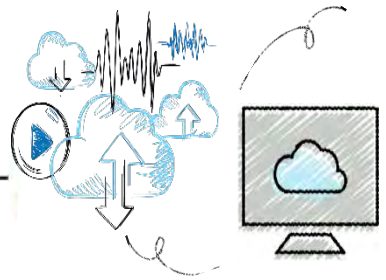
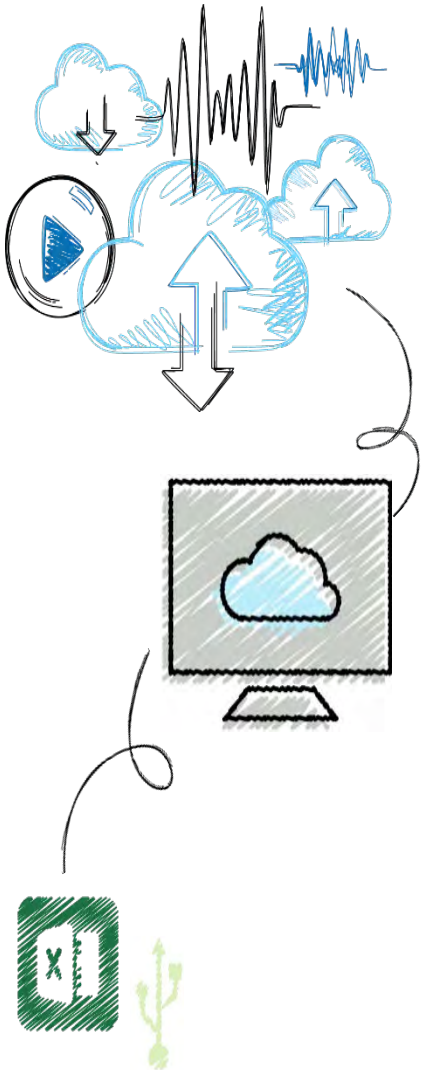
CompTIA Security+

Chapter 9

Client and Application Security





Objectives

9.1 List the steps for securing a client device

9.2 Define application security

9.3 Explain how physical security can be used for protection

Client Security

- Securing the client involves:
  - Using hardware system security
  - Securing the operating system software
  - Protecting peripheral devices connected to the client

Hardware System Security

- Protecting client hardware involves using different tools:
  - Secure booting tools
  - A hardware root of trust
  - Preventing electromagnetic spying

Secure Booting (1 of 2)

- BIOS (Basic Input/Output System)
  - Firmware used on early computers to hold the boot process
  - Ability to update the BIOS with a firmware update opened the door for a threat actor to create malware to infect the BIOS
- To combat BIOS attacks **UEFI (Unified Extensible Firmware Interface)** was developed to replace BIOS
- In conjunction with UEFI
  - **Secure Boot** security standard was also created
- When using UEFI and Secure Boot, a computer checks the digital signature of each piece of boot software
  - If signatures are deemed valid the computer boots
  - If not, computer does not boot

Secure Booting (2 of 2)

Figure 9-1 Booting using a BIOS

Hardware Root of Trust

- Chain of trust
  - Each element (of the boot process) relies on the confirmation of the previous element to know that the entire process is secure
- Hardware root of trust
  - Strongest starting point is hardware, which cannot be modified
- Security checks are “rooted” in hardware checks

Electromagnetic Spying

- Security researcher have found that it is possible to pick up electromagnetic fields and read data that is producing them
- U.S. government has developed a classified standard
  - Intended to prevent attackers from picking up electromagnetic fields from government buildings
  - Known as Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST)

Supply Chain Infections

- Supply chain
  - A network that moves a product from the supplier to the customer
- The different steps in the supply chain has opened the door for malware to be injected into products during their manufacturing or storage
  - Called supply chain infections
- Supply chain infections are considered dangerous
  - If malware is planted in the ROM firmware of a device, it can difficult or impossible to clean an infected device
  - Users may be receiving infected devices at the point of purchase, unaware of the infection
  - Cannot be easily prevented

Securing the Operating System Software

OS type	Uses	Examples
Network OS	Software that runs on a network device like a firewall, router, or switch	Cisco Internetwork OS (IOS), Juniper JUNOS, MikroTik Router OS
Server OS	OS software that runs on a network server to provide resources to network users	Microsoft Windows Server, Apple macOS Server, Red Hat Linux
Workstation OS	Software that manages hardware and software on a client computer	Microsoft Windows, Apple mac OS, Ubuntu Linux
Appliance OS	OS in firmware that is designed to manage a specific device like a digital video recorder or video game console	Linpus Linux
Kiosk OS	System and user interface software for an interactive kiosk	Microsoft Windows, Google Chrome OS, Apple iOS, Instant WebKiosk, KioWare (Android)
Mobile OS	OS for mobile phones, smartphones, tablets, and other handheld devices	Google Android, Apple iOS, Microsoft Windows Mobile

OS Security Configuration

- Typical OS security configuration should include:
  - Disabling unnecessary ports and services
  - Disabling default accounts/passwords
  - Employing least functionality
  - Application whitelisting/blacklisting
- Instead of recreating the same security configuration on each computer
  - Tools can be used to automate the process
- In Microsoft Windows
  - A security template is a collection of security configuration settings that can be deployed to other devices

Patch Management (1 of 5)

- Operating systems have increased in size and complexity
- New attack tools have made secure functions vulnerable
- **Security patch** - software security update to repair discovered vulnerabilities
- **Feature update** – includes enhancements to the software to provide new or expanded functionality
  - Does not address security vulnerability
- **Service pack** - accumulates security updates and additional features
- Patch management tools:
  - Tools for patch distribution
  - Patch reception

Patch Management (2 of 5)

- Patch Distribution
  - Patches can sometimes create new problems
    - Vendor should thoroughly test before deploying
  - **Automated patch update service**
    - Manage patches locally rather than rely on vendor's online update service
  - Advantages of automated patch update service
    - Downloading patches from a local server can save bandwidth and time
    - Administrators can approve or decline updates, force updates to install by specific date, and obtain reports on what updates each computer needs
    - Administrators can approve updates for "detection" only; allows them to see which computers will require the update without actually installing it

Patch Management (3 of 5)

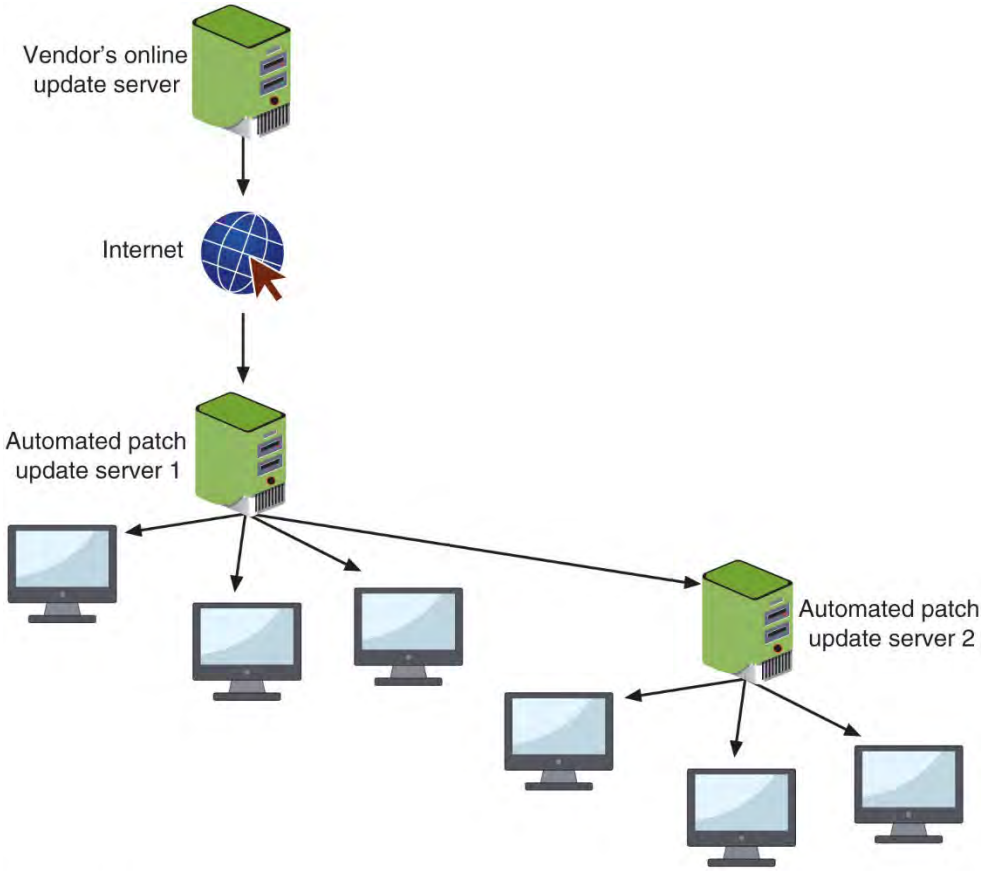


Figure 9-2 Automated patch update service

Patch Management (4 of 5)

- Patch Reception
  - Today, patches are automatically downloaded and installed
  - Ensures the software is always up-to-date
  - Microsoft changed its security update procedures and user options:
    - Forced updates
    - No selective updates
    - More efficient distribution
    - Up-to-date resets

Patch Management (5 of 5)

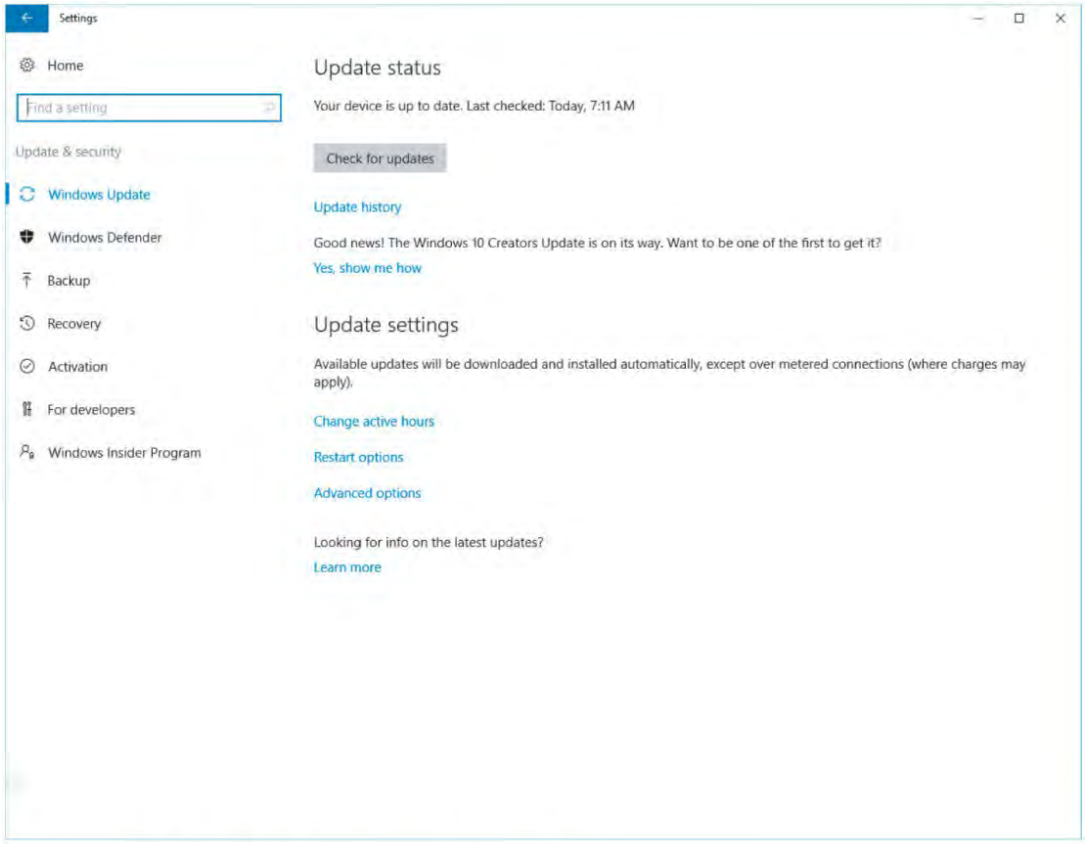


Figure 9-3 Windows 10 update options

Antimalware (1 of 5)

- Antimalware software packages can provide added security
- Antimalware software includes:
  - Antivirus
  - Antispam
  - Antispyware

Antimalware (2 of 5)

- **Antivirus (AV)** - Software that examines a computer for infections
  - Scans new documents that might contain viruses
  - Searches for known virus patterns
- Weakness of anti-virus
  - Vendor must continually search for new viruses, update and distribute signature files to users
- A newer approach to AV is heuristic monitoring (called dynamic analysis)
  - Uses a variety of techniques to spot characteristics of a virus instead of attempting to make matches
- One AV heuristic monitoring technique: **code emulation**
  - Questionable code is executed in virtual environment to determine if it is a virus

Antimalware (3 of 5)

- **Antispam**
  - Mail gateway – monitors emails for spam and other unwanted content
  - Some spam can slip through
  - Antispam filtering software traps spam
- Spam filtering methods
  - Create a list of approved and nonapproved senders
    - Blacklist - nonapproved senders
    - Whitelist - approved senders
  - Blocking certain file attachment types
  - Bayesian filtering - divides email messages into two piles: spam and nonspam

Antimalware (4 of 5)

- **Antispyware** - helps prevent computers from becoming infected by different types of spyware
  - **Pop-up** - small window appearing over Web site
    - Usually created by advertisers
  - **Pop-up blockers** - a separate program as part of anti-spyware package
    - Incorporated within a browser
    - Allows user to limit or block most pop-ups
    - Alert can be displayed in the browser
      - Gives user option to display pop-up

Antimalware (5 of 5)

- Trusted OS
  - **OS hardening** - tightening security during the design and coding of the OS
  - **Trusted OS** - an OS that has been designed through OS hardening

Trusted OS hardening technique	Explanation
Least privilege	Remove all supervisor or administrator accounts that can bypass security settings and provide the least-privileged unit to a user or process
Reduce capabilities	Significantly restrict what resources can be accessed and by whom
Read-only file system	Important OS files cannot be changed
Kernel pruning	Remove all unnecessary features that may compromise an OS

Peripheral Device Security (1 of 5)

- Types of peripheral devices to be secured:
  - Devices using SD Input Output Cards
  - Digital cameras
  - External storage devices
  - Multifunctional devices
  - Displays

Peripheral Device Security (2 of 5)

- Secure Digital Input Output (SDIO) Cards
  - Four families of SD cards:
    - SDSC
    - SDHC
    - SDXC
    - SDIO
  - SDIO – a storage card with integrated wireless transmission capabilities
  - Wi-Fi enabled microSD card – an SDIO device used in devices like digital cameras
  - Security for an SDIO card is the same as for securing a standard Wi-Fi network

Peripheral Device Security (3 of 5)

- Digital Cameras
  - Uses internal storage and external SD cards
  - Three types of speed classes:
    - Standard speed class
    - Ultra-high speed (UHS) class
    - Video speed class
  - Protecting data on SD cards can be accomplished:
    - Password-protecting the card
    - Using encryption
    - Write-protecting the card by moving a small external switch to the **Open** position

Peripheral Device Security (4 of 5)

- External Storage Devices
  - At risk for infection by crypto-malware
    - Crypto-malware encrypts all files on any network or attached device that is connected to that computer
  - Includes:
    - Secondary hard disk drives
    - USB hard drives
    - Network-attached storage devices
    - Network servers
    - Cloud-based data repositories (Dropbox, Apple iCloud, etc…)

Peripheral Device Security (5 of 5)

Device	Recommended protection
External USB or e-SATA storage device	Unplug the device from computer when not in use and attach it when needed
Secondary hard disk drive	Unmount the drive when it is not needed by using the mountvol D: /p command or Windows Disk Management utility then mount the drive when necessary
Network-attached storage device	Create a new folder and then create a new user account with a strong password that is the only account that has access to it, and log in and out of that, share as needed
Cloud storage	Turn off automatic synchronization so that files placed in a folder are not immediately synced to the cloud storage

Multifunctional Devices

- Multifunctional device (MFD)
  - Combines the functions of a printer, copier, scanner, and fax machine
- Recommended protections:
  - Locate the MFD in a secure area
  - Configure the MFD with security in mind by changing any default passwords, turning on hard drive encryption, requiring that all stored images be purged, and setting the device to receive latest security patches
  - Separate the MFD print server from the network server
  - Link the print management software to existing data loss prevention (DLP)
  - Minimize the risk of paper-based thefts by using Secure Job Release
  - Make use of semi-visible watermark technology
  - When disposing of, internal drive should be wiped, removed, or destroyed

Displays

- Computer displays (Monitors)
  - Often considered “passive” peripherals
- Security researchers have demonstrated that a threat actor can target a display’s firmware
  - Could enable attacker to view what is being projected on the display

Physical Security

- Physical security includes:
  - External perimeter defenses
  - Internal physical access security
  - Security for protecting the hardware device itself

External Perimeter Defenses

- External perimeter defenses are designed to restrict access to equipment areas
- This type of defense includes:
  - Barriers
  - Guards
  - Motion detection devices

Barriers (1 of 2)

- Fencing - usually a tall, permanent structure
  - Modern perimeter fences are equipped with other deterrents such as proper lighting and signage
- Cage – a fenced secure waiting station area
  - Such as an area that can contain visitors to a facility until they can be approved for entry
- Barricade - large concrete ones should be used
- Bollard – short but sturdy vertical post that is used as a vehicular traffic barricade to prevent a car from “ramming” into a secured area

Barriers (2 of 2)

Figure 9-5 Bollards

MartineDF/Shutterstock.com

Security Guards

- Human security guards are considered active security elements
- Video surveillance cameras transmit a signal to a specific and limited set of receivers called **closed circuit television** (CCTV)
  - Frequently used for surveillance in areas that require security monitoring such as banks, casinos, airports, and military installations

Motion Detection

- Motion Detection
  - Determining an object's change in position in relation to its surroundings
  - This movement usually generates an audible alarm

Method	**Example**
Visual	CCTV
Radio frequency	Radar, microwave
Vibration	Seismic sensors
Sound	Microphones
Magnetism	Magnetic sensors
Infrared	Passive and active infrared light sensors

Internal Physical Access Security

- These protections include:
  - Door locks
  - Access logs
  - Mantraps
  - Protected distribution systems for cabling

Door Locks (1 of 3)

- Door locks
  - Standard keyed entry lock provides minimal security
  - Deadbolt locks provide additional security and require that a key be used to both open and lock the door
  - Cipher locks are combination locks that use buttons that must be pushed in the proper sequence
    - Can be programmed to allow a certain individual's code to be valid on specific dates and times

Door Locks (2 of 3)

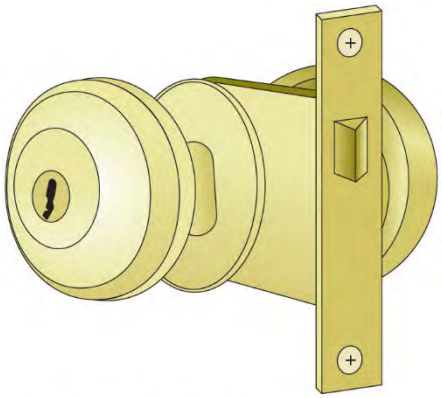


Figure 9-6 Residential keyed entry lock

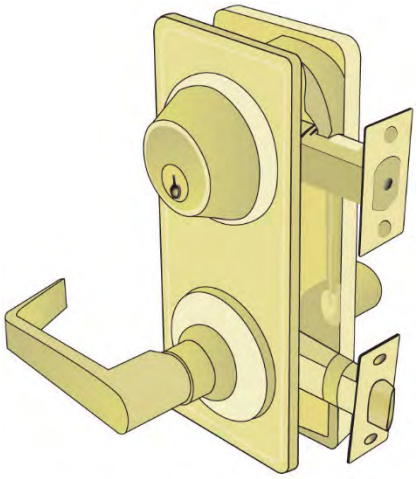


Figure 9-7 Deadbolt lock

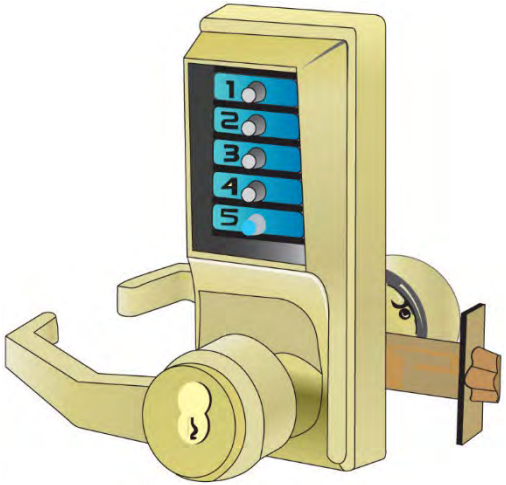


Figure 9-8 Cipher lock

Door Locks (3 of 3)

- Key management procedures:
  - Keep track of keys issued and require users to sign their name when receiving keys
  - Receive the proper approvals of supervisors or other appropriate persons before issuing keys
  - When making duplicates of master keys, mark them “Do Not Duplicate” and wipe out manufacturer’s serial numbers
  - Secure unused keys in a locked safe
  - Change locks immediately upon loss or theft of keys

Access Logs

- Access list
  - Record of individuals who have permission to enter secure area
  - Records time they entered and left
- Today, cipher locks and other technology can create electronic access logs

Mantraps

- Mantrap
  - Separates a secured from a nonsecured area
  - A mantrap device monitors and controls two interlocking doors
    - Only one door may open at any time
  - Used at high-security areas where only authorized persons can enter
    - Such as cash handling areas and research laboratories

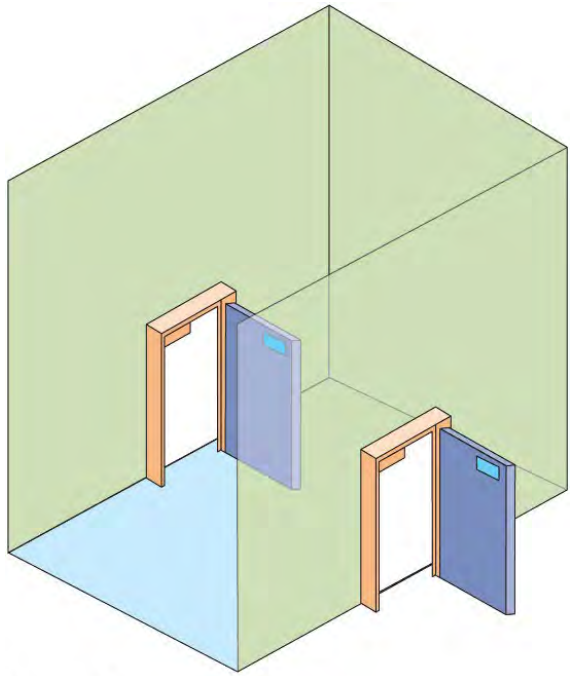


Figure 9-9 Mantrap

Protected Distribution Systems (PDS) (1 of 2)

- Protected Distribution Systems (PDS)
  - A system of cable conduits used to protect classified information that is being transmitted between two secure areas
    - Created by the U.S. Department of Defense (DOD)
  - Two types of PDS:
    - Hardened carrier PDS - conduit constructed of special electrical metallic tubing
    - Alarmed carrier PDS - specialized optical fibers in the conduit that sense acoustic vibrations that occur when an intruder attempts to gain access

Protected Distribution Systems (PDS) (2 of 2)

Figure 9-10 Cable conduits

Peter Sobolev/Shutterstock.com

Computer Hardware Security

- Computer hardware security - the physical security protecting the hardware of the host system
  - Most portable devices have a steel bracket security slot
  - A cable lock can be inserted into slot and secured to device and a cable connected to the lock can be secured to a desk or chair
- Safe or secure cabinet
  - Can be prewired for power and network connections
  - Allow devices to charge while stored as well as receive updates

Application Security

- Besides protecting OS software on hosts, there is a need to protect applications that run on these devices
- Aspects of application security:
  - Application development security
  - Secure coding techniques
  - Code testing

Application Development Concepts (1 of 3)

- Application development stages:
  - Development
  - Testing
  - Staging
  - Production
- Application development lifecycle models:
  - Waterfall model
  - Agile model

Application Development Concepts (2 of 3)

- Secure DevOps methodology includes
  - Security automation
  - Continuous integration
  - Immutable systems
  - Infrastructure as code
  - Baselining
- Provisioning
  - The enterprise-wide configuration, development, and management of multiple types of IT system resources
- Deprovisioning
  - In application development is removing a resource that is no longer needed

Application Development Concepts (3 of 3)

- Because DevOps is based on the agile method
  - There will be continuous modifications throughout the process
  - Important to use tools that support change management
- One tool for change management is version control software that allows changes to be automatically recorded and if necessary “rolled back” to a previous version of the software

Secure Coding Techniques

- There are several coding techniques that should be used to create secure applications and limit data exposure:
  - Determining how encryption will be implemented
  - Ensuring that memory management is handled correctly so as not to introduce memory vulnerabilities

Code Testing (1 of 2)

- At the beginning of the process a **model verification** test is used to ensure that the projected application meets all specifications at that point
- **Compiled code testing**
  - Searches for errors that could prevent the application from properly compiling from source code to application code
- **Runtime code testing**
  - Looks for errors after the program has compiled correctly and is running
  - Most runtime code testing is done in a **sandbox**, which is a testing environment that isolates the untested code from the live production environment

Code Testing (2 of 2)

- **Static program analyzers**
  - Tools that examine software without executing the program
  - Just the source code is reviewed and analyzed
- **Dynamic analysis (fuzzing)**
  - A software testing technique that deliberately provides invalid, unexpected, or random data as inputs to a program
- **Stress testing**
  - Puts the application under a heavier than normal load to determine if the program is robust and can perform all error handling correctly
- **Integrity measurement**
  - An “attestation mechanism” designed to be able to convince a remote party that an application is running only a set of known and approved executables

Review Questions

Which statement about a mantrap is true?

A. It is illegal in the United States.

B. It monitors and controls two interlocking doors to a room.

C. It is a special keyed lock.

D. It requires the use of a cipher lock.

Review Questions

Which statement about a mantrap is true?

A. It is illegal in the United States.

B. **It monitors and controls two interlocking doors to a room**.

C. It is a special keyed lock.

D. It requires the use of a cipher lock.

Review Questions

Which of the following is NOT a typical OS security configuration?

A. Employing least functionality

B. Restricting patch management

C. Disabling default accounts/passwords

D. Disabling unnecessary ports and services

Review Questions

Which of the following is NOT a typical OS security configuration?

A. Employing least functionality

B. **Restricting patch management**

C. Disabling default accounts/passwords

D. Disabling unnecessary ports and services

Review Questions

What allows for a single configuration to be set and then deployed to many or all users?

A. Snap-In Replication (SIR)

B. Active Directory

C. Group Policy

D. Command Configuration

Review Questions

What allows for a single configuration to be set and then deployed to many or all users?

A. Snap-In Replication (SIR)

B. Active Directory

C. **Group Policy**

D. Command Configuration

Review Questions

Which of these is a list of approved email senders?

A. Blacklist

B. Whitelist

C. Bluelist

D. Yellowlist

Review Questions

Which of these is a list of approved email senders?

A. Blacklist

B. **Whitelist**

C. Bluelist

D. Yellowlist

Coming Up Next…

CompTIA Security+

Chapter 10

Mobile and Embedded Device Security