Chapter 5

Securing hosts and data

horizontal line

# Securing OS configurations

One method is to create a master image with a secure config, then deploy it to all systems.

Trusted OS: Ensures only authorised personnel can access data, by using a Mandatory AC model. It meets a set of predefined criteria, which are identified in the Common criteria.

Imaging:

1. Blank source system is configured
2. Admins capture the image, using an application like symantec ghost
3. Admins deploy the image to systems

Benefits:

* Secure starting point: Admin don’t need to remember details of configuration for every device.
* Reduced costs: Admins don’t need to learn all technologies, and can spend more time helping user rather than learning configuration

A master image is deployed, and then additional security templates are applied depending on needs.

**Secure baseline and integrity management**

Baselines work by

1. Initial baseline configuration
2. Integrity measurements for baseline deviation: Tools such as vulnerability scanners report changes from baseline that they detect
3. Remediation: NAC alerts prompt admins to make changes as required

**Patch management**

Patches are tested, then deployed via a systems management tool such as SCCM (systems centre configurations management)

NAC can be used to isolate systems that need patching

**Change management policy**

The goals are:

* To ensure any changes do not result in outages
* To provide an accounting structure to document all changes

Changes are usually documented and submitted for approval first.

**Unauthorised software**

This often contains malware. Also, not complying with vendor rules can result in a company’s license losing integrity.

**Application whitelisting/blacklisting**

Whitelist: Applications that can run on a system

Blacklist: Applications that cannot be downloaded

**Securing staging and deployment**

**Sandboxing**

VM used to test effect of antivirus on malware, or to test patches.

Chroot: Changes root directory of an application, isolating it. It can then be used to test applications within the sandbox.

**Secure staging environment**

* Development: Includes version control and change management to track app development
* Test: Tries to find bugs
* Staging: Simulates production environment, used for late stage testing
* Production: Includes everything needed to support app and allow others to use it.

**Peripherals**

* Wireless keyboards and mice: They can be intercepted, so might be better to use wired
* Displays: Shouldn’t be easily viewable
* External storage device: Can be misplaced, causing data exfiltration or malware infection
* WIFI enabled SD cards: some have wireless capabilities (see above)
* Printers and MFDs (multifunctional devices): Might have internal storage that retains processed documents

**Hardware and firmware**

EMI and EMP: EM interference and pulse.

**EMP** can come from a wide range of sources, damaging equipment

* ESD (electrostatic discharge): Using ESD wrist straps can prevent damage
* Lightning: Can go through electrical equipment, but surge protection strips reduce damage
* Military weapons: Nuclear explosions damage equipment

**FDE**: Full disk encryption encrypts entire disk. Can also have Self-encrypting devices (SEDs) which include all the hardware and software needed to encrypt data on drive.

Users have to enter credentials when they power up a device in order to decrypt the data.

**UEFI and BIOS**: Basic input/output System is a firmware chip that provides the computer with instructions on how to startup.

UEFI (unified extensible firmware interface) is similar, but can boot from larger disks and is cpu independent.

Trusted platform module (TPM): Hardware chip on motherboard that stores cryptographic keys used for encryption.

* Secure boot: Captures key of files used to boot system, and checks their value every time system is booted. If they have changed, due to malware etc, it blocks the boot process to detect data.
* Remote attestation: Sends key report to a remote system

TMP also has an RSA key burned in, used for asymmetric encryption, which is matched with a public key and provides hardware root of trust.

You can use an application within the OS to enable TMP

**Hardware security module: HSM**, a cryptographic key managing device. They can either come as expansion cards installed on server, or external device connected by TCP/IP.

HMP vs TMP: TMP is a chip embedded on motherboard, so can’t be removed. HMP is removable, and also easily added to a system.

**Summarising cloud concepts**

On premise services: All resources owned and operated within organisation’s buildings

Hosted services: Organisations can rent access to resources from another organisation.

**Software as a service (SaaS)**

Apps or services provided to users over the internet, with a web browser, e.g. gmail/google docs

Most CSP responsibility

**Platform as a service (Paas)**

Platform as a service provides customers with preconfigured computing platform as needed. Good for reducing admin workload as the platform is fully managed.

**Infrastructure as a service (IaaS)**

Allows organisations to rent equipment and hardware. It is a self managed solution, as customers must configure it themselves. A company therefore needs fewer resources such as servers and power etc

Least CSP responsibility

**Security as a service (SaaS)**

Antivirus etc

Eliminates need for professionals to focus on security concepts. They can also access Cloud Access Security broker (CASB) for additional security, which is a software tool that monitors all network traffic between organisation’s network and the cloud.

**Cloud deployment models**

1. Public cloud services: Available from third party companies such as amazon etc
2. Private cloud services: Set up for specific organisations and their needs
3. Communities: If communities have shared goals/needs, they can share cloud resources on a community cloud
4. Hybrid: Combination of 2 or more types, which are bridged together

**Deployment models for mobile devices**

* Corporate-owned: Organisation purchases and issues mobiles to employees
* COPE: Corporate-owned, personally enabled, Employees can use it as if it was their own device
* BYOD: Bring your own device
* CYOD: Choose your own device, employees are given a list of acceptable devices they can purchase
* VDI: Virtual desktop infrastructure, which users can access with their own device

**Connection methods**

* Cellular: Ability to connect to cellular network, such as 3G
* WIFI: Wireless networks require you to enter SSID and password. Used with Enterprise mode and 802.1x server
* SATCOM: Connection to networks using satellite connection.
* Bluetooth
* NFC: Used for payment, or P2P network between 2 devices
* ANT: Wireless protocol, used for things such as sending data to mobile app
* IR: Can be used to transfer files between phones
* USB

**Mobile device management (MDM)**

Technologies used to manage mobiles

* Application management: MDM tools can restrict apps used on a device
* Full device encryption: Used on corporate-owned devices, and used to secure data
* Storage segmentation: Corporate data is stored on an encrypted segment, with personal data stored elsewhere
* Content management: Can ensure that data downloaded from company server is stored in encrypted segment. Can also force users to authenticate when accessing data in this segment
* Containerisation: Allows users to run an app in this container, with it being isolated from rest of device. This container can be encrypted
* Passwords and PINs: Authentication method
* Biometrics: Authentication method
* Screenlocks: Can also be used with erase function, where data is erased if someone incorrectly entered PIN a limited no of times
* Remote wipe: Remote signal to wipe data if device is lost. Also deletes cached data
* Geofencing: Apps can only run when they are in a certain location.
* Context-aware authentication: Uses multiple elements to authenticate a user.

**Mobile device enforcement and management**

Issues that an MDM can monitor, combined with a NAC

* Unauthorised software: Such as a third party app obtained through jailbreaking or rooting. This can introduce vulnerabilities, so an MDM can block access to a network it if detects a rooted or jailbroken device. Also, updates to the system overwrite firmware using OTA (Over the air) techniques. Custom firmware can be created which is a method of rooting android devices.
* Sideloading: An application package in the Application packet kit (APK) format is copied to device and activated
* Hardware: Attackers can gain access to camera/microphone. MDM can be configured to disable them.
* Unauthorised connections: Tethering between devices can introduce malware into a network. WIFI Direct allows devices to connect without a WAP or router. These services can be blocked by an MDM.

**Embedded systems**

A device that has a dedicated function, e.g. an embedded system in a printer that hosts a printer configuration page. They all typically use System on a Chip (SoC), and are classified as IoT.

* Wearable technology: They can interact with other devices, such as a smartphone, e.g. fitbit, pet chips etc.
* Home automation: Devices such as wireless thermostats, lighting etc, allowing control over the internet.

A Real Time Operating System (RTOS) is an OS that reacts to input within a specific amount of time, and if it can’t that it raises an alert.

Heating, Ventilation and air cond systems have embedded systems, and if they are attacked it gives the attacker access to these systems.

SCADA has embedded systems that control an Industrial Control System (ICS)

**Protecting data**

**Protecting confidentiality with encryption**

Database security: Some databases include the option to encrypt the data.

We can also implement strong access controls, such as an NTFS configuring permissions with an ACL.

File system security: GNU-PG (GNU privacy guard on LINUX) is a command line tool used to encrypt/decrypt files with a password. Windows has EFS (encrypting file systems). You can therefore encrypt individual files without encrypting entire disk

**Linux permissions**

Here are the 3 main privilege groups in Linux:

* Owner: root user
* Group: Members of a group can be given specific access to files.
* Others: Everyone else

Basic linux permissions:

* Read (r): represented by number 4
* Write (w): number 2
* Execute (x): number 1

If a permission is not assigned, it will be represented by a dash. You can also combine permissions, and their numbers, e.g. all 3 would be 7. The permission types are usually represented in an FACL (File ACL)

Permission such as rwx rw---- would be 760 (rwx = 7, rw = 6, rest is 0)

To change this to rwx r-x r-x, you would type chmod 755 [filename]

In windows, there is Read, write, r+x, modify (which is read execute and write, but with permission to delete folders)

**Data loss prevention**

**Removable media:**

DLP policies can prevent the use of removable data storage devices. DLP software can also scan pages sent to the printer for confidential material, block the printing of it, and log these incidences.

**Data exfiltration**

A network-based DLP can monitor outgoing data, looking for sensitive data. It can also scan attached files.

**Cloud-based DLP**

Data can be stored in the cloud, and cloud-based DLP solutions can help secure this data by blocking attempts to save the data, and alerting admin

**ACRONYMS**

**Securing OS configurations**

SCCM: Systems centre configurations management, systems management tool

**Hardware/firmware**

FDE: Full disk encryption.

SED: Self encrypting device

UEFI: unified extensible firmware interface, firmware chip providing instructions on how to boot

BIOS: Basic input/output system

TPM: Trusted platform module, hardware chip on motherboard which stores cryptographic keys used for encryption

**Cloud concepts**

CASB: Cloud access security broker, used for security management

MDM: Mobile device management

OTA: Over the air. Updates the system overwrite firmware using OTA techniques

**Embedded systems**

SoC: System on chip

TROS: Real time IS, reacts to input in a certain amount of time, and raises alert if it can’t

ICS: Industrial control system

**Protecting data**

Read ® = number 4

Write (w) = number 2

Execute (x) = number 1

Rwx rw---- would be 760 (rwx is 7, rw = 6, rest is 0)