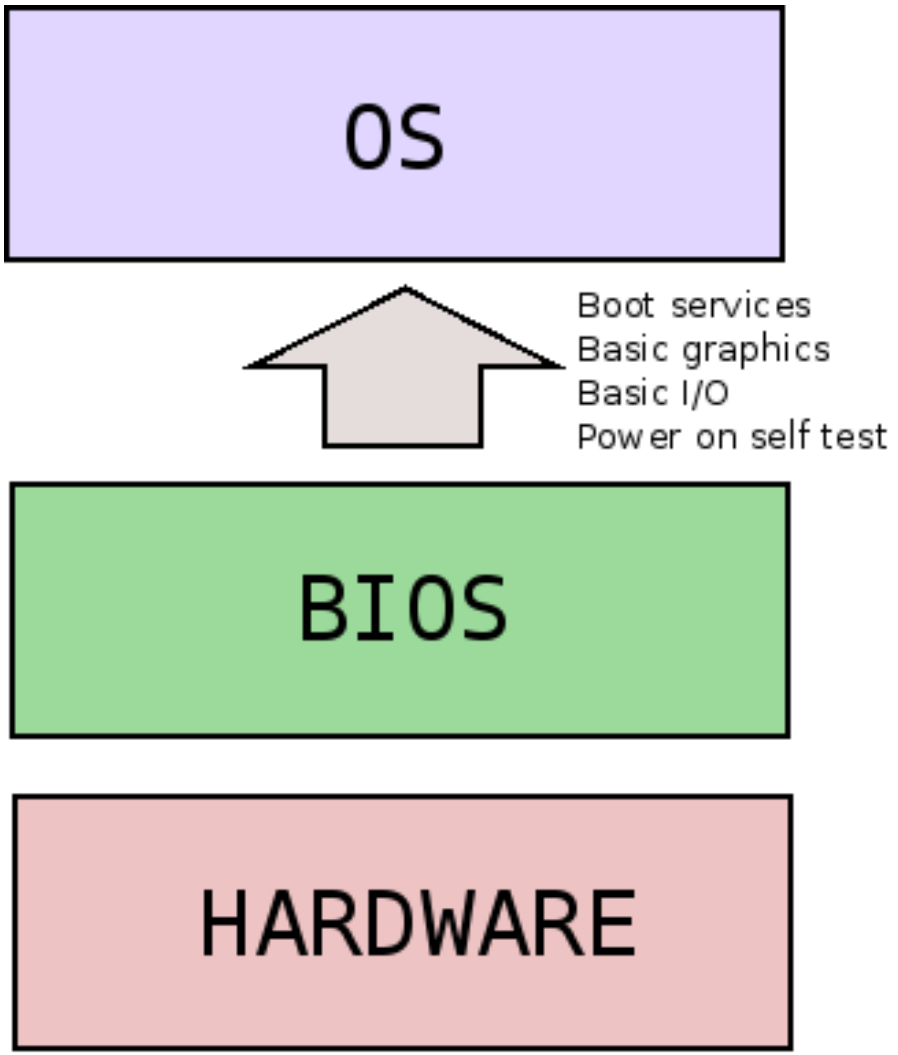
UEFI Secure Boot

Nur Hussein
hussein@bu.edu

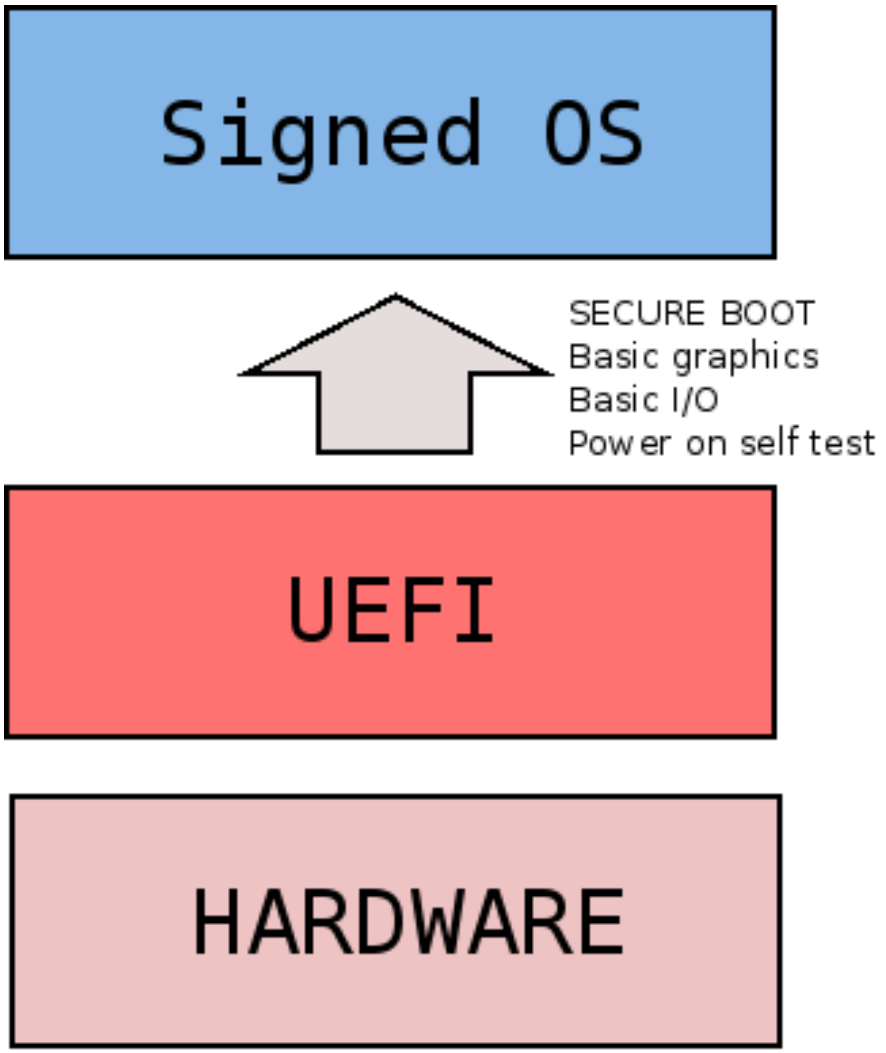
The PC BIOS

- Firmware embedded in non-volatile ROM
- Code that is first run when a PC starts up
- Provides very basic set of drivers for hardware
- Locates bootloader on disk (the program the starts the OS) and passes control to it after starting up.



UEFI As A BIOS Replacement

- Unified Extensible Firmware Interface
- A spec for the replacement of PC BIOS's.
- Has features improving upon what BIOS provides : can read some filesystems, knows where the OS image is, provides secure boot
- Secure boot is to ensure that no untrusted software is loaded before the OS loads : e.g. boot sector viruses

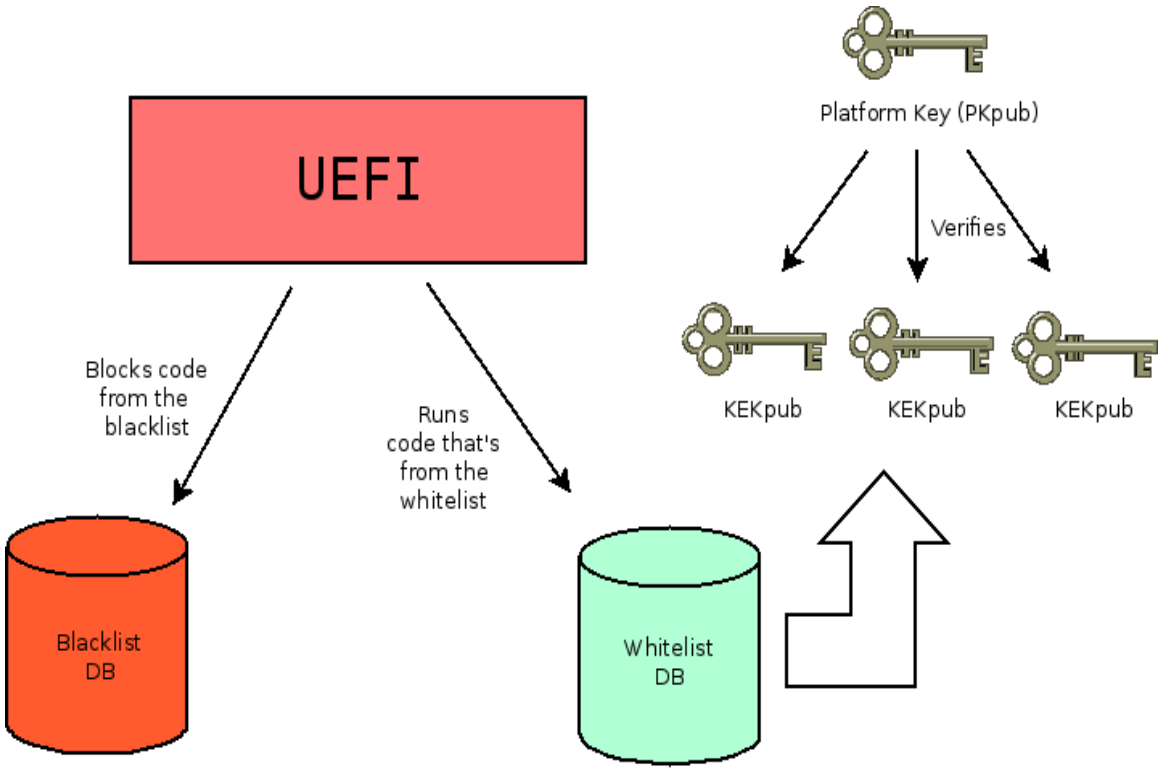


The Security Model

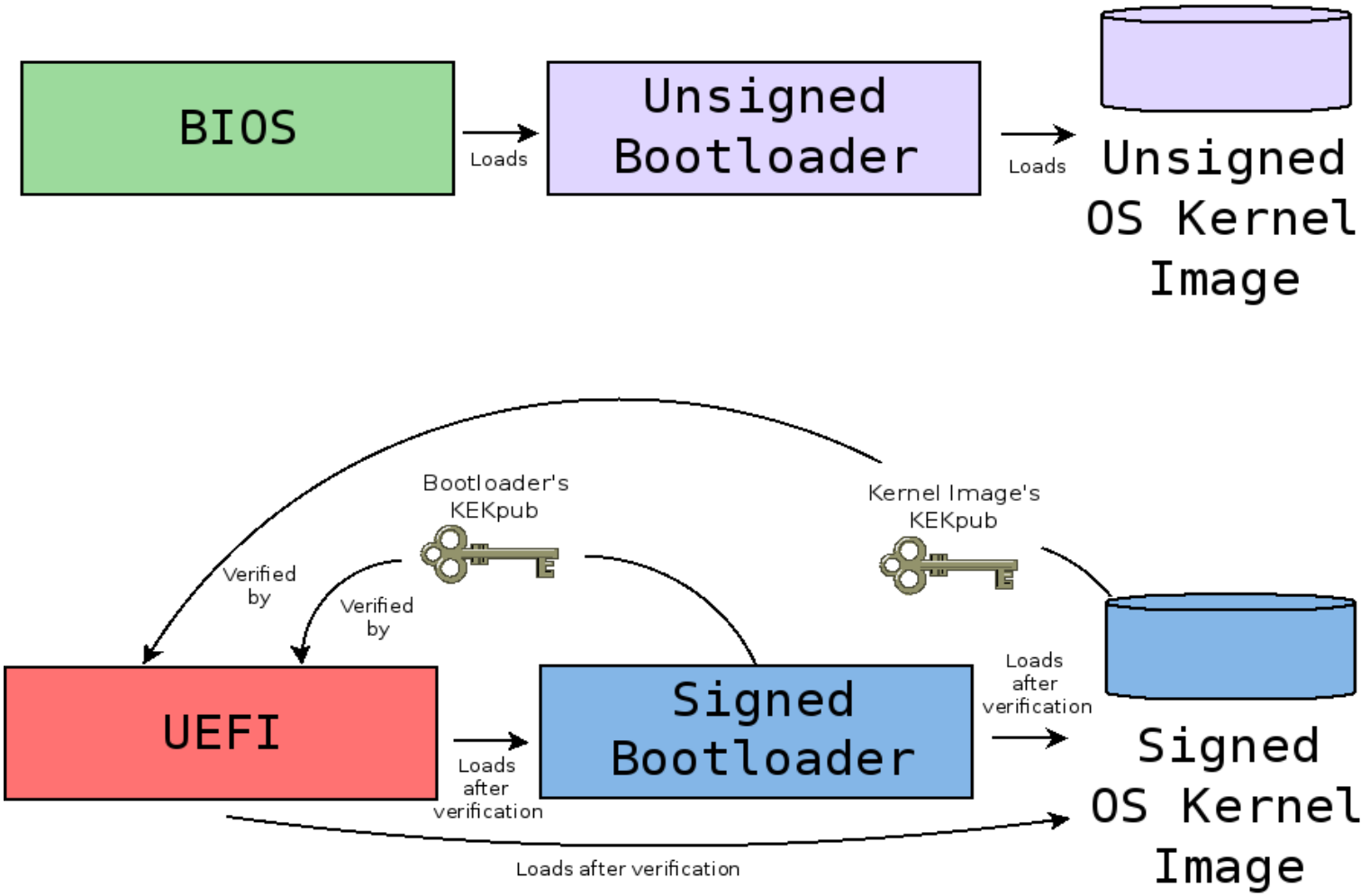
- Public key infrastructure
- GOAL : Make sure no untrusted system code is allowed to boot
- Assumptions:
  - Firmware isn't easily modifiable
  - UEFI implementation is bug-free
  - A signed OS needs to enforce the policy of not allowing ANY unsigned code to be loaded in privileged mode (kernel, drivers)
  - The signed bootloader, OS kernel and all drivers are bug-free

How Does Secure Boot Work?

- Consists of a Platform Key (Pkpub) and 2 databases of Key Exchange Keys (KEKpub): a blacklist and a whitelist
- The Pkpub is used to add or remove keys from the KEKpub database.
- The KEKpub whitelist are signatures for trusted bootloaders and operating systems; the blacklist consist of revoked keys and hashes of known malware
- The databases are updated during firmware updates.



Securing The Boot Process



Root Of Trust

- How do I get signed?
- Who owns the signing key?
- Who decides who gets on the whitelist/blacklist
- Will hardware ownership shift from consumer to a small cabal of key owners?
- Who inspects the bootloader/OS/device driver to ensure it enforces the policy

How Can I Modify An OS Now?

- Who does that anyway?
  - Hobbyists
  - Researchers
  - Device driver writers – device manufac-turers – loadable kernel modules must now be signed
  - Linux companies

General Purpose Computing Being Increasingly Locked Down?

- Don't panic! We can still disable secure boot or have customisable platform keys.
- For now.
- ARM devices that want to be “Windows certified” cannot disable secure boot.
- OEMs don't have to provide the disable secure boot functionality
- Likewise for custom mode
- GPL3 violation

References

- Bottomley, J. and Corbet, J., “Making UEFI Secure Boot Work With Open Platforms”, The Linux Foundation 2011, http://goo.gl/AWUeJ
- Garrett, M, “EFI and Linux: the future is here, and it's awful”, LCA2012 presentation http://www.youtube.com/watch?v=V2aq5M3Q76U
- Garrett, M. “UEFI Secure Boot”, 2011,http://mjg59.dreamwidth.org/5552.html
- Schwartz, M.J., “Will Windows 8 Secure Boot Block Linux?”, Information-week Sept. 2011 http://www.informationweek.com/news/security/management/231602140
- Sinofsky, S., “Protecting the pre-OS environment with UEFI”, Sept 2011 http://goo.gl/hsbp6
- UEFI Home Page: http://www.uefi.org/home/