Secure Boot

4 December 2017

Windows Secure Boot

- Resources for the lecture
- Yes, I will talk about Windows and not Apple.
- https://technet.microsoft.com/en-us/library/hh824987.aspx
- https://msdn.microsoft.com/en-us/library/windows/hardware/dn653311(v=vs.85).aspx
- https://www.grc.com/sn/sn-500.htm

Terms to remember

- Code Signing
- BIOS
- Trust anchor
- Hardware Abstraction Layer
- EFI/UEFI
- Secure Boot

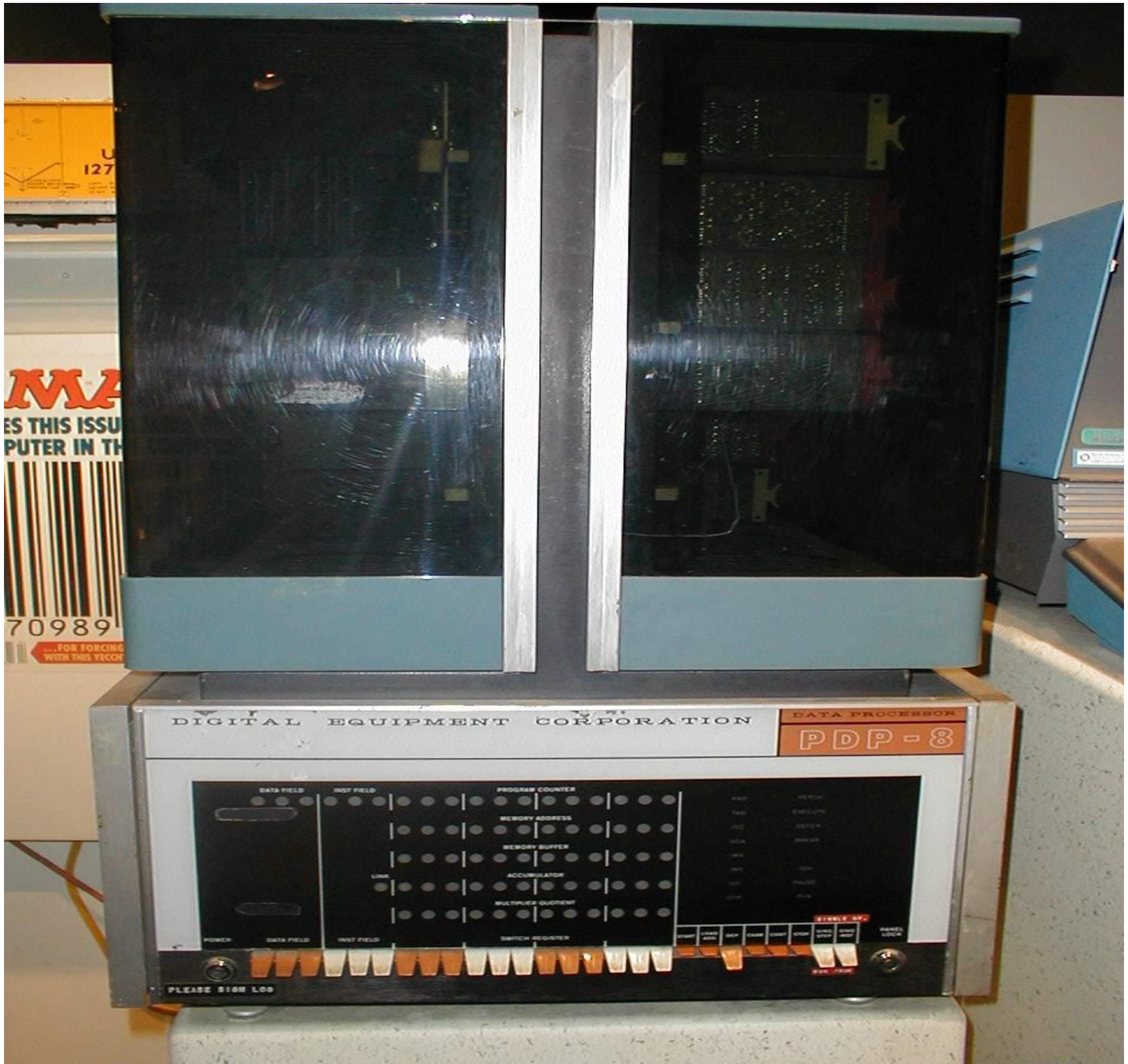
Code Signing

- Allow only approved developers to write code.
- To enforce this, companies (Apple, Windows) will give developers certificates
- Each time a program is executed, the certificate is checked. If it fails, the program is not run.
- https://www.infosecurity-magazine.com/news/code-signing-certs-traded-for-1000/

BIOS

- BIOS is software on a chip.
- Directs the computer how to boot.
- Also, originally, I/O.
- Simple in the beginning, just a listing in the back of a manual. Look on Ebay
  - https://sites.google.com/site/pcdosretro/ibmpcbios
- Was printed on paper, used to be in a manual.
- Or, keyd in on a PDP 8

PDP 8


DIGITAL EQUIPMENT CORPORATION
DATA PROCESSOR
PDP-8
PROGRAM COUNTER
MEMORY ADDRESS
MEMORY BUFFER
ACCUMULATOR
MULTIPLIER QUOTIENT
SWITCH REGISTER
PLEASE SIGN LOG

BIOS

- Helped perform hardware initialization during the boot process.
- Original hardware components from ancient history:
  - Monitor (not VGA, only ASCII)
  - Keyboard
  - Floppy, Cassette, Sound, Disk controller, Printer, Modem
- Life was simple and one person could understand the entire OS and hardware.
- Back in the days, a manual describing how to operate the device would come with the computer.

It looked like this

- This is an IBM PC.
- http://www.davesvintagepcs.com/images/IBM%20PC.JPG
- https://upload.wikimedia.org/wikipedia/commons/5/57/IBM_PC_Motherboard_(1981).jpg
- Before Bill Gates got the bright idea to acquire the OS and resell it to IBM.
- Contained in io.sys and IBMBIO.COM, …

Phoenix BIOS

- IBM Clones
- Phoenix supplied a functionally compatible BIOS
- Chinese Wall technique
    - One team looked at the IBM BIOS source listings and wrote the specifications
    - Another unrelated team wrote the code.
- Clones of the IBM PC (Compaq) could now be built.

OSBORNE

Commodore 64
Commodore

OK

- Enough reminiscing.
- Professor, please remember we are discussing how computers boot.

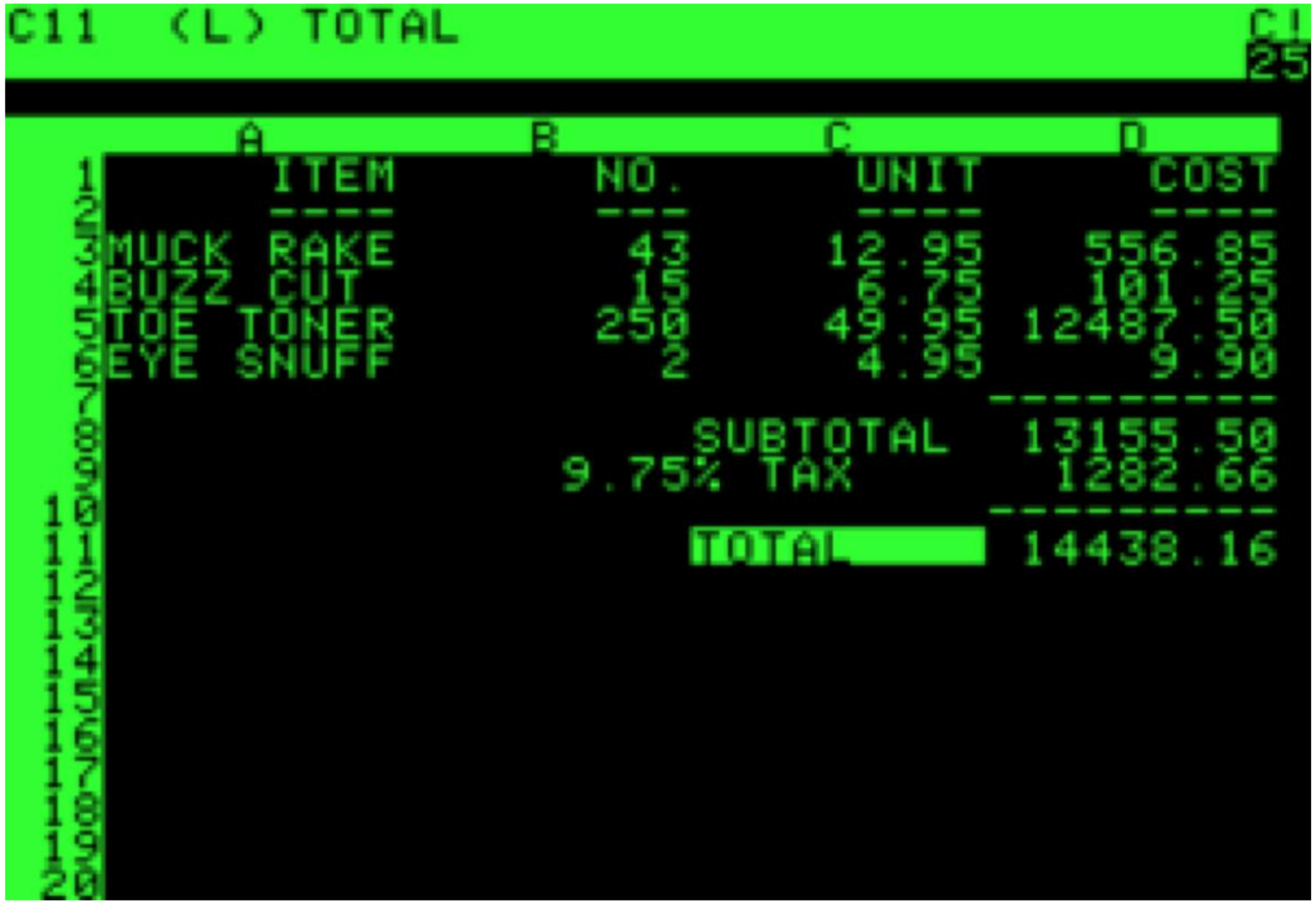
Hardware Abstraction Layer (HAL)

- BIOS was designed to be a layer between the OS and the hardware.
- There were different kinds and sizes of disks, makes and models and the HAL took care abstracting the differences.
- Kind of like the original kernel drivers for hardware.
- The BIOS does not have code for every hardware device.
- Getting back to the First Security Principles, which of the principles allows one command to manipulate many similar devices such as hardware with different geometries?

BIOS

- But, there were problems.
- SLOW. Normally when you put things in hardware, they are sped up, but BIOS was slow. It has to go over a bus.
- VisiCalc was an original spreadsheet. It wanted to scroll vertically and horizontally. However, it was ssssllllllooooowwwww.
- Solution, rewrite the BIOS. It was simple at that time and you could do it. You had the source and it was not going to change quickly
- IBM BIOS was reverse engineered and we had compatible computers
- And thus we have a program with compatibility. When the OS was upgraded, problems.

VisiCalc
The first killer app



```
C11   (L) TOTAL                              C!
                                             25

           A            B           C            D
 1        ITEM         NO.        UNIT        COST
 2        ----         ---        ----        ----
 3MUCK  RAKE            43       12.95      556.85
 4BUZZ  CUT             15        6.75      101.25
 5TOE  TONER           250       49.95    12487.50
 6EYE  SNUFF             2        4.95        9.90
 7                                       ---------
 8                        SUBTOTAL        13155.50
 9                    9.75% TAX            1282.66
10                                       ---------
11                        TOTAL           14438.16
12
13
14
15
16
17
18
19
20
```

www.wikipedia.org

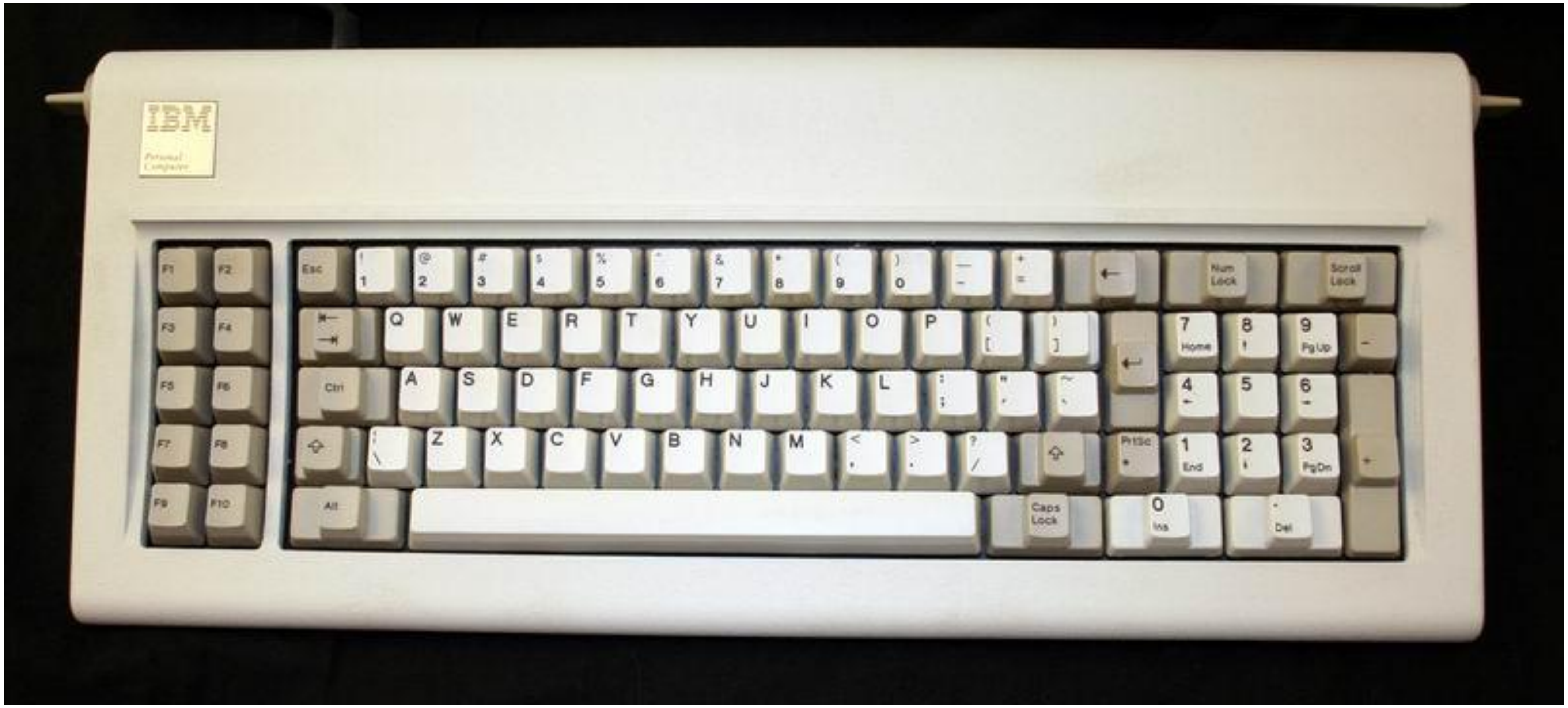
BIOS today

- Used in power up
- Initialize the hardware
- Look through the boot devices
- Which device is bootable and first in the list?
- Then, the OS would take over for the BIOS
- Windows supplied their own drivers

BIOS today

- Mid 1990s, BIOS is starting to show its age
- Wanted to boot over the network
    - RAID
    - Thin client - Virtual Machines
- Security
- Motherboard wanted to monitor itself
    - Voltage, Temperature, Fans, Power Supply
- As an aside, you can see the beginning of the IoT.

IBM PC Keyboard



Alienware

Modern Hardware

Liquid Cooling

Very Modern Hardware

EFI and UEFI

- Problem: computers are more complicated and need a more sophisticated boot process.
- **Extensible Firmware Interface**
    - And then
- **Unified Extensible Firmware Interface** - which is SOTA in firmware today
- http://www.uefi.org /* There is even a conference!
- Has things like the APCI, monitors the power consumption.
- Does this disk drive need to be spinning, or can I save power and spin up when needed?

UEFI

- Not necessary for every maker to write their own “BIOS”. We standard for this.
- Want the hardware makers to come together on the standard: http://www.uefi.org/members
- Really about chassis and motherboard management.
- At version 2.2 of UEFI, we need some security.
- Secure Boot, why is this needed?
- https://www.youtube.com/watch?v=f45QyFdMt5Q

Secure Boot

- Secure Boot is a technology where the system firmware checks if the system boot loader is signed with a cryptographic key authorized by a database contained in the firmware. With adequate signature verification in the next-stage boot loader(s), kernel, and, potentially, user space, it is possible to prevent the execution of unsigned code.

- Source: https://docs.fedoraproject.org/en-US/Fedora/18/html/UEFI_Secure_Boot_Guide/chap-UEFI_Secure_Boot_Guide-What_is_Secure_Boot.html

Secure Boot

- Platform Key - manufacturer signs the firmware.
- Crypto is not only in software, but also hardware
- Firmware is signed with the manufacturer’s **private** key.
- Thus, the manufacturer becomes the CA and the cert is self signed.
- This means that there is a public key burned into the ROM that verifies the signature of the startup firmware.
- Thus, only signed firmware can be booted on this mother board.
- Is there a problem? It is beginning to sounds like Apple. Lockdown.

Secure Boot DB

- Key Exchange DB
- Allowed DB
- Forbidden DB

Key Exchange DB

- Contains public keys or **trust anchors**
- Crypto signatures that are allowed to modify the other two databases.
- These are trusted “programs”

Allowed and Forbidden

- Allowed Database
- Forbidden Database

Allowed and Forbidden

- Allowed Database
- Forbidden Database
- Yes, but what do they contain?
- What does the Forbidden DB sound like?
  - Where have I heard that before?
    - Certificate Revocation List?

Secure Boot

- To summarize.
- Secure Boot’s goal is to make sure nothing that is known bad or unknown is ever allowed to run before the OS starts.
- It requires code signing.
- Perhaps this is not as critical in your home PC, but in industrial control systems that monitor pipelines, aircraft controls systems, power plants, SCADA, …

Measured Boot

- Strange name.
- Runs through out the boot process
- Creates an audit trail
- Makes sure all firmware that is expected is initialized.

Windows

- After all the firmware has been checked, it is time for Windows to start.
- All Windows 64-bit kernel drivers are digitally signed.
- On boot, the UEFI “reaches up” from the firmware and ensure the first drivers are signed appropriately.
- Checks the “Allowed and Forbidden” DB before allowing the computer to continue.
- Thus, they are authenticated and not modified.
  - Integrity and authenticity

Windows Boot Drivers

- Some kernel drivers need to start early in the boot process.
- Handoff between the UEFI and Microsoft boot process
- At this point, Microsoft is able to say that only only signed and trusted modules from power on to now have been able to operate.

Windows Boot Drivers

- One such driver is Early Launch Anti Malware (ELAM)
- Being launched first enables the inspection of any further drivers.
- Inspects each boot-start driver for authenticity (Signed)
- Can send a report outside of the machine that the machine is verified.
- The audit trail signed.
- If you have a large installation that needs high security, this feature might be useful to keep foreign devices on your network.

Secure Boot

- Secure Boot and Audited Boot for Windows
- Perhaps a large enterprise does not allow a computer on the network unless it has passed the measured boot.
- It must be in full trusted mode.

Secure Boot

- What happens if you cannot turn Secure Boot off?
- You have an appliance that only does one thing.
- It is difficult to turn Secure Boot off.
- https://www.youtube.com/watch?v=2OCpJP4Eh88
- To get the Windows 8 logo, the machine must be shipped in Secure Boot Mode.

Secure Boot

- Do you think there is a programatic interface to manipulate Secure Boot?
- Asked a slightly different way, should there be a programatic interface?

Secure Boot

- Do you think there is a programatic interface to turn off Secure Boot?
- No. This could be a vector for a root kit.
- That is why it was so difficult to change in the video.

Secure Boot

- With secure boot, does all hardware have to be trusted and “approved”?
- Why should a company want secure boot?
- http://www.pcworld.com/article/2901262/microsoft-tightens-windows-10s-secure-boot-screws-where-does-that-leave-linux.html

Secure Boot

- Why should a company want secure boot?
- http://www.pcworld.com/article/2901262/microsoft-tightens-windows-10s-secure-boot-screws-where-does-that-leave-linux.html
- People are on the local network.
- If you load another OS, problems.
  - Insider threat
  - Behind the firewall
- Substitute a different random number generator, …

Summary

- UEFI is the modern version of BIOS
- Secure Boot ensures no unexpected software is loaded on a computer when booting.
- All of this is done with crypto.

Terms to remember

- Code Signing
- BIOS
- Trust anchor
- Hardware Abstraction Layer
- EFI/UEFI
- Secure Boot

All safe, correct?

- Meet Samy Kamkar
- https://www.youtube.com/watch?v=Aatp5gCskvk

Last slide

- See subject.