissions (rwx), Group has read and write permissions (rw-), and other users have read permissions (r- -).
- **UCanPass.exe.** Owner has read, write, and execute permissions (rwx), Group has read and execute permissions (r-x), and other users have read and execute permissions (r-x).

Table 5.2 shows these same permissions represented as numbers.



File Name	Number	Owner	Group	All Other Users
Success.exe	760	111	110	000
Study.docx	764	111	110	100
UCanPass.exe	755	111	101	101

Table 5.2: Linux permissions in octal notation

Administrators typically use the chmod command (short for change mode) to change permissions for files. As an example, imagine that a file named *Success.exe* currently has the permissions set as 760 (rwx rw- - - -), but you want to change the permissions to 755 (rwx r-x r-x). You could use the following command:

```
chmod 755 success.exe
```

Remember this

File- and folder-level protection protects individual files. Full disk encryption protects entire disks, including USB flash drives and drives on mobile devices. The chmod command changes permissions on Linux systems.

Windows Permissions

Windows file and folder permissions are a little easier to understand because they are assigned by just pointing and clicking. For example, to modify the permissions for a file or folder, an administrator would right-click the file within File Explorer, select the Security tab, and modify the permissions. The following list shows the basic Windows permissions:

- **Read.** Users granted read permission can view the contents of a file or folder.
- **Read & Execute.** Users granted the Read & Execute permission have Read permission and they can also run or execute programs.
- **Write.** Users can create new files and folders, and they can also make changes to existing files and folders. This would typically be assigned with Read permission.
- **Modify.** When granted the Modify permission to a file or a folder, a user can read, execute, write, and delete files and folders. The primary addition is the ability to delete files and folders.

Data Loss Prevention

Organizations often use data loss prevention (***DLP***) techniques and technologies to prevent data loss. They can block the use of USB flash drives and control the use of removable media. They can also examine outgoing data and detect many types of unauthorized data transfers.

Removable Media

Removable media refers to any storage system that you can attach to a computer and easily copy data. It primarily refers to USB hard drives and USB flash drives, but many personal music devices, such as MP3 players, use the same type of flash drive memory as a USB flash drive. Users can plug them into a system and easily copy data to and from a system. Additionally, many of today’s smartphones include storage capabilities using the same type of memory.

It’s common for an organization to include security policy statements to prohibit the use of USB flash drives and other removable media. Some technical policies block use of USB drives completely.

A DLP solution is more selective and it can prevent a user from copying or printing files with specific content. For example, it’s possible to configure a DLP solution to prevent users from copying or printing any classified documents marked with a label of Confidential. The DLP software scans all documents sent to the printer, and if it contains the label, the DLP software blocks it from reaching the printer.

In addition to blocking the transfer, a DLP solution will typically log these events. Some DLP solutions will also alert security administrators of the event. Depending on the organization's policy, personnel may be disciplined for unauthorized attempts to copy or print files.

Data Exfiltration

Data exfiltration is the unauthorized transfer of data outside an organization and is a significant concern. In some cases, attackers take control of systems and transfer data outside an organization using malware. It's also possible for malicious insiders to transfer data.

Chapter 3 discusses different types of content filters used in unified threat management (UTM) devices. These devices monitor incoming data streams looking for malicious code. In contrast, a network-based DLP monitors outgoing data looking for sensitive data, specified by an administrator.

DLP systems can scan the text of all emails and the content of any attached files, including documents, spreadsheets, presentations, and databases. Even if a user compresses a file as a zipped file before sending it, the DLP examines the contents by simply unzipping it.

As an example, I know of one organization that routinely scans all outgoing emails looking for Personally Identifiable Information (PII), such as Social Security numbers. The network-based DLP includes a mask to identify Social Security numbers as a string of numbers in the following format: ###-##-####. If an email or an attachment includes this string of numbers, the DLP detects it, blocks the email, and sends an alert to a security administrator.

Many organizations classify and label data using terms such as Confidential, Private, and Proprietary. It is easy to include these search terms in the DLP application, or any other terms considered important by the organization.

Network-based DLP systems are not limited to scanning only email. Many can scan the content of other traffic, such as FTP and HTTP traffic. Sophisticated data exfiltration attacks often encrypt data before sending it out, making it more difficult for a DLP system to inspect the data. However, a

DLP system can typically be configured to look for outgoing encrypted data and alert security administrators when it is detected.

Cloud-Based DLP

It’s common for personnel within organizations to store data in the cloud. This makes it easier to access the data from any location and from almost any device. Cloud-based DLP solutions allow an organization to implement policies for data stored in the cloud.

As an example, an organization can implement policies to detect Personally Identifiable Information (PII) or Protected Health Information (PHI) stored in the cloud. After detecting the data, a DLP policy can be configured to take one or more actions such as sending an alert to a security administrator, blocking any attempts to save the data in the cloud, and quarantining the data.

Remember this

Data exfiltration is the unauthorized transfer of data out of a network. Data loss prevention (DLP) techniques and technologies can block the use of USB devices to prevent data loss and monitor outgoing email traffic for unauthorized data transfers. A cloud-based DLP can enforce security policies for data stored in the cloud, such as ensuring that Personally Identifiable Information (PII) is encrypted.

Chapter 5 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Implementing Secure Systems

- Least functionality is a core secure system design principle. It states that systems should be deployed with only the applications, services, and protocols they need to function.
- A trusted operating system meets a set of predetermined requirements such as those defined in the Common Criteria. It typically uses the mandatory access control (MAC) model.
- A master image provides a secure starting point for systems. Master images are typically created with templates or other baselines to provide a secure starting point for systems. Integrity measurement tools detect when a system deviates from the baseline.
- Patch management procedures ensure operating systems and applications are kept up to date with current patches. This ensures they are protected against known vulnerabilities.
- Change management policies define the process for making changes and help reduce unintended outages from changes.
- Application whitelisting allows authorized software to run, but blocks all other software. Application blacklisting blocks unauthorized software, but allows other software to run.
- Sandboxing provides a high level of flexibility for testing security controls and testing patches. You can create sandboxes in virtual machines (VMs) and with the chroot command on Linux systems.
- Electromagnetic interference (EMI) comes from sources such as motors, power lines, and fluorescent lights and can be prevented with shielding.
- Electromagnetic pulse (EMP) is a short burst of electromagnetic energy. Mild forms such as electrostatic discharge and lightning can be prevented but EMP damage from military weapons may not be preventable.
- Full disk encryption (FDE) encrypts an entire disk. A self-

encrypting drive (SED) includes the hardware and software necessary to automatically encrypt a drive.

- A Trusted Platform Module (TPM) is a chip included with many laptops and some mobile devices and it provides full disk encryption, a secure boot process, and supports remote attestation. TPMs have an encryption key burned into them that provides a hardware root of trust.
- A hardware security module (HSM) is a removable or external device used for encryption. An HSM generates and stores RSA encryption keys and can be integrated with servers to provide hardware-based encryption.

Summarizing Cloud Concepts

- Cloud computing provides an organization with additional resources. Most cloud services are provided via the Internet or a hosting provider. On-premise clouds are owned and maintained by an organization.
- Software as a Service (SaaS) includes web-based applications such as web-based email.
- Infrastructure as a Service (IaaS) provides hardware resources via the cloud. It can help an organization limit the size of their hardware footprint and reduce personnel costs.
- Platform as a Service (PaaS) provides an easy-to-configure operating system and on- demand computing for customers.
- A cloud access security broker (CASB) is a software tool or service deployed between an organization’s network and the cloud provider. It monitors all network traffic and can enforce security policies acting as Security as a Service.
- Private clouds are only available for a specific organization. Public cloud services are provided by third-party companies and available to anyone. A community cloud is shared by multiple organizations. A hybrid cloud is a combination of two or more clouds.

Deploying Mobile Devices Securely

- Mobile devices include smartphones and tablets and run a mobile operating system.

- Corporate-owned, personally enabled (COPE) mobile devices are owned by the organization, but employees can use them for personal reasons.
- Bring your own device (BYOD) policies allow employees to connect their mobile device to the organization’s network. Choose your own device (CYOD) policies include a list of acceptable devices and allow employees with one of these devices to connect them to the network.
- A virtual desktop infrastructure (VDI) is a virtual desktop and these can be created so that users can access them from a mobile device.
- Mobile devices can connect to the Internet, networks, and other devices using cellular, wireless, satellite, Bluetooth, near field communication (NFC), ANT, infrared, and USB connections.
- Mobile device management (MDM) tools help ensure that devices meet minimum security requirements. They can monitor devices, enforce security policies, and block network access if devices do not meet these requirements.
- MDM tools can restrict applications on devices, segment and encrypt data, enforce strong authentication methods, and implement security methods such as screen locks and remote wipe.
- A screen lock is like a password-protected screen saver on desktop systems that automatically locks the device after a period of time. A remote wipe signal removes all the data from a lost phone.
- Geolocation uses Global Positioning System (GPS) to identify a device’s location. Geofencing uses GPS to create a virtual fence or geographic boundary. Organizations use geofencing to enable access to services or devices when they are within the boundary, and block access when they are outside of the boundary.
- Geotagging uses GPS to add geographical information to files (such as pictures) when posting them on social media sites.
- A third-party app store is something other than the primary store for a mobile device. Apple’s App Store is the primary store for Apple devices. Google Play is a primary store for Android devices.
- Jailbreaking removes all software restrictions on Apple devices. Rooting provides users with root-level access to an Android device. Custom firmware can also root an Android device. MDM tools block

network access for jailbroken or rooted devices.

- Sideloading is the process of copying an application to an Android device instead of installing it from an online store.
- A Universal Serial Bus On-The-Go (USB OTG) cable allows you to connect mobile devices.
- Tethering allows one mobile device to share its Internet connection with other devices. Wi-Fi Direct allows you to connect devices together without a wireless router.

Exploring Embedded Systems

- An embedded system is any device that has a dedicated function and uses a computer system to perform that function. A security challenge with embedded systems is keeping them up to date.
- Embedded systems include smart devices sometimes called the Internet of things (IoT), such as wearable technology and home automation devices.
- A system on a chip (SoC) is an integrated circuit that includes a full computing system.
- A supervisory control and data acquisition (SCADA) system controls an industrial control system (ICS). The ICS is used in large facilities such as power plants or water treatment facilities. SCADA and ICS systems are typically in isolated networks without access to the Internet, and are sometimes protected by network intrusion prevention systems (NIPSs).
- A real-time operating system (RTOS) is an operating system that reacts to input within a specific time.
- Embedded systems are found in many common and special-purpose devices. This includes multi-function devices (MFDs), such as printers; heating, ventilation, and air conditioning (HVAC) systems; medical devices; automotive vehicles; aircraft; and unmanned aerial vehicles (UAVs).

Protecting Data

- The primary method of protecting the confidentiality of data is with encryption and strong access controls. File system security includes the use of encryption to encrypt files and folders.

- You can encrypt individual columns in a database (such as credit card numbers), entire databases, individual files, entire disks, and removable media.
- Users should be given only the permissions they need. When they have too much access, it can result in access violations or the unauthorized access of data.
- You can use the chmod command to change permissions on a Linux system.
- Data exfiltration is the unauthorized transfer of data outside an organization.
- Data loss prevention (DLP) techniques and technologies help prevent data loss. They can block transfer of data to USB devices and analyze outgoing data via email to detect unauthorized transfers. Cloud-based DLP systems can enforce security policies for any data stored in the cloud.

Online References

- Are you ready for performance-based questions? Don't forget to check out the online content at *http://gcgapremium.com/501-extras.*

Chapter 5 Practice Questions

1. Attackers recently attacked a web server hosted by your organization. Management has tasked administrators with configuring the servers following the principle of least functionality. Which of the following will meet this goal?

   A. Disabling unnecessary services
   B. Installing and updating antivirus software
   C. Identifying the baseline
   D. Installing a NIDS

2. Network administrators have identified what appears to be malicious traffic coming from an internal computer, but only when no one is logged on to the computer. You suspect the system is infected with malware. It periodically runs an application that attempts to connect to web sites over port 80 with Telnet. After comparing the computer with a list of applications from the master image, you verify this application is very likely the problem. What allowed you to make this determination?

   A. Least functionality
   B. Sandbox
   C. Blacklist
   D. Integrity measurements

3. Security experts want to reduce risks associated with updating critical operating systems. Which of the following will BEST meet this goal?

   A. Implement patches when they are released.
   B. Implement a change management policy.
   C. Use only trusted operating systems.
   D. Implement operating systems with secure configurations.

4. Your organization wants to ensure that employees do not install any unauthorized software on their computers. Which of the following is the BEST choice to prevent this?

   A. Master image
   B. Application whitelisting
   C. Anti-malware software
   D. Antivirus software

5. A software vendor recently developed a patch for one of its applications. Before releasing the patch to customers, the vendor needs to test it in different environments. Which of the following solutions provides the BEST method to test the patch in different environments?

A. Baseline image
B. BYOD
C. Sandbox
D. Change management

6. Managers within your organization want to implement a secure boot process for some key computers. During the boot process, each computer should send data to a remote system to check the computer's configuration. Which of the following will meet this goal?

A. Trusted Platform Module
B. Hardware root of trust
C. Remote attestation
D. Trusted operating system

7. The Springfield Nuclear Power Plant has created an online application teaching nuclear physics. Only students and teachers in the Springfield Elementary school can access this application via the cloud. What type of cloud service model is this?

A. IaaS
B. PaaS
C. SaaS
D. Public

8. An organization has a critical SCADA network it is using to manage a water treatment plant for a large city. Availability of this system is important. Which of the following security controls would be MOST relevant to protect this system?

A. DLP
B. TPM
C. EMP
D. NIPS

9. Bizzfad is planning to implement a CYOD deployment model. You're asked to provide input for the new policy. Which of the following concepts are appropriate for this policy?

A. SCADA access

B. Storage segmentation
C. Database security
D. Embedded RTOS

10. A new mobile device security policy has authorized the use of employee-owned devices, but mandates additional security controls to protect them if they are lost or stolen. Which of the following meets this goal?

A. Screen locks and GPS tagging
B. Patch management and change management
C. Screen locks and device encryption
D. Full device encryption and IaaS

11. Management within your company wants to restrict access to the Bizz app from mobile devices. If users are within the company's property, they should be granted access. If they are not within the company's property, their access should be blocked. Which of the following answers provides the BEST solution to meet this goal?

A. Geofencing
B. Geolocation
C. GPS tagging
D. Containerization

12. Management within your company wants to implement a method that will authorize employees based on several elements, including the employee's identity, location, time of day, and type of device used by the employee. Which of the following will meet this need?

A. Geofence
B. Containerization
C. Tethering
D. Context-aware authentication

13. Lisa does not have access to the *project.doc* file, but she needs access to this file for her job. Homer is the system administrator and he has identified the following permissions for the file:

rwx rw- ---

What should Homer use to grant Lisa read access to the file?

A. The chmod command
B. A remote wipe
C. Push notification
D. The chroot command

14. Management within your organization wants to prevent users from copying documents to USB flash drives. Which of the following can be used to meet this goal?

A. DLP
B. HSM
C. COPE
D. SED

15. Your organization hosts a web site with a back-end database. The database stores customer data, including credit card numbers. Which of the following is the BEST way to protect the credit card data?

A. Full database encryption
B. Whole disk encryption
C. Database column encryption
D. File-level encryption

Chapter 5 Practice Question Answers

1. **A.** Disabling unnecessary services is one of the elements of the principle of least functionality. Other elements include deploying the server with only the applications and protocols they need to meet their purpose. Installing up-to-date antivirus software is a valid preventive control, but it isn't related to least functionality. Identifying the baseline should be done after disabling unnecessary services. A network-based intrusion detection system (NIDS) helps protect the server, but it doesn't implement least functionality.

2. **D.** The master image is the baseline and the administrators performed integrity measurements to identify baseline deviations. By comparing the list of applications in the baseline with the applications running on the suspect computer, you can identify unauthorized applications. None of the other answers include the troubleshooting steps necessary to discover the problem. The master image would include only the applications, services, and protocols needed to meet the principle of least functionality. A sandbox is an isolated area of a system, typically used to test applications. A blacklist is a list of prohibited applications.

3. **B.** A change management policy helps reduce risk associated with making any changes to systems, including updating them. Patches should be tested and evaluated before implementing them and implementing them when they are released sometimes causes unintended consequences. The use of a trusted operating system or operating systems with secure configurations doesn't address how they are updated.

4. **B.** Application whitelisting identifies authorized applications and prevents users from installing unauthorized software. Alternately, you can use a blacklist to identify specific applications that cannot be installed or run on a system. A master image provides a secure baseline, but it doesn't prevent users from installing additional applications. Anti-malware software and antivirus software can detect and block malware, but they don't prevent users from installing unauthorized software.

5. **C.** A sandbox provides a simple method of testing patches and would

be used with snapshots so that the virtual machine (VM) can easily be reverted to the original state. A baseline image is a starting point of a single environment. Bring your own device (BYOD) refers to allowing employee-owned mobile devices in a network, and is not related to this question. Change management practices ensure changes are not applied until they are approved and documented.

6. **C.** A remote attestation process checks a computer during the boot cycle and sends a report to a remote system. The remote system attests, or confirms, that the computer is secure. None of the other answers sends data to a remote system. A Trusted Platform Module (TPM) is a hardware chip on a motherboard and provides a local secure boot process. A TPM includes an encryption key burned into the CPU, which provides a hardware root of trust. A trusted operating system meets a set of predetermined requirements typically enforced with the mandatory access control (MAC) model.

7. **C.** This is a Software as a Service (SaaS) model. The software is the online application and the cloud provider (the Springfield Nuclear Power Plant in this example) maintains it. Infrastructure as a Service (IaaS) provides customers with the hardware via the cloud. Customers are responsible for installing the operating system and any applications. Platform as a Service (PaaS) is a computing platform. For example, a cloud provider can provide a server with a preconfigured operating system. Anyone can access a public cloud. However, the question states that only students and teachers can access it.

8. **D.** A network intrusion prevention system (NIPS) is the most relevant security control of those listed to ensure availability of the supervisory control and data acquisition (SCADA) system. A data loss prevention (DLP) system helps prevent loss of data, but wouldn’t protect a SCADA system from potential attacks. A Trusted Platform Module (TPM) is a hardware chip on a computer’s motherboard that stores cryptographic keys used for encryption. An electromagnetic pulse (EMP) is a short burst of electromagnetic energy and unrelated to a SCADA system.

9. **B.** Storage segmentation creates separate storage areas in mobile devices and can be used with a choose your own device (CYOD) mobile device deployment model. None of the other answers are directly related to mobile devices. A supervisory control and data acquisition (SCADA) system controls an industrial control system (ICS), such as those used in nuclear power plants or water treatment facilities, and it should be isolated. Database security includes the use of permissions and encryption to protect data in a database. Some embedded systems use a real-time operating system (RTOS) when the system must react within a specific time.

10. **C.** Screen locks provide protection for lost devices by making it more difficult for someone to access the device. Device encryption protects the confidentiality of the data. Global Positioning System (GPS) tagging includes location information on pictures and other files but won’t help protect a lost or stolen device. Patch management keeps devices up to date and change management helps prevent outages from unauthorized changes. Infrastructure as a Service (IaaS) is a cloud computing option.

11. **A.** Geofencing can be used to create a virtual fence or geographic boundary, outlining the company’s property. Geofencing will use geolocation to identify the mobile device’s location, but geolocation without geofencing won’t detect if a user is on the company’s property. Global Positioning System (GPS) tagging adds geographic data (such as latitude and longitude data) to files and is unrelated to this question. Containerization runs applications in a container to isolate them.

12. **D.** Context-aware authentication can authenticate a user and a mobile device using multiple elements, including identity, geolocation, time of day, and type of device. None of the other answers meets all the requirements of the question. A geofence creates a virtual fence, or geographic boundary, and can be used with context-aware authentication. Containerization isolates an application, protecting it and its data. Tethering allows one device to share its Internet connection with other devices.

13. **A.** The system administrator should modify permissions with the

chmod (short for change mode) command. Remote wipe sends a remote signal to a mobile device to wipe or erase all the data and is unrelated to this question. Push notification services send messages to users but don’t change permissions. The chroot command is used to create a sandbox for testing an application.

14. **A.** A data loss prevention (DLP) solution can prevent users from copying documents to a USB drive. None of the other answers control USB drives. A hardware security module (HSM) is an external security device used to manage, generate, and securely store cryptographic keys. COPE (corporate-owned, personally enabled) is a mobile device deployment model. A self-encrypting drive (SED) includes the hardware and software to encrypt all data on the drive and securely store the encryption keys.

15. **C.** Database column (or field) encryption is the best choice because it can be used to encrypt the fields holding credit card data, but not fields that don’t need to be encrypted. Full database encryption and whole disk encryption aren’t appropriate because everything doesn’t need to be encrypted to protect the credit card data. File-level encryption isn’t appropriate on a database and will often make it inaccessible to the database application.