Week 6 Windows boot process & Windows recovery tools

Windows Boot Process

The windows boot process applies to Windows and Unix.

- Windows Vista introduced a new boot configuration and storage system called Boot Configuration Data (BCD) to Windows operating systems.

-This replaced text based Boot.ini file

(This is the first thing that the BIOS/UEFI launches which then loads the rest of windows).

https://en.wikipedia.org/wiki/Windows_Boot_Manager

- BCDEdit.exe is an editing tool that can be used to configure boot options for debugging, testing and troubleshooting.

- Administrative privileges are required to use BCDEdit to modify the BCD.

- When changes are made, they are made right away so if you configure it wrong, it can break the system and cause the machine not to boot. In this case you will have to run recovery mode.

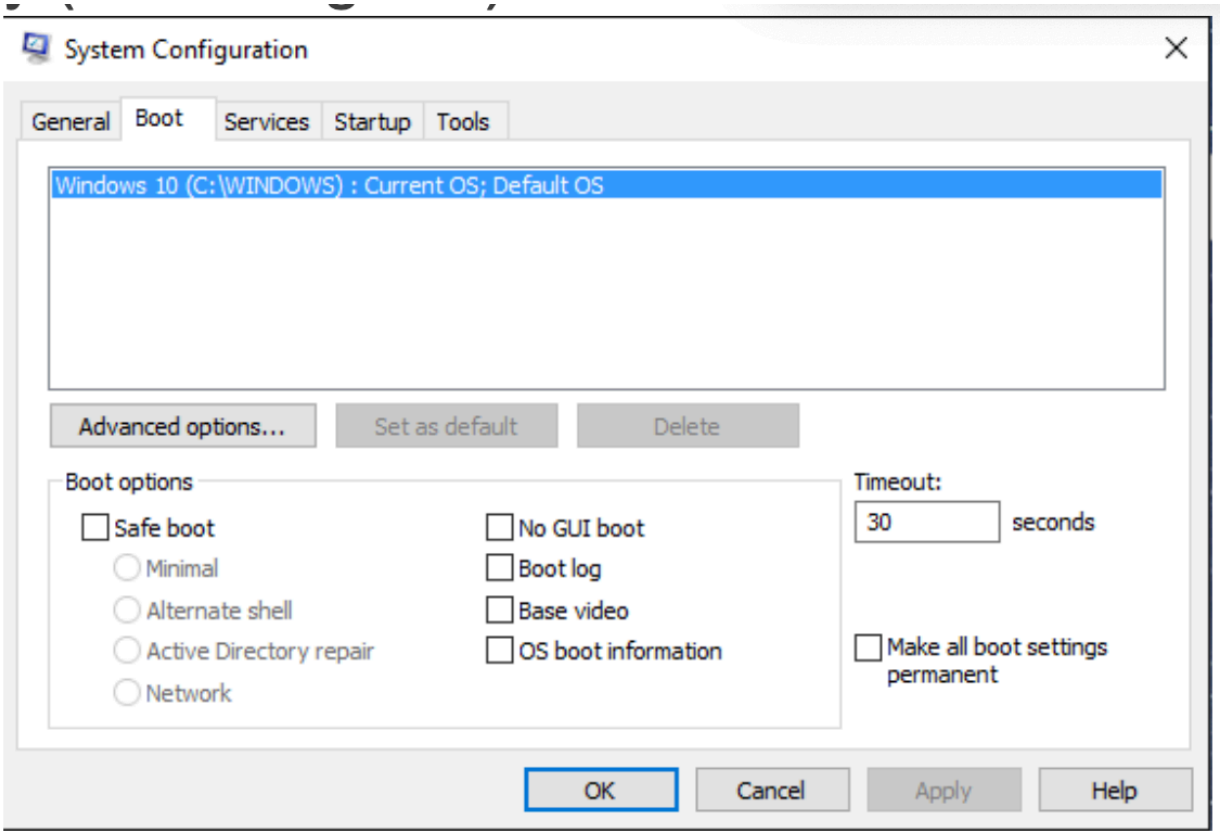
- Alternatively, some boot options can be modified using the System Configuration utility (MSConfig.exe).

- Here you can do things like edit the programs that will start up with the system. If there are programs like bloat ware you want to not start up with the system they can be taken out. Just check the boot tab and startup tab.

- Safe boot can also be used to start in safe mode to correct any errors that may stop the system from starting up properly.

No GUI Boot
Will load with no GUI

Base Video
Will start with only using the system video drivers



- The Boot configuration Data (BCD) store works with both BIOS-based and EFI based computers.

Boot Loading Architecture

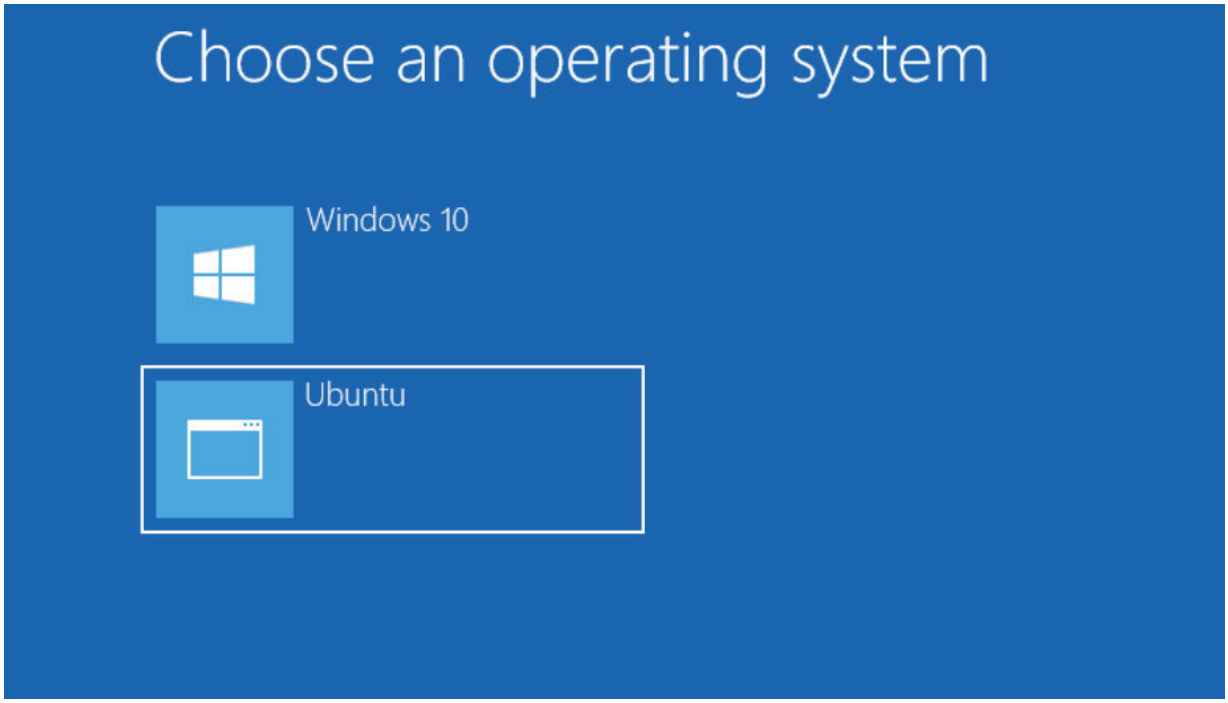
Before windows used Windows ntldr.exe (new

technology loader) it has been replaced by 3 programs.

Current Windows operating systems include the following boot loader components:

Windows Boot Manager (Bootmgr.exe)

- Runs independent of the operating system
- Loads the Windows boot loader either from a particular disk partition or over a network connection.
- If there are multiple OS's on the machine it will allow you to choose what one to load.



Windows Operating System Loader (Winload.exe)

- Loads after the boot manager. If there is only one OS installed this will auto run and load the installed version of Windows.
- Is part of the OS, loads specific version of Windows.
- Loads the operating system kernel and critical device drivers from a local disk.

Windows Resume Loader (Winresume.exe)

- Finds a hibernation image and then reads the hibernation file into RAM to resume the OS from the hibernation state.

Windows 8.X / 10 Boot Process

Windows 8/ Server 2012 introduced the following changes in an attempt to protect against malware like root kits, being loaded on boot up. This protection continues in Windows 10.

Measured Boot

-The PC's firmware logs the boot process, Windows can send it to a trusted server that can objectively assess the PC's health.

Trusted Boot

Windows checks the integrity of every component of the startup process before loading it. If there is something loading that is not from a trusted boot it will give you a warning that the system is loading untrusted software and refuse to boot.

Support for Secure Boot

PC's and devices with UEFI (Unified Extensible Firmware Interface: https://en.wikipedia.org/wiki/UEFI) firmware and a Trusted Platform Module (TPM) can be configured to load only trusted operating system boot loaders. TPM is a physical chip on the motherboard.

https://docs.microsoft.com/en-us/windows/win32/w8cookbook/measured-boot

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

https://docs.microsoft.com/en-us/windows/threat-

protection/secure-the-windows-10-boot-process

BIOS vs UEFI

BIOS

-Loaded from the Master Boot Record (MBR) located in the first sector of the hard disk

-16-bit code, simply locates and runs the OS Boot Loader

EFI/UEFI

-Loads EFI program files (with .efi filename extensions) from a EFI System Partition (ESP) on the hard disk. This partition is always the 1st partition on the HD.

-The EFI boot loader programs can read files, such as digital signatures, from the hard disk.

Trusted Platform Module (TPM)

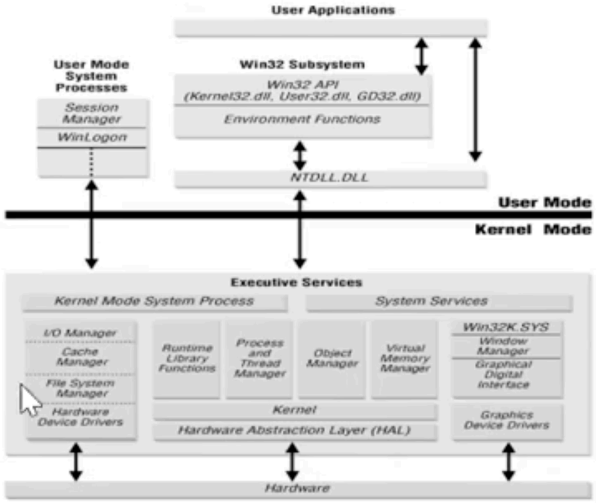
- Physical hardware that can be read/written to.

- Used to store authentication data IE passwords, certificates or encryption keys.

- Measurements that help ensure that the platform remains trustworthy. ~Hash values of operating system files and drivers.

- The data can be used for authentication and provide evidence of validity (attestation).

Windows OS Structure



What are drivers?

A driver is a specialized program that interfaces with some hardware. Think of every time you had to re-DL a driver for your printer. Annoying right?

Every manufacturer will make and distribute drivers for their hardware. If you use third party, grey market or black market drivers, chances are there will be malware in it.

What is the boot process?

The boot process takes the machine from power on to its ready state.

Seven Steps:

1 PreBoot - Runs checks to see if all the components to run the machine are present and what hardware is attached to the machine. It will also tell different hardwares to run its own checks to make sure its systems are OK.

2 Windows Boot Manager - Will allow the user

to choose what OS to run, OR run the default OS if there is only 1.

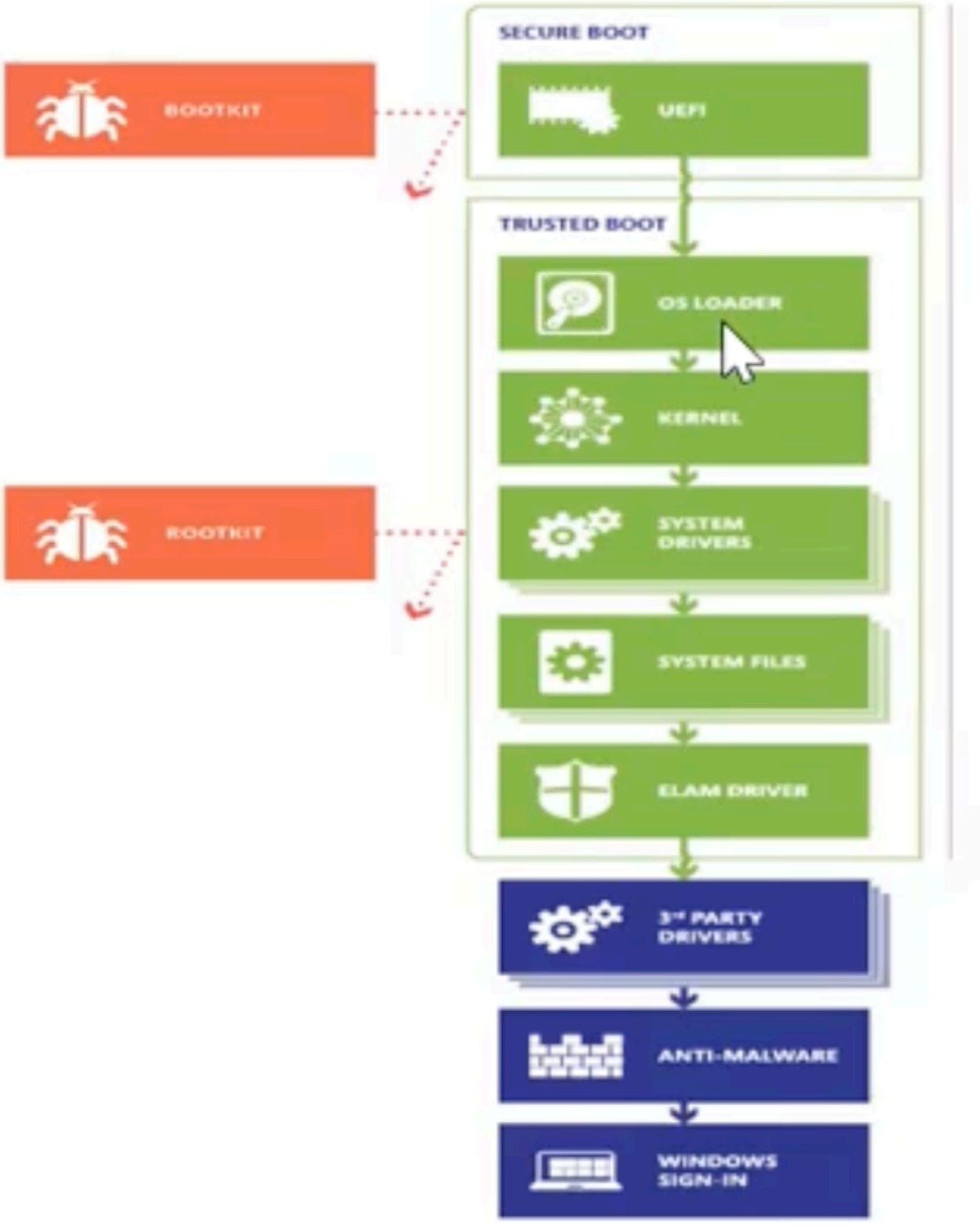
3 Windows OS loader - Runs the Kernel and the drivers.

4 Windows NT OS Kernel - Starts running softwares for the OS

5 Session Initialization (SMSS.exe, Csrss.exe) Starts running background programs

6 Winlogon initialization (dwm.exe, wining.exe) starts the logon page and the GUI

7 Explorer Initialization - windows explorer starts up



We can boot from:

Disk

USB

LAN

CD/DVD

In the lab

Use the BCDEdit to query, backup and modify the boot configuration data

Research details of the secure boot, measured boot and trusted boot process.

Windows Recovery Tools

Windows recovery console

- On operating systems prior to Vista and Server 2008, Microsoft offered the recovery console.

- Can be used to perform basic recovery tasks like access the file system, enable and disable

services, manage disk partitions and volumes, fix boot sector and MBR errors.

- It was not installed by default, it had to be installed OS medium post installation.

- The recovery console had some limitations:
    - It did not have access to the entire file system
    - It could not be used to re-image a system
    - It was not able to automatically detect and fix system errors

Windows recovery environment

Windows recovery environment (Windows RE) is a recovery environment that can repair common causes of unbeatable operating systems.

- Includes automatic repair functionality
- Troubleshooting and diagnostic tools
- System image recovery
- System reset (Windows 8 and 8.1 only)

By default, Windows RE is preloaded into Windows OS's beginning with Windows 7 and server 2008.

A version was available in Windows Vista but it was not installed by default.

Windows RE is based on Windows Preinstallation Environment (Windows PE)

A minimal Win32 operating system with limited services, used to prepare a computer for Windows installation

Can be customized with additional drivers, languages, Windows PE Optional Components

Provides command line access to a computer's operating system files.

Boots from a special system partition, allowing access to files that would normally be locked by the Operating System such as Registry files

Can run automatically or manually.

Starting Windows RE

In windows 8.1, 8, Server 2012R2 and server 2012, Windows RE can be accessed in the following ways:

- Search for advanced startup options > Restart now

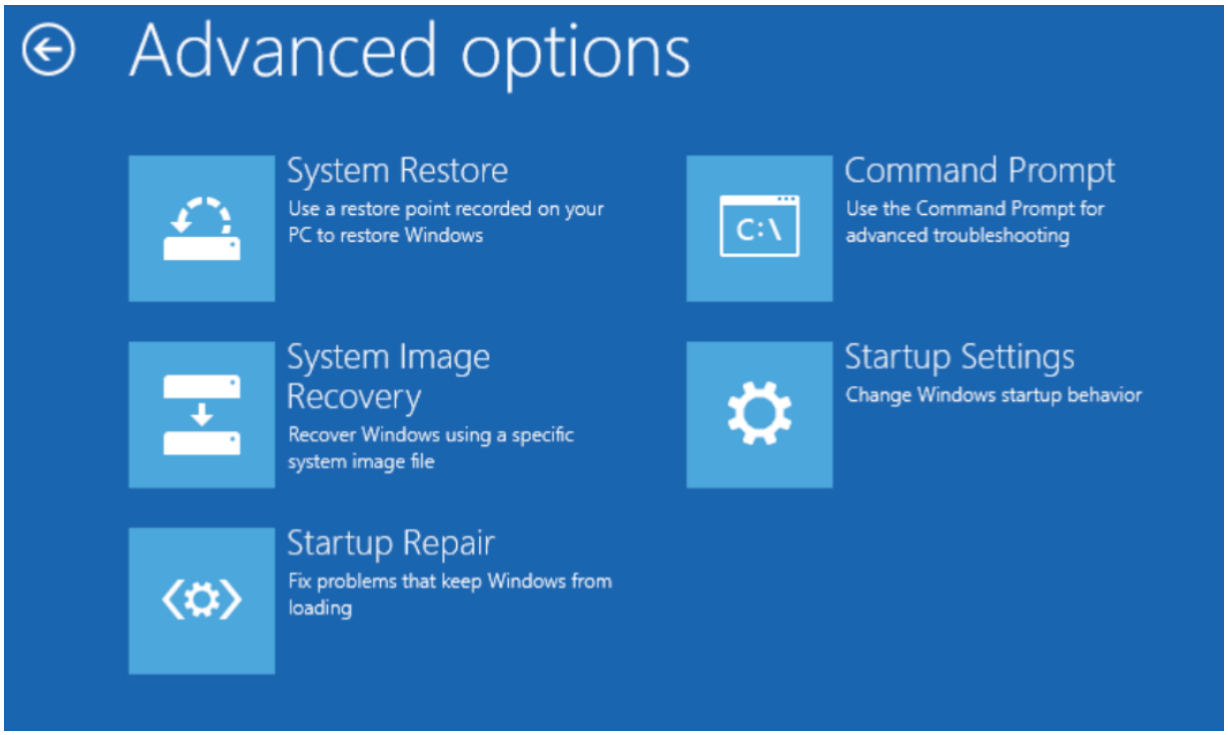
- Select the settings charm > Power, and then hold the Shift key while clicking restart.

- Select the settings charm > Change PS settings > Update & recovery > recovery. Under advanced startup, click Restart now.

- At the command prompt, type: **shutdown /r /o**

Windows RE Troubleshooting options

Windows RE Advanced options



Windows RE Command Prompt

All Windows RE command line tools are available from a command prompt window, including notepad.exe

The following commands will be used in the lab:

Diskpart.exe - A command line tool used for managing disks, partitions or volumes in an interactive command line environment for scripts.

Reg.exe - A command line based registry for loading, querying and editing registry hives and files.

Regedit.exe - Windows registry editor

In the lab

Create a system image file

Configure the registry to run a program each time a user logs on

Use the Windows Recovery Environment to:

Recover from a critical file system error

Remove unwanted ‘Autorun’ entries from the registry

Restore a system image