Windows

Windows und Windows Phone

Boot Vorgang

Christoph Stephan

November 13, 2015

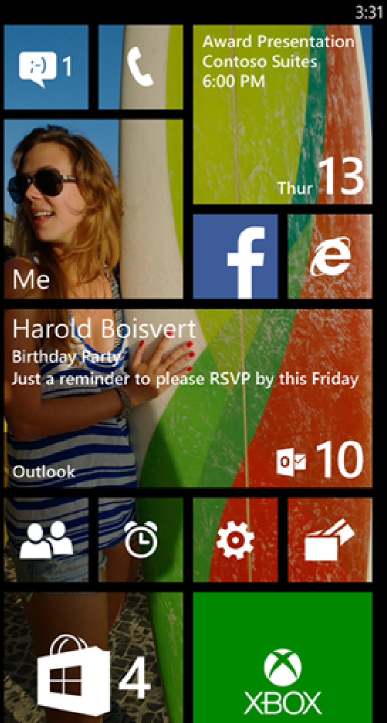
Gliederung

Windows Phone

Windows

UEFI

Quellen



Award Presentation
Contoso Suites
6:00 PM

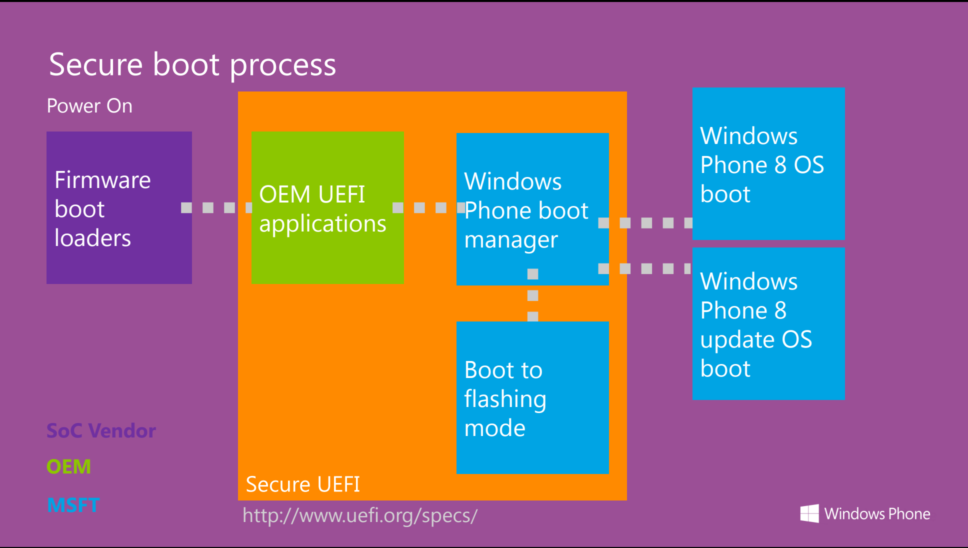
Harold Boisvert
Birthday Party
Just a reminder to please RSVP by this Friday

UEFI Secure Boot

Windows Phone

- Integrität des OS
- Implementiert in SoC
  - pre-UEFI boot loader → initialisieren Hardware
  - UEFI secure boot

    Integrität von UEFI Applicationen und Windows OS
- Es kann keine Malware installiert werden



Secure boot process

Power On

Firmware boot loaders

OEM UEFI applications

Windows Phone boot manager

Windows Phone 8 OS boot

Windows Phone 8 update OS boot

Boot to flashing mode

Secure UEFI

SoC Vendor

OEM

MSFT

http://www.uefi.org/specs/

[https://www.msec.be/mobcom/ws2013/presentations/david_hernie.pdf]

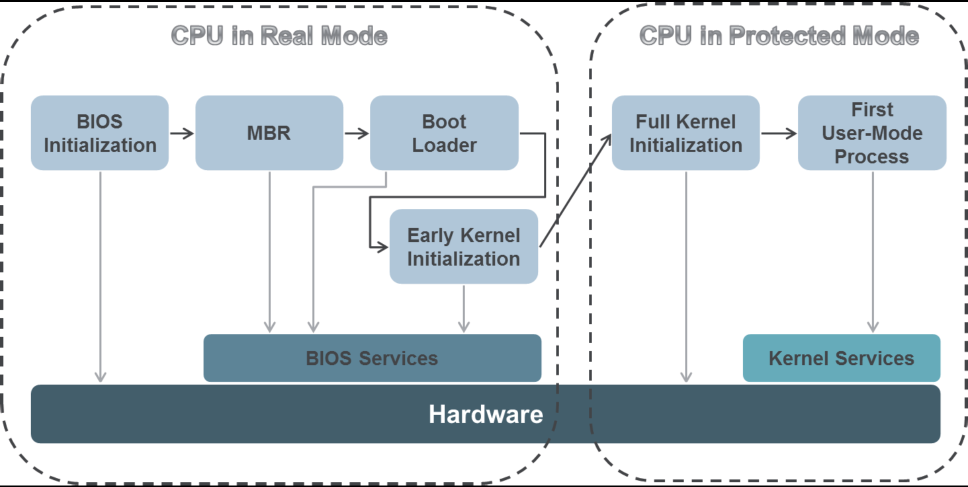
5:11
Backgrounds Wallpapers HD
9:00 AM 12:00 PM
Tuesday, October 11
5
2

UEFI Secure Boot

Windows

- UEFI Secure Boot

UNIFIED EXTENSIBLE
FIRMWARE INTERFACE



CPU in Real Mode

BIOS Initialization

MBR

Boot Loader

Early Kernel Initialization

BIOS Services

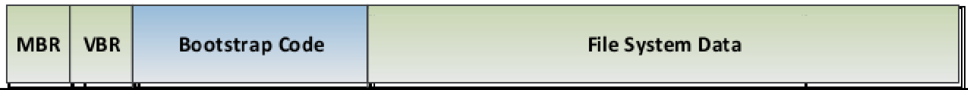
CPU in Protected Mode

Full Kernel Initialization

First User-Mode Process

Kernel Services

Hardware



MBR

VBR

Bootstrap Code

File System Data

UEFI

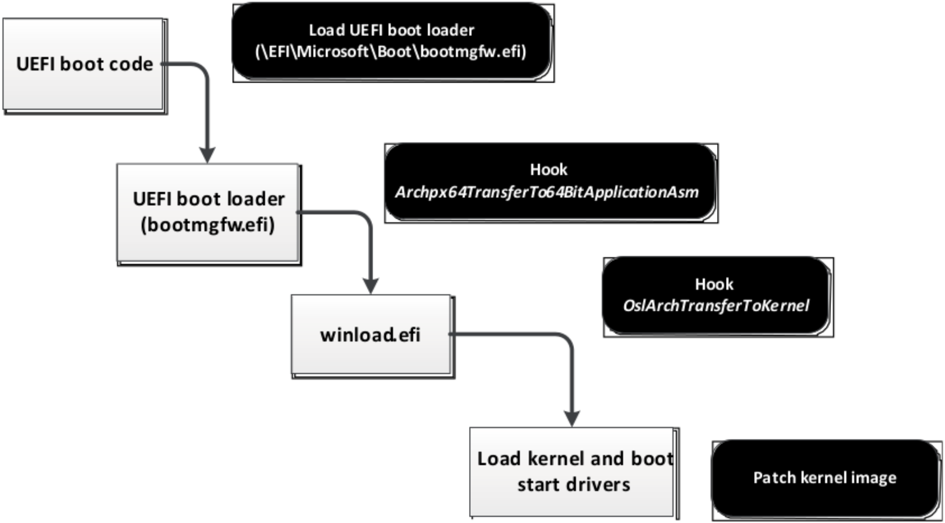
- MBR und VBR code ersetzt durch UEFI boot code

  früher: lädt den bootmgr oder winload
- MBR-based partitioning scheme ersetzt durch GPT (GUID Partition Table)
- UEFI bootloader in eigener Partition (EFI System Partition, FAT32/FAT16/FAT12)
  - NVRAM-Variable enthält Pfad zum bootloader

    zum Beispiel: Microsoft Windows 8 →

    «\EFI\Microsoft\Boot\bootmgfw.efi»

    lädt den Kernel winload.efi



UEFI boot code

Load UEFI boot loader (\EFI\Microsoft\Boot\bootmgfw.efi)

UEFI boot loader (bootmgfw.efi)

Hook *Archpx64TransferTo64BitApplicationAsm*

winload.efi

Hook *OslArchTransferToKernel*

Load kernel and boot start drivers

Patch kernel image

Secure Boot

UEFI

- Schützt vor solchen Angriffen mit erweiterten security features
  - key signing
  - signature checking
- Optionales Feature

Secure Boot

UEFI

- Schützt vor solchen Angriffen mit erweiterten security features
    - key signing
    - signature checking
- Optionales Feature

UEFI Secure Boot in Modern Computer Security

no one has claimed or demonstrated an attack that can circumvent UEFI Secure Boot on a system on which it is properly implemented and enabled[1].

Secure Boot

UEFI

- Schützt vor solchen Angriffen mit erweiterten security features
  - key signing
  - signature checking
- Optionales Feature

UEFI Secure Boot in Modern Computer Security

no one has claimed or demonstrated an attack that can circumvent UEFI Secure Boot on a system on which it is properly implemented and enabled[1].

[1] While it may be possible to circumvent UEFI Secure Boot on some machines, this is due to errors in implementation – as opposed to a security flaw of UEFI.

Quellen

- https://www.msec.be/mobcom/ws2013/presentations/david_hernie.pdf
- https://www.virusbtn.com/pdf/conference/vb2014/VB2014-RodionovMatrosov.pdf
- http://uefi.org/sites/default/files/resources/UEFI_Clarifying_Common_Misconceptions_White_Paper_April%202014_Final.pdf
- http://winaero.com/blog/windows-10-pc-install-linux/
- http://winblog.blob.core.windows.net/win/sites/3/2014/05/clip_5F00_image002_5F00_thumb_5F00_64CD0725.png
- https://store-images.s-microsoft.com/image/apps.58687.9007199266504034.3a6a2450-8df4-4c37-b331-cd7f086c3fcf.d33a79ae-732f-4ea9-aa85-a11008ee02df?w=712&h=400&mode=letterbox&background=black
- http://winaero.com/blog/wp-content/uploads/2015/03/13_02-368px-Uefi-logo-svg.png