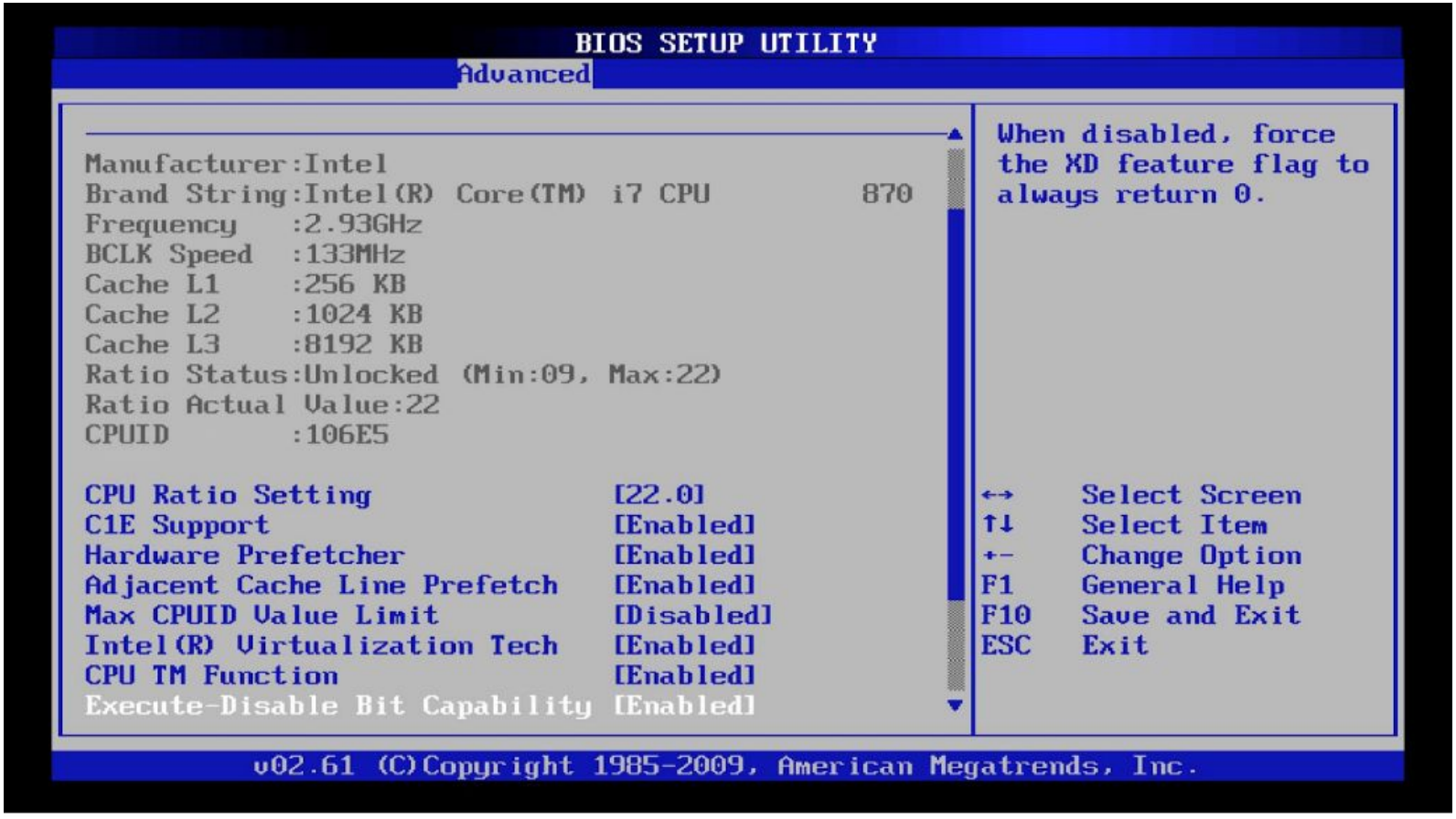
Overenie vhodnosti používania UEFI firmvéru na bežných PC

Michal Škuta

História BIOS a UEFI

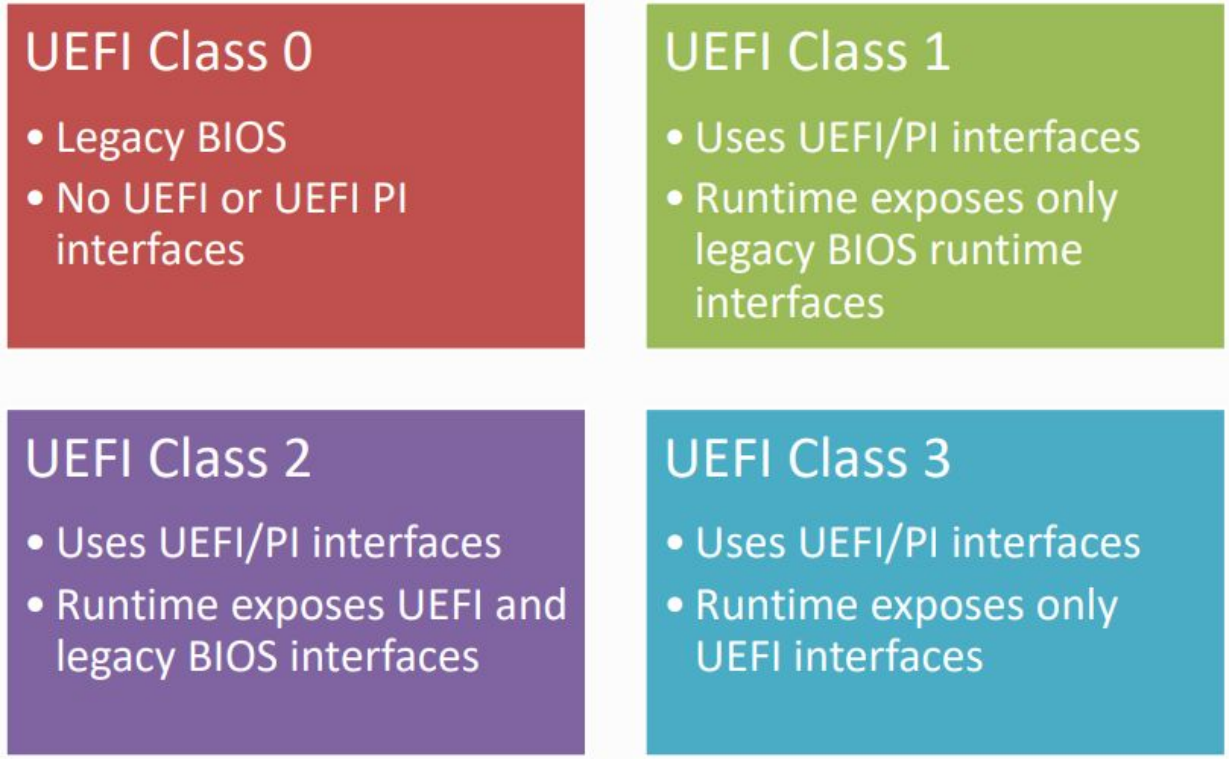
- 1981 Prvý PC od IBM s BIOSom
- 2005 Založenie UEFI fóra
- 2010 SecureBoot bol pridaný do špecifikácie
- 2012 Windows 8 a nutnosť UEFI
- 2012 Podpora UEFI SecureBoot na systémoch Ubuntu (12.04.2, 12.10)

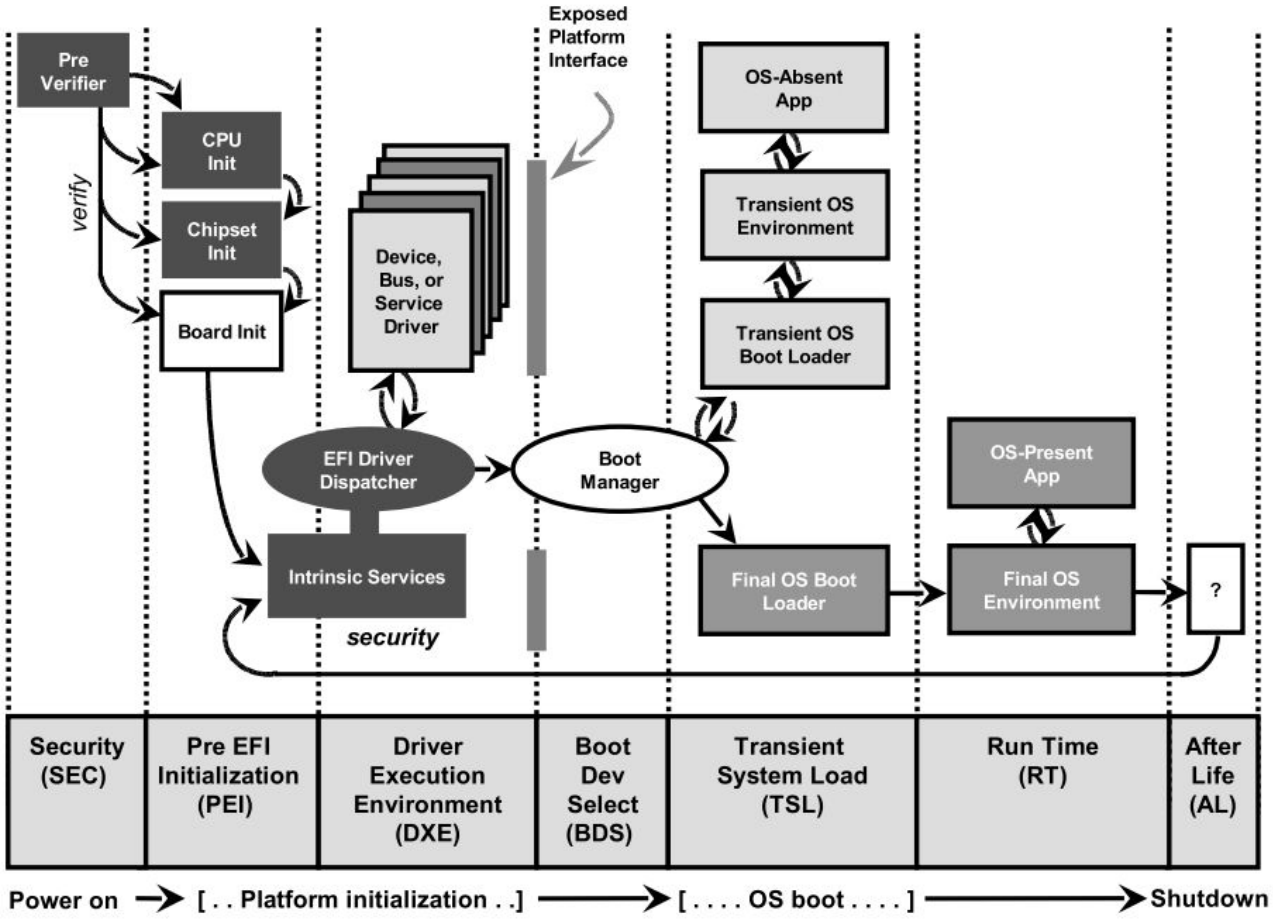
Používateľsky zážitok


BIOS SETUP UTILITY
Advanced
Manufacturer:Intel
Brand String:Intel(R) Core(TM) i7 CPU 870
Frequency :2.93GHz
BCLK Speed :133MHz
Cache L1 :256 KB
Cache L2 :1024 KB
Cache L3 :8192 KB
Ratio Status:Unlocked (Min:09, Max:22)
Ratio Actual Value:22
CPUID :106E5
CPU Ratio Setting [22.0]
C1E Support [Enabled]
Hardware Prefetcher [Enabled]
Adjacent Cache Line Prefetch [Enabled]
Max CPUID Value Limit [Disabled]
Intel(R) Virtualization Tech [Enabled]
CPU TM Function [Enabled]
Execute-Disable Bit Capability [Enabled]
When disabled, force the XD feature flag to always return 0.
↔ Select Screen
↑↓ Select Item
+- Change Option
F1 General Help
F10 Save and Exit
ESC Exit
v02.61 (C)Copyright 1985-2009, American Megatrends, Inc.


GIGABYTE - UEFI DualBIOS
M.I.T.
System Information
BIOS Features
Peripherals
Power Management
Save & Exit
English
Q-Flash
M.I.T. Current Status
Advanced Frequency Settings
Advanced Memory Settings
Advanced Voltage Settings
PC Health Status
Miscellaneous Settings
Show all information about M.I.T. status
BIOS Version F7
BCLK 99.85MHz
CPU Frequency 3694.69MHz
Memory Frequency 1597.67MHz
Total Memory Size 8192MB
CPU Temperature 75.0°C
Vcore 1.320V
DRAM Voltage 1.476V
→←: Select Screen ↑↓/Click: Select Item
Enter/Dbl Click: Select
+/-/PU/PD: Change Opt.
F1 : General Help
F5 : Previous Values
F7 : Optimized Defaults
F8 : Q-Flash
F9 : System Information
F10 : Save & Exit
F12 : Print Screen(FAT16/32 Format Only)
ESC/Right Click: Exit
Copyright (C) 2014 American Megatrends, Inc.

UEFI triedy

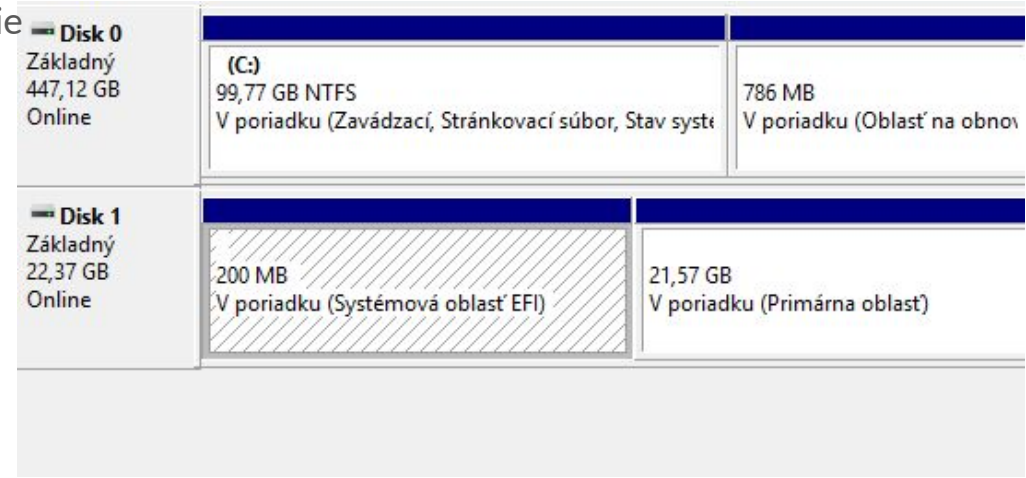

UEFI Class 0
• Legacy BIOS
• No UEFI or UEFI PI interfaces
UEFI Class 1
• Uses UEFI/PI interfaces
• Runtime exposes only legacy BIOS runtime interfaces
UEFI Class 2
• Uses UEFI/PI interfaces
• Runtime exposes UEFI and legacy BIOS interfaces
UEFI Class 3
• Uses UEFI/PI interfaces
• Runtime exposes only UEFI interfaces


Pre Verifier
verify
CPU Init
Chipset Init
Board Init
Device, Bus, or Service Driver
Exposed Platform Interface
EFI Driver Dispatcher
Intrinsic Services
security
Boot Manager
OS-Absent App
Transient OS Environment
Transient OS Boot Loader
Final OS Boot Loader
OS-Present App
Final OS Environment
?
Security (SEC)
Pre EFI Initialization (PEI)
Driver Execution Environment (DXE)
Boot Dev Select (BDS)
Transient System Load (TSL)
Run Time (RT)
After Life (AL)
Power on
[. . Platform initialization . .]
[. . . . OS boot . . . .]
Shutdown

ESP a bootovanie

- GPT oproti MBR
- pre ESP sa používa FAT32 formátovanie
- viacero volieb v BDS

- \EFI\Boot\BOOTX64.efi
- \EFI\ubuntu\grubx64.efi
- \EFI\Microsoft\



Secureboot

- PK (platform key) na správu KEK kľúčov
- KEK (key exchange keys) na podpísanie DB a DBX
- DB databáza povolených aplikácii (konkrétny HASH alebo certifikát)
- DBX databáza zakázaných aplikácii

Ubuntu:

- SHIM podpísaný Microsoft Corporation UEFI CA (zvyčajne nachádzajúci sa v DB)

Vývoj SW

- GNU-EFI a EDK2 (TianoCore)
- Protokoly zadefinované v UEFI špecifikácii
- RunTime Services
  (práca s NVRAM , reset systému)
- BootTime Services
  (alokácia pamäte, vstup klávesnice prístup k protokolom)

```c
#include <efi.h>
#include <efilib.h>

EFI_STATUS
EFIAPI
efi_main (EFI_HANDLE ImageHandle, EFI_SYSTEM_TABLE *ST) {
    InitializeLib(ImageHandle, ST);
    uefi_call_wrapper(ST->ConOut->OutputString, 2,
                      ST->ConOut, L"Hello World!\n");

    return EFI_SUCCESS;
}
```

Bezpečnosť

- EFI rootkit
- článok z Wikileaks Vault7 opisuje spôsob ako napadnúť systém s UEFI
- Intel Chipsec pre zistenie problémov

Coreboot

- open source
- dostupný zariadeniach s ChromeOS + na pár vybraných PC sa dá nainštalovať
- X86, ARM/64, MIPS, POWER8 and RISC-V
- Payload (SeaBios,EFI,Grub)

Zhrnutie

- UEFI firmvér je nástupca BIOSu
- podporovaný OS Microsoft Windows
- Otázky?