"BIOS"
TO
"UEFI" WITH
"SECURE BOOT"
AND "CSM"

by Francis Chao
fchao2@yahoo.com

Web location for this presentation:

http://aztcs.org

Click on

“Meeting Notes”

SUMMARY

The venerable "BIOS" is now being replaced with a "UEFI" with "Secure Boot", as mandated by Microsoft since August 2012. However, legacy BIOS firmware has found a new life inside the "CSM" in the new-fangled "UEFI".

TOPICS

- Acronyms galore!
- "Secure Boot"
- "CSM"
- "Linux" and "Secure Boot"
- "Virtual Machines" and "Secure Boot"

ACRONYMS GALORE!

- "BIOS"
- "UEFI"
- "Secure Boot" inside the "UEFI"
- "CSM" inside the "UEFI"

"BIOS"

- **"BIOS" = "Basic Input/Output System"**
- **Invented by Gary Kildall in 1975**
- **Boots up operating systems located on hard drives that have a "Master Boot Record" (MBR)**

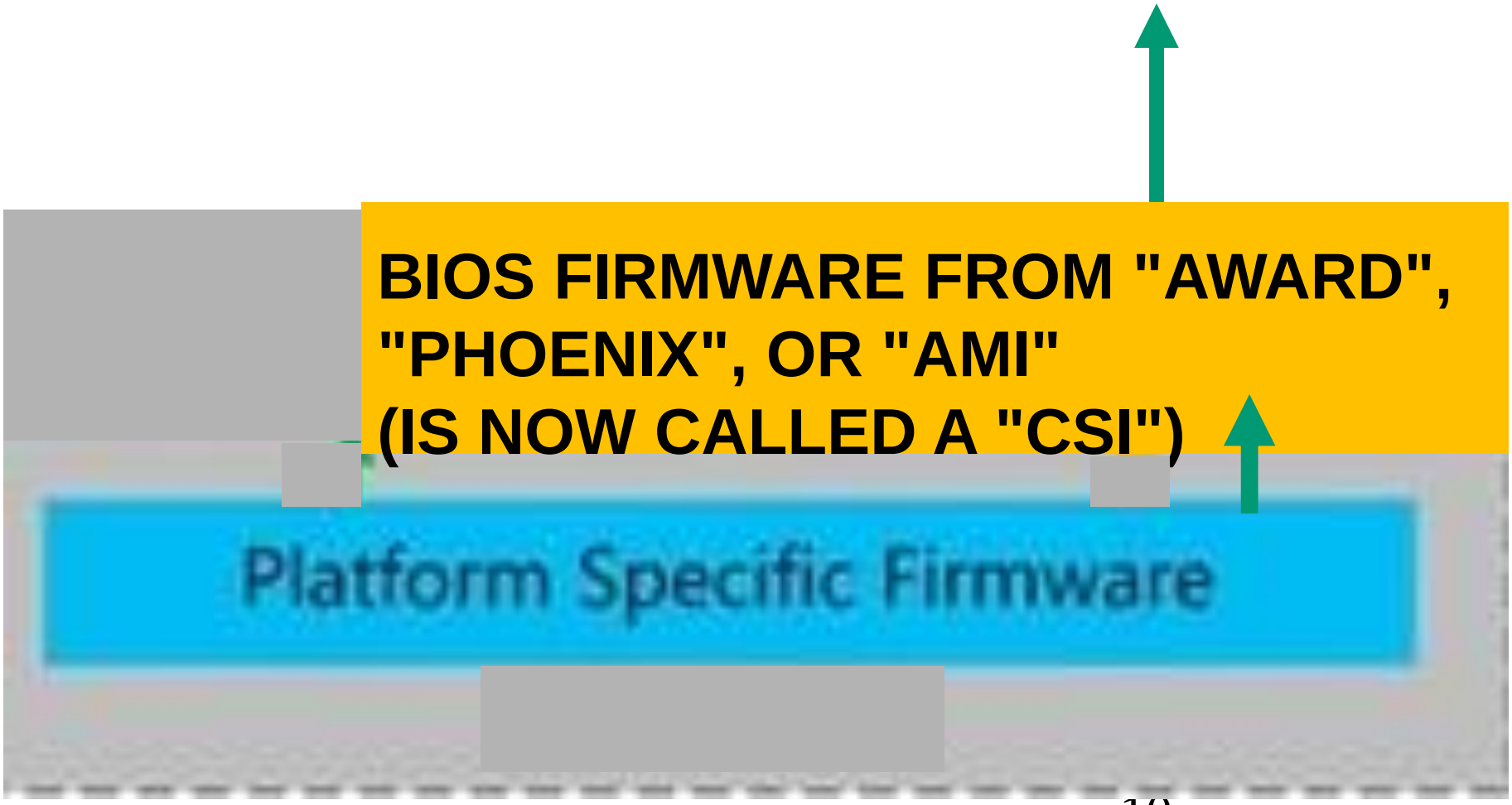
"UEFI"

- **"UEFI" = "Unified Extensible Firmware Interface"**
- **Invented by Intel and the "UEFI Forum"**

"UEFI" (continued)

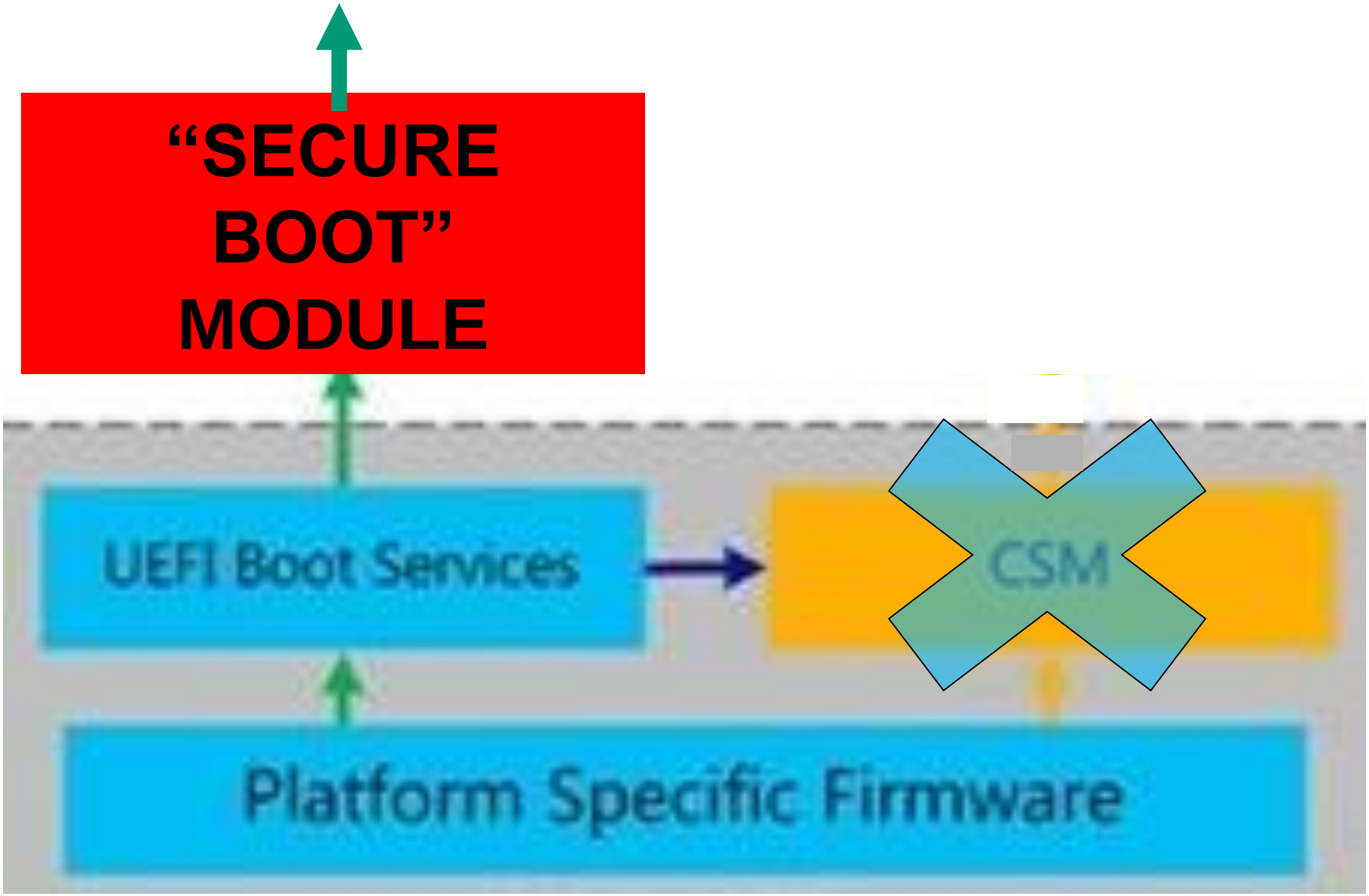
- **"UEFI" has a "Secure Boot Module" and a "CSM" inside it**
  "CSM" stands for "Compatibility Support Module"

A LEGACY "BIOS" CHIP ON THE MOTHERBOARD IS THE DEFAULT CONFIGURATION FOR ANY COMPUTER SOLD AT RETAIL PRIOR TO OCTOBER 26, 2012:



ORIGINAL BIOS

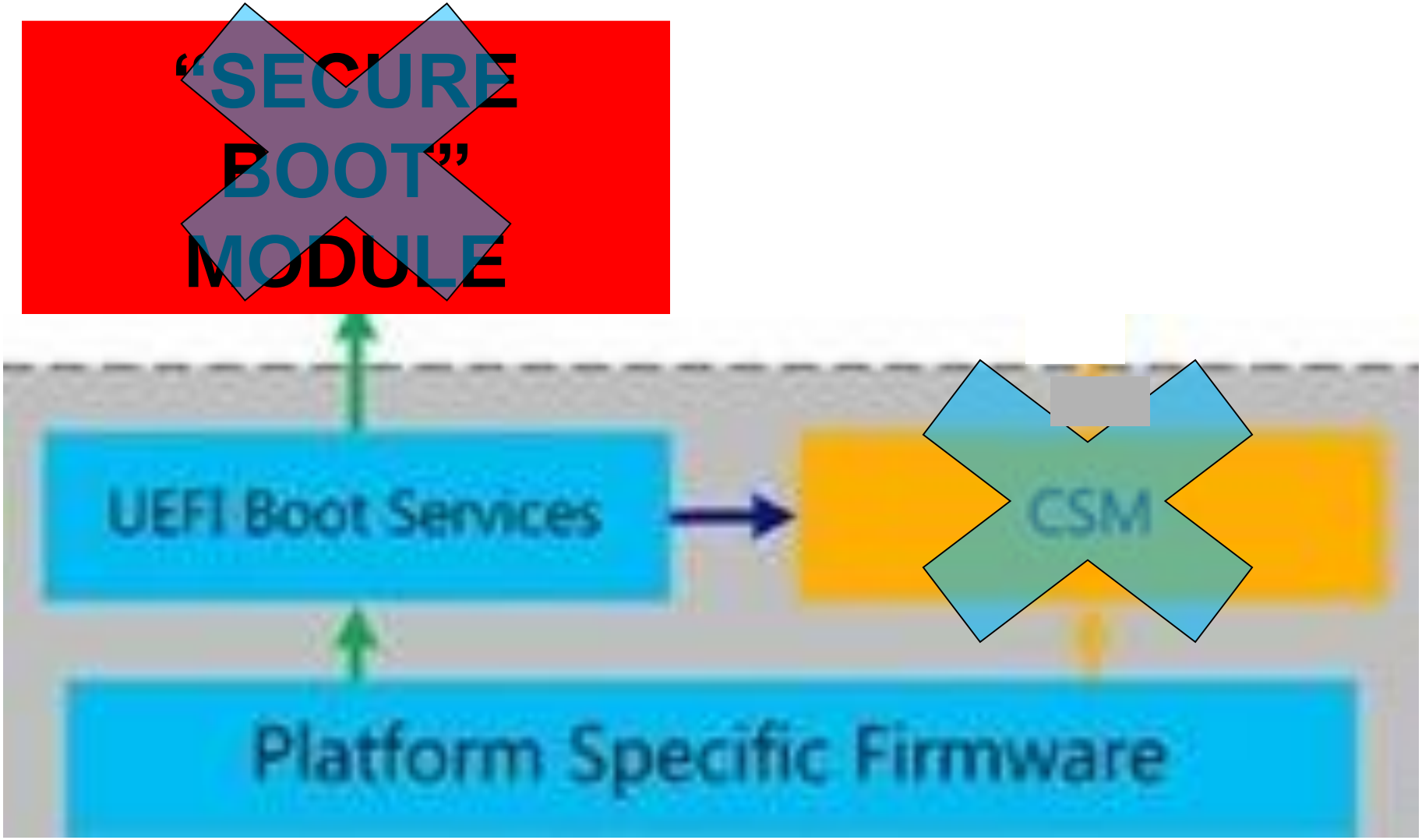
A "UEFI" CHIP ON THE MOTHERBOARD IS THE DEFAULT CONFIGURATION FOR ANY COMPUTER SOLD AT RETAIL SINCE OCTOBER 26, 2012:



UEFI (= "UEFI BIOS")

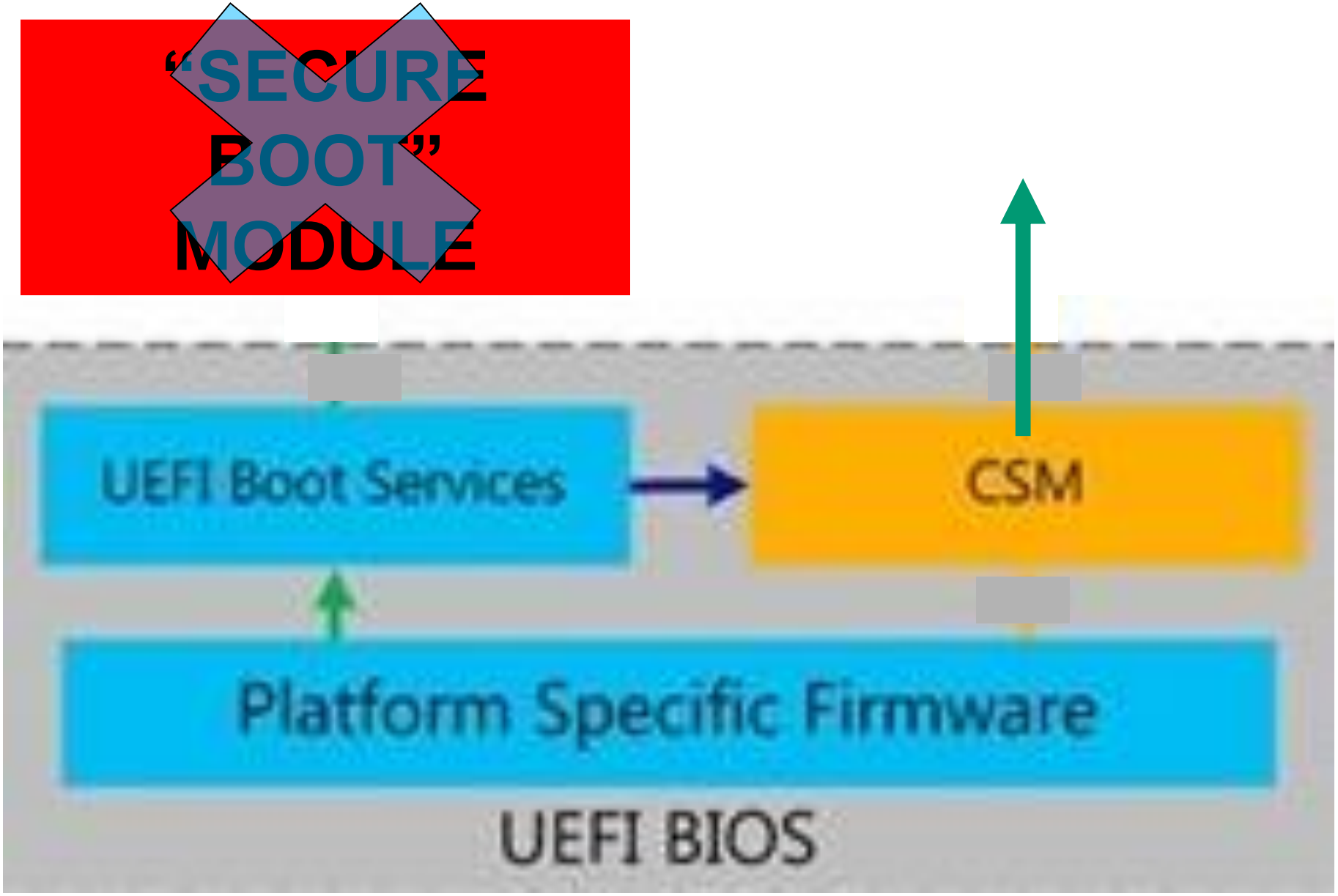
“SECURE BOOT MODULE” CAN BE DISABLED BY YOU FOR OPERATING SYSTEMS THAT DO NOT SUPPORT IT OR FOR USING SOFTWARE REPAIR TOOLS THAT SUPPORT “UEFI MODE” BUT DO NOT SUPPORT “SECURE BOOT”:

IF YOU DISABLE THE "SECURE BOOT MODULE", YOUR "POST AUGUST 2012" "WINDOWS.." OR "LINUX" COMPUTER WILL STILL BOOT. HOWEVER, IT WILL BE A LITTLE LESS SECURE IN ITS ABILITY TO RESIST MALWARE INFECTIONS.



UEFI (= "UEFI BIOS")

FOR BACKWARD COMPATIBILITY FOR OPERATING SYSTEMS AND SOFTWARE TOOLS THAT DO NO SUPPORT “UEFI”, THE “CSM” CAN BE ENABLED (WHICH AUTOMATICALLY DISABLES “SECURE BOOT”):


"SECURE BOOT" MODULE
UEFI Boot Services
CSM
Platform Specific Firmware
UEFI BIOS

- Reference for previous diagram: http://blogs.msdn.com/b/olivnie/archive/2012/12/20/windows-8-uefi-support.aspx

"SECURE BOOT"

- The UEFI 2.2 specification adds a protocol known as *secure boot*, which can secure the boot process by preventing the loading of drivers or OS loaders that are not signed with an acceptable digital signature.

"SECURE BOOT" (continued)

- "Secure Boot" is an optional module that resides inside and is part of the "UEFI". See http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Secure_boot

"SECURE BOOT" (continued)

- **Mandated by Microsoft for all Windows 8+ computers sold at retail after Oct. 26, 2012 via the "Windows Hardware Certification Program"**

"SECURE BOOT" (continued)

- According to http://download.microsoft.com/download/7/0/E/70E74967-B0FE-477A-974F-C1ED16EE31DF/windows8-1-hardware-cert-requirements-system.pdf at http://msdn.microsoft.com/en-us/library/windows/hardware/dn423132:

"SECURE BOOT" (continued)

- **The "Secure Boot" module of the UEFI can be enabled or disabled by the computer user at any time before or after the operating system is installed into the computer.**

"SECURE BOOT" (continued)

- If you access the configuration screens of the "UEFI" to enable or disable the "Secure Boot" module, expect to get some temporary non-fatal complaints when you boot up the operating system for the first time afterwards.

All client systems must support UEFI Secure boot

Target Feature	System.Fundamentals.Firmware
Applies to	• Windows 8 Client x86, x64, ARM (Windows RT) • Windows 8.1 Client x86, x64, ARM (Windows RT 8.1) • Windows Server 2012 R2 x64 • Windows Server 2012 x64

"CSM"

- **"CSM" = "Compatibility Support Module"**
- **"CSM" is an optional module that resides inside and is part of a "UEFI"**
- **All UEFIs currently sold have a "CSM"**

"CSM" (continued)

- **Several years from now, UEFIs will not have CSMs in them**

CSM (continued)

- **Inside the "UEFI", the "CSM" and the "Secure Boot" module cannot both be enabled at the same time:**

CSM (continued)

- **Enabling the "CSM" disables the "Secure Boot" module**
- **Enabling the "Secure Boot" moduel disables the "CSM"**

"SECURE BOOT" COMPATIBILITY FOR A COMPUTER OPERATING SYSTEM

- Requirement 1: Installation media DVD or CD can boot up a computer with a "UEFI" with "Secure Boot" enabled

"SECURE BOOT" COMPATIBILITY FOR A COMPUTER OPERATING SYSTEM (continued)

- Requirement 2:
  Once it is installed, an operating system can boot up a computer with a "UEFI" with "Secure Boot" enabled

LINUX AND "SECURE BOOT"

- "Secure Boot" is supported by "Windows 8", "Windows 8.1", "Windows Server 2012", the previews of "Windows 10, "FreeBSD", and a number of Linux distributions including Fedora, OpenSuse, and Ubuntu.

LINUX AND "SECURE BOOT" (continued)

- Reference for previous slide: http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT"

- At the present time, the only virtual machine program that can provide a virtual machine with a UEFI with Secure Boot enabled is the bundled "Hyper-V" applet in the 64-bit versions of Windows 8, 8.1, or 10

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT" (continued)

- When you create a new virtual machine inside "Hyper-V", you can select either a "Generation 1" virtual machine which has a legacy BIOS or a "Generation 2" virtual machine that has a "UEFI".

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT" (continued)

- When you create a "Generation 2" virtual machine that has a "UEFI", the "Firmware" settings screen of the virtual machine lets you turn the "Secure Boot" module on or off an any time before or after the creation of the virtual machine.

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT" (continued)

- To run "Windows 8", "Windows 8.1", "Windows 10 Technical Preview“, or “Windows 10 Enterprise Technical Preview” as a “guest operating system”
  inside a virtual machine that has a virtual UEFI with "Secure Boot" enabled, you can use "Hyper-V" running in the 64-bit versions of the following (host) operating systems:

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT" (continued)

- "Hyper-V" running in running in "Windows 8 Pro", "Windows 8 Enterprise", "Windows 8.1 Pro", "Windows 8.1 Enterprise", "Windows 10 Pro Technical Preview", or "Windows 10 Enterprise Technical Preview"

VIRTUAL MACHINES WITH "UEFI AND SECURE BOOT" (continued)

- To run distros of Linux that support "Secure Boot"
  as a “guest operating system” inside a virtual machine that has a virtual UEFI with "Secure Boot",
  you can use the "Hyper-V" module that is bundled in a "Windows 10 Pro Technical Preview, 64-bit" or a “Windows 10 Enterprise Technical Preview” host computer.

LINUX DISTROS THAT WE INSTALLED SUCCESSFULLY INTO "HYPER-V" VIRTUAL MACHINES WITH SECURE BOOT ENABLED

- Ubuntu Desktop 14.10 64-bit
- Ubuntu Desktop 14.04 64-bit
- Linux Mint 17.1 with Cinnamon 64-bit
- OpenSUSE 64-bit 13.2 x86_64
- Fedora Server 21 64-bit

DOES MY "WINDOWS.." COMPUTER HAVE A "BIOS" OR A "UEFI"?

- **If you get into the firmware setup screens for you computer and your mouse still works, then you have a "UEFI" instead of a "BIOS"**

DOES MY "WINDOWS.." COMPUTER HAVE A "BIOS" OR A "UEFI"? (continued)

- Run msinfo32 and look at the BIOS mode
- Or run "Disk Management" and see if the computer has a "EFI System Partition"

IF MY "WINDOWS.." COMPUTER HAS A "UEFI", IS "SECURE BOOT" ENABLED OR DISABLED?

- Get an admin "Command Prompt".
- Type in powershell, hit the enter key, type in confirm-securebootuefi

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 1:**
  Use the computer manufacturer's bootup key sequence
  See https://neosmart.net/wiki/disabling-secure-boot/

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2:**
  Use the access method in "Windows.." as described at the following Web sites:

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2 (continued):**
  http://www.recoverlostpassword.com/windows-8-1/how-to-disable-uefi-secure-boot-in-windows-8-1-and-8.html

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2(continued): http://itsfoss.com/disable-uefi-secure-boot-in-windows-8/**

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2 (continued): http://www.reddit.com/r/linux/comments/16sscv/how_bypass_secure_boot_in_windows_8/**

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2 (continued):**
  http://www.recoverlostpassword.com/windows-8-1/how-to-disable-uefi-secure-boot-in-windows-8-1-and-8.html

ACCESSING THE UEFI CONFIGURATION SCREENS FROM "WINDOWS 8, 8.1, OR 10"

- **Method 2 (continued):**
  http://www.recoverlostpassword.com/windows-8-1/how-to-disable-uefi-secure-boot-in-windows-8-1-and-8.html

SCREENSHOTS OF “UEFI” CONFIGURATION SCREENS

- http://www.top-password.com/blog/set-windows-8-pc-to-boot-with-legacy-bios-mode-instead-of-uefi-mode/

SCREENSHOTS OF “UEFI” CONFIGURATION SCREENS (continued)

- See http://rog.asus.com/220572013/rampage-motherboards/rampage-iv-uefi-boot-installation-guide-on-windows-7-or-8/