dobrý sluha nebo špatný pán?

Radek Zajíc, radek@zajic.v.pytli.cz • LinuxDays 2018, 7. 10. 2018

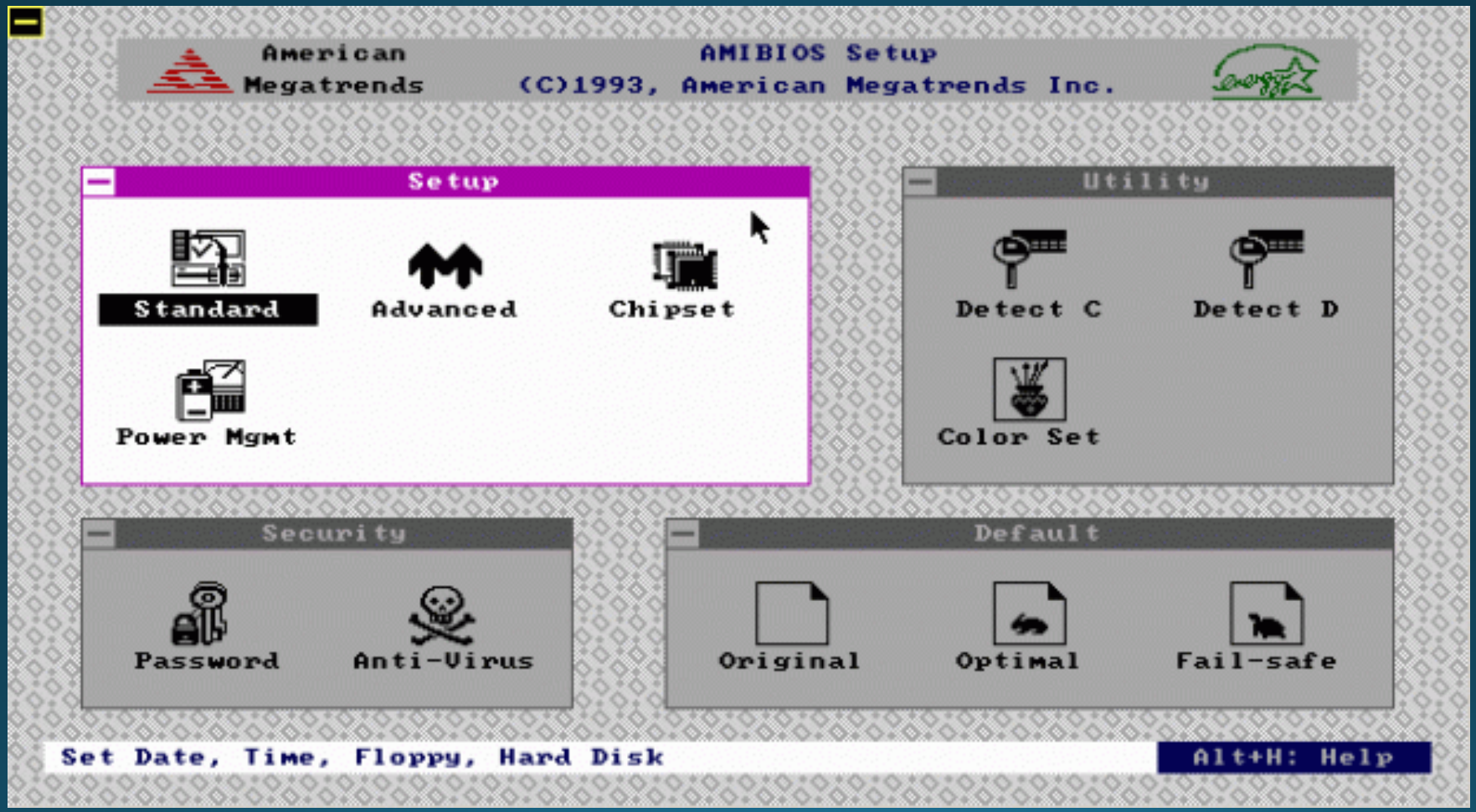
O mně

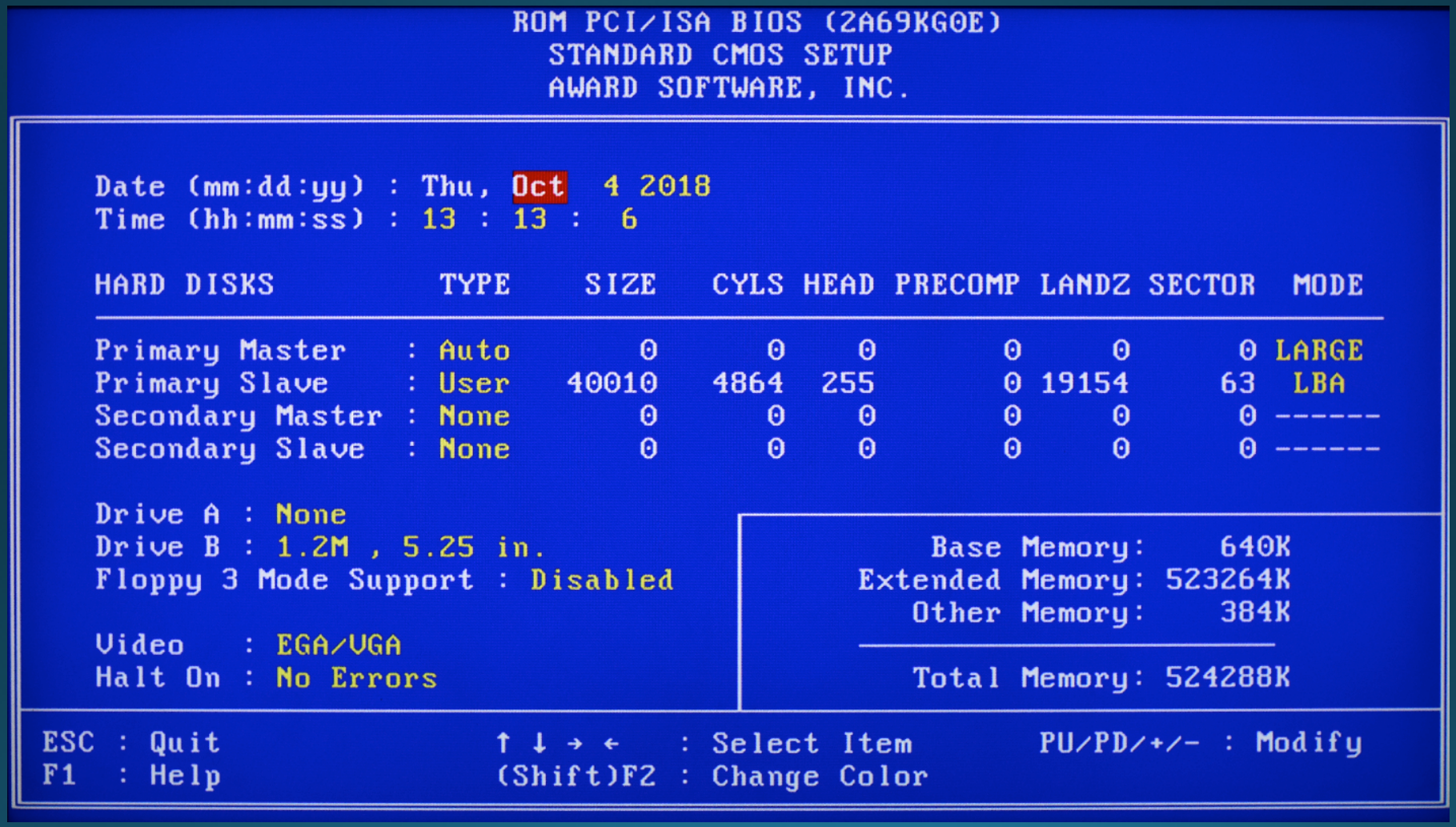
Radek Zajíc

IPv6?

Blog: tech.showmax.com
Twitter: @ShowmaxDevs

ASUS UEFI BIOS Utility - EZ Mode
Exit/Advanced Mode
09:29
Sunday [02/08/2015]
P8Z77-M PRO
English
BIOS Version : 2105
CPU Type : Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz
Speed : 3100 MHz
Total Memory : 16384 MB (DDR3 1333MHz)
Temperature
CPU +104.0°F/+40.0°C
MB +80.6°F/+27.0°C
Voltage
CPU 0.960V
5V 5.120V
3.3V 3.376V
12V 12.384V
Fan Speed
CPU_FAN 1314RPM
CHA_FAN1 805RPM
CHA_FAN2 808RPM
CHA_FAN3 N/A
System Performance
Quiet
Performance
Energy Saving
Normal
Boot Priority
UEFI
UEFI
Use the mouse to drag or keyboard to navigate to decide the boot priority.
Shortcut(F3)
Advanced Mode(F7)
Boot Menu(F8)
Default(F5)


American
Megatrends
AMIBIOS Setup
(C)1993, American Megatrends Inc.
Setup
Standard
Advanced
Chipset
Power Mgmt
Utility
Detect C
Detect D
Color Set
Security
Password
Anti-Virus
Default
Original
Optimal
Fail-safe
Set Date, Time, Floppy, Hard Disk
Alt+H: Help


ROM PCI/ISA BIOS (2A69KG0E)
STANDARD CMOS SETUP
AWARD SOFTWARE, INC.
Date (mm:dd:yy) : Thu, Oct 4 2018
Time (hh:mm:ss) : 13 : 13 : 6
HARD DISKS TYPE SIZE CYLS HEAD PRECOMP LANDZ SECTOR MODE
Primary Master : Auto 0 0 0 0 0 0 LARGE
Primary Slave : User 40010 4864 255 0 19154 63 LBA
Secondary Master : None 0 0 0 0 0 0 ------
Secondary Slave : None 0 0 0 0 0 0 ------
Drive A : None
Drive B : 1.2M , 5.25 in.
Floppy 3 Mode Support : Disabled
Video : EGA/VGA
Halt On : No Errors
Base Memory: 640K
Extended Memory: 523264K
Other Memory: 384K
Total Memory: 524288K
ESC : Quit
F1 : Help
↑ ↓ → ← : Select Item
(Shift)F2 : Change Color
PU/PD/+/- : Modify

SETUP utility

není

BIOS

ani

(U)EFI

```
/*
CP/M
BASIC I/O SYSTEM (BIOS)
COPYRIGHT (C) GARY A. KILDALL JUNE, 1975
*/
```

BIOS

```
000fff30  ef 6f ef 00 00 00 00 00  00 00 00 00 00 00 00 00  |.o..............|
000fff40  00 00 00 ff ff 00 00 00  00 30 30 30 30 30 30 30  |.........0000000|
000fff50  30 30 30 cf 60 1e b8 40  00 50 1f b0 01 86 06 00  |000.`..@.P......|
000fff60  01 3c 01 74 6f fb b3 ff  b4 02 33 d2 cd 17 80 e4  |.<.to.....3.....|
000fff70  a0 79 5c 7a 5a b4 0f cd  10 8a dc b4 03 cd 10 8b  |.y\zZ...........|
000fff80  fa 33 c9 32 f6 b0 0d e8  2e 00 b0 0a e8 29 00 3a  |.3.2.........).:|
000fff90  36 84 00 76 04 32 db eb  30 32 d2 3a d3 72 04 fe  |6..v.2..02.:.r..|
000fffa0  c6 eb e2 b4 02 cd 10 b4  08 cd 10 0a c0 75 02 b0  |.............u..|
000fffb0  20 e8 04 00 fe c2 eb e3  32 e4 87 ca cd 17 87 ca  | .......2.......|
000fffc0  f6 c4 29 75 01 c3 5a b3  ff 8b d7 b4 02 cd 10 fa  |..)u..Z.........|
000fffd0  88 1e 00 01 1f 61 cf 00  00 50 43 49 2f 49 53 41  |.....a...PCI/ISA|
000fffe0  00 60 03 3c e7 45 84 01  02 01 80 00 80 05 12 f0  |.`.<.E..........|
000ffff0  ea 5b e0 00 f0 30 38 2f  32 36 2f 39 39 00 fc c4  |.[...08/26/99...|
```

BIOS

startuje systém v 16 bit režimu

2 způsoby práce s diskem (CHS a LBA)

CHS-Normal
CHS-Large
LBA28 (1994)
LBA48 (2003)

4 způsoby detekce velikosti paměti

nemá mechanismy ověření integrity

de facto API
malá část standardi-zovaná

maximálně 4 primární oddíly na disku

limit 2 TiB na jeden diskový oddíl

440 bajtů pro zavaděč systému

zavaděč squattuje v „prostoru nikoho"

emuluje disk(etu) v případě bootu z CD

USB zařízení emuluje jako PS/2

BIOS

je omezen na architekturu Intel x86

(Unified) Extensible Firmware Interface

Specifikace (2899 s.)
(definuje rozhraní mezi OS a firmwarem)
Nahrazuje BIOS*
Odstraňuje jeho neduhy
Zavádí nové problémy

Proč znát a použít (U)EFI

NVMe

TPM 2.0

Secure Boot

Zařízení bez CSM

Intel 2020+

2+TB disk

UEFI vs. BIOS

startuje systém v 32/64 bit režimu	2 způsoby práce s diskem (CHS a LBA)	CHS-Normal CHS-Large LBA28 (1994) LBA48 (2003)	**1 způsob detekce velikosti paměti**	nemá mechanismy ověření integrity	**Kompletní specifikace API**
maximálně 4 primární oddíly na disku	limit 2 TiB na jeden diskový oddíl	440 bajtů pro zavaděč systému	zavaděč squattuje v „prostoru nikoho“	emuluje disk(etu) v případě bootu z CD	**USB zařízení nemusí emulovat**

1998 – Intel Boot Initiative

2001 – Intel EFI 1.02

2005 – Intel přispívá EFI 1.1 do UEFI fóra

2006 – UEFI 2.0

2012 – UEFI 2.3.1 Errata C

2015 – UEFI 2.5

2017 – UEFI 2.7

Třídy UEFI zařízení

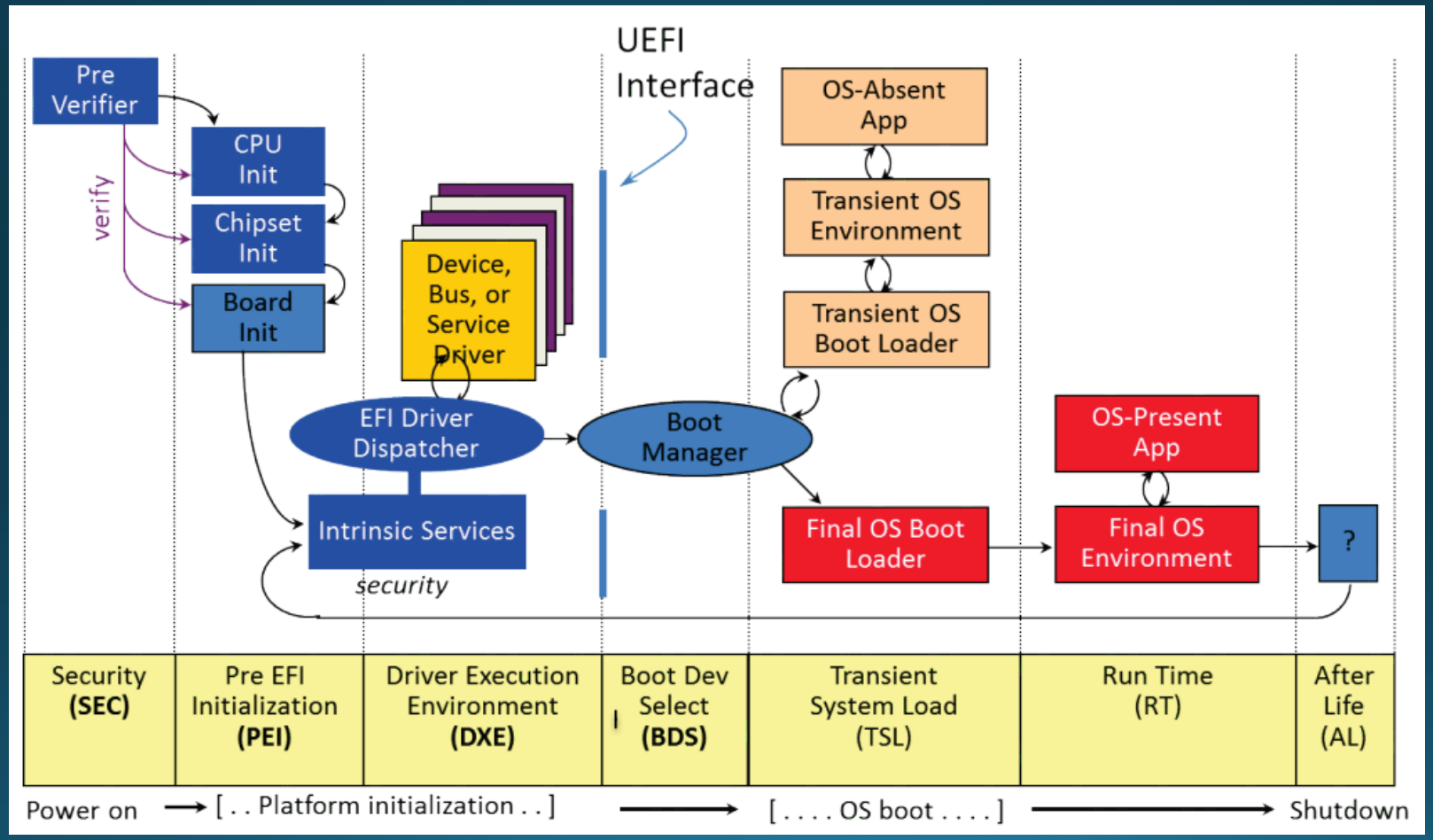
UEFI Class 0
Pouze Legacy BIOS
Žádná podpora UEFI

UEFI Class 1
Interně UEFI
Navenek emuluje Legacy BIOS

UEFI Class 2
Interně UEFI
Aplikacím dostupné UEFI i Legacy BIOS

UEFI Class 3
Interně UEFI
Aplikacím dostupné UEFI
Legacy BIOS nepřítomen

Architektura



Architektura

x86 (32bit) | x86-64 | Itanium | RISC-V | ARM (32/64)

FLAT MEMORY MODEL | RING 0 | SINGLE THREADED | DRIVERS/APPS

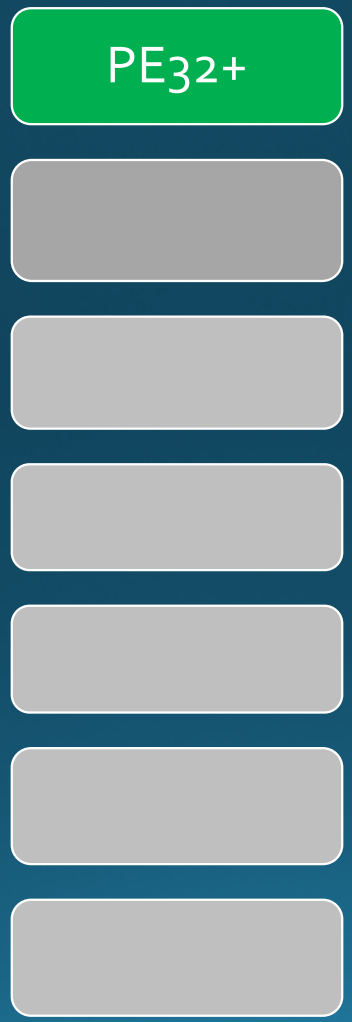
FAT32 | ISO9660 | UDF | NTFS/BTRFS/EXT/...

NVRAM | X.509 | EFI BOOT MANAGER | EFI SHELL | CSM

PE32+ | APPLICATION | BOOT_SERVICE_DRIVER | EFI_RUNTIME_DRIVER

Architektura

```
00000000  4d 5a 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |MZ..............|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000030  00 00 00 00 00 00 00 00  00 00 00 00 c0 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000000c0  50 45 00 00 64 86 05 00  f2 7e 1a 54 00 00 00 00  |PE..d....~.T....|
000000d0  00 00 00 00 f0 00 22 00  0b 02 00 00 00 fe 07 00  |......".........|
000000e0  00 32 09 00 00 00 00 00  60 10 00 00 00 10 00 00  |.2......`.......|
000000f0  00 00 40 00 00 00 00 00  00 10 00 00 00 02 00 00  |..@.............|
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000110  00 50 11 00 00 04 00 00  46 76 11 00 0b 00 00 00  |.P......Fv......|
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000140  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |................|
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000160  00 00 00 00 00 00 00 00  00 28 11 00 e8 21 00 00  |.........(...!..|
00000170  00 40 11 00 ac 01 00 00  00 00 00 00 00 00 00 00  |.@..............|
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```


PE32+

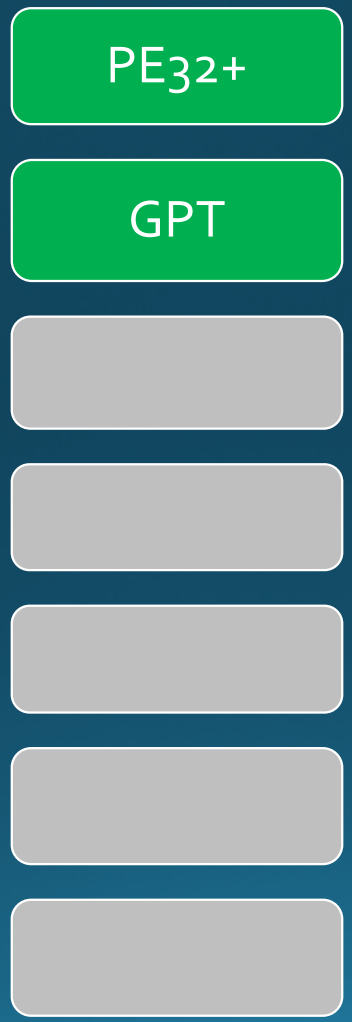
Partitioning: MBR vs. GPT

MBR	GPT
LBA 0: kód pro boot (GRUB stage 1) + tabulka oddílů	LBA 0: ochranný (protective) MBR
LBA 1 až n-1: prostor nikoho (GRUB stage 1.5)	LBA 1: GPT header (informace o velikosti GPT apod.)
	LBA 2 až n-1: tabulka oddílů
LBA n: první oddíl	LBA n: první oddíl

Schéma GPT je **plnohodnotně** podporováno Linuxem i GRUBem

Hybridní MBR

```
# sfdisk -d (…)
label: dos
unit: sectors

sdg.mbr1  : start=   2048, size=    2048, type=83
sdg.mbr2  : start=   4096, size=  102400, type=ef
sdg.mbr3  : start= 106496, size= 7806943, type=c, bootable
sdg.mbr4  : start=      1, size=    2047, type=ee

# sfdisk -d (…)
label: gpt
label-id: 1B17D4FE-3C51-44CD-9DA1-4F1AAF7948EB
unit: sectors
first-lba: 34
last-lba: 7913438

/dev/sdg1 : start=   2048, size=    2048, type=0FC63DAF-8483-4772-8E79-3D69D8477DE4
/dev/sdg2 : start=   4096, size=  102400, type=C12A7328-F81F-11D2-BA4B-00A0C93EC93B
/dev/sdg3 : start= 106496, size= 7806943, type=EBD0A0A2-B9E5-4433-87C0-68B6B72699C7
```


PE32+
GPT

Proměnné v NVRAM

```
# ls /sys/firmware/efi/efivars/ | wc -l
77

# ls -1 /sys/firmware/efi/efivars/SecureBoot* /sys/firmware/efi/efivars/BootOrder*
/sys/firmware/efi/efivars/BootOrder-<GUID>
/sys/firmware/efi/efivars/SecureBoot-<GUID>
/sys/firmware/efi/efivars/SecureBootSetup-<GUID>
```

```
Shell> dmpstore AMITSESetup -b
Dump Variable AMITSESetup
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
  00000000: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 01                                                *.*
```

Proměnné v NVRAM

```
[2.422809] EFI Variables Facility v0.08 2004-May-17
[2.427033] efivars: duplicate variable: AMITSESetup-c811fa38-42c8-4579-
a9bb-60e94eddfb34
```

```
Dump Variable AMITSESetup
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
  00000000: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00                                                *.*
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
  00000000: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00                                                *.*
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
  00000000: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000010: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000020: 00                                                *.*
```

Proměnné v NVRAM

```
Shell> dmpstore -d AMITSESetup
Delete Variable AMITSESetup
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Variable NV+RT+BS 'C811FA38-42C8-4579-A9BB-60E94EDDFB34:AMITSESetup' DataSize = 21
Failed to delete variable
```

PE32+

GPT

NVRAM

efibootmgr

```
# efibootmgr -v
BootCurrent: 0000
Timeout: 1 seconds
BootOrder: 0000,000A,0002,0003,0006
Boot0000* ubuntu HD(3,GPT,<GUID>,0xfa800,0x106000)/File(\EFI\UBUNTU\GRUBX64.EFI)
Boot0002* Hard Drive BBS(HD,,0x0)
Boot0003* USB BBS(USB,,0x0)
Boot0006* UEFI: Built-in EFI Shell VenMedia(5023b95c-db26-429b-a648-bd47664c8012)
Boot000A* UEFI OS HD(3,GPT,<GUID>,0xfa800,0x106000)/File(\EFI\BOOT\BOOTX64.EFI)

# ls -1 /sys/firmware/efi/efivars/Boot*
/sys/firmware/efi/efivars/Boot0000-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/Boot0002-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/Boot0003-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/Boot0006-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/Boot000A-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/BootCurrent-8be4df61-93ca-11d2-aa0d-00e098032b8c
/sys/firmware/efi/efivars/BootOrder-8be4df61-93ca-11d2-aa0d-00e098032b8c
```

EFI System Partition

```
# tree /boot/efi
.
`-- EFI
    `-- BOOT
        `-- BOOTX64.EFI
```

PE32+

GPT

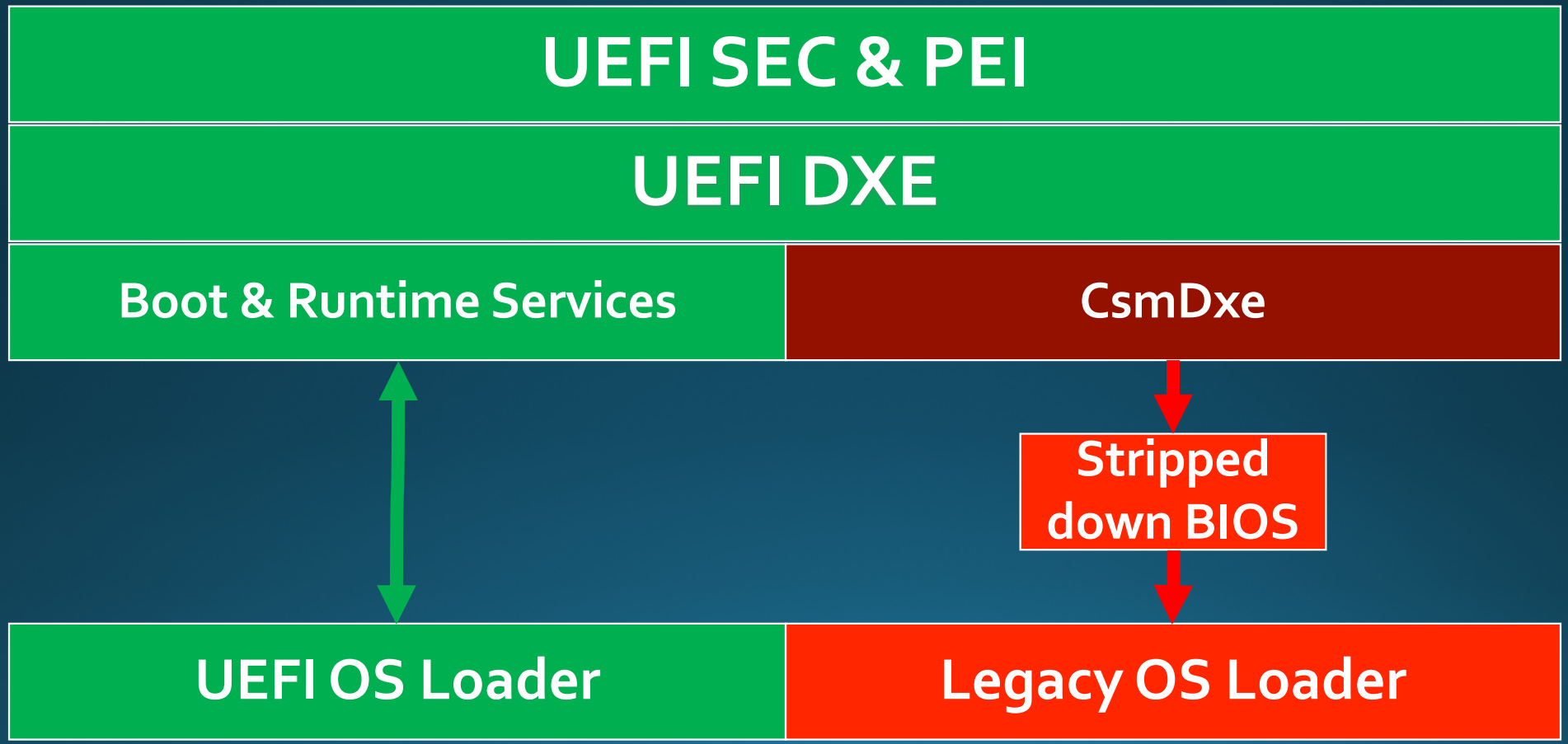
NVRAM

EFI Partition

UEFI vs. BIOS

startuje systém v 32/64 bit režimu	1 způsob práce s diskem (LBA)	LBA48	1 způsob detekce velikosti paměti	nemá mechanismy ověření integrity	Kompletní specifikace API
neomezené množství oddílů na disku	limit 8 ZiB na jeden diskový oddíl	neomezený prostor pro zavaděč systému	zavaděč je běžný soubor, nesquattuje	není nutná emulace při bootu z CD/DVD	USB zařízení nemusí emulovat

UEFI CSM


UEFI SEC & PEI
UEFI DXE
Boot & Runtime Services
CsmDxe
Stripped down BIOS
UEFI OS Loader
Legacy OS Loader

Option ROMs

```
# lspci -v
02:00.0 Serial Attached SCSI controller: LSI Logic / Symbios Logic SAS3008 PCI
-Express Fusion-MPT SAS-3 (rev 02)
        Subsystem: SAS3008 PCI-Express Fusion-MPT SAS-3
        Physical Slot: 0-1
        Flags: bus master, fast devsel, latency 0, IRQ 26, NUMA node 0
        I/O ports at 6000 [size=256]
        (…)
        Expansion ROM at c7100000 [disabled] [size=1M]
        (…)
        Kernel driver in use: mpt3sas
        Kernel modules: mpt3sas

# echo 1 > '/sys/bus/pci/devices/0000:02:00.0/rom'
# cp '/sys/bus/pci/devices/0000:02:00.0/rom' sas.rom
# hexdump -C sas.rom
```

Option ROMs

```
# fcode-utils/romheaders/romheaders sas.rom

Image 1:
PCI Expansion ROM Header:
  Signature: 0x55aa (Ok)

PCI Data Structure:
  Signature: 0x50434952 'PCIR' (Ok)
  Vendor ID: 0x1000
  Device ID: 0x0097
  Vital Product Data:  0x0032
  PCI Data Structure Length: 0x001c (28 bytes)
  PCI Data Structure Revision: 0x03
  Class Code: 0x010000 (SCSI bus controller)
  Image Length: 0x0068 blocks (53248 bytes)
  Code Type: 0x00 (Intel x86)
  Last-Image Flag: 0x00 (not last image in rom)
  Reserved: 0x5500
```

Option ROMs

```
Image 2:
PCI Expansion ROM Header:
  Signature: 0x55aa (Ok)

PCI Data Structure:
  Signature: 0x50434952 'PCIR' (Ok)
  Vendor ID: 0x1000
  Device ID: 0x0097
  Class Code: 0x010000 (SCSI bus controller)
  Image Length: 0x01be blocks (228352 bytes)
  Code Type: 0x03 (Intel EFI (unofficial))
  Last-Image Flag: 0x80 (last image in rom)

Platform specific data for EFI compliant option rom:
  EFI subsystem: 11 (EFI Boot Service Driver)
  EFI machine type: 0x8664 (AMD64 (x86-64))
  EFI image is compressed
  EFI image header offset: 0x34
```

Option ROMs

```
0000d000  55 aa be 01 f1 0e 00 00  0b 00 64 86 01 00 00 00  |U.........d.....|
0000d010  00 00 00 00 00 00 34 00  1c 00 00 02 50 43 49 52  |......4.....PCIR|
0000d020  00 10 97 00 00 00 18 00  00 00 00 01 be 01 00 0f  |................|
0000d030  03 80 00 00 80 7a 03 00  08 6c 0c 00 1f 70 85 be  |.....z...l...p..|
0000d040  fb 7a b4 9c 9f ef be fa  7a 49 24 20 49 22 08 01  |.z......zI$ I"..|
```

```
# 0xd000 + 0x34 = 0xd034 = 53300
# dd if=sas.rom of=sas.efi bs=1 skip=53300 count=228352
# python decompress.py sas.efi.compressed sas.efi
# ls -l sas.efi
-rw-r--r-- 1 root root 814088 Oct  5 22:59 sas.efi
```

```
00000000  4d 5a 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |MZ..............|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000030  00 00 00 00 00 00 00 00  00 00 00 00 c0 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000000c0  50 45 00 00 64 86 04 00  00 00 00 00 00 00 00 00  |PE..d...........|
000000d0  00 00 00 00 f0 00 22 20  0b 02 09 00 c0 10 0c 00  |......" ........|
000000e0  80 36 00 00 00 00 00 00  44 65 07 00 80 02 00 00  |.6......De......|
```

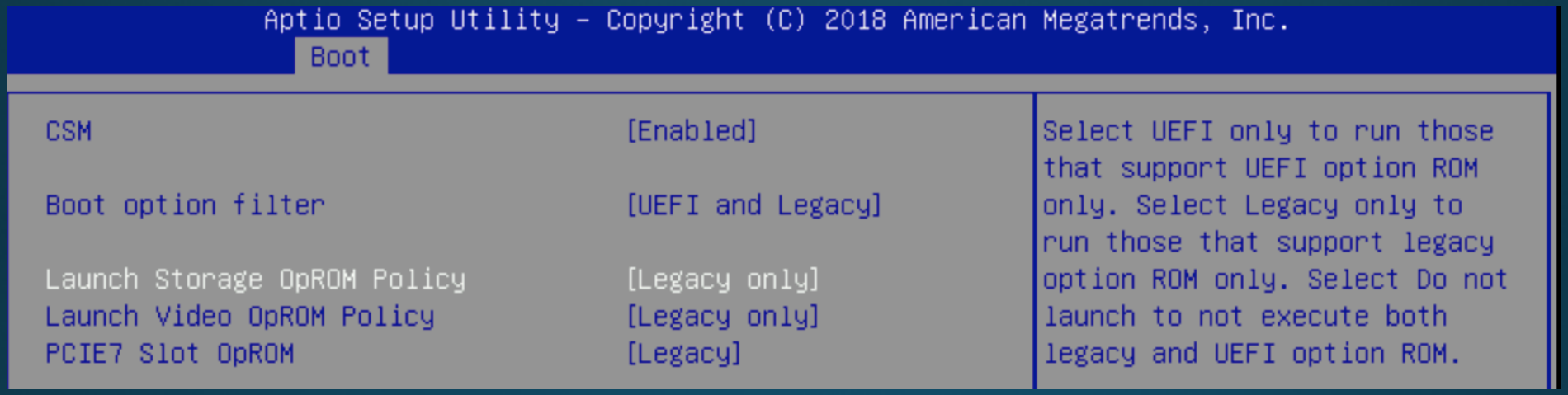
Option ROMs

```
# apt install pev
# readpe --header coff --header optional sas.efi
COFF/File header
    Machine:                        0x8664 IMAGE_FILE_MACHINE_AMD64
    Number of sections:             4
    Symbol Table offset:            0
    Number of symbols:              0
    Size of optional header:        0xf0
    Characteristics names           IMAGE_FILE_EXECUTABLE_IMAGE
                                    IMAGE_FILE_LARGE_ADDRESS_AWARE
                                    IMAGE_FILE_DLL
Optional/Image header
    Magic number:                   0x20b (PE32+)
(…)
    Size of image:                  0xc49c0
    Size of headers:                0x280
    Checksum:                       0xcc267
    Subsystem required:             0xb (IMAGE_SUBSYSTEM_EFI_BOOT_SERVICE_DRIVER)
```

Option ROMs

```
# apt install osslsigncode
# osslsigncode verify sas.efi
Current PE checksum   : 000CC267
Calculated PE checksum: 000CC267

Message digest algorithm  : SHA256
Current message digest    : D2390C85F9500E0B0A775E8BFB778D6D4F889BB36318790BC18F40C5C713397E
Calculated message digest : D2390C85F9500E0B0A775E8BFB778D6D4F889BB36318790BC18F40C5C713397E

Signature verification: ok

Number of signers: 1
Signer #0:
Subject: /C=US/O=Microsoft Corporation/OU=MOPR/CN=Microsoft Windows UEFI Driver Publisher
Issuer : /C=US/O=Microsoft Corporation/CN=Microsoft Corporation UEFI CA 2011

Number of certificates: 2
Cert #0:
Subject: /C=US/O=Microsoft Corporation/OU=MOPR/CN=Microsoft Windows UEFI Driver Publisher
Issuer : /C=US/O=Microsoft Corporation/CN=Microsoft Corporation UEFI CA 2011
Cert #1:
Subject: /C=US/O=Microsoft Corporation/CN=Microsoft Corporation UEFI CA 2011
Issuer : /C=US/O=Microsoft Corporation/CN=Microsoft Corporation Third Party Marketplace Root
```

Option ROMs


Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Boot
CSM [Enabled]
Boot option filter [UEFI and Legacy]
Launch Storage OpROM Policy [Legacy only]
Launch Video OpROM Policy [Legacy only]
PCIE7 Slot OpROM [Legacy]
Select UEFI only to run those that support UEFI option ROM only. Select Legacy only to run those that support legacy option ROM only. Select Do not launch to not execute both legacy and UEFI option ROM.

Secure Boot

Integrita (kontrola hashů)

Autenticita (PKI/certifikáty)

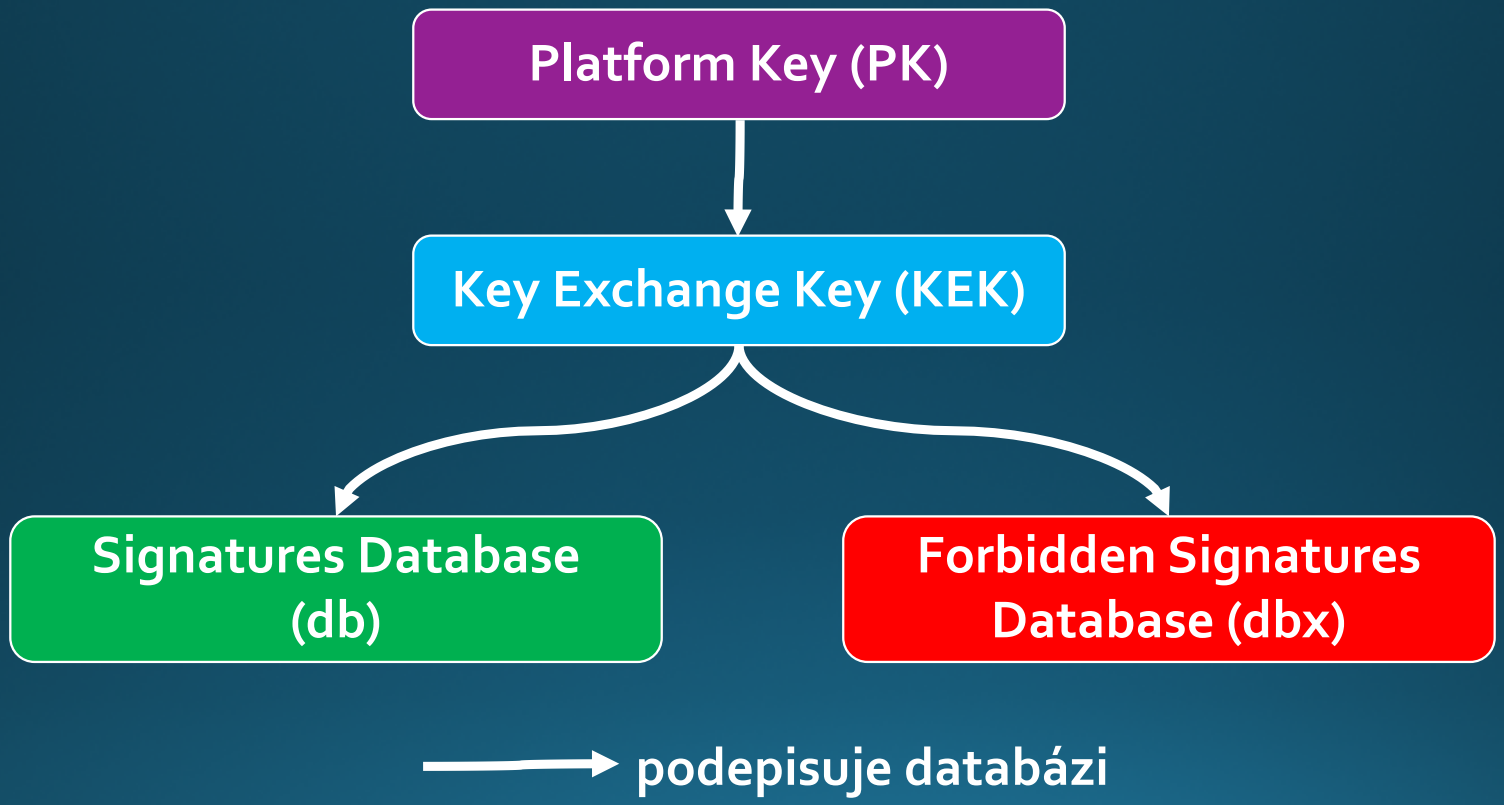
Off

User mode

Setup mode

Sakaki's EFI Install Guide/Configuring Secure Boot

Secure Boot



Sakaki's EFI Install Guide/Configuring Secure Boot

Secure Boot

	PK	KEK	db	dbx
Signatures	✓	✓	✓	✓
Hashes	✗	✗	✓	✓

Sakaki's EFI Install Guide/Configuring Secure Boot

Secure Boot

```
# efi-readvar
Variable PK, length 1395
PK: List 0, type X509
    Signature 0, size 1367, owner 70564dce-9afc-4ee3-85fc-949649d7e45c
        Subject:
            DC=com, DC=dell, OU=1, OU=Signing, CN=Dell Inc. UEFI Platform Key
        Issuer:
            DC=com, DC=dell, CN=Configuration, CN=Services, CN=Public Key Services, CN=AIA,
 CN=Dell Inc. Issuing CA 1

Variable KEK, length 1560
KEK: List 0, type X509
    Signature 0, size 1532, owner 77fa9abd-0359-4d32-bd60-28f4e78f784b
        Subject:
            C=US, O=Microsoft Corporation, CN=Microsoft Corporation KEK CA 2011
        Issuer:
            C=US, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace
 Root
```

Secure Boot

```
Variable db, length 3143
db: List 0, type X509
    Signature 0, size 1515, owner 77fa9abd-0359-4d32-bd60-28f4e78f784b
        Subject:
            C=US, O=Microsoft Corporation, CN=Microsoft Windows Production PCA 2011
        Issuer:
            C=US, O=Microsoft Corporation, CN=Microsoft Root Certificate Authority 2010
db: List 1, type X509
    Signature 0, size 1572, owner 77fa9abd-0359-4d32-bd60-28f4e78f784b
        Subject:
            C=US, O=Microsoft Corporation, CN=Microsoft Corporation UEFI CA 2011
        Issuer:
            C=US, O=Microsoft Corporation, CN=Microsoft Corporation Third Party Marketplace
 Root

Variable dbx, length 5415
dbx: List 0, type X509
    Signature 0, size 1663, owner 00000000-0000-0000-0000-000000000000
        Subject:
            C=US, O=Microsoft Corporation, CN=Microsoft Windows PCA 2010
        Issuer:
            C=US, O=Microsoft Corporation, CN=Microsoft Root Certificate Authority 2010
```

UEFI vs. BIOS

startuje systém v 32/64 bit režimu	1 způsob práce s diskem (LBA)	LBA48	1 způsob detekce velikosti paměti	umí ověřit integritu a autenticitu	Kompletní specifikace API
neomezené množství oddílů na disku	limit 8 ZiB na jeden diskový oddíl	neomezený prostor pro zavaděč systému	zavaděč je běžný soubor, nesquattuje	není nutná emulace při bootu z CD/DVD	USB zařízení nemusí emulovat

Legacy vs. UEFI boot

Legacy boot	UEFI boot
BIOS nabízí bootloaderu jen omezené služby	Aplikace může využívat všech služeb UEFI
Nemůže jednoduše vrátit řízení BIOSu	Může skončit a UEFI pak startuje další app v řadě

Boot z disku

BIOS boot (MBR)

GRUB stage 1 z disku s platným MBR (1. sektor 1. takového disku; 16 bit)

↓

GRUB stage 1.5 z prostoru nikoho (16b)

↓

GRUB stage 2 (16/32/64b) z /boot

↓

čti a bootuj kernel, initrd

UEFI boot (GPT)

Hledej disky s platnou EFI partition a boot items z NVRAM

↓

Spouštěj postupně nalezené aplikace

↓

SHIM: MSFT podepsaný meziloader

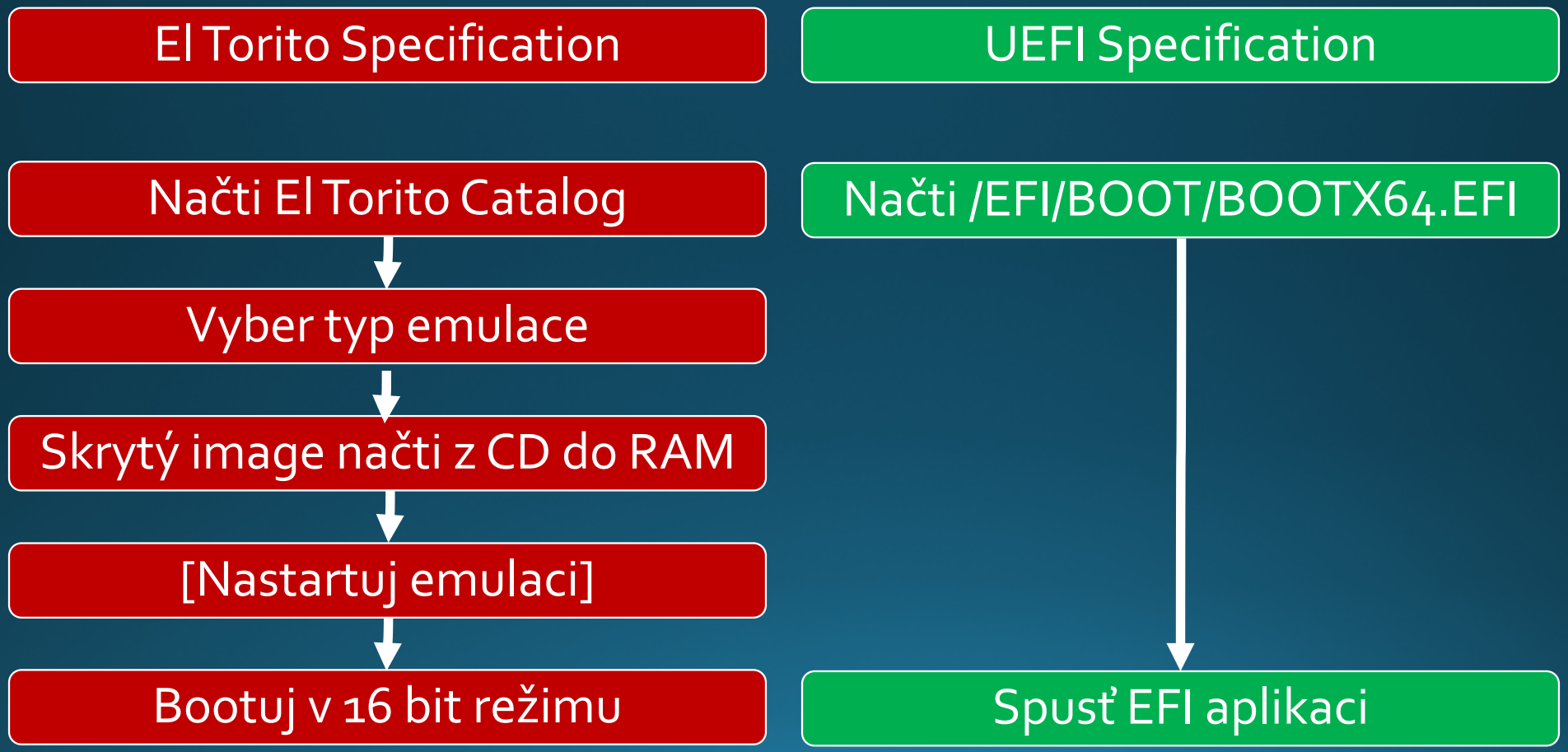
↓

GRUB: podepsaný meziloader

↓

(podepsaný) kernel, initrd

Boot z CD/DVD


El Torito Specification
UEFI Specification
Načti El Torito Catalog
Vyber typ emulace
Skrytý image načti z CD do RAM
[Nastartuj emulaci]
Bootuj v 16 bit režimu
Načti /EFI/BOOT/BOOTX64.EFI
Spusť EFI aplikaci

Boot ze sítě

BIOS	UEFI TFTP	UEFI 2.5+ HTTP
next-server + filename z DHCP(v4)	next-server + filename z DHCP(v4/v6)	HTTP URL („filename“) z DHCP(v4/v6)
↓	↓	↓
načti pxelinux.0 z TFTP	načti BOOTX64.EFI z TFTP	načti BOOTX64.EFI z HTTP (☹)
↓	↓	↓
Bootuj v 16b režimu	Spusť EFI aplikaci	Spusť EFI aplikaci

https://github.com/tianocore/tianocore.github.io/wiki/Configuring-PXE-Boot-Servers-for-UEFI

PE32+

GPT

NVRAM

EFI Partition

Option ROM

Alternativní boot loadery

EFISTUB

---

eLILO ☠

rEFIt ☠

PE32+

GPT

NVRAM

EFI Partition

Option ROM

Bootloader

Linux a EFISTUB

```
00000000  4d 5a ea 07 00 c0 07 8c  c8 8e d8 8e c0 8e d0 31  |MZ.............1|
00000010  e4 fb fc be 40 00 ac 20  c0 74 09 b4 0e bb 07 00  |....@.. .t......|
00000020  cd 10 eb f2 31 c0 cd 16  cd 19 ea f0 ff 00 f0 00  |....1...........|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 82 00 00 00  |................|
00000040  55 73 65 20 61 20 62 6f  6f 74 20 6c 6f 61 64 65  |Use a boot loade|
00000050  72 2e 0d 0a 0a 52 65 6d  6f 76 65 20 64 69 73 6b  |r....Remove disk|
00000060  20 61 6e 64 20 70 72 65  73 73 20 61 6e 79 20 6b  | and press any k|
00000070  65 79 20 74 6f 20 72 65  62 6f 6f 74 2e 2e 2e 0d  |ey to reboot....|
00000080  0a 00 50 45 00 00 64 86  04 00 00 00 00 00 00 00  |..PE..d.........|
```

```
# readpe --header coff --header optional /boot/vmlinuz-4.15.0-36-generic
COFF/File header
    Machine:                    0x8664 IMAGE_FILE_MACHINE_AMD64
    Characteristics names       IMAGE_FILE_EXECUTABLE_IMAGE
                                IMAGE_FILE_LINE_NUMS_STRIPPED
                                IMAGE_FILE_DEBUG_STRIPPED
Optional/Image header
    Magic number:               0x20b (PE32+)
    Subsystem required:         0xa (IMAGE_SUBSYSTEM_EFI_APPLICATION)
```

Linux a EFISTUB

```
# osslsigncode verify /boot/vmlinuz-4.15.0-36-generic
Signature verification: ok

Number of signers: 1
    Signer #0:
        Subject: /C=GB/ST=Isle of Man/O=Canonical Ltd./
            OU=Secure Boot/CN=Canonical Ltd. Secure Boot Signing
        Issuer : /C=GB/ST=Isle of Man/L=Douglas/O=Canonical Ltd./
            CN=Canonical Ltd. Master Certificate Authority

Number of certificates: 1
    Cert #0:
        Subject: /C=GB/ST=Isle of Man/O=Canonical Ltd./
            OU=Secure Boot/CN=Canonical Ltd. Secure Boot Signing
        Issuer : /C=GB/ST=Isle of Man/L=Douglas/O=Canonical Ltd./
            CN=Canonical Ltd. Master Certificate Authority
```

EFI Shell

```
EFI Shell version 2.00 [4096.1]
Current running mode 1.1.2
Device mapping table
  fs0     :Removable HardDisk - Alias hd52g0b blk0
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)/HD(Part1,Sig90909090)
  blk0    :Removable HardDisk - Alias hd52g0b fs0
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)/HD(Part1,Sig90909090)
  blk1    :HardDisk - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part1,SigD5BAE38B)
  blk2    :HardDisk - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part2,SigD5BAE38B)
  blk3    :BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)
  blk4    :BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Secondary,Master)
  blk5    :Removable BlockDevice - Alias (null)
           Acpi(PNP0A03,0)/Pci(1D|7)/Usb(6,0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> _
```

PE32+

GPT

NVRAM

EFI Partition

Option ROM

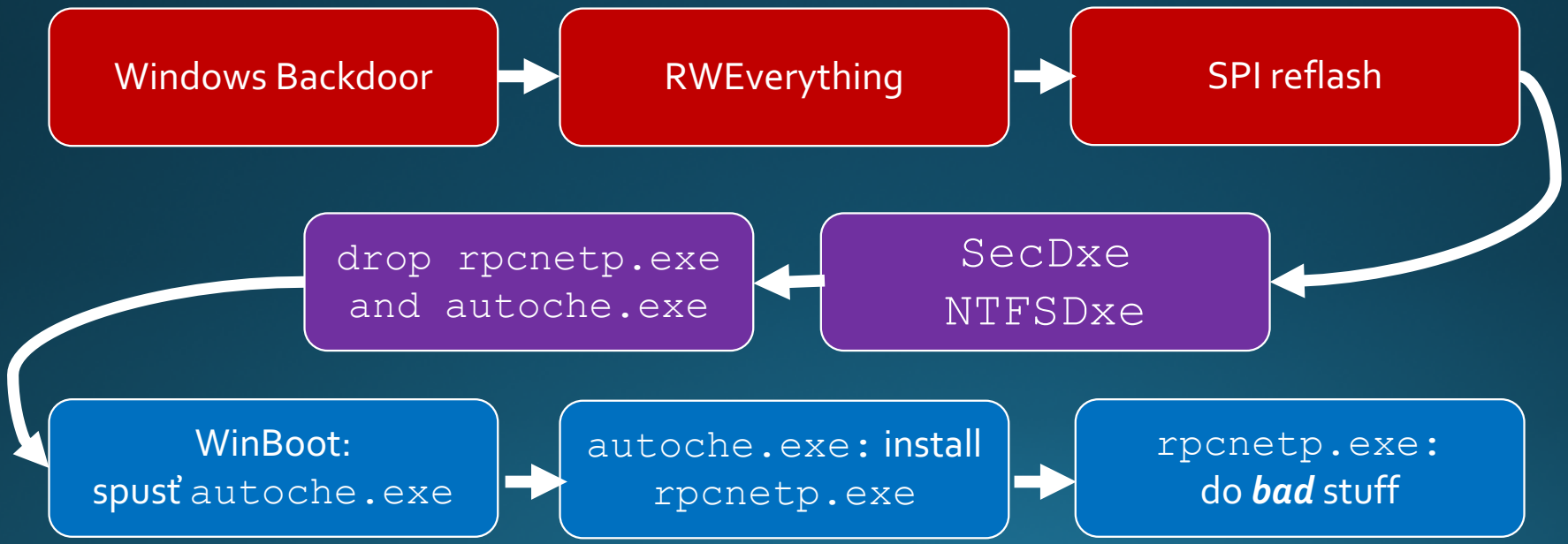
Bootloader

Kernel

DEMO

LoJax

ESET analyzoval LoJax, jeden z prvních škodlivých kódů, který infikuje UEFI. Útočí na evropské vládní instituce



https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

Security…?

CVE-2014-8273	Intel BIOS locking mechanism contains race condition that enables write protectionbypass
CVE-2017-3197	GIGABYTE UEFI does not securely implement BIOSWE, BLE, SMM_BWP, and PRx features.
CVE-2017-3775	Some Lenovo System x do not properly authenticate signed code before booting it. As a result, an attacker with physical access to the system could boot unsigned code.
CVE-2017-3198	GIGABYTE UEFI does not cryptographically validate images prior to updating the system firmware. Additionally, the firmware updates are served over HTTP.
CVE-2016-8222	A signed driver (LenovoDeviceGuardDxe) for the BIOS of some ThinkPad systems that can allow an attacker with Windows administrator-level privileges to call System Management Mode (SMM) services
CVE-2017-5721	Insufficient input validation in system firmware for Intel NUC allows local attackers to execute arbitrary code via manipulation of memory.

Embedi: UEFI BIOS holes. So Much Magic. Don't Come Inside.

Moduly načtené z SPI FLASH při aktivním SecureBootu neprochází kontrolou integrity/podpisů

atd.

EFI Byte Code

Proč nechtít UEFI?

SWRAID 1

non-EFI OptionROM

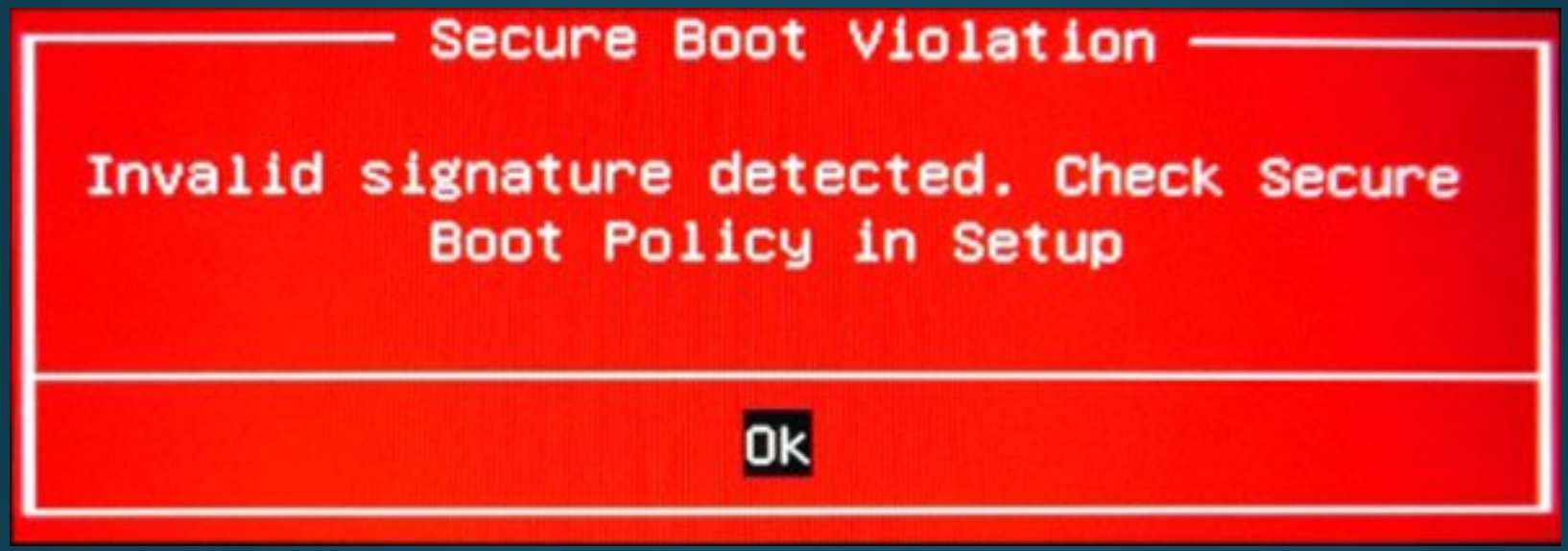
poškozená NVRAM

bugy v implementaci

Referenční implementace

https://www.tianocore.org/

Secure Boot Violation
Invalid signature detected. Check Secure Boot Policy in Setup
Ok



Díky za pozornost a dobrou chuť!

@zajdee • radek@zajic.v.pytli.cz

Hello, EFI World!

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

EFI_STATUS
EFIAPI
efi_main (EFI_HANDLE ImageHandle, EFI_SYSTEM_TABLE *SystemTable) {
   InitializeLib(ImageHandle, SystemTable);
   Print(L"Hello, EFI world!\n");

   return EFI_SUCCESS;
}
```

https://www.rodsbooks.com/efi-programming/hello.html

decompress.py

```
#!/usr/bin/env python
import argparse
import EfiCompressor

def decompress_efi_rom(pe_img):
    pe_img = EfiCompressor.UefiDecompress(pe_img, len(pe_img))[:]
    return pe_img

if __name__ == "__main__":
   parser = argparse.ArgumentParser()
   parser.add_argument('infile', type=argparse.FileType('rb'))
   parser.add_argument('outfile', type=argparse.FileType('wc'))
   args = parser.parse_args()
   o = args.outfile
   i = args.infile.read()
   o.write(decompress_efi_rom(i))
   o.close()
   args.infile.close()
```