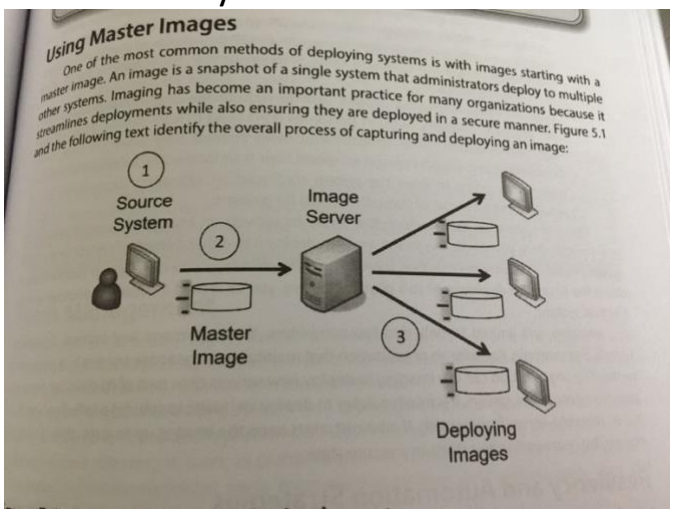
Sec+ 501 Get Certified Topic 5 – Securing Hosts and Data

CH 5

- Least Functionality – Core security principle stating systems should be deployed with the least amount of applications, services and protocols.
- Three types of computer based OS: Windows, Apple, Linux
- Kiosk: Small structure in an open area used to sell something
- Network: Network devices such as switches, routers and firewalls
- Appliance: Dedicated hardware device bundling several features within it.
    - E.G: UTM – Unified Threat Management
- Trusted OS:
    - An operating system that meets the requirements set forth by government and has multilevel security. Uses MAC (Mandatory Access Control Model – Security Labels)
    - Windows 7 (and newer)
    - Mac OS X 10.6 (and newer)
    - FreeBSD (TrustedBSD)
    - Red Hat Enterprise Server
- Image: Snapshot of a single system that admins deploy to multiple other systems.



    - 1. Administrators start with a blank Source System. Install and configure OS, desired applications and modify security settings

    - 2. Admins capture the image, becoming master image.
    - 3. Admins deploy image to multiple systems.
- Benefits of Imaging:
    - Secure starting point
    - Reduced costs
- Can use Resiliency and automation strategies such as automation, scripting and templates to deploy systems securely. Can also use group policy.
- Benefits of baselines:
    - Initial baseline configuration allow to deploy systems consistently in a secure state
    - Integrity measurements for baseline deviation – Automated tools monitor system for baseline changes.
    - Remediation – NAC methods can detect baseline settings and automatically isolate or quarantine systems in a remediation network.
- **Remember this: Master image provides a secure starting point for systems. Admins sometimes create them with templates or with other tools to create a secure baseline. Then use integrity measurements to discover when a system deviates from the baseline.**
- **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/ Change management policy define 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.**
- Application Whitelist
    - Only applications that are on the list are allowed to be run by the operating system while all other applications are blocked
- Application Blacklist
    - Any application placed on the list will be prevented from running while all others will be permitted to run
- o Whitelisting and blacklisting can be centrally managed

- **Remember this: Sandboxing – use of an isolated area and it often used for testing. You can create a sandbox with a VM and on Linux Systems with the chroot command. A secure deployment environment includes development, testing, staging, and production elements.**
- Computer Peripherals:
    - Wireless Keyboards and mice – can be intercepted sometimes.
    - Displays – If displays show sensitive or private data, their view should be limited.
    - External storage devices – External USB drives, MP3 players, smartphones, tablets, cameras etc. Can transport malware without user knowledge and can be a source of data leakage.
    - Digital Cameras
    - WiFi enabled MicroSD cards – Micro Secure Digital cards need to be plugged into a port to read the data. Usually used with digital cameras and also include wireless capabilities and can be intercepted.
    - Printers and other multi-function devices (MFD's). MFDs often have extra features that should be considered when purchasing. Have internal storage that might retain documents that they process. Have embedded systems with their own risks.
- **Remember this:**
    - **Secure systems design considers electromagnetic Interference (EMI) and electromagnetic pulse (EMP). EMI comes from sources such as motors, powerlines, lights and can be prevented with shielding. Systems can be protected from mild forms of EMP (short burst of electromagnetic energy) such as electrostatic discharge and lightning.**
        - ESD – Electrostatic Discharge. Basic ESD prevention practices, such as ESD wrist straps can prevent ESD damage.
        - Lighting- Protect through surge protection strips
        - Military weapons – can cause EMP's and damage equipment

- FDE – Full disk encryption
- SED – Self Encrypting Drive
- Basic Input Output System (BIOS)
    - Firmware that provides the computer instructions for how to accept input and send output
- Unified Extensible Firmware Interface (UEFI)
    - BIOS and UEFI are used interchangeable
        - 1. Flash the BIOS
        - 2. Use a BIOS password
        - 3.Configure the BIOS boot order
        - 4.Disable the external ports and devices
        - 5.Enable the secure boot option
- **Remember this: A TPM (Trusted platform module) is a hardware chip included on many laptops and mobile devices. Provides full disk encryption and supports a secure boot process and remote attestation. A TPM includes unique RSA asymmetric key burned into the chip that provides a hardware root of trust.**

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.

- Remember this: A HSM (Hardware security module) 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.

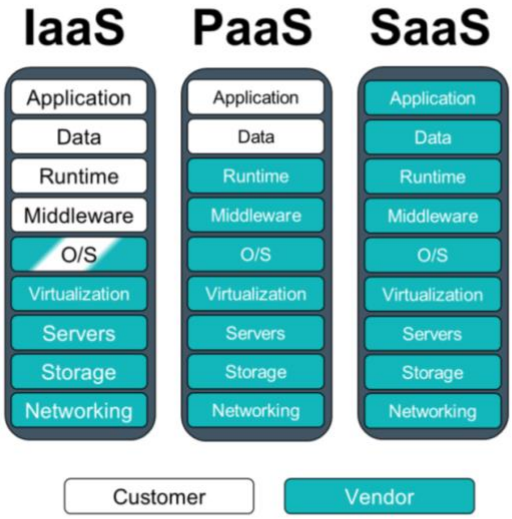
A hardware security module (HSM) is an external security device used to manage, generate, and securely store cryptographic keys.

- Additional Vulnerabilities.
    - End of Life Systems
    - Lack of Vendor Support

CLOUD CONCEPTS

- 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.
- **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 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 as a Service (SECaaS)**
  - Provides your organization with various types of security services without the need to maintain a cybersecurity staff
  - Anti-malware solutions were one of the first SECaaS products
- **Some solutions may not scan all the files on your system**
- **Cloud-based vulnerability scans can better provide the attacker's perspective**
- **Your vulnerability data may be stored on the cloud provider's server**

- Cloud Types:
- Public Cloud
  - A service provider makes resources available to the end users over the Internet
- Private Cloud
  - A company creates its own cloud environment that only it can utilize as an internal enterprise resource
- A private cloud should be chosen when security is more important than cost
- Hybrid – Combination of two or more clouds
- Community Cloud
  - Resources and costs are shared among several different organizations who have common service needs
- **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 organisations. A hybrid cloud is a combination of two or more clouds.

MOBILE DEVICES SECURITY

- Deployment Models:
  - Corporate Owned – Organization Purchases devices and issues them to employees
  - COPE (Corporate owned, personally enable). Similar to corporate model but employees are free to use the device as if it was their personally owned device.
  - BYOD – Bring your own device
  - CYOD – Choose your own device
  - VDI – Virtual Desktop infrastructure – users can access a VDI through mobile device, allowing users to access any applications installed on their desktop.
- Connection Methods:
  - Cellular – 3G,4G on smartphones
  - WiFi -with SSID. Most secure networks use Enterprise mode with 802.1x
  - SATCIN – Some mobile devices support connections to networks with satellite communications (SATCOM). Can Purchase satellite hot spots.
  - Bluetooth – Wireless protocol used with personal area networks
  - NFC – Near field Communication, used to usually make payments
  - ANT/ANT+ - Are proprietary wireless protocols used by some mobile devices. Sport and Fitness sensors like Fitbit collecting data on users such as heart rate, steps taken use ANT.
  - Infrared
  - USB – USB Cable
- **Remember this:**

    - **Mobile Device Management (MDM) tools help enforce security policies on mobile devices. This includes use of storage segmentation, containerization and full device encryption to protect data. Also include strong authentication methods to prevent unauthorized access.**
- MDM- Mobile Device Management: Technologies to manage devices.
    - Application Management through application whitelists
    - Full Device Encryption
    - Storage Segmentation to isolate data
    - Content Management – content received from an organization source (server) is stored in an encrypted segment
    - Containerization
    - Passwords and PINS
    - Biometrics
    - Screen locks
    - Remote Wipe – Useful if phone is lost. Remote signal to device to wipe/erase data
    - Geolocation – GPS for geolocation
    - Geofencing – Organizations use GPS to create virtual fence or geographical boundary using geofencing technologies.
    - GPS Tagging – Geographic information to files such as pictures
    - Context- Aware authentication – Authentication using multiple elements such as geolocation, verification of geofence, time of day, type of device etc.
    - Push Notification services.
- **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.**
- Risks of Text Messaging:

- Text sent in plaintext
- MMS (Multimedia message service) can provide remote code execution privileges on user's phone

- **Hardening Mobile Devices**
  - **1. Update your device to the latest version of the software**
  - **2. Install AntiVirus**
  - **3. Train users on proper security and use of the device**

https://www.DionTraining.com 18

CompTIA Security+ (Study Notes)

- **4. Only install apps from the official mobile stores**
- **5. Do not root or jailbreak your devices**
- **6. Only use v2 SIM cards with your devices**
- **7. Turn off all unnecessary features**
- **8. Turn on encryption for voice and data**
- **9. Use strong passwords or biometrics**
- **10. Don't allow BYOD**
- **Ensure your organization has a good security policy for mobile devices**

- Also turn off camera and microphone
- **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.**
- **Remember this: Embedded System**
  - **Embedded system is any device that has a dedicated function and uses a computer system to perform that function like a printer. Includes any devices in the IoT category, such as wearable technology (Fitbit) and home automation systems (Wireless thermostats, coffee makers, cameras). Some embedded systems use a system on a chip (SoC).**
- ICS – Industrial Control System
  - Systems within large facilities such as power plants or water treatment facilities. E.G: SCAADA system.

- RTO – Real time OS
  - OS that reacts to input at a specific time
- HVAC – Heating, Ventilation and air condition systems keep computing systems at proper temperature.
  - HVAC systems may be connected to ICS and SCADA networks
  - Keep humidity at 40%
- UAV – Unmanned Aerial vehicles include embedded systems.
- **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 UAV's**
- **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 Systems and Hard Drives**
  - **Level of security of a system is affected by its file system type**
    - NTFS
    - FAT32
    - ext4
    - HFS+
    - APFS
  - **Windows systems can utilize NTFS or FAT32**
  - **NTFS**
    - New Technology File System is the default file system format for Windows and is more secure because it supports logging, encryption, larger partition sizes, and larger file sizes than FAT32
  - **Linux systems should use ext4 and OSX should use the APFS**
  - **All hard drives will eventually fail**
    - 1. Remove temporary files by using Disk Cleanup
    - 2. Periodic system file checks

https://www.DionTraining.com

    - 3. Defragment your disk drive
    - 4. Back up your data
    - 5. Use and practice restoration techniques
-
- **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. Chmod command changes permissions on Linux systems.**
- Permissions in Windows:
  - Permissions are broken down into Read, Write, and Execute inside Linux
    - Full Control
    - Modify
    - Read & Execute
    - List Folder Contents
    - Read
    - Write
    - Permissions are assigned to Owners (U), Groups (G), and All Users (O or A)

- **chmod**
  - Program in Linux that is used to change the permissions or rights of a file or folder using a shorthand number system
- **R (Read) = 4**
  W (Write) = 2
  X (Execute) = 1
- **# chmod 760 filename**
  7 = Owner can RWX
  6 = Group can RW
  0 = All Users (no access)
- **777 allows everyone to Read, Write, and Execute**
- **Privilege Creep**
  - Occurs when a user gets additional permission over time as they rotate through different positions or roles
  - Privilege creep violates the principles of least privilege
- **User Access Recertification**
  - Process where each user's rights and permissions are revalidated to ensure they are correct
    - Hired
    - Fired
    - Promoted

- **Permissions**
  - **Permissions are inherited by default from the parent when a new folder is created**
  - **Any permissions added/removed from the parent folder will pass to the child by default too!**
  - **Propagation**
    - Occurs when permissions are passed to a subfolder from the parent through inheritance

- **Use Groups for roles and do not assign users directly to a folder's permissions**
- **Review Note: CompTIA A+**
- **If you copy a folder, then permissions are inherited from the parent folder it is copied into**
- **If you move a folder, then permissions are retained from its original permissions**

- **Remember this:**

- **Data exfiltration is the unauthorized transfer of data out of a network. Data loss prevent (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 PII (personally identifiable information) is encrypted.**