black hat®
USA 2017

BETRAYING THE BIOS:

WHERE THE GUARDIANS OF THE BIOS ARE FAILING

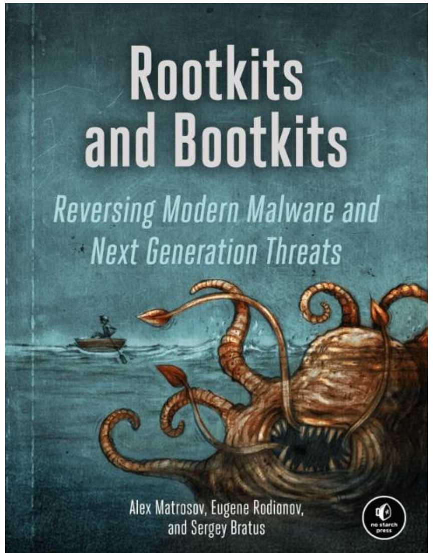
Alex Matrosov
@matrosov

Have a lot of fun with UEFI Security and RE at CYLANCE

Former Security Researcher @Intel

Reverse Engineering since 1997

Book co-author nostarch.com/rootkits



Rootkits and Bootkits

Reversing Modern Malware and Next Generation Threats

Alex Matrosov, Eugene Rodionov, and Sergey Bratus

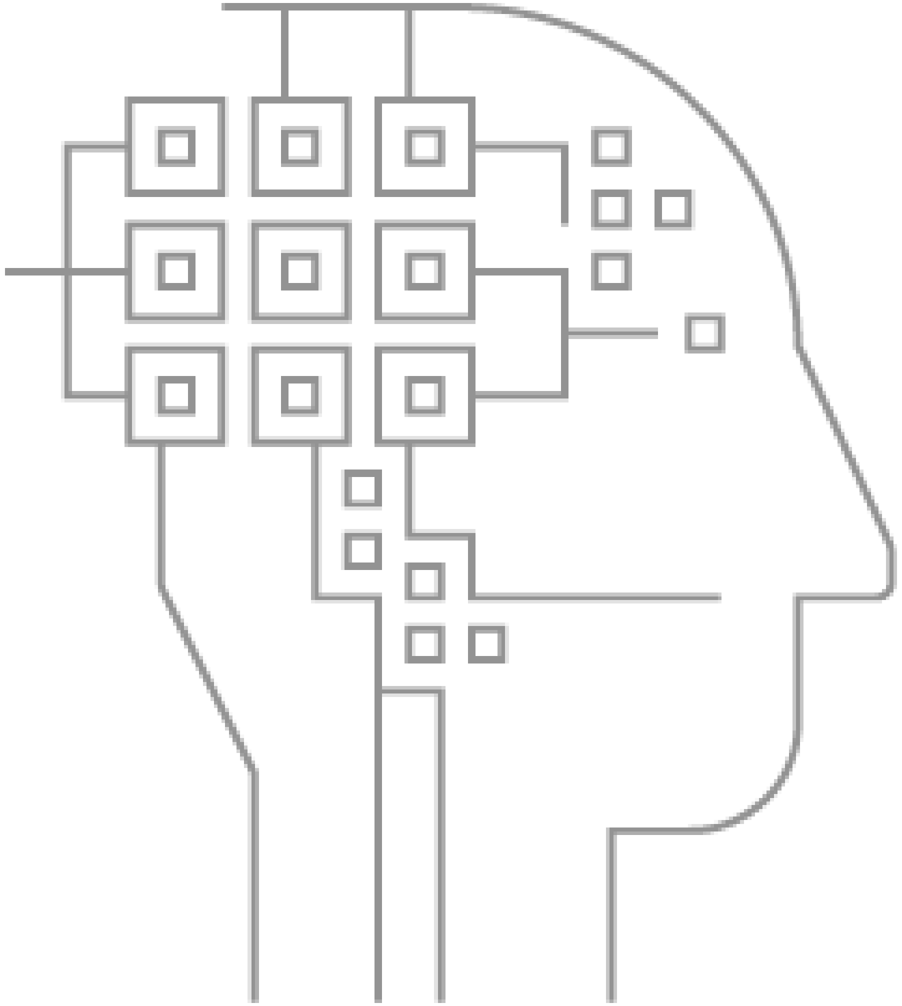
@matrosov

- **Intro**

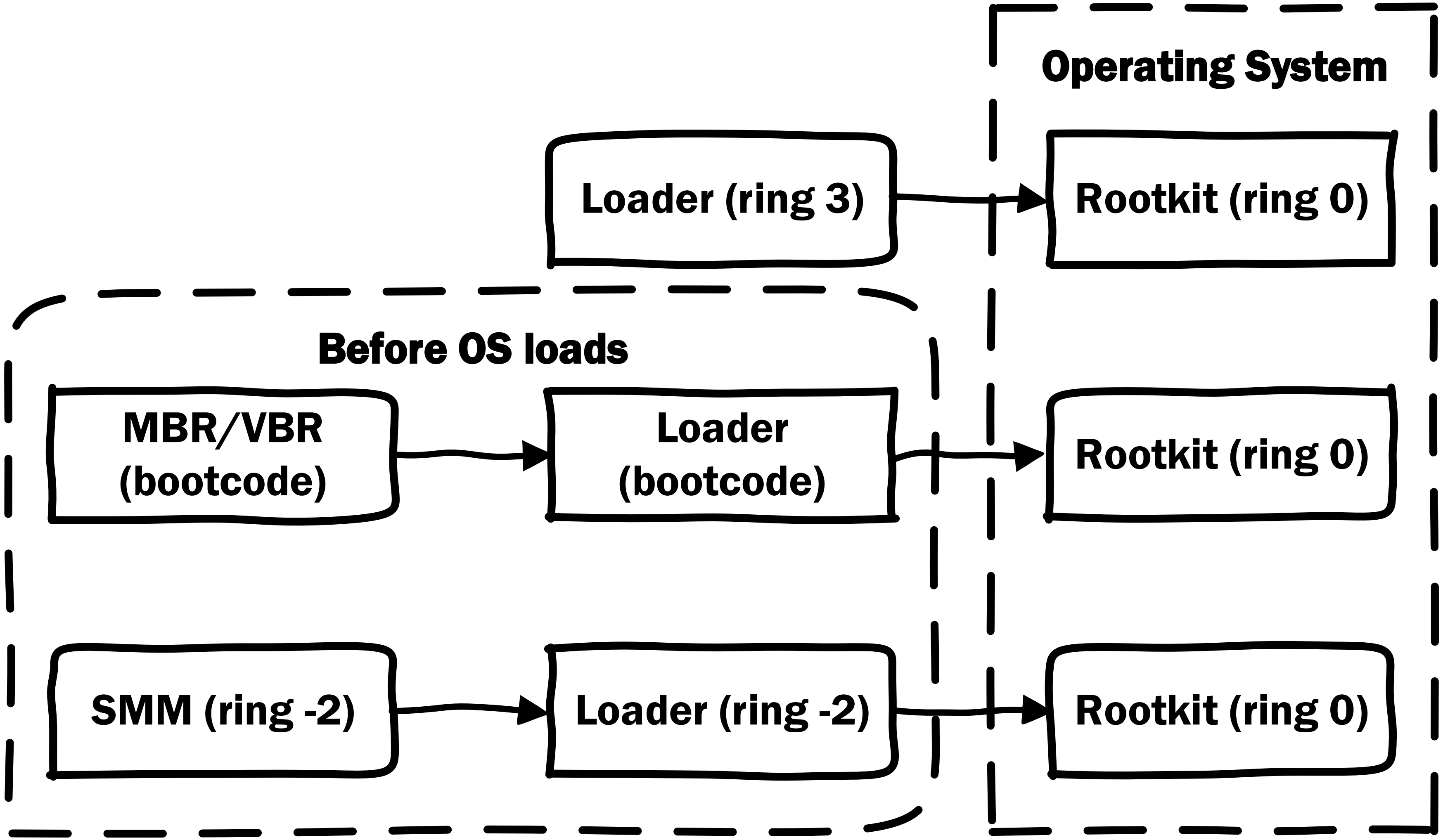
- **Attacks on BIOS Updates**
  - ✓ Unsigned Updates
  - ✓ BIOS protection bits
  - ✓ SmiFlash and SecSmiFlash

- **Intel Boot Guard**
  - ✓ AMI implementation details
  - ✓ Discover ACM secrets
  - ✓ Vulns
  - ✓ Boot Guard Bypass!

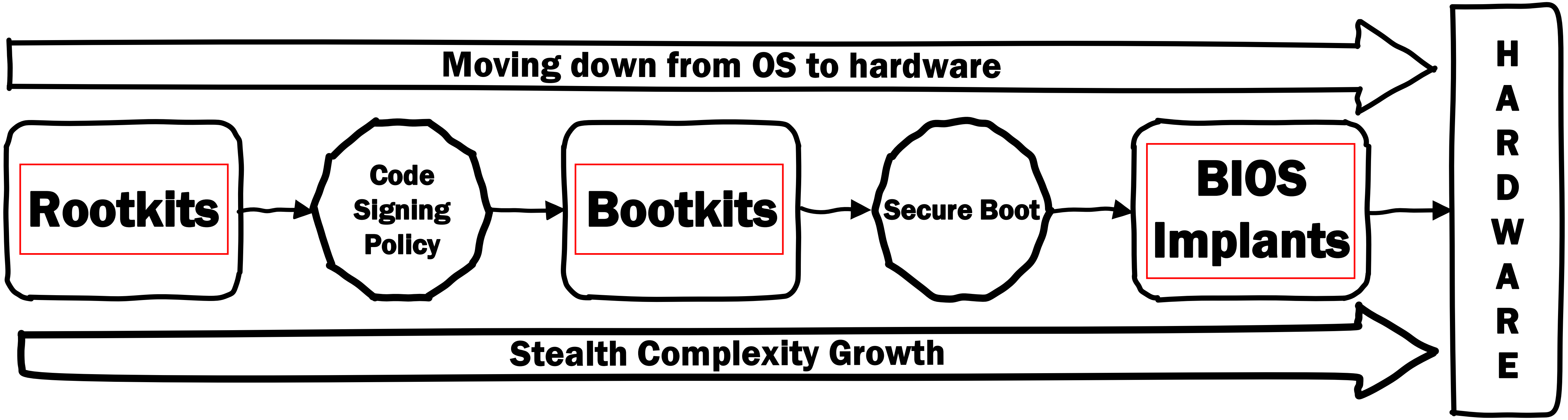
- **Intel BIOS Guard**
  - ✓ AMI implementation details



All rootkits want to get into Ring 0



More mitigations, more rootkits complexity



Moving down from OS to hardware

Rootkits

Code Signing Policy

Bootkits

Secure Boot

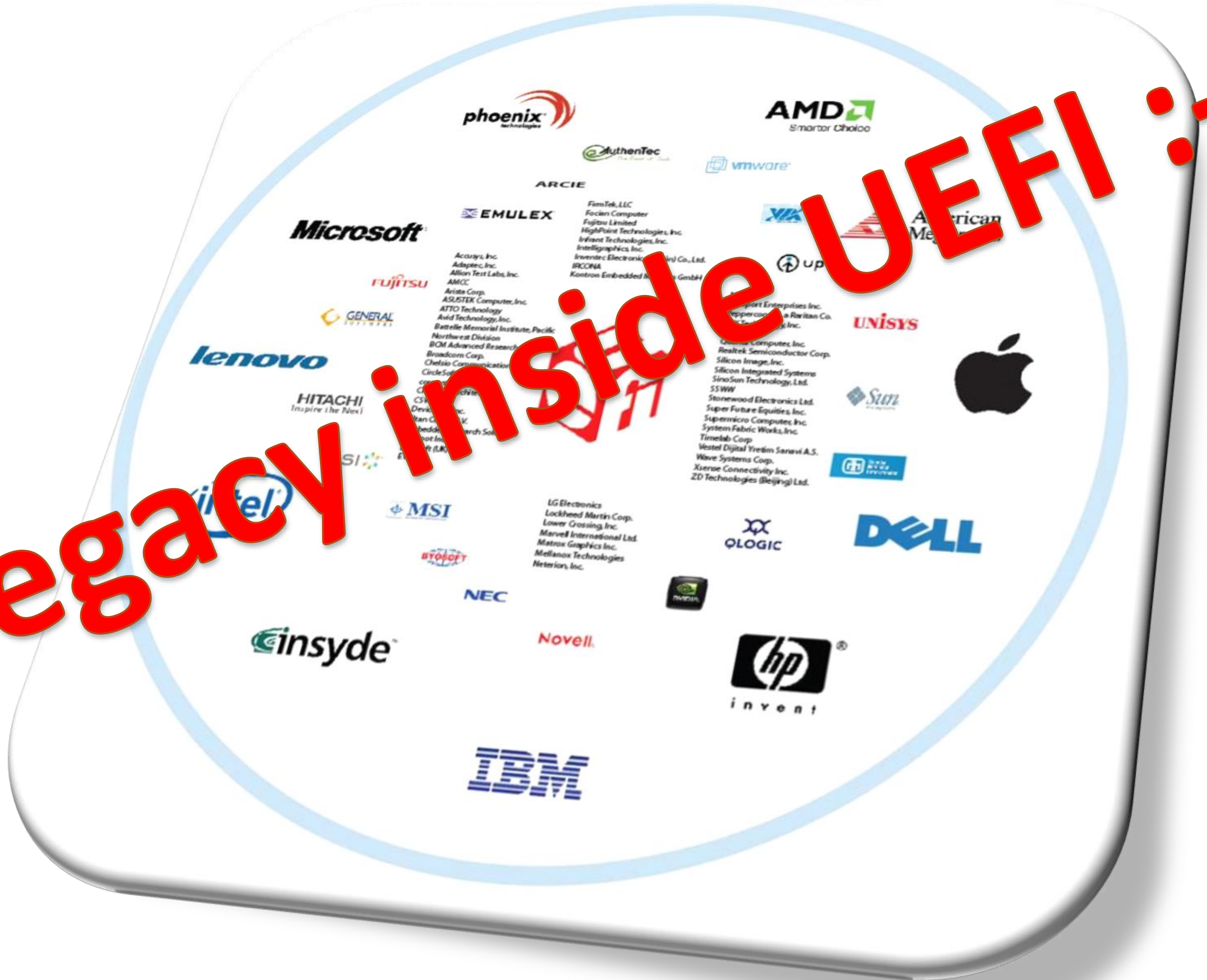
BIOS Implants

HARDWARE

Stealth Complexity Growth

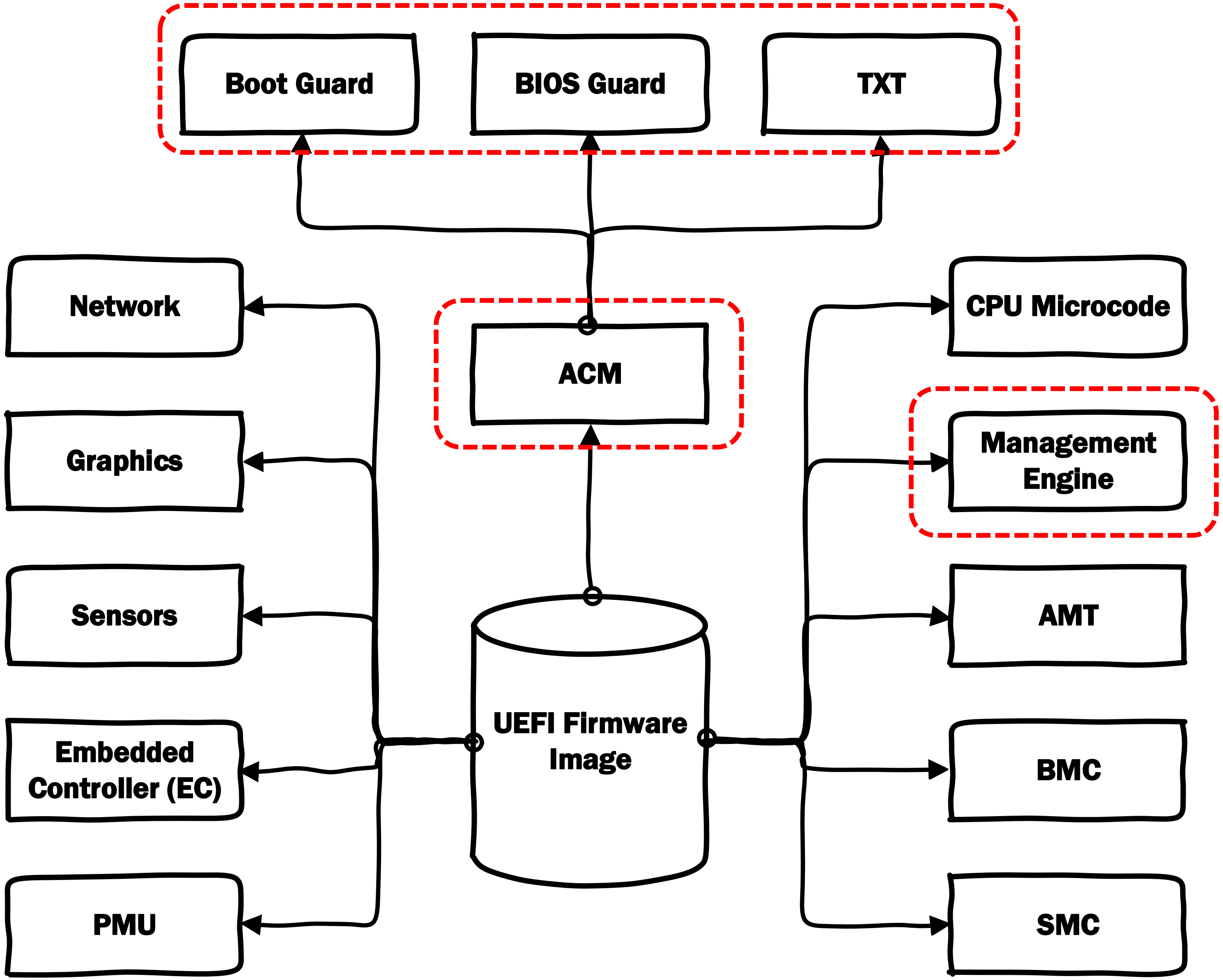
BIOS Update Issues

No more legacy! UEFI is everywhere!!



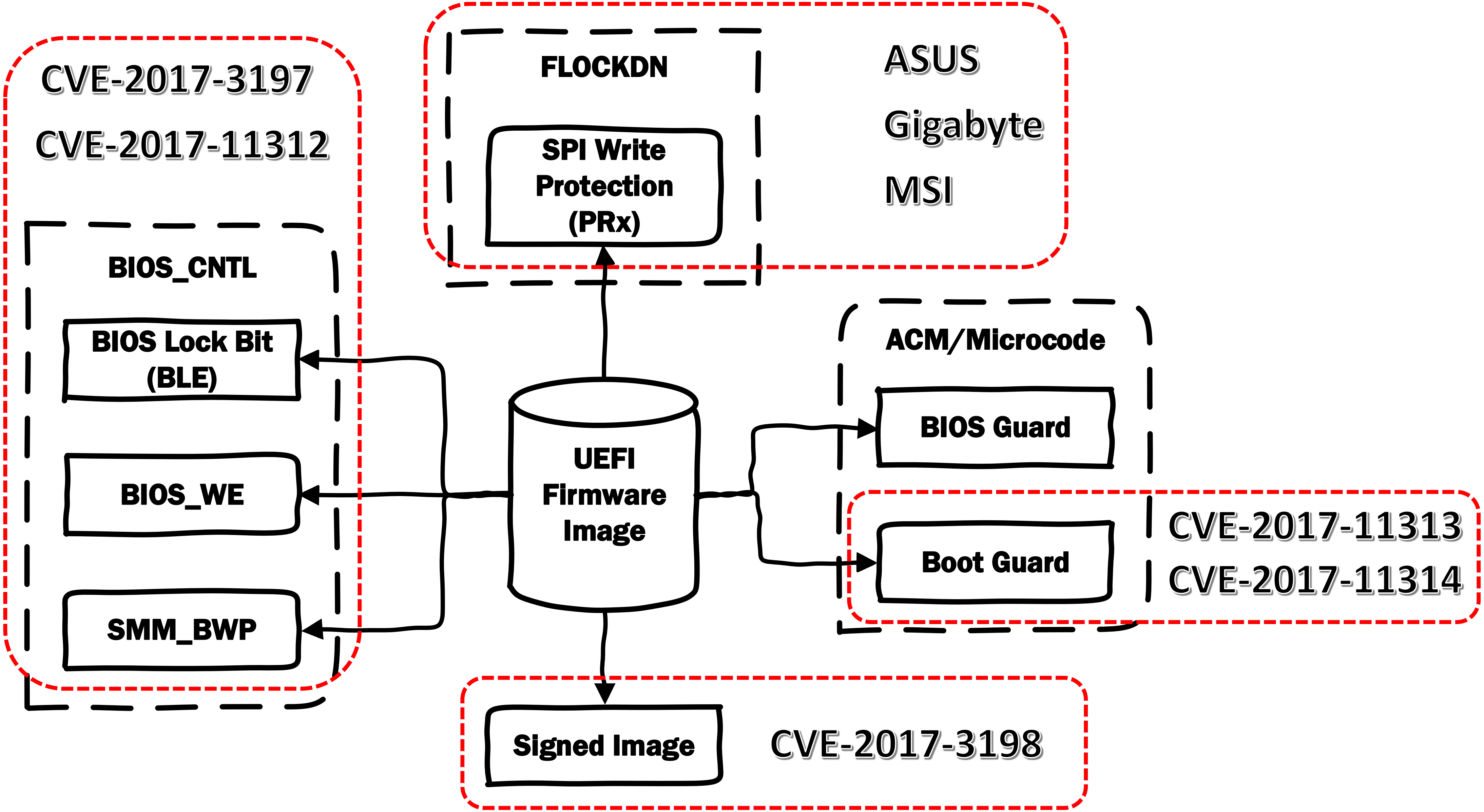
Now the legacy inside UEFI :-)

How many different firmware's inside BIOS update?



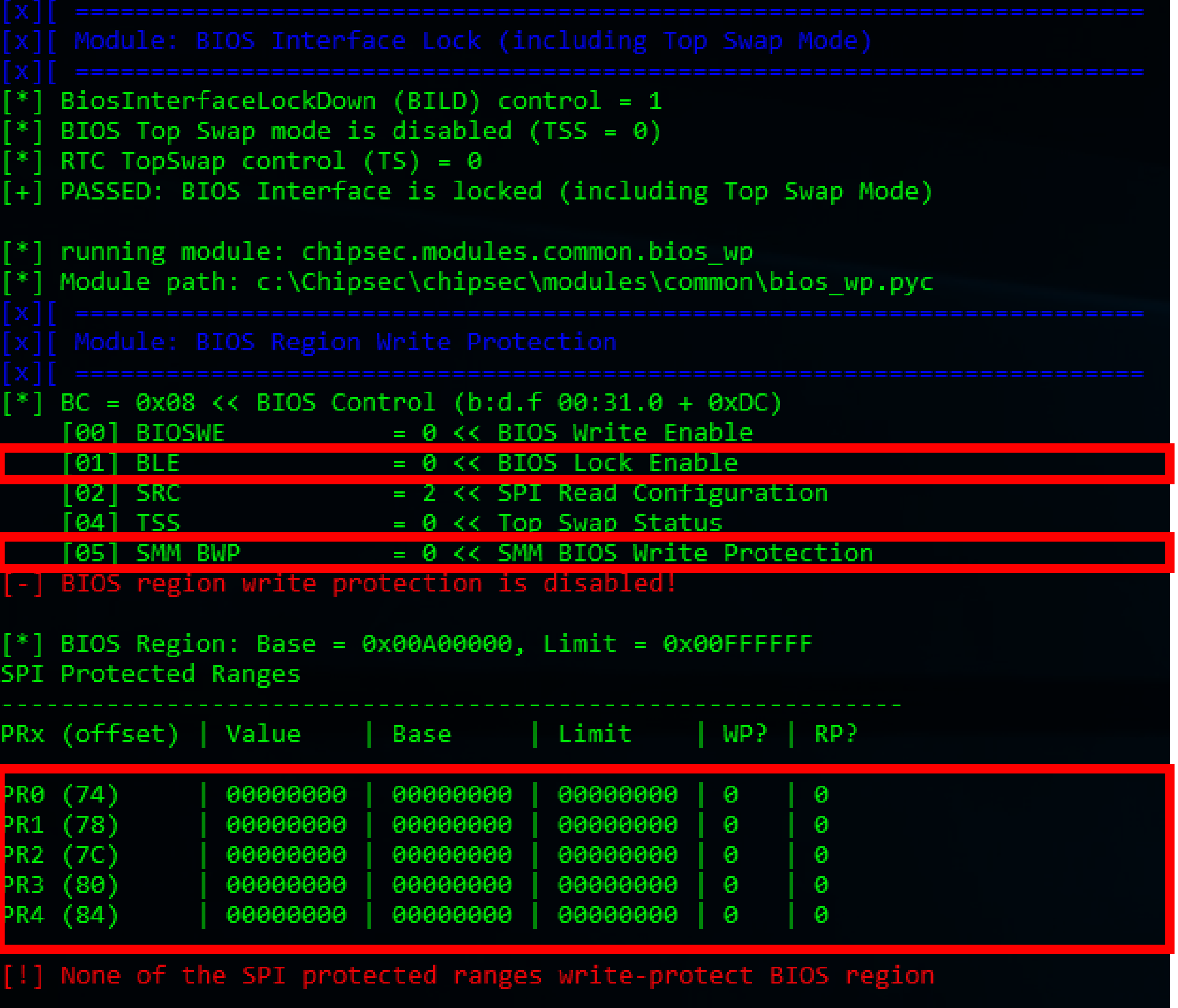
All the vulnerabilities mention in this research found inside AMI-based UEFI firmware's

All Guardians of the BIOS on one slide

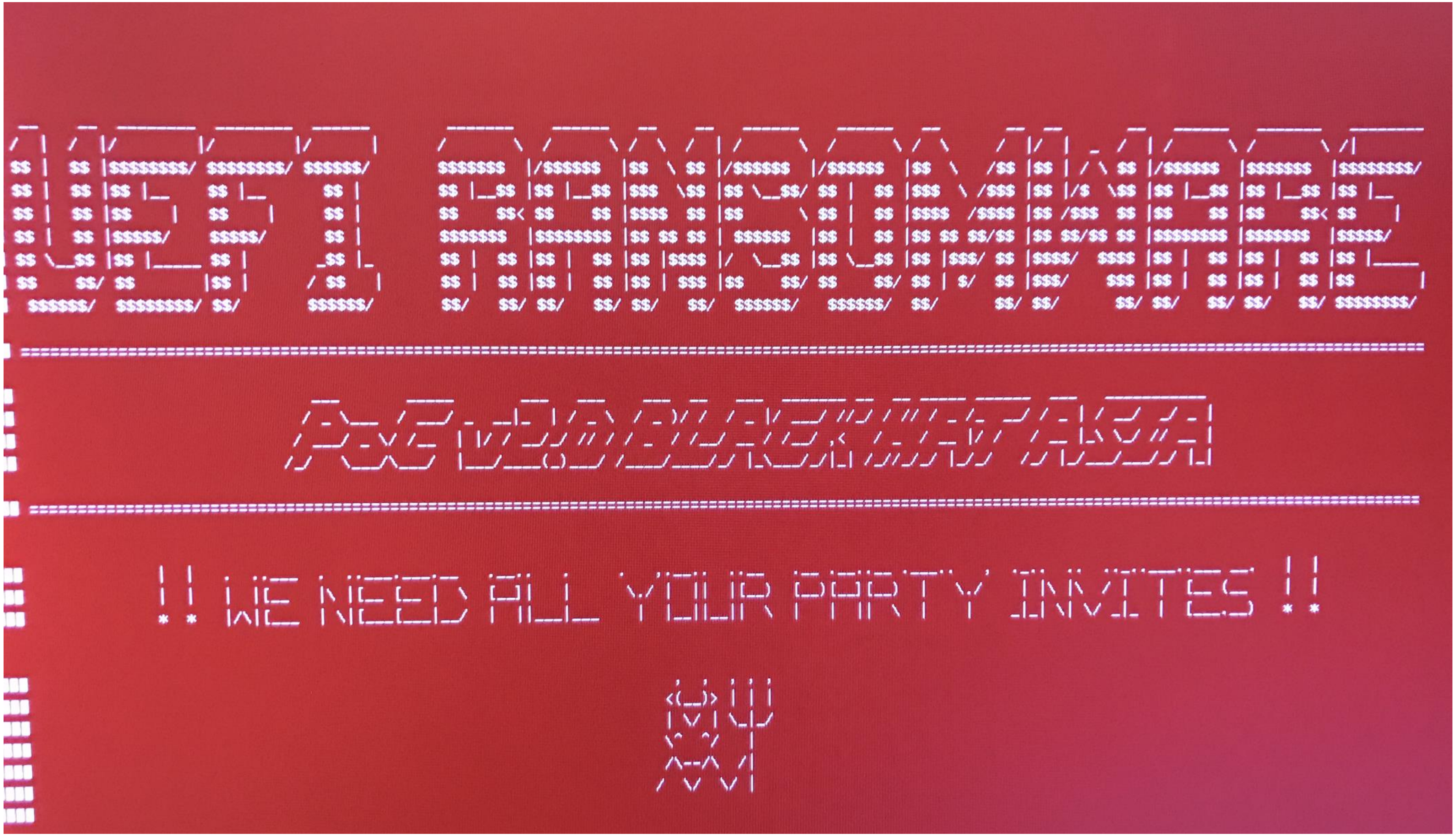


How different vendors care about security?

Vendor Name	BLE	SMM_BWP	PRx	Authenticated Update
ASUS	+	+	-	-
MSI	-	-	-	-
Gigabyte	+	+	-	-
Dell	+	+	-+	+
Lenovo	+	+	RP	+
HP	+	+	RP/WP	+
Intel	+	+	-	+
Apple	-	-	WP	+



```
[x][ =======================================================================
[x][ Module: BIOS Interface Lock (including Top Swap Mode)
[x][ =======================================================================
[*] BiosInterfaceLockDown (BILD) control = 1
[*] BIOS Top Swap mode is disabled (TSS = 0)
[*] RTC TopSwap control (TS) = 0
[+] PASSED: BIOS Interface is locked (including Top Swap Mode)

[*] running module: chipsec.modules.common.bios_wp
[*] Module path: c:\Chipsec\chipsec\modules\common\bios_wp.pyc
[x][ =======================================================================
[x][ Module: BIOS Region Write Protection
[x][ =======================================================================
[*] BC = 0x08 << BIOS Control (b:d.f 00:31.0 + 0xDC)
    [00] BIOSWE           = 0 << BIOS Write Enable
    [01] BLE              = 0 << BIOS Lock Enable
    [02] SRC              = 2 << SPI Read Configuration
    [04] TSS              = 0 << Top Swap Status
    [05] SMM_BWP          = 0 << SMM BIOS Write Protection
[-] BIOS region write protection is disabled!

[*] BIOS Region: Base = 0x00A00000, Limit = 0x00FFFFFF
SPI Protected Ranges
------------------------------------------------------------
PRx (offset) | Value    | Base     | Limit    | WP? | RP?

PR0 (74)     | 00000000 | 00000000 | 00000000 | 0   | 0
PR1 (78)     | 00000000 | 00000000 | 00000000 | 0   | 0
PR2 (7C)     | 00000000 | 00000000 | 00000000 | 0   | 0
PR3 (80)     | 00000000 | 00000000 | 00000000 | 0   | 0
PR4 (84)     | 00000000 | 00000000 | 00000000 | 0   | 0

[!] None of the SPI protected ranges write-protect BIOS region
```



UEFI RANSOMWARE

PoC v2.0 BLACKHAT ASIA

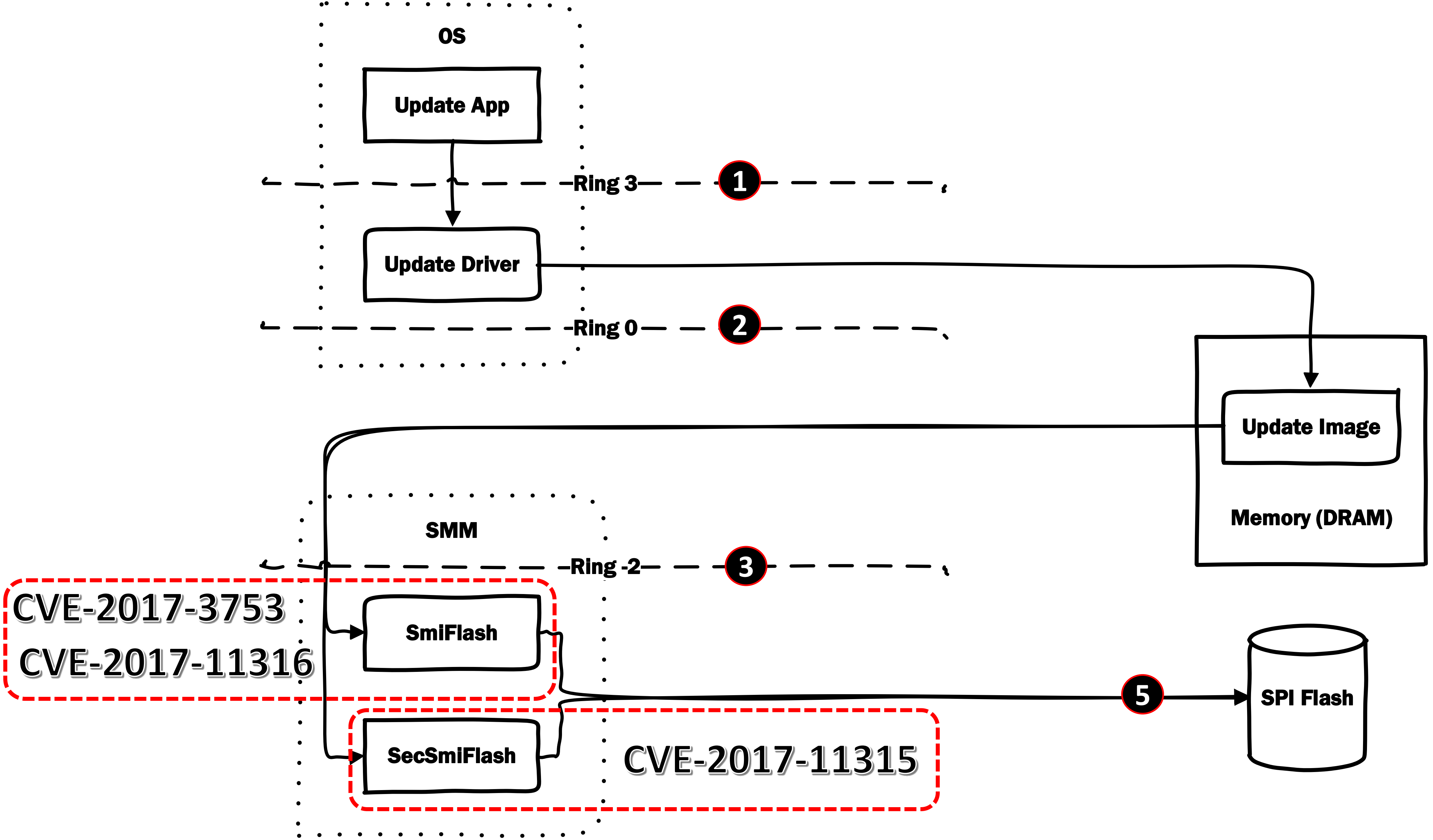
!! WE NEED ALL YOUR PARTY INVITES !!

blackhat.com/docs/asia-17/materials/asia-17-Matrosov-The-UEFI-Firmware-Rootkits-Myths-And-Reality.pdf

Why so vulnerable?

- ➢ BIOS LOCK (BLE) not enabled (CLVA-2016-12-001/CVE-2017-3197)
  - ✓ Attacker is able to modify BIOSWE bit
  - ✓ Attacker can arbitrary write to SPI flash from OS
- ➢ FW update process don’t verify signature
  - ✓ Attacker is able to abuse BIOS updater with signed driver
- ➢ SmiFlash Handler multiple vulns (CLVA-2016-12-002/CVE-2017-3198)
  - ✓ Attacker can elevate privileges to SMM (ring -2)

How BIOS Update Guardians Fail?



SMIFlash Handler Issues: Gigabyte, Lenovo, MSI

➢ SmiFlash HANDLERS (SMiFlash.efi)→ CVE-2017-3753, CVE-2017-11316

[BC327DBD-B982-4f55-9F79-056AD7E987C5]

✓ ENABLE	0x20
✓ READ	0x21
✓ ERASE	0x22
✓ WRITE	0x23
✓ DISABLE	0x24
✓ GET_INFO	0x25

➢ No checks for the input pointers

SmmIsBufferOutsideSmmValid()

SecSMIFlash Handler Issues: ASUS

- SecSmiFlash HANDLERS (SecSMiFlash.efi) → CVE-2017-11315

[3370A4BD-8C23-4565-A2A2-065FEEDE6080]

✓ LOAD_IMAGE	0x1d
✓ GET_POLICY	0x1e
✓ SET_POLICY	0x1f

- No checks for the input pointers
  SmmIsBufferOutsideSmmValid()

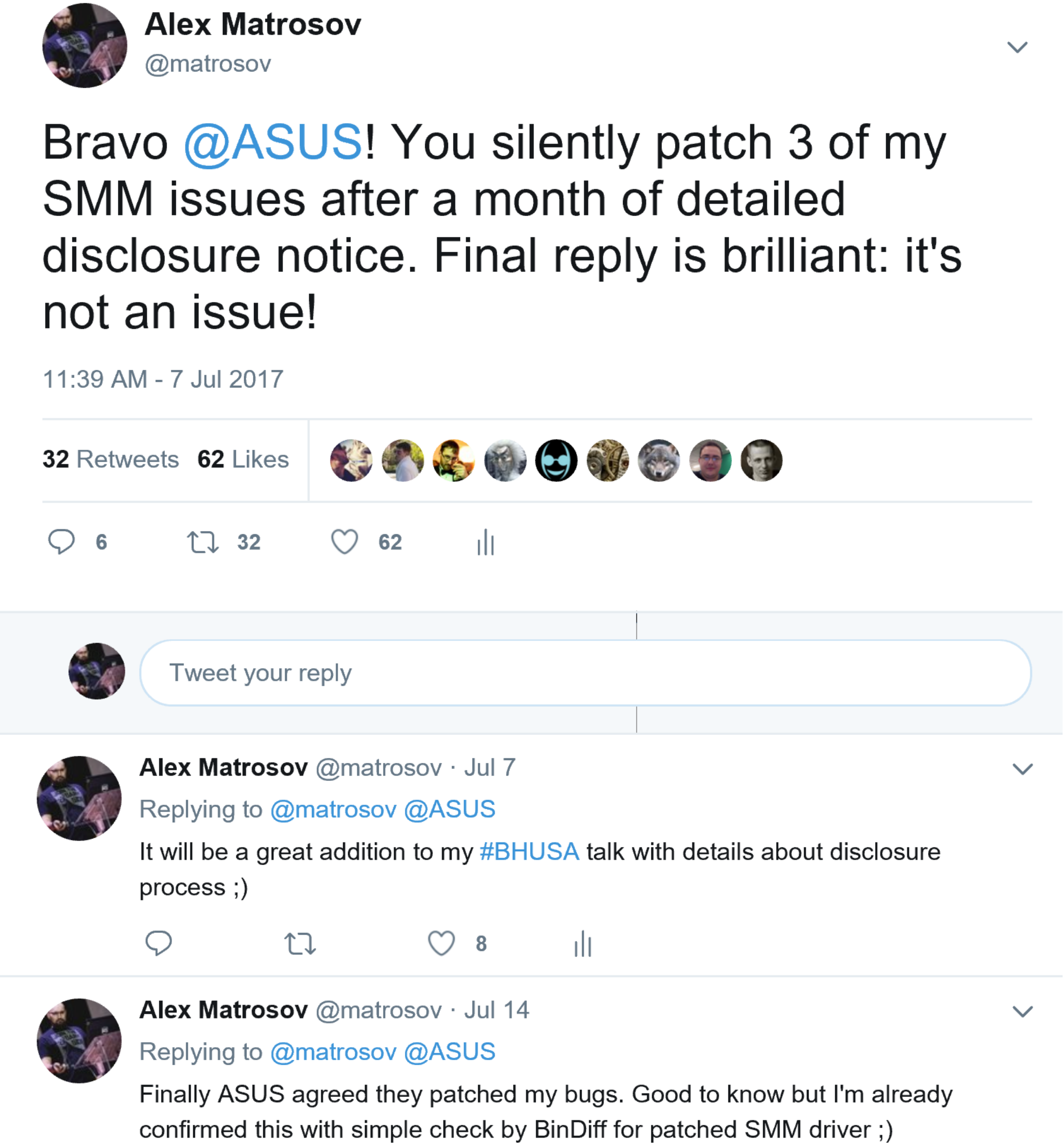
That's why BIOS Guard created

Responsible Disclosure Fun

- ✓ Discovery Date: 2017-04-20
- ✓ Intel PSIRT Notified: 2017-05-22
- ✓ All the Vendors Notified: 2017-05-26
- ✓ Disclosure Notification Date: 2017-05-30
- ✓ Lenovo Released a Patch: 2017-07-11
- ✓ ASUS Released a Patch: 2017-06-23
- ✓ MITRE Assign 6 CVE’s: 2017-07-13
- ✓ Gigabyte Released a Patch: 2017-07-25
- ✓ Public Disclosure Date: 2017-07-27

https://github.com/CylanceVulnResearch/disclosures

ASUS Responsible Disclosure Fun



Alex Matrosov
@matrosov

Bravo @ASUS! You silently patch 3 of my SMM issues after a month of detailed disclosure notice. Final reply is brilliant: it's not an issue!

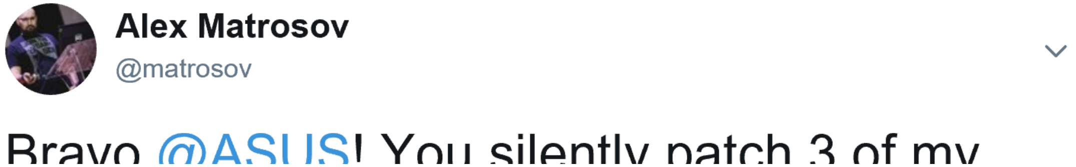
11:39 AM - 7 Jul 2017

32 Retweets **62** Likes

Alex Matrosov @matrosov · Jul 7
Replying to @matrosov @ASUS
It will be a great addition to my #BHUSA talk with details about disclosure process ;)

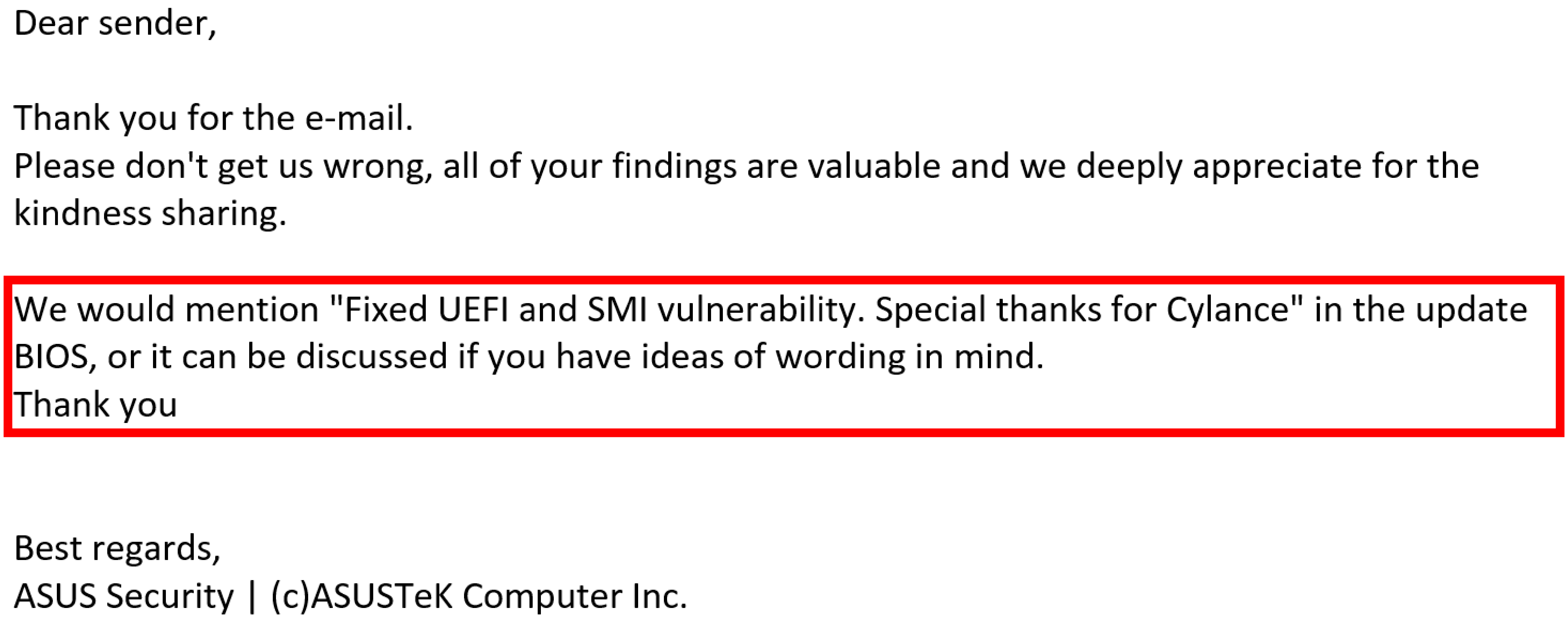
Alex Matrosov @matrosov · Jul 14
Replying to @matrosov @ASUS
Finally ASUS agreed they patched my bugs. Good to know but I'm already confirmed this with simple check by BinDiff for patched SMM driver ;)

ASUS Responsible Disclosure Fun



Alex Matrosov
@matrosov

Bravo @ASUS! You silently patch 3 of my

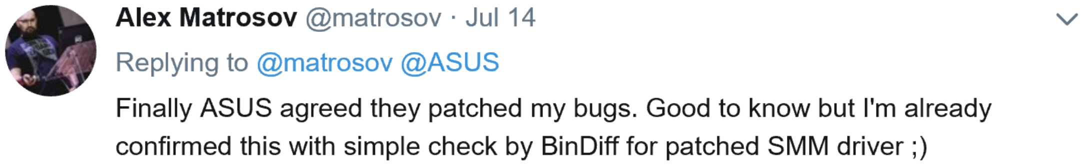


Dear sender,

Thank you for the e-mail.
Please don't get us wrong, all of your findings are valuable and we deeply appreciate for the kindness sharing.

We would mention "Fixed UEFI and SMI vulnerability. Special thanks for Cylance" in the update BIOS, or it can be discussed if you have ideas of wording in mind.
Thank you

Best regards,
ASUS Security | (c)ASUSTeK Computer Inc.



Alex Matrosov @matrosov · Jul 14
Replying to @matrosov @ASUS
Finally ASUS agreed they patched my bugs. Good to know but I'm already confirmed this with simple check by BinDiff for patched SMM driver ;)

Intel Boot Guard

Different shades of Secure Boot

- **Secure Boot -> since 2012**
  - ✓ Root of Trust = Firmware -> BIOS
  - ✓ Attack Surface = Firmware

- **Measured Boot (Boot Guard) -> since 2013**
  - ✓ Root of Trust = Hardware -> Trusted Platform Module (TPM)
  - ✓ Attack Surface = Firmware

- **Verified Boot (Boot Guard) -> since 2013**
  - ✓ Root of Trust = Hardware -> Field Programming Fuse (FPF)->Locked
  - ✓ Attack Surface = Firmware + Hardware

Different shades of Secure Boot

- ➢ Secure Boot -> since 2012
  - ✓ Root of Trust = Firmware -> BIOS
  - ✓ Attack Surface = Firmware

- ➢ Measured Boot (Boot Guard) -> since 2013
  - ✓ Root of Trust = Hardware -> Trusted Platform Module (TPM)
  - ✓ Attack Surface = Firmware

- ➢ Verified Boot (Boot Guard) -> since 2013
  - ✓ Root of Trust = Hardware -> Field Programming Fuse (FPF)->Locked
  - ✓ Attack Surface = Firmware + Hardware

First bypass today?!

Why Boot Guard has been created?

- **Secure Boot** starts from DXE phase and impacted with any SMM issues/implants

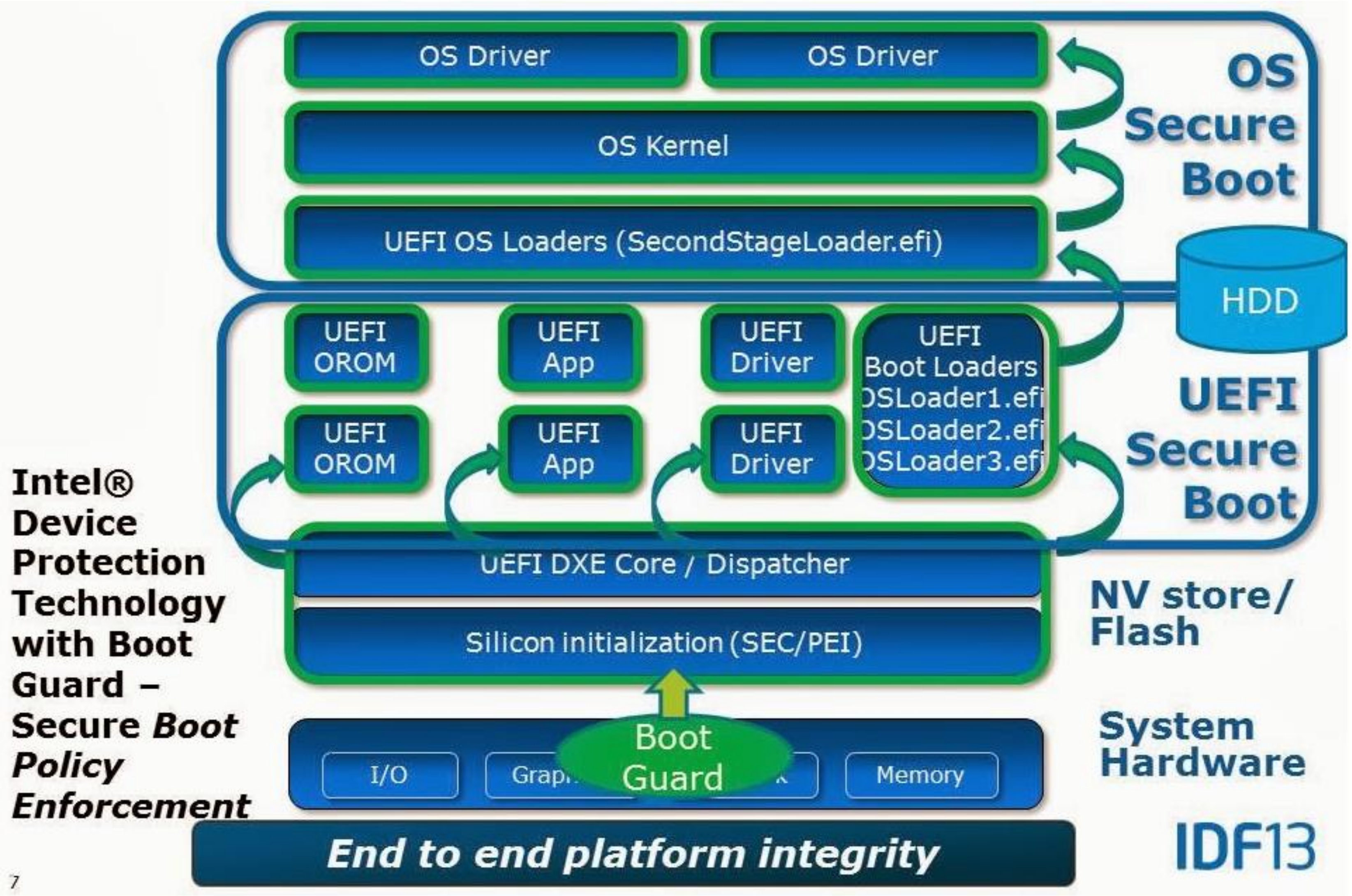
- No verification on early boot for SEC/PEI boot phases

- **Measured Boot** starts before PEI phase but also impacted with any SMM issues/implants

- The Root of Trust must be locked by hardware (**Verified Boot**)

- The first step of verification should rely on microcode authentication

Intel Boot Guard Technology



OS Driver

OS Driver

OS Kernel

UEFI OS Loaders (SecondStageLoader.efi)

OS Secure Boot

HDD

UEFI OROM

UEFI App

UEFI Driver

UEFI Boot Loaders
OSLoader1.efi
OSLoader2.efi
OSLoader3.efi

UEFI OROM

UEFI App

UEFI Driver

UEFI Secure Boot

UEFI DXE Core / Dispatcher

Silicon initialization (SEC/PEI)

NV store/ Flash

Boot Guard

I/O

Grap…

Memory

System Hardware

Intel® Device Protection Technology with Boot Guard – Secure *Boot Policy Enforcement*

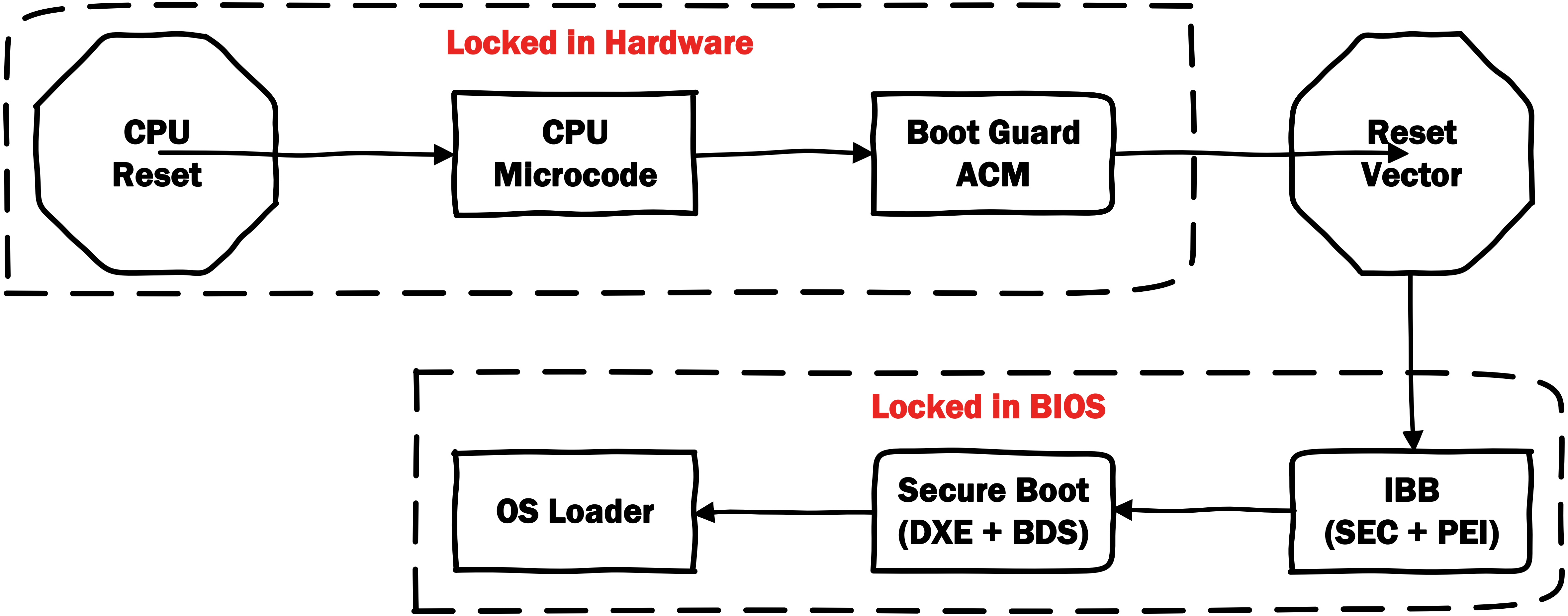
End to end platform integrity

IDF13

7

http://vzimmer.blogspot.com/2013/09/where-do-i-sign-up.html

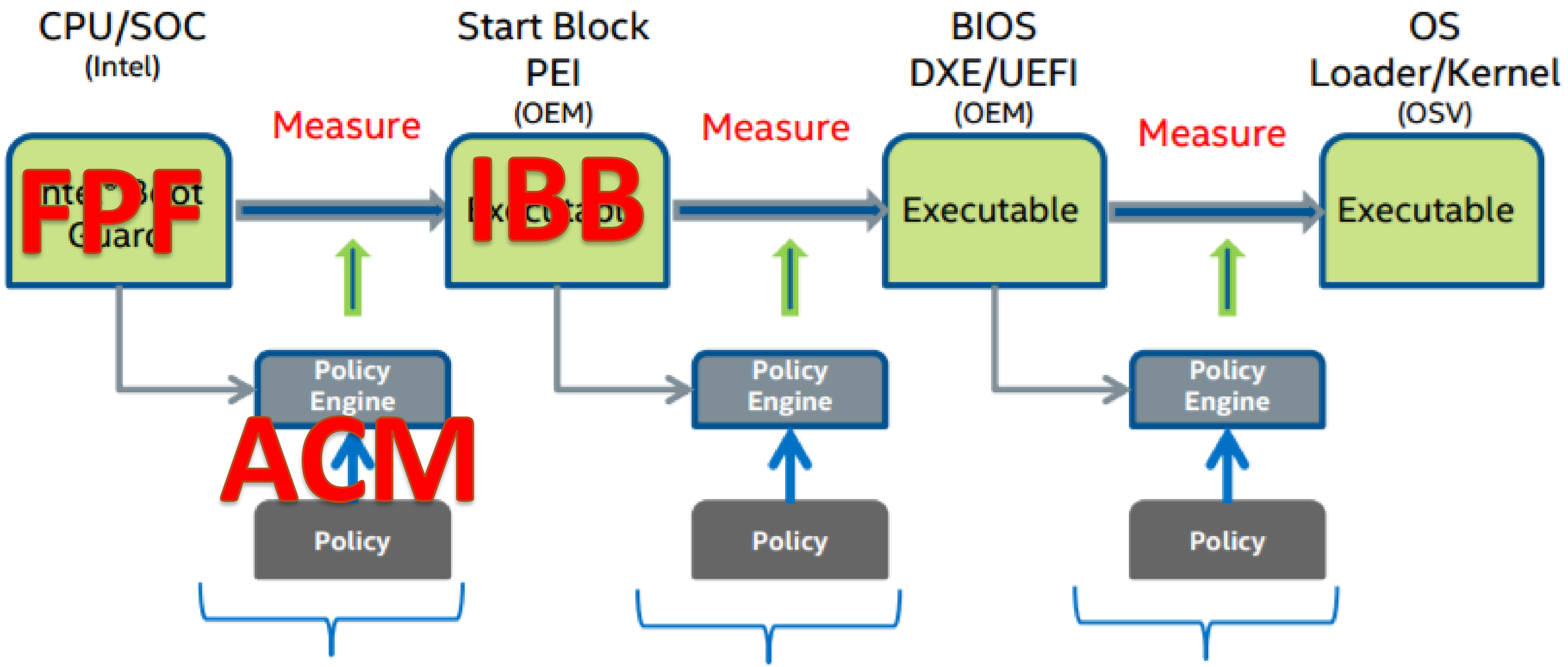
Boot Guard: Boot Flow



Intel Boot Guard operating modes

- Not Enabled
- Measured Boot (root of trust = TPM)
- Verified Boot (root of trust = FPF)
- Measured + Verified Boot (root of trust = FPF + TPM)

Demystifying Intel Boot Guard



Intel® Device Protection Technology with Boot Guard

http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/4th-gen-core-family-mobile-brief.pdf

OEM PI Verification Using PI Signed Firmware Volumes

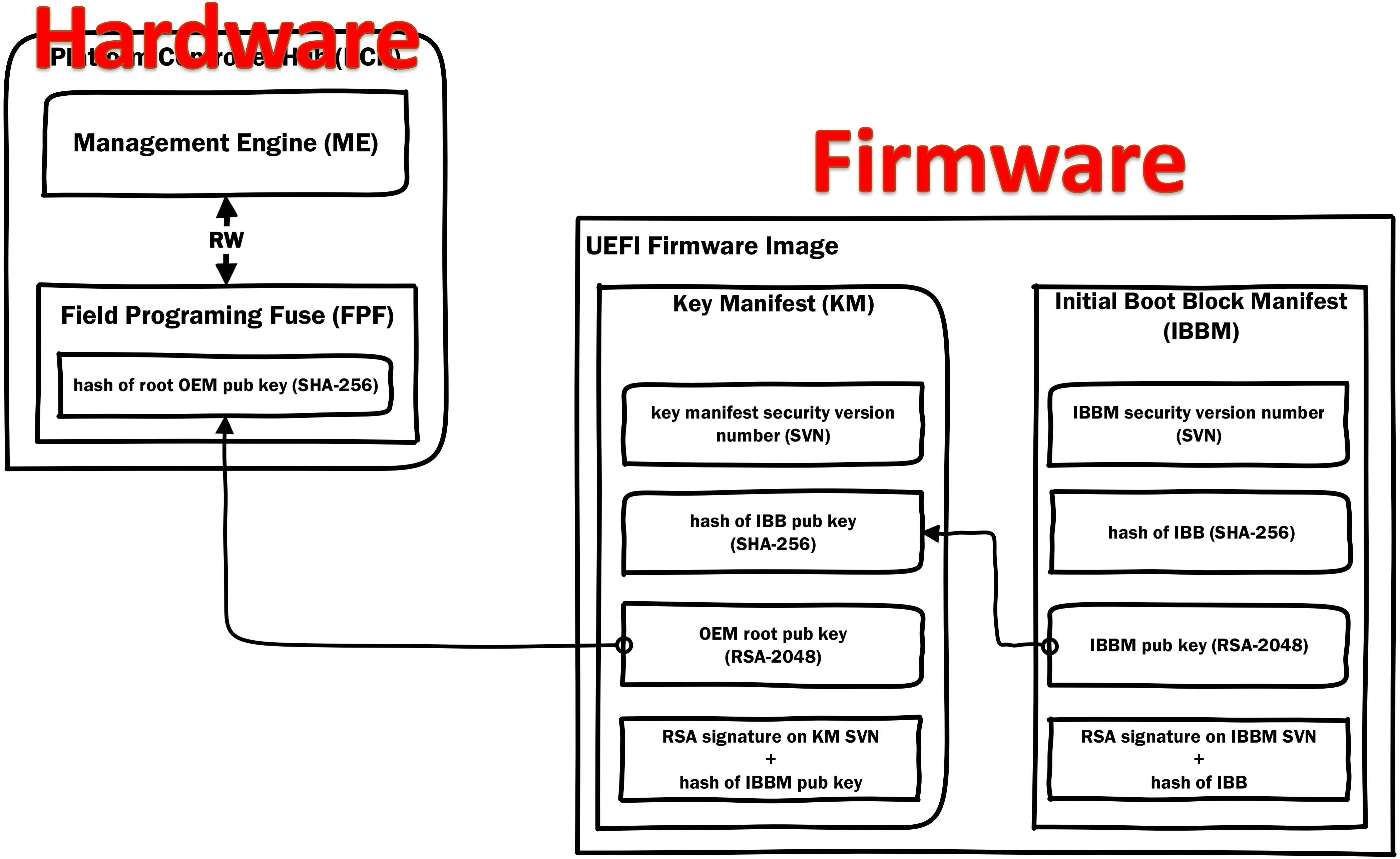
Vol 3, section 3.2.1.1 of PI 1.3 Specification

OEM UEFI 2.4 Secure Boot

Chapter 27.2 of The UEFI 2.4 Specification

https://firmware.intel.com/sites/default/files/STTS003%20-%20SF15_STTS003_100f.pdf

Boot Guard: Chain of Trust



Hardware

Platform Controller Hub (PCH)

Management Engine (ME)

RW

Field Programing Fuse (FPF)

hash of root OEM pub key (SHA-256)

Firmware

UEFI Firmware Image

Key Manifest (KM)

key manifest security version number (SVN)

hash of IBB pub key (SHA-256)

OEM root pub key (RSA-2048)

RSA signature on KM SVN
+
hash of IBBM pub key

Initial Boot Block Manifest (IBBM)

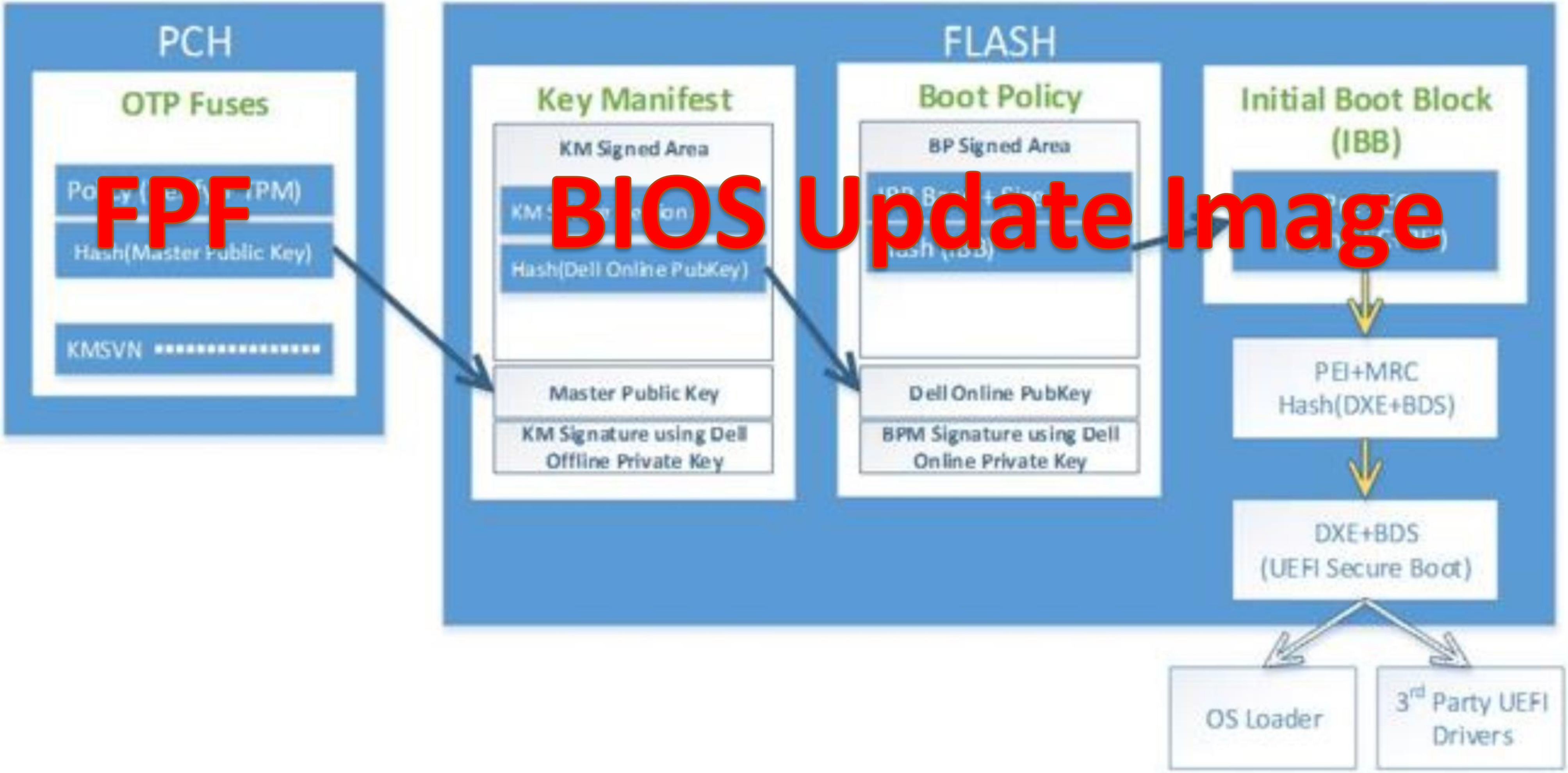
IBBM security version number (SVN)

hash of IBB (SHA-256)

IBBM pub key (RSA-2048)

RSA signature on IBBM SVN
+
hash of IBB

Demystifying Intel Boot Guard



http://en.community.dell.com/techcenter/extras/m/white_papers/20444061

Guard’s Configuration of Tested Hardware

Vendor Name	ME Access	EC Access	CPU Debugging (DCI)	Boot Guard	Forced Boot Guard ACM	Boot Guard FPF	BIOS Guard
ASUS VivoMini	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
MSI Cubi2	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Gigabyte Brix	Read/Write Enabled	Read/Write Enabled	Enabled	Measured Verified	Enabled (FPF not set)	Not Set	Disabled
Dell	Disabled	Disabled	Enabled	Measured Verified	Enabled	Enabled	Enabled
Lenovo ThinkCentre	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
HP Elitedesk	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Intel NUC	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled
Apple	Read Enabled	Disabled	Disabled	Not Supported	Not Supported	Not Supported	Not Supported

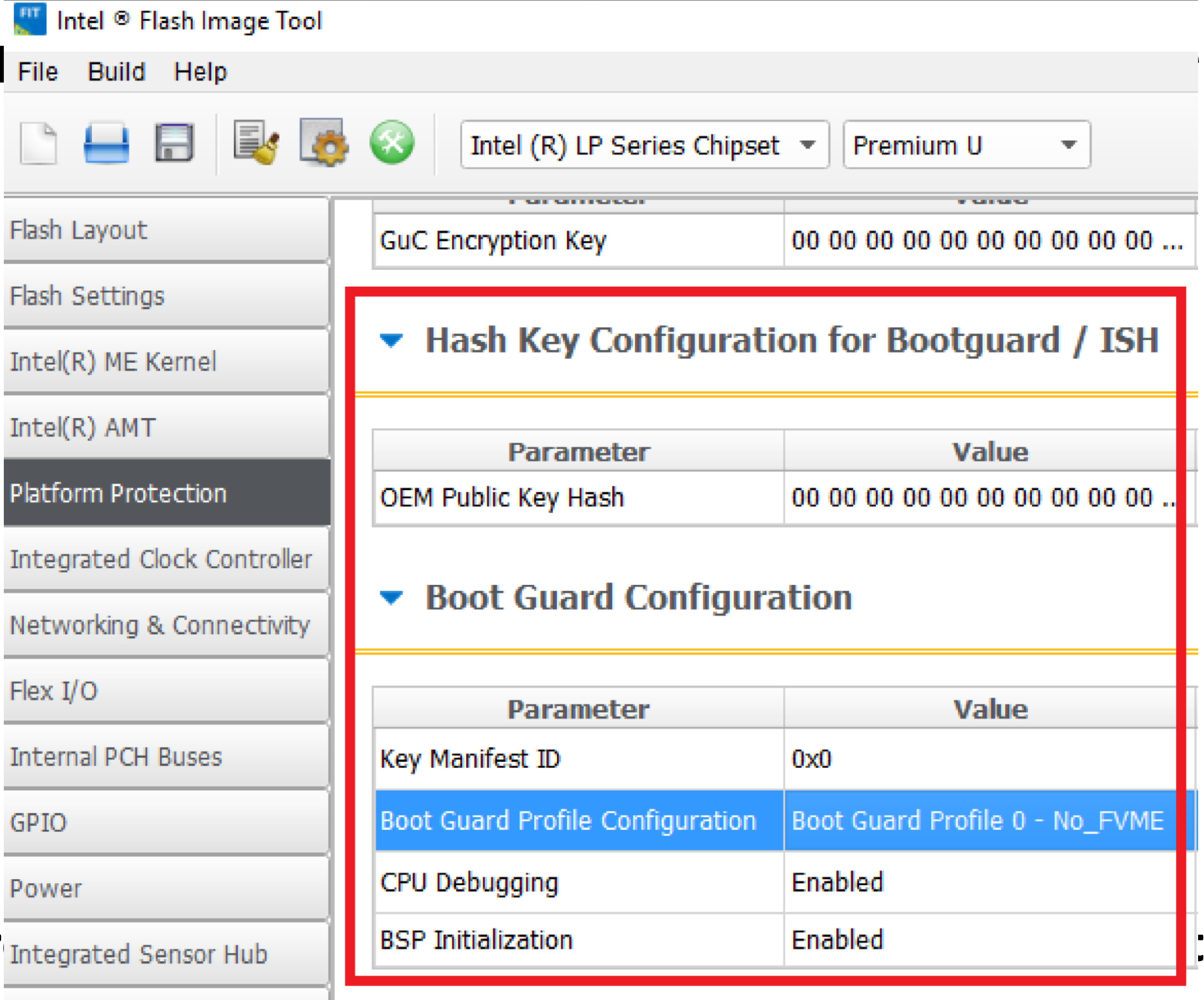
TRUST
NO
ONE

Safeguarding Rootkits: Intel BootGuard

by Alex Ermolov

2016.zeronights.ru/wp-content/uploads/2017/03/Intel-BootGuard.pdf

Safegu d



Parameter	Value
GuC Encryption Key	00 00 00 00 00 00 00 00 00 00 ...

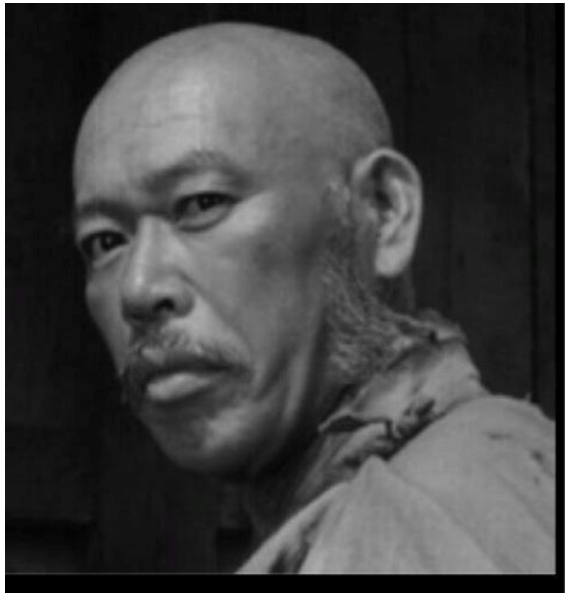
Hash Key Configuration for Bootguard / ISH

Parameter	Value
OEM Public Key Hash	00 00 00 00 00 00 00 00 00 00 ..

Boot Guard Configuration

Parameter	Value
Key Manifest ID	0x0
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME
CPU Debugging	Enabled
BSP Initialization	Enabled

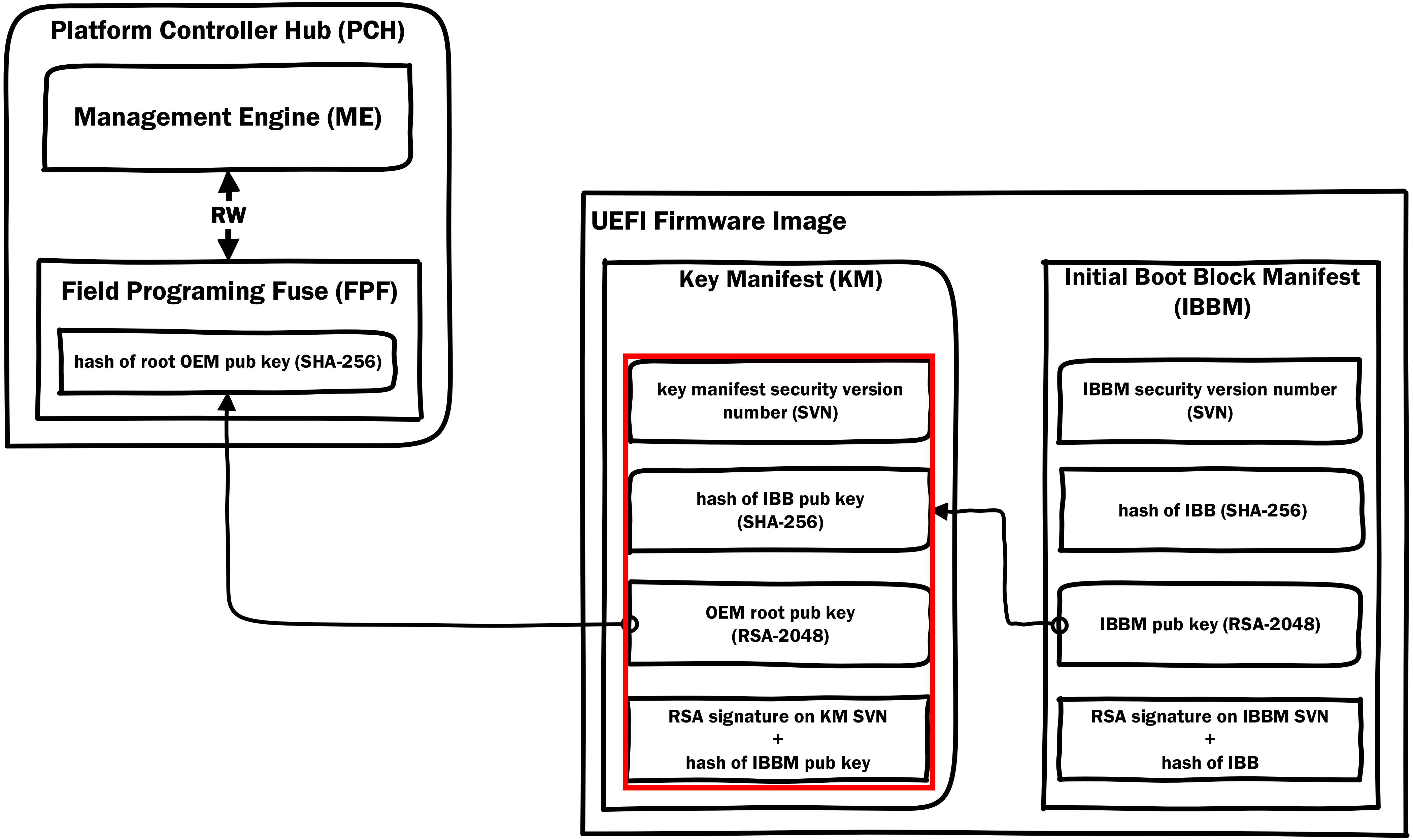
2016.zer :Guard.pdf



You never attack the standard, you attack the implementation, including the process

Grugq

Boot Guard: Chain of Trust



Platform Controller Hub (PCH)

Management Engine (ME)

RW

Field Programing Fuse (FPF)

hash of root OEM pub key (SHA-256)

UEFI Firmware Image

Key Manifest (KM)

key manifest security version number (SVN)

hash of IBB pub key (SHA-256)

OEM root pub key (RSA-2048)

RSA signature on KM SVN + hash of IBBM pub key

Initial Boot Block Manifest (IBBM)

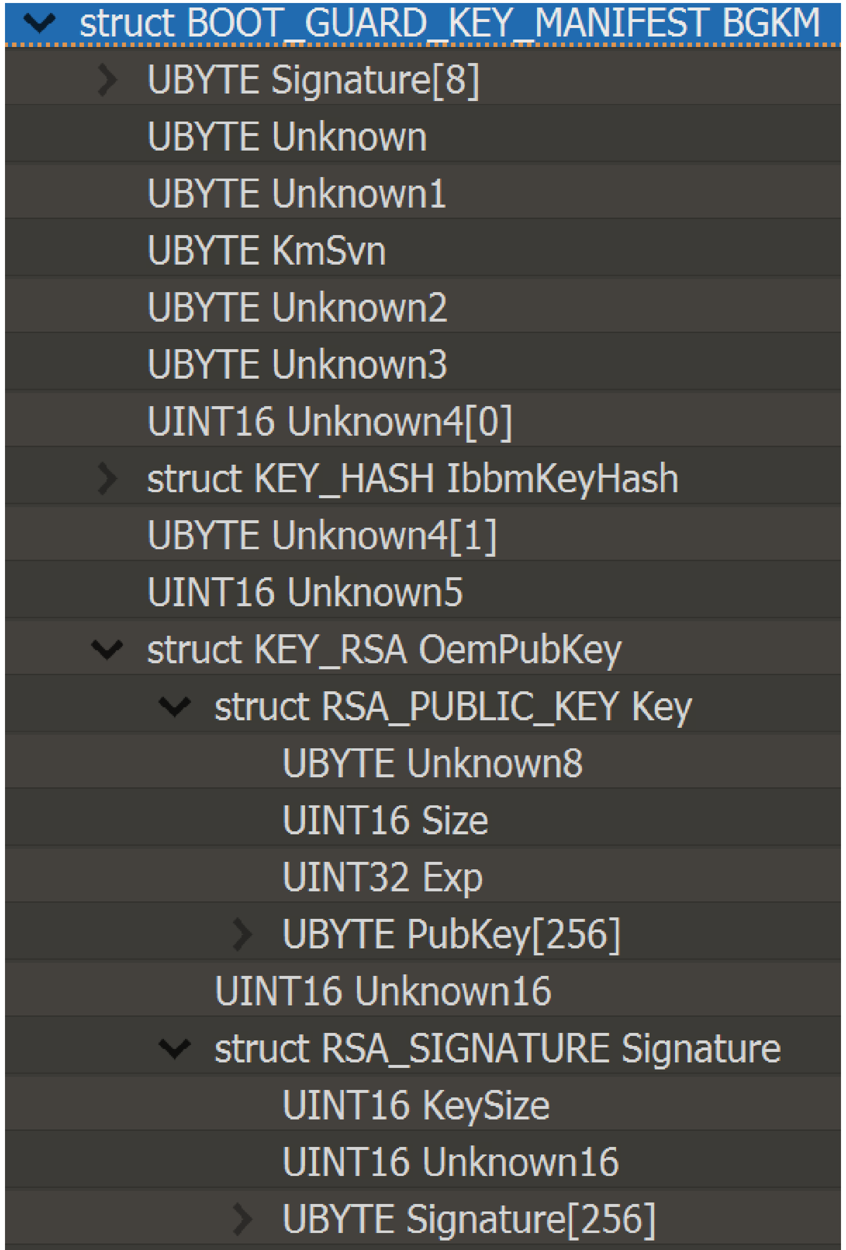
IBBM security version number (SVN)

hash of IBB (SHA-256)

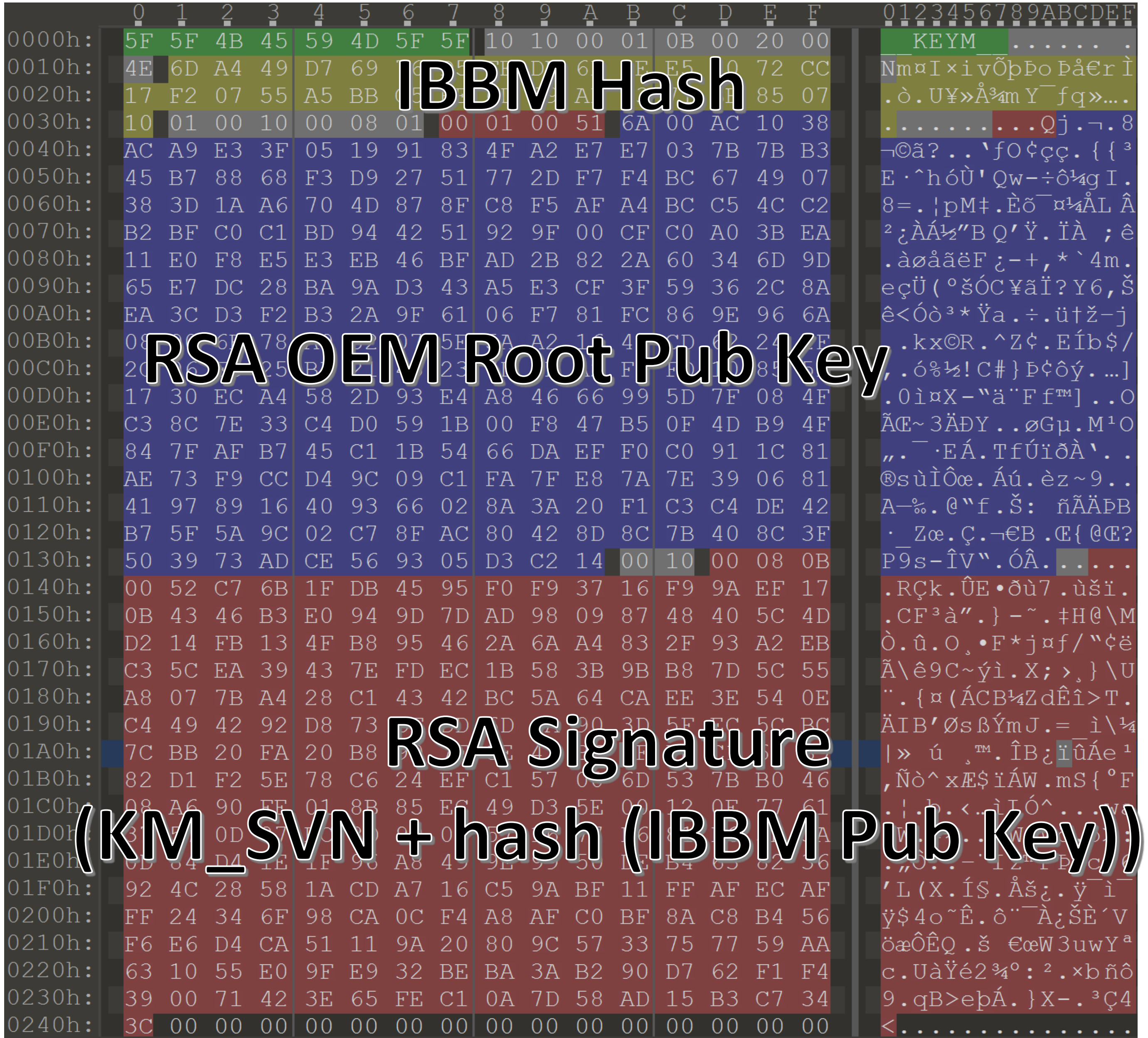
IBBM pub key (RSA-2048)

RSA signature on IBBM SVN + hash of IBB

Boot Guard: Key Manifest (KM)



```
struct BOOT_GUARD_KEY_MANIFEST BGKM
    UBYTE Signature[8]
    UBYTE Unknown
    UBYTE Unknown1
    UBYTE KmSvn
    UBYTE Unknown2
    UBYTE Unknown3
    UINT16 Unknown4[0]
    struct KEY_HASH IbbmKeyHash
    UBYTE Unknown4[1]
    UINT16 Unknown5
    struct KEY_RSA OemPubKey
        struct RSA_PUBLIC_KEY Key
            UBYTE Unknown8
            UINT16 Size
            UINT32 Exp
            UBYTE PubKey[256]
        UINT16 Unknown16
        struct RSA_SIGNATURE Signature
            UINT16 KeySize
            UINT16 Unknown16
            UBYTE Signature[256]
```



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 5F 5F 4B 45 59 4D 5F 5F 10 10 00 01 0B 00 20 00   __KEYM__........
0010h: 4E 6D A4 49 D7 69 [illegible]          72 CC
0020h: 17 F2 07 55 A5 BB [illegible]          85 07
0030h: 10 01 00 10 00 08 01 00 01 00 51 6A 00 AC 10 38   ..........Qj.¬.8
0040h: AC A9 E3 3F 05 19 91 83 4F A2 E7 E7 03 7B 7B B3
0050h: 45 B7 88 68 F3 D9 27 51 77 2D F7 F4 BC 67 49 07
0060h: 38 3D 1A A6 70 4D 87 8F C8 F5 AF A4 BC C5 4C C2
0070h: B2 BF C0 C1 BD 94 42 51 92 9F 00 CF C0 A0 3B EA
0080h: 11 E0 F8 E5 E3 EB 46 BF AD 2B 82 2A 60 34 6D 9D
0090h: 65 E7 DC 28 BA 9A D3 43 A5 E3 CF 3F 59 36 2C 8A
00A0h: EA 3C D3 F2 B3 2A 9F 61 06 F7 81 FC 86 9E 96 6A
00B0h: [illegible]
00C0h: [illegible]
00D0h: 17 30 EC A4 58 2D 93 E4 A8 46 66 99 5D 7F 08 4F
00E0h: C3 8C 7E 33 C4 D0 59 1B 00 F8 47 B5 0F 4D B9 4F
00F0h: 84 7F AF B7 45 C1 1B 54 66 DA EF F0 C0 91 1C 81
0100h: AE 73 F9 CC D4 9C 09 C1 FA 7F E8 7A 7E 39 06 81
0110h: 41 97 89 16 40 93 66 02 8A 3A 20 F1 C3 C4 DE 42
0120h: B7 5F 5A 9C 02 C7 8F AC 80 42 8D 8C 7B 40 8C 3F
0130h: 50 39 73 AD CE 56 93 05 D3 C2 14 00 10 00 08 0B
0140h: 00 52 C7 6B 1F DB 45 95 F0 F9 37 16 F9 9A EF 17
0150h: 0B 43 46 B3 E0 94 9D 7D AD 98 09 87 48 40 5C 4D
0160h: D2 14 FB 13 4F B8 95 46 2A 6A A4 83 2F 93 A2 EB
0170h: C3 5C EA 39 43 7E FD EC 1B 58 3B 9B B8 7D 5C 55
0180h: A8 07 7B A4 28 C1 43 42 BC 5A 64 CA EE 3E 54 0E
0190h: C4 49 42 92 D8 73 [illegible]
01A0h: 7C BB 20 FA 20 B8 [illegible]
01B0h: 82 D1 F2 5E 78 C6 24 EF C1 57 [illegible] 6D 53 7B B0 46
01C0h: [illegible]
01D0h: [illegible]
01E0h: [illegible]
01F0h: 92 4C 28 58 1A CD A7 16 C5 9A BF 11 FF AF EC AF
0200h: FF 24 34 6F 98 CA 0C F4 A8 AF C0 BF 8A C8 B4 56
0210h: F6 E6 D4 CA 51 11 9A 20 80 9C 57 33 75 77 59 AA
0220h: 63 10 55 E0 9F E9 32 BE BA 3A B2 90 D7 62 F1 F4
0230h: 39 00 71 42 3E 65 FE C1 0A 7D 58 AD 15 B3 C7 34
0240h: 3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   <...............
```

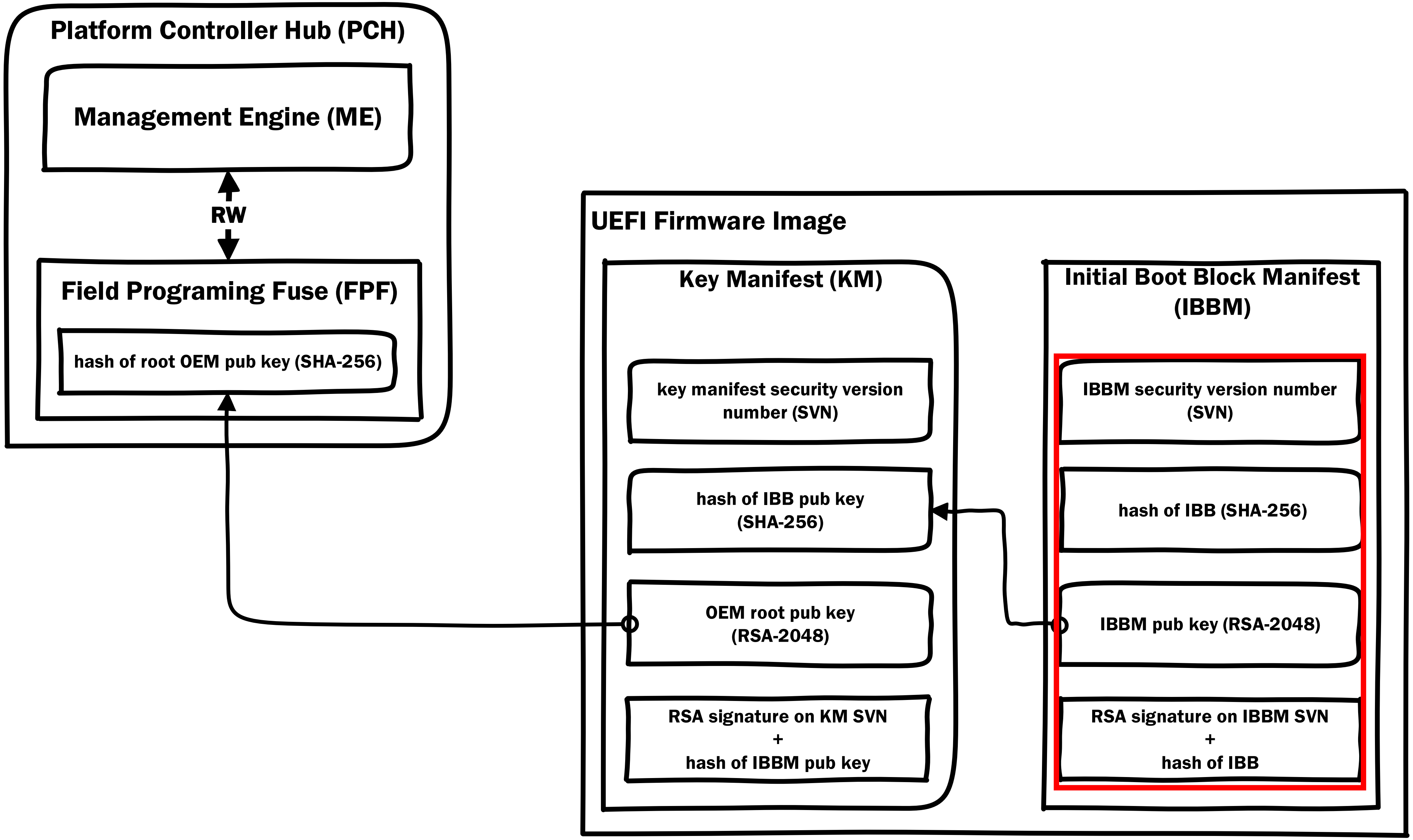
IBBM Hash

RSA OEM Root Pub Key

RSA Signature

(KM_SVN + hash (IBBM Pub Key))

Boot Guard: Chain of Trust



Platform Controller Hub (PCH)

Management Engine (ME)

RW

Field Programing Fuse (FPF)

hash of root OEM pub key (SHA-256)

UEFI Firmware Image

Key Manifest (KM)

key manifest security version number (SVN)

hash of IBB pub key (SHA-256)

OEM root pub key (RSA-2048)

RSA signature on KM SVN + hash of IBBM pub key

Initial Boot Block Manifest (IBBM)

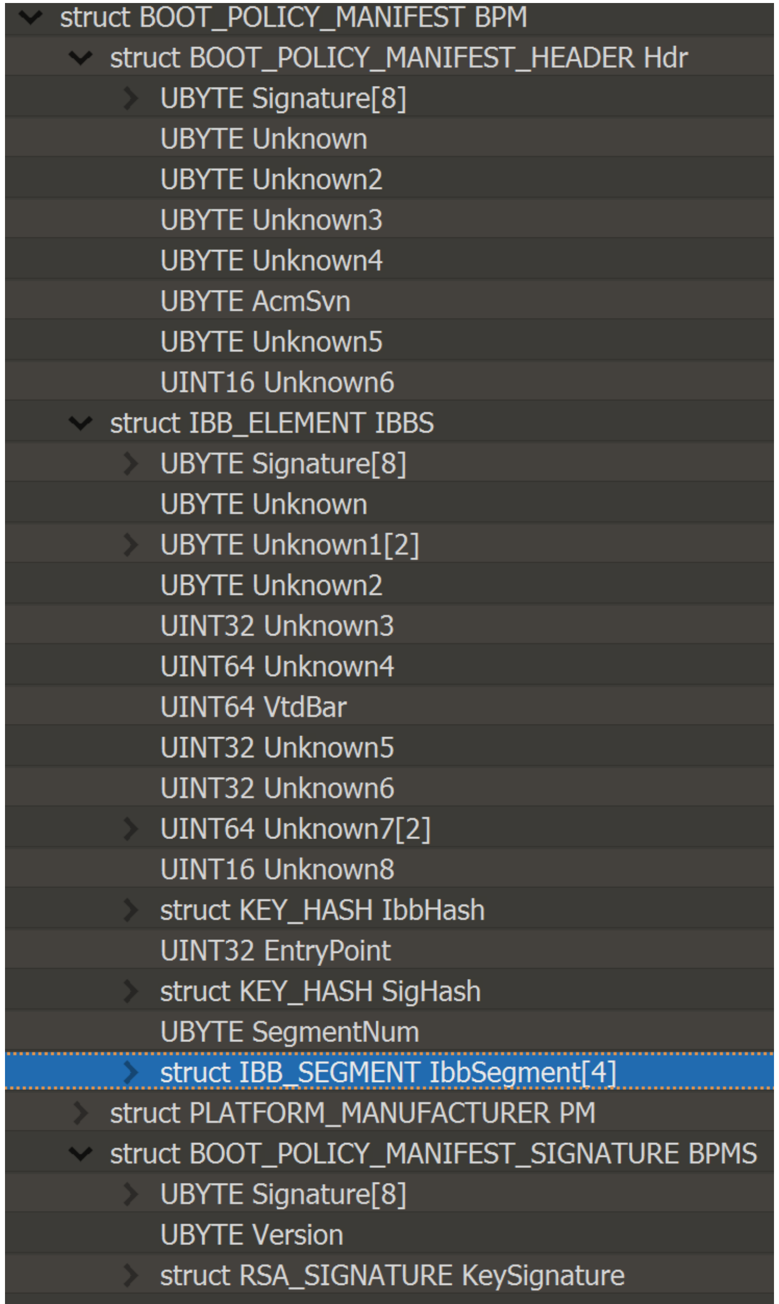
IBBM security version number (SVN)

hash of IBB (SHA-256)

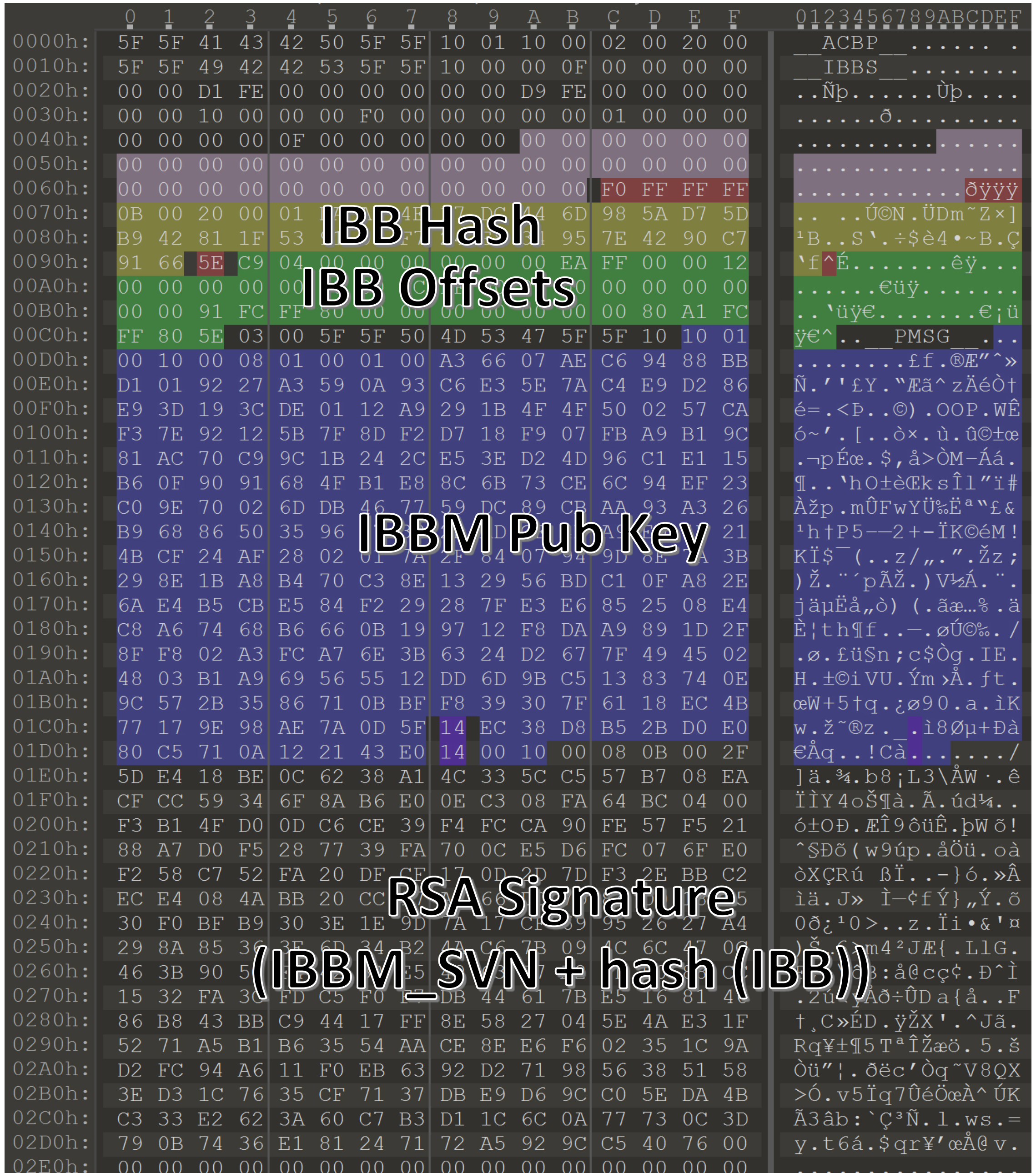
IBBM pub key (RSA-2048)

RSA signature on IBBM SVN + hash of IBB

Boot Guard: Boot Policy Manifest (BPM)



- struct BOOT_POLICY_MANIFEST BPM
  - struct BOOT_POLICY_MANIFEST_HEADER Hdr
    - UBYTE Signature[8]
    - UBYTE Unknown
    - UBYTE Unknown2
    - UBYTE Unknown3
    - UBYTE Unknown4
    - UBYTE AcmSvn
    - UBYTE Unknown5
    - UINT16 Unknown6
  - struct IBB_ELEMENT IBBS
    - UBYTE Signature[8]
    - UBYTE Unknown
    - UBYTE Unknown1[2]
    - UBYTE Unknown2
    - UINT32 Unknown3
    - UINT64 Unknown4
    - UINT64 VtdBar
    - UINT32 Unknown5
    - UINT32 Unknown6
    - UINT64 Unknown7[2]
    - UINT16 Unknown8
    - struct KEY_HASH IbbHash
    - UINT32 EntryPoint
    - struct KEY_HASH SigHash
    - UBYTE SegmentNum
    - struct IBB_SEGMENT IbbSegment[4]
  - struct PLATFORM_MANUFACTURER PM
  - struct BOOT_POLICY_MANIFEST_SIGNATURE BPMS
    - UBYTE Signature[8]
    - UBYTE Version
    - struct RSA_SIGNATURE KeySignature



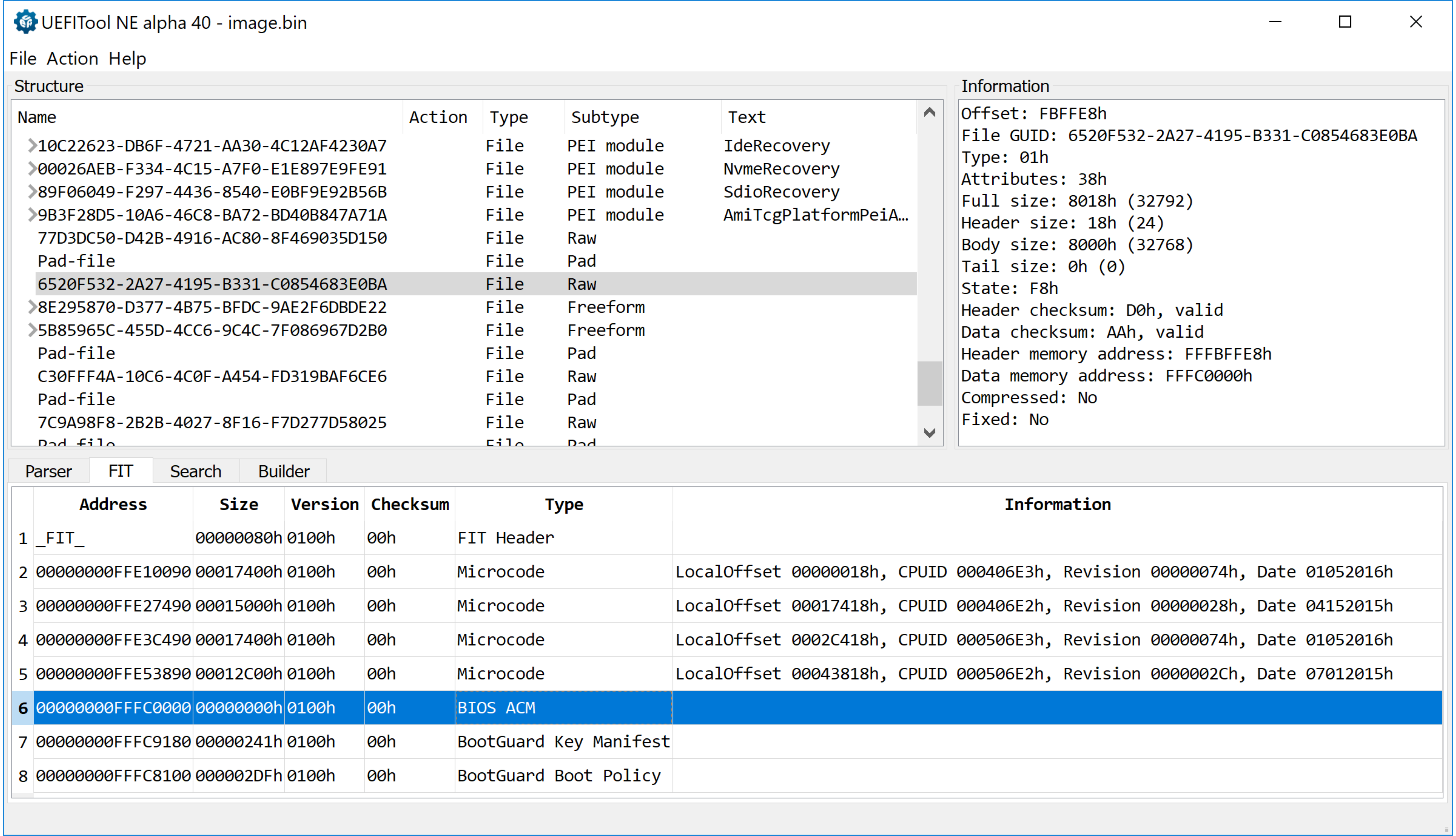
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h:  5F 5F 41 43 42 50 5F 5F 10 01 10 00 02 00 20 00   __ACBP__...... .
0010h:  5F 5F 49 42 42 53 5F 5F 10 00 00 0F 00 00 00 00   __IBBS__........
0020h:  00 00 D1 FE 00 00 00 00 00 00 D9 FE 00 00 00 00   ..Ñþ......Ùþ....
0030h:  00 00 10 00 00 00 F0 00 00 00 00 00 01 00 00 00   ......ð.........
0040h:  00 00 00 00 0F 00 00 00 00 00 00 00 00 00 00 00   ................
0050h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060h:  00 00 00 00 00 00 00 00 00 00 00 00 F0 FF FF FF   ............ðÿÿÿ
0070h:  0B 00 20 00 01 [illegible]          6D 98 5A D7 5D   .. ..Ú©N.ÜDm˜Z×]
0080h:  B9 42 81 1F 53 [illegible]             95 7E 42 90 C7   ¹B..S‘.÷$è4•~B.Ç
0090h:  91 66 5E C9 04 00 00 00 00 00 00 EA FF 00 00 12   ‘f^É.......êÿ...
00A0h:  00 00 00 00 00 [illegible]          00 00 00 00   ......€üÿ.......
00B0h:  00 00 91 FC FF 80 00 00 00 00 00 00 00 80 A1 FC   ..‘üÿ€.......€¡ü
00C0h:  FF 80 5E 03 00 5F 5F 50 4D 53 47 5F 5F 10 10 01   ÿ€^..__PMSG__...
00D0h:  00 10 00 08 01 00 01 00 A3 66 07 AE C6 94 88 BB   ........£f.®Æ”ˆ»
00E0h:  D1 01 92 27 A3 59 0A 93 C6 E3 5E 7A C4 E9 D2 86   Ñ.’'£Y.“Æã^zÄéÒ†
00F0h:  E9 3D 19 3C DE 01 12 A9 29 1B 4F 4F 50 02 57 CA   é=.<Þ..©).OOP.WÊ
0100h:  F3 7E 92 12 5B 7F 8D F2 D7 18 F9 07 FB A9 B1 9C   ó~’.[..ò×.ù.û©±œ
0110h:  81 AC 70 C9 9C 1B 24 2C E5 3E D2 4D 96 C1 E1 15   .¬pÉœ.$,å>ÒM–Áá.
0120h:  B6 0F 90 91 68 4F B1 E8 8C 6B 73 CE 6C 94 EF 23   ¶..‘hO±èŒksÎl”ï#
0130h:  C0 9E 70 02 6D DB 46 77 59 DC 89 CB AA 93 A3 26   Àžp.mÛFwYÜ‰Ëª“£&
0140h:  B9 68 86 50 35 96 [illegible]                   21   ¹h†P5–—2+-ÏK©éM!
0150h:  4B CF 24 AF 28 02 01 7A 2F 84 07 94 9D 8E 7A 3B   KÏ$¯(..z/„.”.Žz;
0160h:  29 8E 1B A8 B4 70 C3 8E 13 29 56 BD C1 0F A8 2E   )Ž.¨´pÃŽ.)V½Á.¨.
0170h:  6A E4 B5 CB E5 84 F2 29 28 7F E3 E6 85 25 08 E4   jäµËå„ò)(.ãæ…%.ä
0180h:  C8 A6 74 68 B6 66 0B 19 97 12 F8 DA A9 89 1D 2F   È¦th¶f..—.øÚ©‰./
0190h:  8F F8 02 A3 FC A7 6E 3B 63 24 D2 67 7F 49 45 02   .ø.£ü§n;c$Òg.IE.
01A0h:  48 03 B1 A9 69 56 55 12 DD 6D 9B C5 13 83 74 0E   H.±©iVU.Ým›Å.ƒt.
01B0h:  9C 57 2B 35 86 71 0B BF F8 39 30 7F 61 18 EC 4B   œW+5†q.¿ø90.a.ìK
01C0h:  77 17 9E 98 AE 7A 0D 5F 14 EC 38 D8 B5 2B D0 E0   w.ž˜®z._.ì8Øµ+Ðà
01D0h:  80 C5 71 0A 12 21 43 E0 14 00 10 00 08 0B 00 2F   €Åq..!Cà......./
01E0h:  5D E4 18 BE 0C 62 38 A1 4C 33 5C C5 57 B7 08 EA   ]ä.¾.b8¡L3\ÅW·.ê
01F0h:  CF CC 59 34 6F 8A B6 E0 0E C3 08 FA 64 BC 04 00   ÏÌY4oŠ¶à.Ã.úd¼..
0200h:  F3 B1 4F D0 0D C6 CE 39 F4 FC CA 90 FE 57 F5 21   ó±OÐ.ÆÎ9ôüÊ.þWõ!
0210h:  88 A7 D0 F5 28 77 39 FA 70 0C E5 D6 FC 07 6F E0   ˆ§Ðõ(w9úp.åÖü.oà
0220h:  F2 58 C7 52 FA 20 DF CF 17 0D 2D 7D F3 2E BB C2   òXÇRú ßÏ..-}ó.»Â
0230h:  EC E4 08 4A BB 20 CC [illegible]                 5   ìä.J» Ì–¢fÝ}„Ý.õ
0240h:  30 F0 BF B9 30 3E 1E 9D 7A 17 CF [illegible] 95 26 27 A4   0ð¿¹0>..z.Ïi•&'¤
0250h:  29 8A 85 36 3E 6D 34 B2 4A C6 7B 09 4C 6C 47 00   )Š…6>m4²JÆ{.LlG.
0260h:  46 3B 90 5[illegible]                                   [illegible]:å@cç¢.Ð^Ì
0270h:  15 32 FA 30 FD C5 F0 [illegible] DB 44 61 7B E5 16 81 40   .2ú0ýÅð÷ÛDa{å..F
0280h:  86 B8 43 BB C9 44 17 FF 8E 58 27 04 5E 4A E3 1F   †¸C»ÉD.ÿŽX'.^Jã.
0290h:  52 71 A5 B1 B6 35 54 AA CE 8E E6 F6 02 35 1C 9A   Rq¥±¶5TªÎŽæö.5.š
02A0h:  D2 FC 94 A6 11 F0 EB 63 92 D2 71 98 56 38 51 58   Òü”¦.ðëc’Òq˜V8QX
02B0h:  3E D3 1C 76 35 CF 71 37 DB E9 D6 9C C0 5E DA 4B   >Ó.v5Ïq7ÛéÖœÀ^ÚK
02C0h:  C3 33 E2 62 3A 60 C7 B3 D1 1C 6C 0A 77 73 0C 3D   Ã3âb:`Ç³Ñ.l.ws.=
02D0h:  79 0B 74 36 E1 81 24 71 72 A5 92 9C C5 40 76 00   y.t6á.$qr¥’œÅ@v.
02E0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

IBB Hash

IBB Offsets

IBBM Pub Key

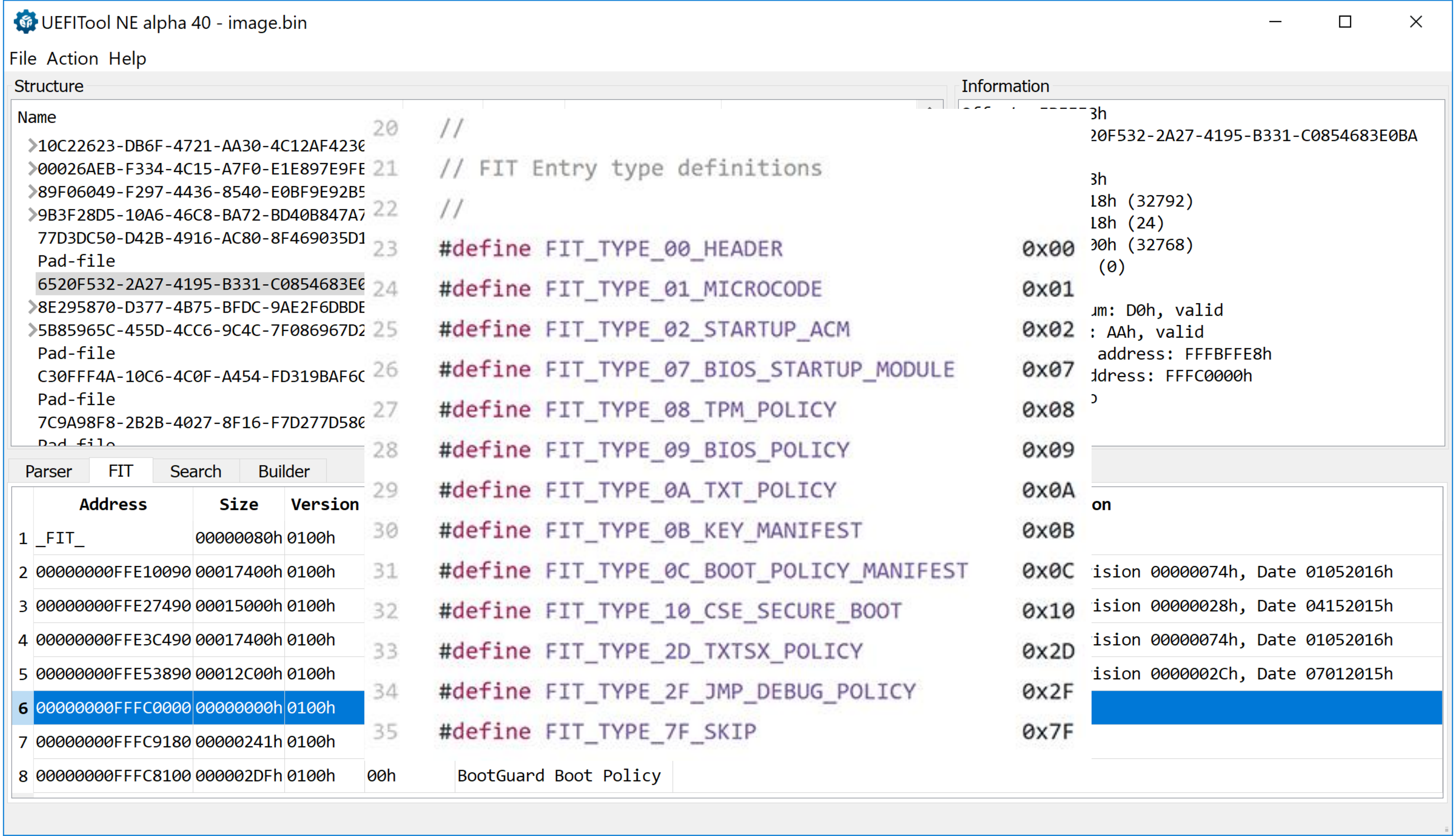
RSA Signature (IBBM_SVN + hash (IBB))



Name	Action	Type	Subtype	Text
10C22623-DB6F-4721-AA30-4C12AF4230A7		File	PEI module	IdeRecovery
00026AEB-F334-4C15-A7F0-E1E897E9FE91		File	PEI module	NvmeRecovery
89F06049-F297-4436-8540-E0BF9E92B56B		File	PEI module	SdioRecovery
9B3F28D5-10A6-46C8-BA72-BD40B847A71A		File	PEI module	AmiTcgPlatformPeiA…
77D3DC50-D42B-4916-AC80-8F469035D150		File	Raw	
Pad-file		File	Pad	
6520F532-2A27-4195-B331-C0854683E0BA		File	Raw	
8E295870-D377-4B75-BFDC-9AE2F6DBDE22		File	Freeform	
5B85965C-455D-4CC6-9C4C-7F086967D2B0		File	Freeform	
Pad-file		File	Pad	
C30FFF4A-10C6-4C0F-A454-FD319BAF6CE6		File	Raw	
Pad-file		File	Pad	
7C9A98F8-2B2B-4027-8F16-F7D277D58025		File	Raw	
Pad-file		File	Pad	

```
Offset: FBFFE8h
File GUID: 6520F532-2A27-4195-B331-C0854683E0BA
Type: 01h
Attributes: 38h
Full size: 8018h (32792)
Header size: 18h (24)
Body size: 8000h (32768)
Tail size: 0h (0)
State: F8h
Header checksum: D0h, valid
Data checksum: AAh, valid
Header memory address: FFFBFFE8h
Data memory address: FFFC0000h
Compressed: No
Fixed: No
```

	Address	Size	Version	Checksum	Type	Information
1	_FIT_	00000080h	0100h	00h	FIT Header	
2	00000000FFE10090	00017400h	0100h	00h	Microcode	LocalOffset 00000018h, CPUID 000406E3h, Revision 00000074h, Date 01052016h
3	00000000FFE27490	00015000h	0100h	00h	Microcode	LocalOffset 00017418h, CPUID 000406E2h, Revision 00000028h, Date 04152015h
4	00000000FFE3C490	00017400h	0100h	00h	Microcode	LocalOffset 0002C418h, CPUID 000506E3h, Revision 00000074h, Date 01052016h
5	00000000FFE53890	00012C00h	0100h	00h	Microcode	LocalOffset 00043818h, CPUID 000506E2h, Revision 0000002Ch, Date 07012015h
6	00000000FFFC0000	00000000h	0100h	00h	BIOS ACM	
7	00000000FFFC9180	00000241h	0100h	00h	BootGuard Key Manifest	
8	00000000FFFC8100	000002DFh	0100h	00h	BootGuard Boot Policy	



Name

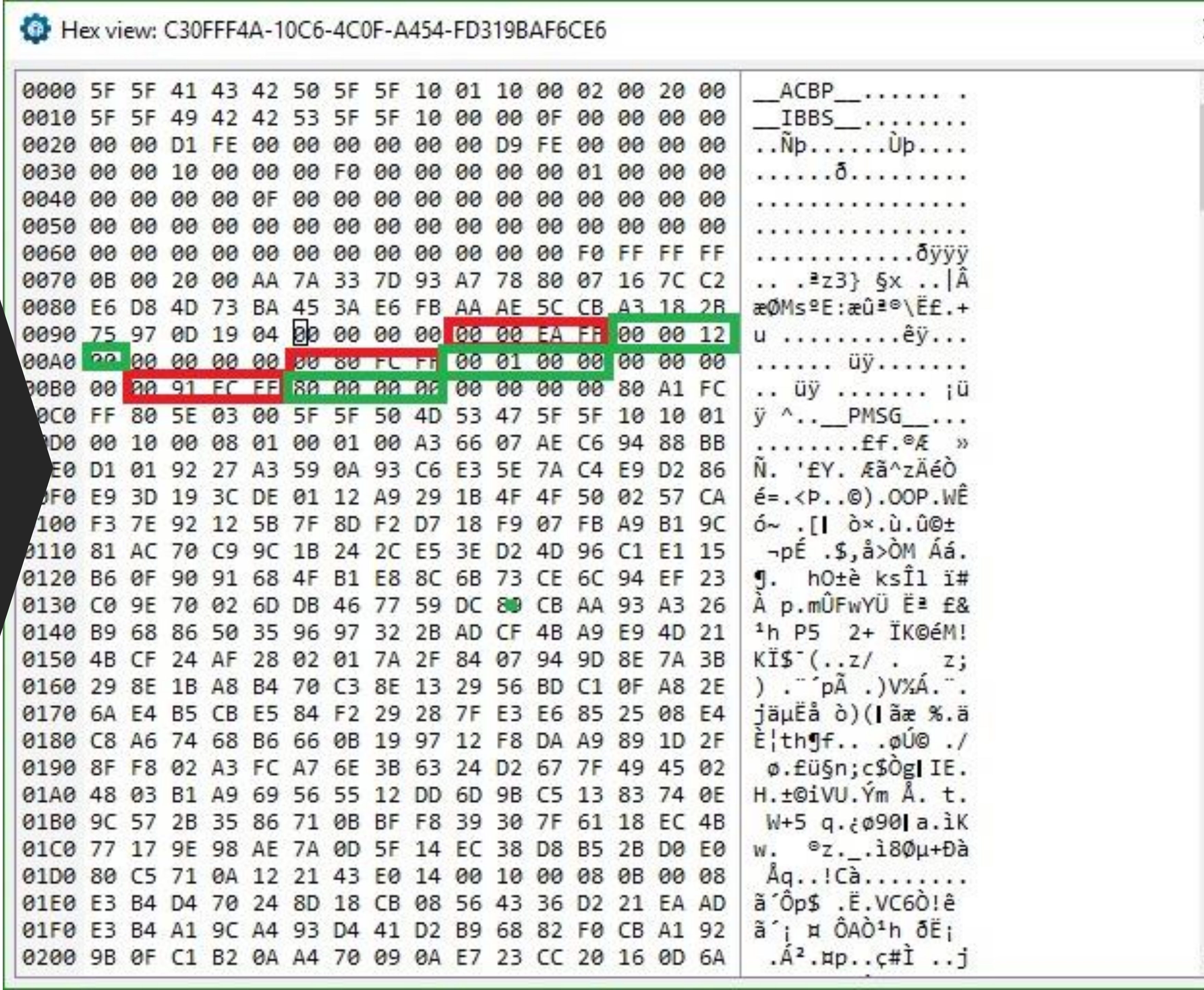
- 10C22623-DB6F-4721-AA30-4C12AF4236
- 00026AEB-F334-4C15-A7F0-E1E897E9FE
- 89F06049-F297-4436-8540-E0BF9E92B5
- 9B3F28D5-10A6-46C8-BA72-BD40B847A7
- 77D3DC50-D42B-4916-AC80-8F469035D1
- Pad-file
- 6520F532-2A27-4195-B331-C0854683E0
- 8E295870-D377-4B75-BFDC-9AE2F6DBDE
- 5B85965C-455D-4CC6-9C4C-7F086967D2
- Pad-file
- C30FFF4A-10C6-4C0F-A454-FD319BAF6C
- Pad-file
- 7C9A98F8-2B2B-4027-8F16-F7D277D580
- Pad-file

```
3h
20F532-2A27-4195-B331-C0854683E0BA

3h
18h (32792)
18h (24)
00h (32768)
 (0)

um: D0h, valid
: AAh, valid
 address: FFFBFFE8h
ddress: FFFC0000h
)
```

```
//
// FIT Entry type definitions
//
#define FIT_TYPE_00_HEADER                     0x00
#define FIT_TYPE_01_MICROCODE                  0x01
#define FIT_TYPE_02_STARTUP_ACM                0x02
#define FIT_TYPE_07_BIOS_STARTUP_MODULE        0x07
#define FIT_TYPE_08_TPM_POLICY                 0x08
#define FIT_TYPE_09_BIOS_POLICY                0x09
#define FIT_TYPE_0A_TXT_POLICY                 0x0A
#define FIT_TYPE_0B_KEY_MANIFEST               0x0B
#define FIT_TYPE_0C_BOOT_POLICY_MANIFEST       0x0C
#define FIT_TYPE_10_CSE_SECURE_BOOT            0x10
#define FIT_TYPE_2D_TXTSX_POLICY               0x2D
#define FIT_TYPE_2F_JMP_DEBUG_POLICY           0x2F
#define FIT_TYPE_7F_SKIP                       0x7F
```

	Address	Size	Version			on
1	_FIT_	00000080h	0100h			
2	00000000FFE10090	00017400h	0100h			ision 00000074h, Date 01052016h
3	00000000FFE27490	00015000h	0100h			ision 00000028h, Date 04152015h
4	00000000FFE3C490	00017400h	0100h			ision 00000074h, Date 01052016h
5	00000000FFE53890	00012C00h	0100h			ision 0000002Ch, Date 07012015h
6	00000000FFFC0000	00000000h	0100h			
7	00000000FFFC9180	00000241h	0100h			
8	00000000FFFC8100	000002DFh	0100h	00h	BootGuard Boot Policy	

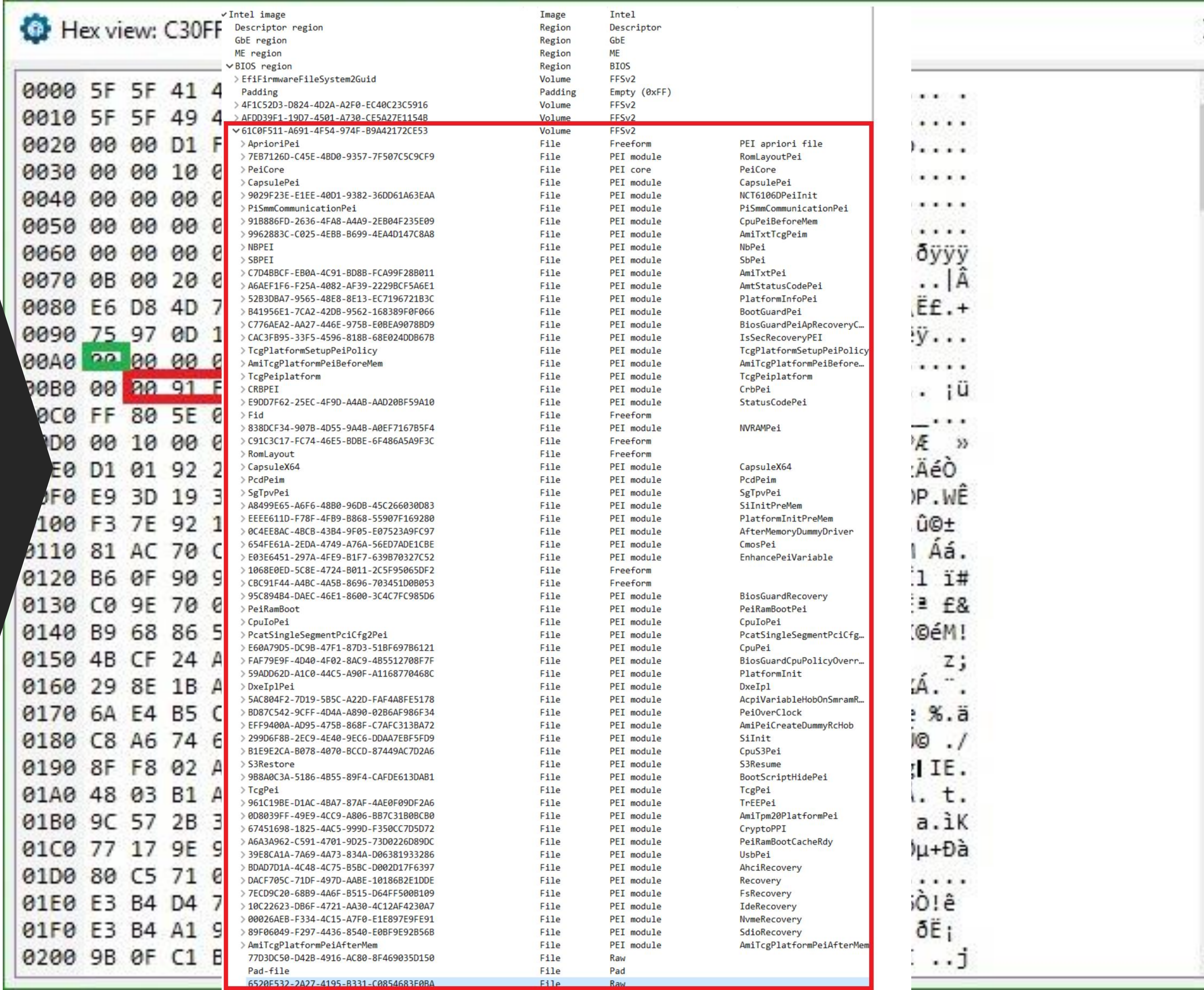
Boot Guard: Initial Boot Block (IBB)



Hex view: C30FFF4A-10C6-4C0F-A454-FD319BAF6CE6

```
0000 5F 5F 41 43 42 50 5F 5F 10 01 10 00 02 00 20 00  __ACBP__...... .
0010 5F 5F 49 42 42 53 5F 5F 10 00 00 0F 00 00 00 00  __IBBS__........
0020 00 00 D1 FE 00 00 00 00 00 00 D9 FE 00 00 00 00  ..Ñþ......Ùþ....
0030 00 00 10 00 00 00 F0 00 00 00 00 01 00 00 00 00  ......ð.........
0040 00 00 00 00 0F 00 00 00 00 00 00 00 00 00 00 00  ................
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0060 00 00 00 00 00 00 00 00 00 00 00 00 F0 FF FF FF  ............ðÿÿÿ
0070 0B 00 20 00 AA 7A 33 7D 93 A7 78 80 07 16 7C C2  .. .ªz3} §x ..|Â
0080 E6 D8 4D 73 BA 45 3A E6 FB AA AE 5C CB A3 18 2B  æØMsºE:æûª®\Ë£.+
0090 75 97 0D 19 04 00 00 00 00 00 00 EA FF 00 00 12  u .........êÿ...
00A0 00 00 00 00 00 00 80 FC FF 00 01 00 00 00 00 00  ...... üÿ.......
00B0 00 00 91 FC FF 80 00 00 00 00 00 00 00 80 A1 FC  .. üÿ ....... ¡ü
00C0 FF 80 5E 03 00 5F 5F 50 4D 53 47 5F 5F 10 10 01  ÿ ^..__PMSG__...
00D0 00 10 00 08 01 00 01 00 A3 66 07 AE C6 94 88 BB  ........£f.®Æ  »
00E0 D1 01 92 27 A3 59 0A 93 C6 E3 5E 7A C4 E9 D2 86  Ñ. '£Y. Æã^zÄéÒ
00F0 E9 3D 19 3C DE 01 12 A9 29 1B 4F 4F 50 02 57 CA  é=.<Þ..©).OOP.WÊ
0100 F3 7E 92 12 5B 7F 8D F2 D7 18 F9 07 FB A9 B1 9C  ó~ .[| ò×.ù.û©±
0110 81 AC 70 C9 9C 1B 24 2C E5 3E D2 4D 96 C1 E1 15   ¬pÉ .$,å>ÒM Áá.
0120 B6 0F 90 91 68 4F B1 E8 8C 6B 73 CE 6C 94 EF 23  ¶.  hO±è ksÎl ï#
0130 C0 9E 70 02 6D DB 46 77 59 DC 80 CB AA 93 A3 26  À p.mÛFwYÜ Ëª £&
0140 B9 68 86 50 35 96 97 32 2B AD CF 4B A9 E9 4D 21  ¹h P5  2+ ÏK©éM!
0150 4B CF 24 AF 28 02 01 7A 2F 84 07 94 9D 8E 7A 3B  KÏ$¯(..z/ .   z;
0160 29 8E 1B A8 B4 70 C3 8E 13 29 56 BD C1 0F A8 2E  ) .¨´pÃ .)V½Á.¨.
0170 6A E4 B5 CB E5 84 F2 29 28 7F E3 E6 85 25 08 E4  jäµËå ò)(|ãæ %.ä
0180 C8 A6 74 68 B6 66 0B 19 97 12 F8 DA A9 89 1D 2F  È¦th¶f.. .øÚ© ./
0190 8F F8 02 A3 FC A7 6E 3B 63 24 D2 67 7F 49 45 02   ø.£ü§n;c$Òg|IE.
01A0 48 03 B1 A9 69 56 55 12 DD 6D 9B C5 13 83 74 0E  H.±©iVU.Ým Å. t.
01B0 9C 57 2B 35 86 71 0B BF F8 39 30 7F 61 18 EC 4B   W+5 q.¿ø90|a.ìK
01C0 77 17 9E 98 AE 7A 0D 5F 14 EC 38 D8 B5 2B D0 E0  w.  ®z._.ì8Øµ+Ðà
01D0 80 C5 71 0A 12 21 43 E0 14 00 10 00 08 0B 00 08   Åq..!Cà........
01E0 E3 B4 D4 70 24 8D 18 CB 08 56 43 36 D2 21 EA AD  ã´Ôp$ .Ë.VC6Ò!ê
01F0 E3 B4 A1 9C A4 93 D4 41 D2 B9 68 82 F0 CB A1 92  ã´¡ ¤ ÔAÒ¹h ðË¡
0200 9B 0F C1 B2 0A A4 70 09 0A E7 23 CC 20 16 0D 6A   .Á².¤p..ç#Ì ..j
```

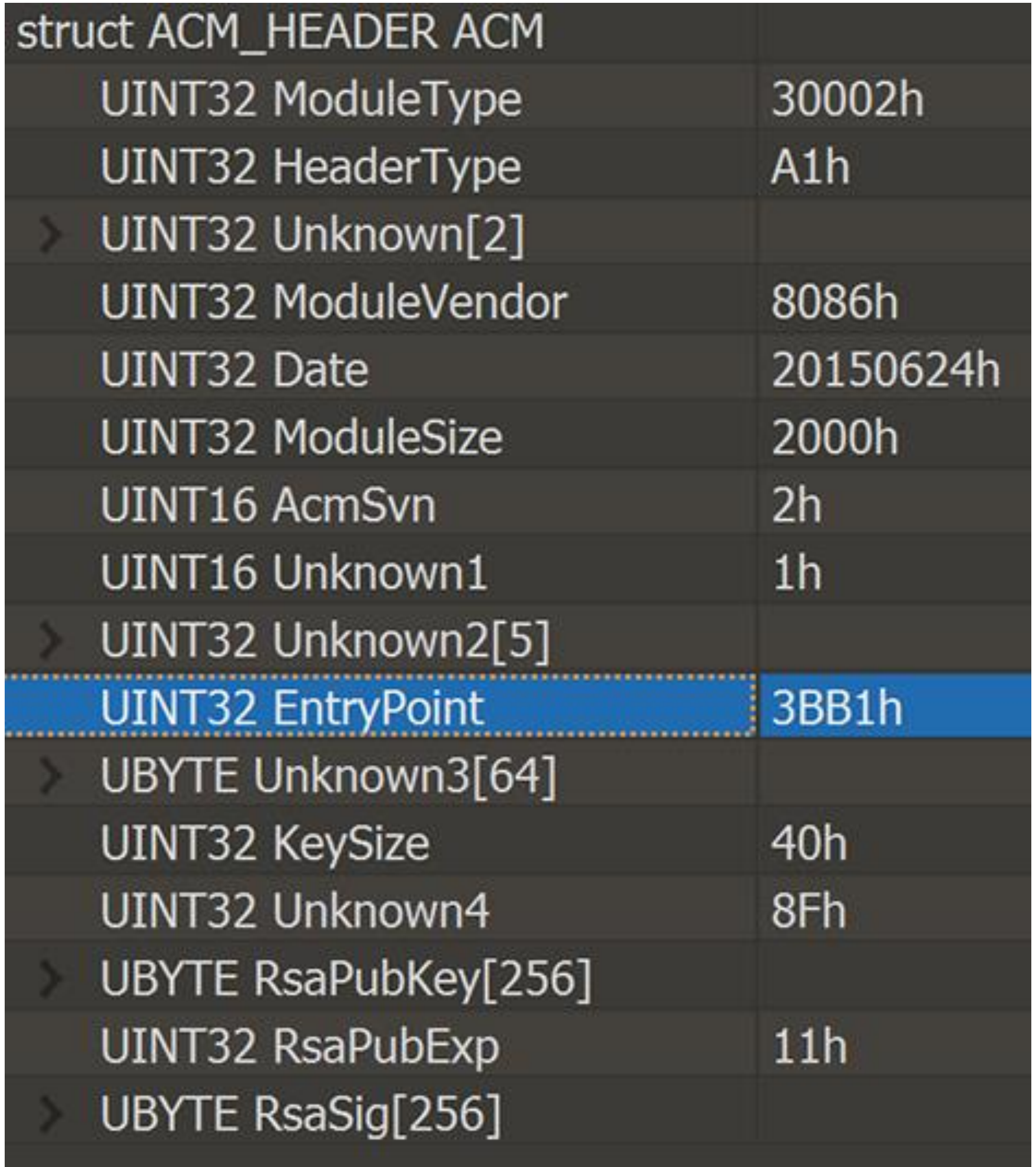
Boot Guard: Initial Boot Block (IBB)



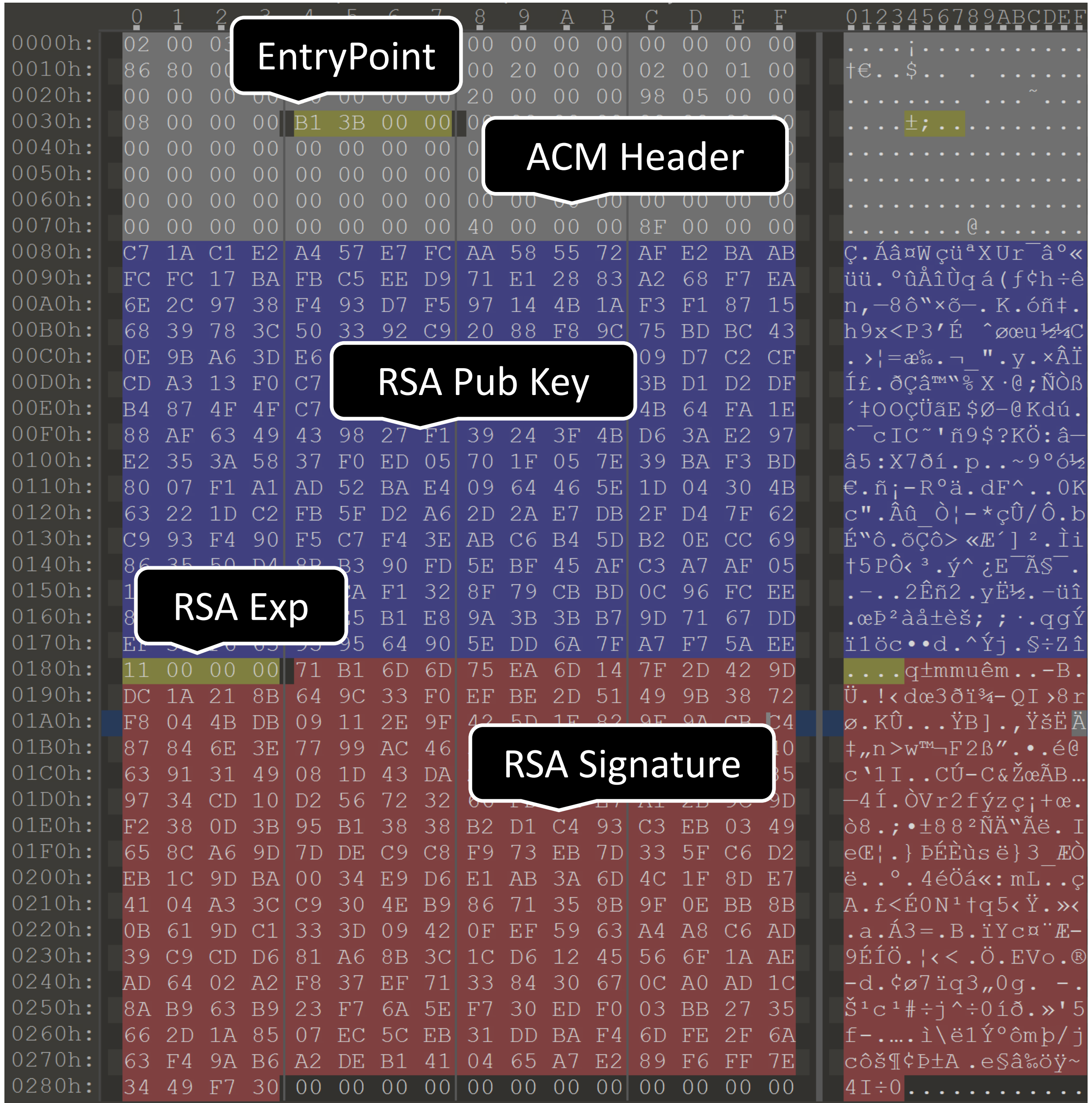
```
0000 5F 5F 41 4
0010 5F 5F 49 4
0020 00 00 D1 F
0030 00 00 10 0
0040 00 00 00 0
0050 00 00 00 0
0060 00 00 00 0
0070 0B 00 20 0
0080 E6 D8 4D 7
0090 75 97 0D 1
00A0 00 00 00 0
0B0 00 00 91 F
0C0 FF 80 5E 0
D0 00 10 00 0
E0 D1 01 92 2
F0 E9 3D 19 3
100 F3 7E 92 1
0110 81 AC 70 C
0120 B6 0F 90 9
0130 C0 9E 70 0
0140 B9 68 86 5
0150 4B CF 24 A
0160 29 8E 1B A
0170 6A E4 B5 C
0180 C8 A6 74 6
0190 8F F8 02 A
01A0 48 03 B1 A
01B0 9C 57 2B 3
01C0 77 17 9E 9
01D0 80 C5 71 0
01E0 E3 B4 D4 7
01F0 E3 B4 A1 9
0200 9B 0F C1 B
```

```
Intel image                                   Image     Intel
 Descriptor region                            Region    Descriptor
 GbE region                                   Region    GbE
 ME region                                    Region    ME
 BIOS region                                  Region    BIOS
  EfiFirmwareFileSystem2Guid                  Volume    FFSv2
  Padding                                     Padding   Empty (0xFF)
  4F1C52D3-D824-4D2A-A2F0-EC40C23C5916        Volume    FFSv2
  AFDD39F1-19D7-4501-A730-CE5A27E1154B        Volume    FFSv2
  61C0F511-A691-4F54-974F-B9A42172CE53        Volume    FFSv2
   AprioriPei                                 File      Freeform      PEI apriori file
   7EB7126D-C45E-4BD0-9357-7F507C5C9CF9       File      PEI module    RomLayoutPei
   PeiCore                                    File      PEI core      PeiCore
   CapsulePei                                 File      PEI module    CapsulePei
   9029F23E-E1EE-40D1-9382-36DD61A63EAA       File      PEI module    NCT6106DPeiInit
   PiSmmCommunicationPei                      File      PEI module    PiSmmCommunicationPei
   91B886FD-2636-4FA8-A4A9-2EB04F235E09       File      PEI module    CpuPeiBeforeMem
   9962883C-C025-4EBB-B699-4EA4D147C8A8       File      PEI module    AmiTxtTcgPeim
   NBPEI                                      File      PEI module    NbPei
   SBPEI                                      File      PEI module    SbPei
   C7D4BBCF-EB0A-4C91-BD8B-FCA99F28B011       File      PEI module    AmiTxtPei
   A6AEF1F6-F25A-4082-AF39-2229BCF5A6E1       File      PEI module    AmtStatusCodePei
   52B3DBA7-9565-48E8-8E13-EC7196721B3C       File      PEI module    PlatformInfoPei
   B41956E1-7CA2-42DB-9562-168389F0F066       File      PEI module    BootGuardPei
   C776AEA2-AA27-446E-975B-E0BEA9078BD9       File      PEI module    BiosGuardPeiApRecoveryC…
   CAC3FB95-33F5-4596-818B-68E024DDB67B       File      PEI module    IsSecRecoveryPEI
   TcgPlatformSetupPeiPolicy                  File      PEI module    TcgPlatformSetupPeiPolicy
   AmiTcgPlatformPeiBeforeMem                 File      PEI module    AmiTcgPlatformPeiBefore…
   TcgPeiplatform                             File      PEI module    TcgPeiplatform
   CRBPEI                                     File      PEI module    CrbPei
   E9DD7F62-25EC-4F9D-A4AB-AAD20BF59A10       File      PEI module    StatusCodePei
   Fid                                        File      Freeform
   838DCF34-907B-4D55-9A4B-A0EF7167B5F4       File      PEI module    NVRAMPei
   C91C3C17-FC74-46E5-BDBE-6F486A5A9F3C       File      Freeform
   RomLayout                                  File      Freeform
   CapsuleX64                                 File      PEI module    CapsuleX64
   PcdPeim                                    File      PEI module    PcdPeim
   SgTpvPei                                   File      PEI module    SgTpvPei
   A8499E65-A6F6-48B0-96DB-45C266030D83       File      PEI module    SiInitPreMem
   EEEE611D-F78F-4FB9-B868-55907F169280       File      PEI module    PlatformInitPreMem
   0C4EE8AC-4BCB-43B4-9F05-E07523A9FC97       File      PEI module    AfterMemoryDummyDriver
   654FE61A-2EDA-4749-A76A-56ED7ADE1CBE       File      PEI module    CmosPei
   E03E6451-297A-4FE9-B1F7-639B70327C52       File      PEI module    EnhancePeiVariable
   1068E0ED-5C8E-4724-B011-2C5F95065DF2       File      Freeform
   CBC91F44-A4BC-4A5B-8696-703451D0B053       File      Freeform
   95C894B4-DAEC-46E1-8600-3C4C7FC985D6       File      PEI module    BiosGuardRecovery
   PeiRamBoot                                 File      PEI module    PeiRamBootPei
   CpuIoPei                                   File      PEI module    CpuIoPei
   PcatSingleSegmentPciCfg2Pei                File      PEI module    PcatSingleSegmentPciCfg…
   E60A79D5-DC9B-47F1-87D3-51BF697B6121       File      PEI module    CpuPei
   FAF79E9F-4D40-4F02-8AC9-4B5512708F7F       File      PEI module    BiosGuardCpuPolicyOverr…
   59ADD62D-A1C0-44C5-A90F-A1168770468C       File      PEI module    PlatformInit
   DxeIplPei                                  File      PEI module    DxeIpl
   5AC804F2-7D19-5B5C-A22D-FAF4A8FE5178       File      PEI module    AcpiVariableHobOnSmramR…
   BD87C542-9CFF-4D4A-A890-02B6AF986F34       File      PEI module    PeiOverClock
   EFF9400A-AD95-475B-868F-C7AFC313BA72       File      PEI module    AmiPeiCreateDummyRcHob
   299D6F8B-2EC9-4E40-9EC6-DDAA7EBF5FD9       File      PEI module    SiInit
   B1E9E2CA-B078-4070-BCCD-87449AC7D2A6       File      PEI module    CpuS3Pei
   S3Restore                                  File      PEI module    S3Resume
   9B8A0C3A-5186-4B55-89F4-CAFDE613DAB1       File      PEI module    BootScriptHidePei
   TcgPei                                     File      PEI module    TcgPei
   961C19BE-D1AC-4BA7-87AF-4AE0F09DF2A6       File      PEI module    TrEEPei
   0D8039FF-49E9-4CC9-A806-BB7C31B0BCB0       File      PEI module    AmiTpm20PlatformPei
   67451698-1825-4AC5-999D-F350CC7D5D72       File      PEI module    CryptoPPI
   A6A3A962-C591-4701-9D25-73D0226D89DC       File      PEI module    PeiRamBootCacheRdy
   39E8CA1A-7A69-4A73-834A-D06381933286       File      PEI module    UsbPei
   BDAD7D1A-4C48-4C75-B5BC-D002D17F6397       File      PEI module    AhciRecovery
   DACF705C-71DF-497D-AABE-10186B2E1DDE       File      PEI module    Recovery
   7ECD9C20-68B9-4A6F-B515-D64FF500B109       File      PEI module    FsRecovery
   10C22623-DB6F-4721-AA30-4C12AF4230A7       File      PEI module    IdeRecovery
   00026AEB-F334-4C15-A7F0-E1E897E9FE91       File      PEI module    NvmeRecovery
   89F06049-F297-4436-8540-E0BF9E92B56B       File      PEI module    SdioRecovery
   AmiTcgPlatformPeiAfterMem                  File      PEI module    AmiTcgPlatformPeiAfterMem
   77D3DC50-D42B-4916-AC80-8F469035D150       File      Raw
   Pad-file                                   File      Pad
   6520F532-2A27-4195-B331-C0854683F0BA       File      Raw
```

Boot Guard: Authenticated Code Module (ACM)



struct ACM_HEADER ACM	
UINT32 ModuleType	30002h
UINT32 HeaderType	A1h
› UINT32 Unknown[2]	
UINT32 ModuleVendor	8086h
UINT32 Date	20150624h
UINT32 ModuleSize	2000h
UINT16 AcmSvn	2h
UINT16 Unknown1	1h
› UINT32 Unknown2[5]	
UINT32 EntryPoint	3BB1h
› UBYTE Unknown3[64]	
UINT32 KeySize	40h
UINT32 Unknown4	8Fh
› UBYTE RsaPubKey[256]	
UINT32 RsaPubExp	11h
› UBYTE RsaSig[256]	



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 02 00                   00 00 00 00 00 00 00 00   ....¡...........
0010h: 86 80                   00 20 00 00 02 00 01 00   †€..$.. . ......
0020h: 00 00                   20 00 00 00 98 05 00 00   .........  ...˜...
0030h: 08 00 00 00 B1 3B 00 00                           ....±;..........
0040h: 00 00 00 00 00 00 00 00                           ................
0050h: 00 00 00 00 00 00 00 00                           ................
0060h: 00 00 00 00 00 00 00 00 00             00 00 00 00 ................
0070h: 00 00 00 00 00 00 00 00 40 00 00 00 8F 00 00 00   .........@......
0080h: C7 1A C1 E2 A4 57 E7 FC AA 58 55 72 AF E2 BA AB   Ç.Áâ¤WçüªXUr¯âº«
0090h: FC FC 17 BA FB C5 EE D9 71 E1 28 83 A2 68 F7 EA   üü.ºûÅîÙqá(ƒ¢h÷ê
00A0h: 6E 2C 97 38 F4 93 D7 F5 97 14 4B 1A F3 F1 87 15   n,—8ô“×õ—.K.óñ‡.
00B0h: 68 39 78 3C 50 33 92 C9 20 88 F8 9C 75 BD BC 43   h9x<P3’É ˆøœu½¼C
00C0h: 0E 9B A6 3D E6                      09 D7 C2 CF   .›¦=æ‰.¬_".y.×ÂÏ
00D0h: CD A3 13 F0 C7                      3B D1 D2 DF   Í£.ðÇâ™"§X·@;ÑÒß
00E0h: B4 87 4F 4F C7                      4B 64 FA 1E   ´‡OOÇÜãE$Ø–@Kdú.
00F0h: 88 AF 63 49 43 98 27 F1 39 24 3F 4B D6 3A E2 97   ˆ¯cIC˜'ñ9$?KÖ:â—
0100h: E2 35 3A 58 37 F0 ED 05 70 1F 05 7E 39 BA F3 BD   â5:X7ðí.p..~9ºó½
0110h: 80 07 F1 A1 AD 52 BA E4 09 64 46 5E 1D 04 30 4B   €.ñ¡-Rºä.dF^..0K
0120h: 63 22 1D C2 FB 5F D2 A6 2D 2A E7 DB 2F D4 7F 62   c".Âû_Ò¦-*çÛ/Ô.b
0130h: C9 93 F4 90 F5 C7 F4 3E AB C6 B4 5D B2 0E CC 69   É“ô.õÇô>«Æ´]².Ìi
0140h:             B3 90 FD 5E BF 45 AF C3 A7 AF 05   †5PÔ‹³.ý^¿E¯Ã§¯.
0150h:                F1 32 8F 79 CB BD 0C 96 FC EE   .–..2Êñ2.yË½.–üî
0160h:                B1 E8 9A 3B 3B B7 9D 71 67 DD   .œÞ²àå±èš;;·.qgÝ
0170h:                95 64 90 5E DD 6A 7F A7 F7 5A EE   ï1öc••d.^Ýj.§÷Zî
0180h: 11 00 00 00 71 B1 6D 6D 75 EA 6D 14 7F 2D 42 9D   ....q±mmuêm..-B.
0190h: DC 1A 21 8B 64 9C 33 F0 EF BE 2D 51 49 9B 38 72   Ü.!‹dœ3ðï¾-QI›8r
01A0h: F8 04 4B DB 09 11 2E 9F                      C4   ø.KÛ...ŸB].‚ŸšËÄ
01B0h: 87 84 6E 3E 77 99 AC 46                           ‡„n>w™¬F2ß”.•.é@
01C0h: 63 91 31 49 08 1D 43 DA                           c‘1I..CÚ-C&ŽœÃB…
01D0h: 97 34 CD 10 D2 56 72 32                      9D   —4Í.ÒVr2fýzç¡+œ.
01E0h: F2 38 0D 3B 95 B1 38 38 B2 D1 C4 93 C3 EB 03 49   ò8.;•±88²ÑÄ“Ãë.I
01F0h: 65 8C A6 9D 7D DE C9 C8 F9 73 EB 7D 33 5F C6 D2   eŒ¦.}ÞÉÈùsë}3_ÆÒ
0200h: EB 1C 9D BA 00 34 E9 D6 E1 AB 3A 6D 4C 1F 8D E7   ë..º.4éÖá«:mL..ç
0210h: 41 04 A3 3C C9 30 4E B9 86 71 35 8B 9F 0E BB 8B   A.£<É0N¹†q5‹Ÿ.»‹
0220h: 0B 61 9D C1 33 3D 09 42 0F EF 59 63 A4 A8 C6 AD   .a.Á3=.B.ïYc¤¨Æ-
0230h: 39 C9 CD D6 81 A6 8B 3C 1C D6 12 45 56 6F 1A AE   9ÉÍÖ.¦‹<.Ö.EVo.®
0240h: AD 64 02 A2 F8 37 EF 71 33 84 30 67 0C A0 AD 1C   -d.¢ø7ïq3„0g. -.
0250h: 8A B9 63 B9 23 F7 6A 5E F7 30 ED F0 03 BB 27 35   Š¹c¹#÷j^÷0íð.»'5
0260h: 66 2D 1A 85 07 EC 5C EB 31 DD BA F4 6D FE 2F 6A   f-.….ì\ë1Ýºômþ/j
0270h: 63 F4 9A B6 A2 DE B1 41 04 65 A7 E2 89 F6 FF 7E   côš¶¢Þ±A.e§â‰öÿ~
0280h: 34 49 F7 30 00 00 00 00 00 00 00 00 00 00 00 00   4I÷0............
```

EntryPoint

ACM Header

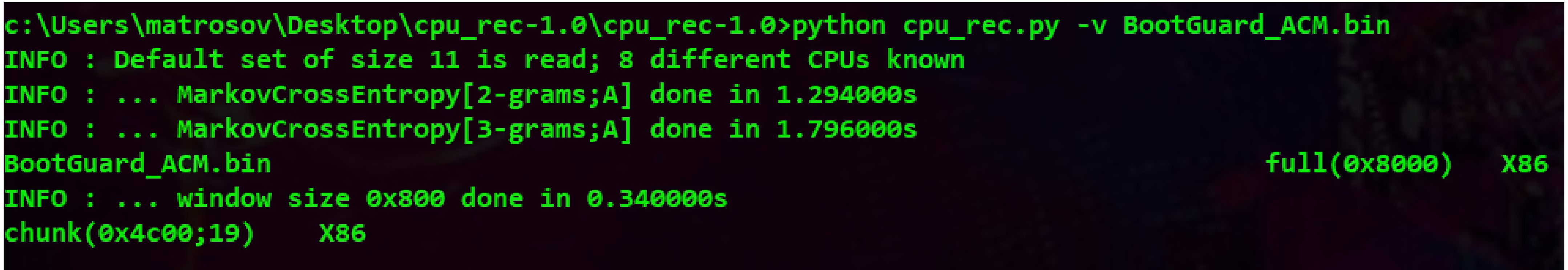
RSA Pub Key

RSA Exp

RSA Signature

Boot Guard: Authenticated Code Module (ACM)

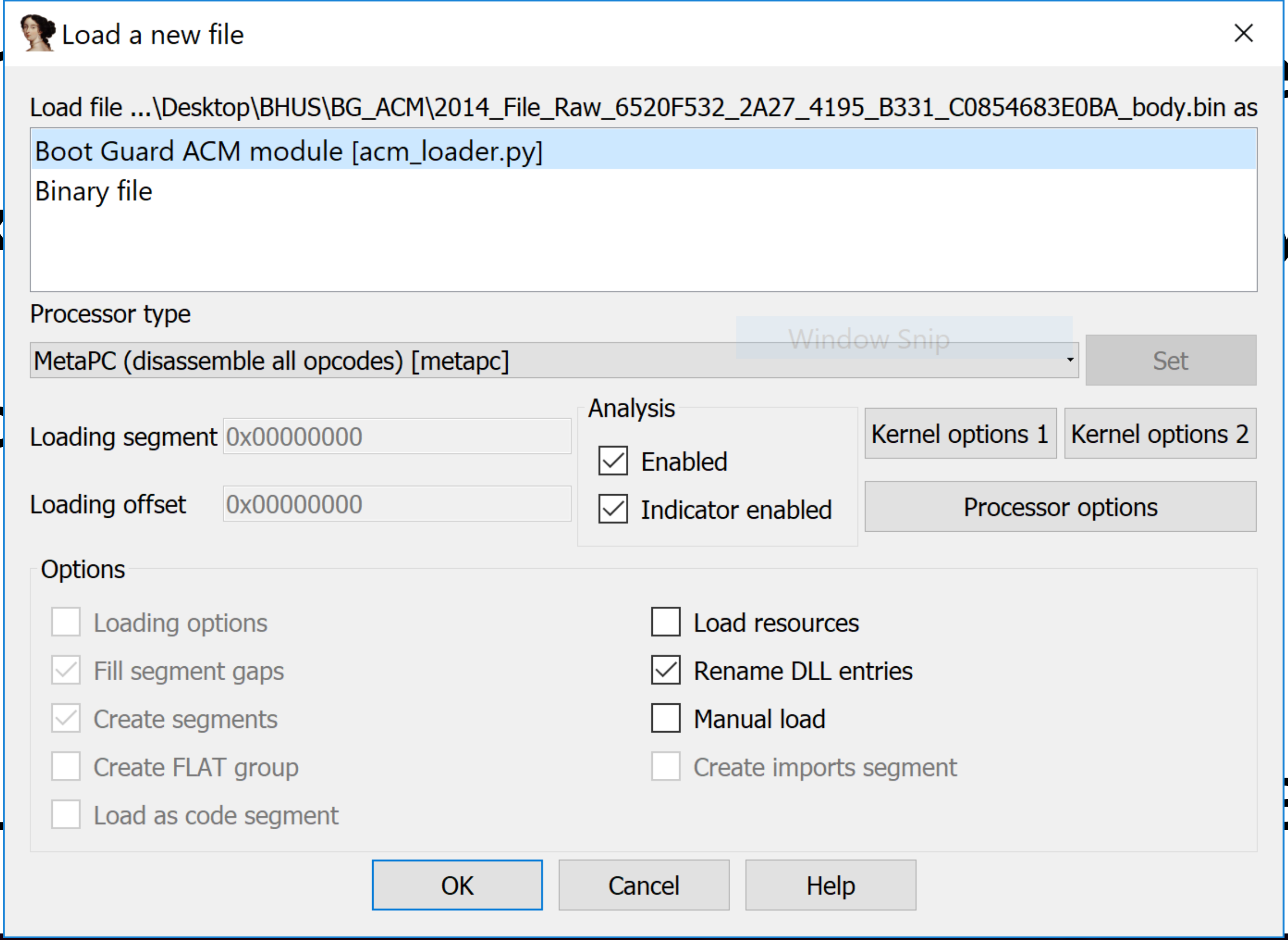
- ACM is x86 (32-bit) code developed by Intel
- ACM executes in AC-RAM (Cache-as-RAM or NEM)
- ACM has CPU and Chipset specifics
- ACM verifies Key Manifest (KEYM) + IBB (IBBM)



```
c:\Users\matrosov\Desktop\cpu_rec-1.0\cpu_rec-1.0>python cpu_rec.py -v BootGuard_ACM.bin
INFO : Default set of size 11 is read; 8 different CPUs known
INFO : ... MarkovCrossEntropy[2-grams;A] done in 1.294000s
INFO : ... MarkovCrossEntropy[3-grams;A] done in 1.796000s
BootGuard_ACM.bin                                                             full(0x8000)   X86
INFO : ... window size 0x800 done in 0.340000s
chunk(0x4c00;19)    X86
```

Boot Guar e (ACM)

- ACM is x y Intel
- ACM exec or NEM)
- ACM has
- ACM veri BB (IBBM)



Load a new file

Load file ...\Desktop\BHUS\BG_ACM\2014_File_Raw_6520F532_2A27_4195_B331_C0854683E0BA_body.bin as

Boot Guard ACM module [acm_loader.py]
Binary file

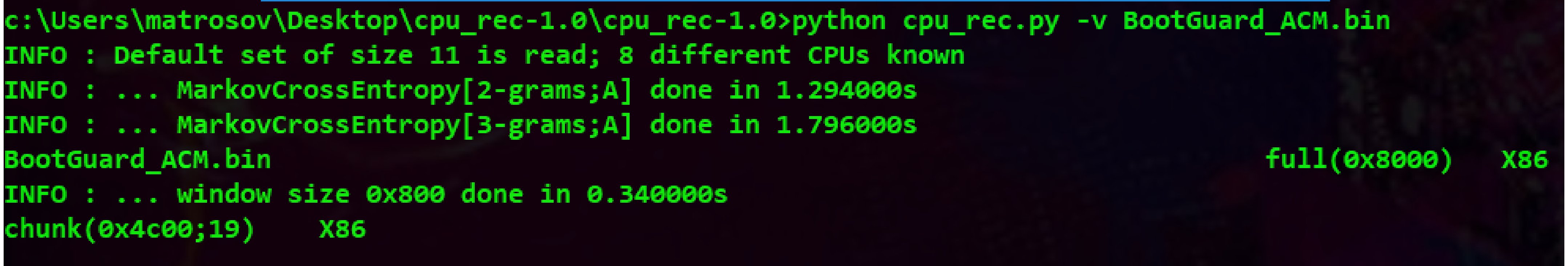
Processor type: MetaPC (disassemble all opcodes) [metapc]

Loading segment: 0x00000000

Loading offset: 0x00000000

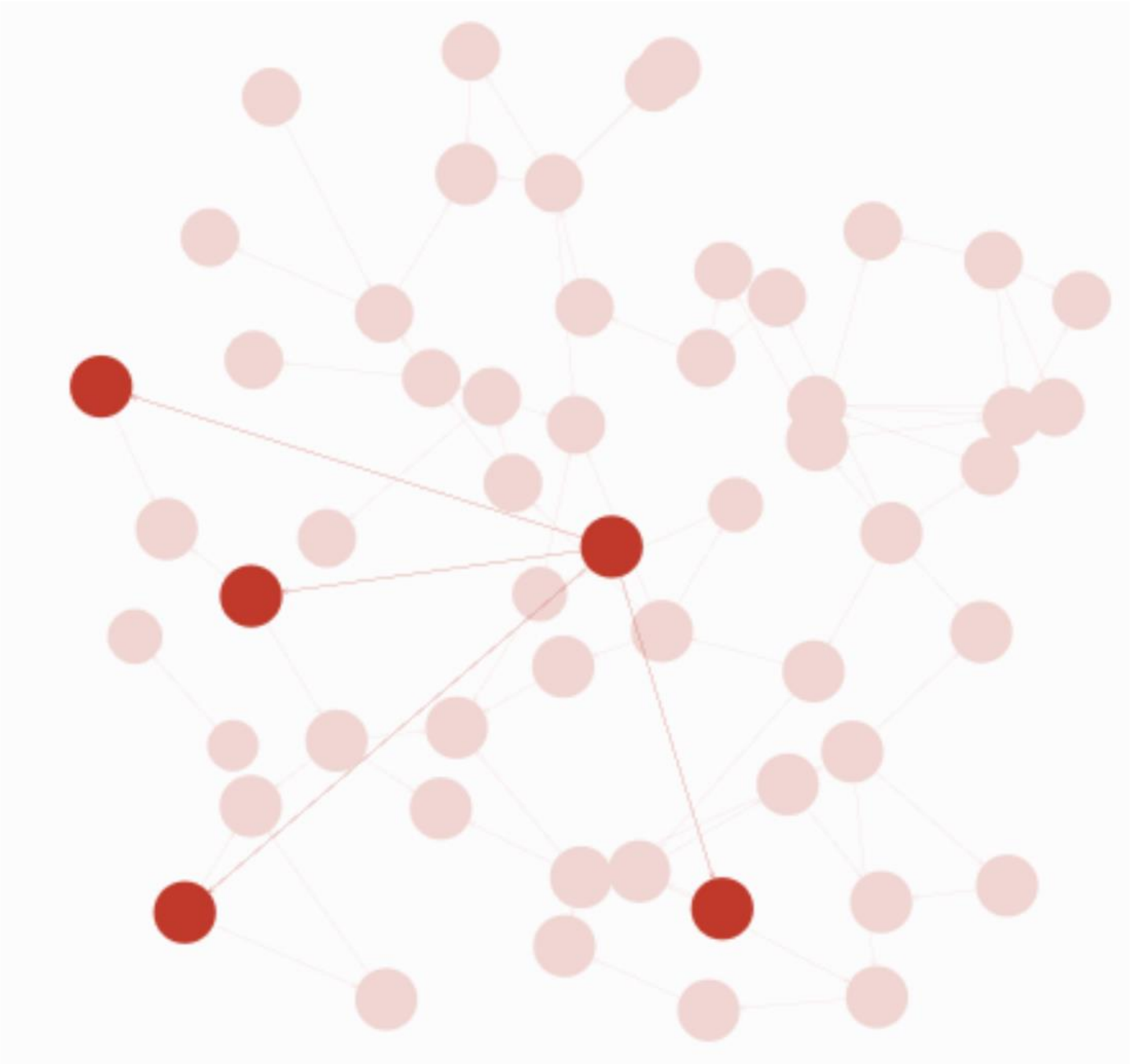
Analysis
☑ Enabled
☑ Indicator enabled

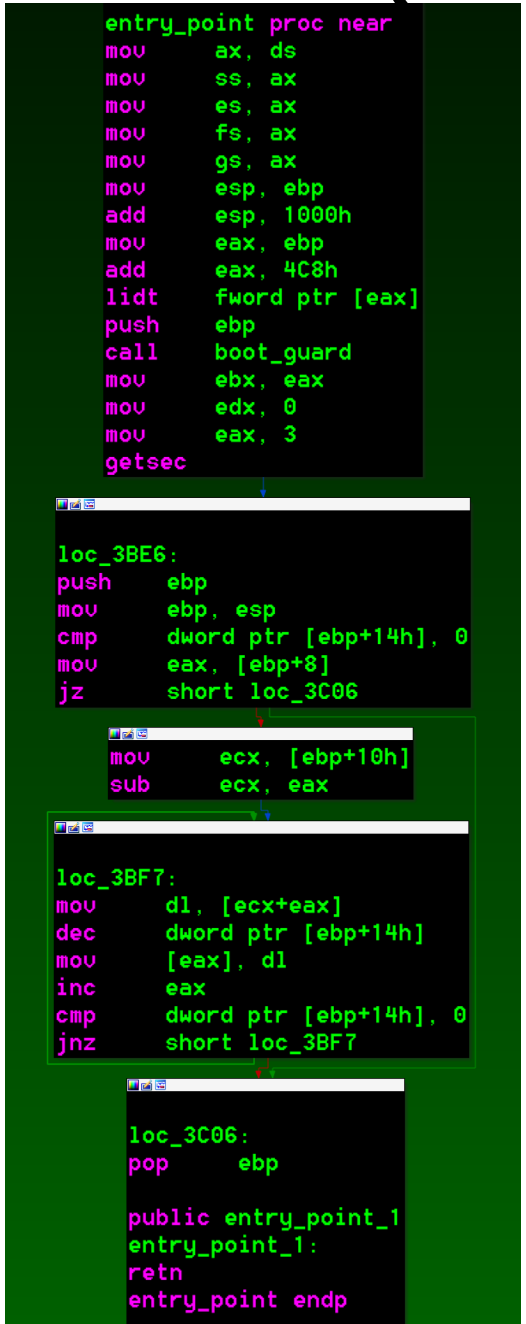
Options
☐ Loading options
☑ Fill segment gaps
☑ Create segments
☐ Create FLAT group
☐ Load as code segment
☐ Load resources
☑ Rename DLL entries
☐ Manual load
☐ Create imports segment



```
c:\Users\matrosov\Desktop\cpu_rec-1.0\cpu_rec-1.0>python cpu_rec.py -v BootGuard_ACM.bin
INFO : Default set of size 11 is read; 8 different CPUs known
INFO : ... MarkovCrossEntropy[2-grams;A] done in 1.294000s
INFO : ... MarkovCrossEntropy[3-grams;A] done in 1.796000s
BootGuard_ACM.bin                                                          full(0x8000)   X86
INFO : ... window size 0x800 done in 0.340000s
chunk(0x4c00;19)    X86
```

Boot Guard: Authenticated Code Module (ACM)





```
entry_point proc near
mov     ax, ds
mov     ss, ax
mov     es, ax
mov     fs, ax
mov     gs, ax
mov     esp, ebp
add     esp, 1000h
mov     eax, ebp
add     eax, 4C8h
lidt    fword ptr [eax]
push    ebp
call    boot_guard
mov     ebx, eax
mov     edx, 0
mov     eax, 3
getsec
```

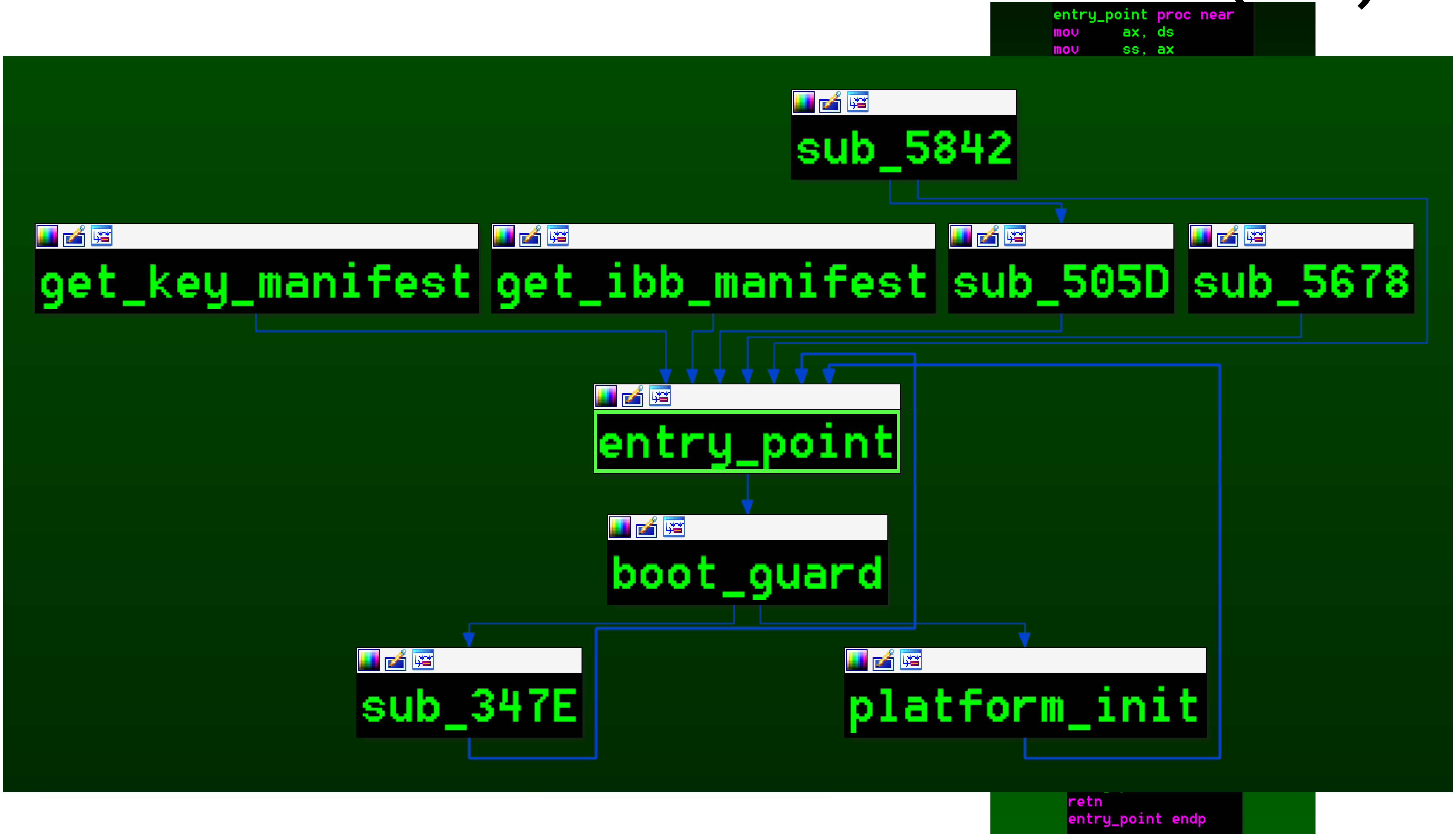
```
loc_3BE6:
push    ebp
mov     ebp, esp
cmp     dword ptr [ebp+14h], 0
mov     eax, [ebp+8]
jz      short loc_3C06
```

```
mov     ecx, [ebp+10h]
sub     ecx, eax
```

```
loc_3BF7:
mov     dl, [ecx+eax]
dec     dword ptr [ebp+14h]
mov     [eax], dl
inc     eax
cmp     dword ptr [ebp+14h], 0
jnz     short loc_3BF7
```

```
loc_3C06:
pop     ebp

public entry_point_1
entry_point_1:
retn
entry_point endp
```

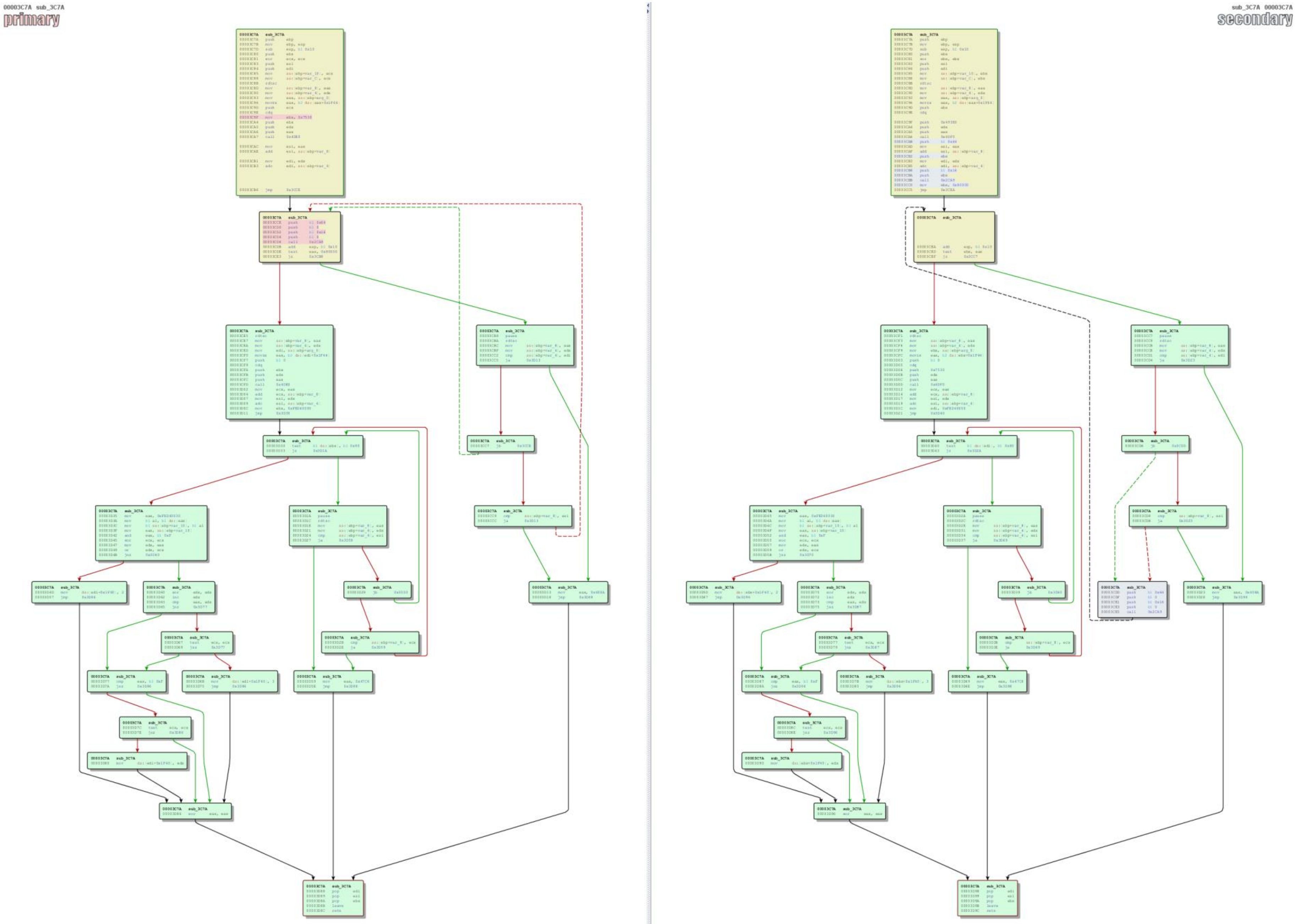
Boot Guard: Authenticated Code Module (ACM)

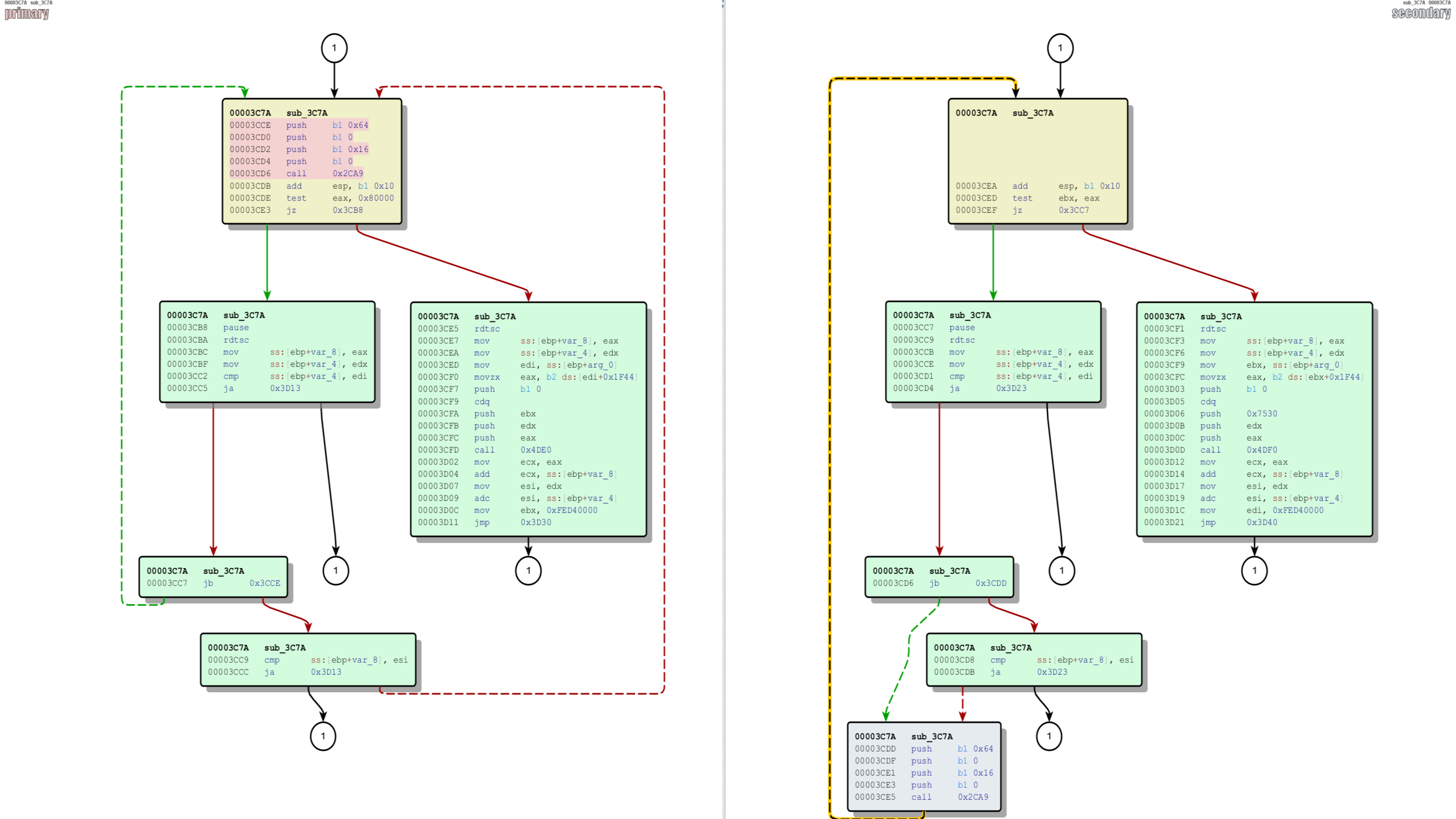


```
entry_point proc near
mov     ax, ds
mov     ss, ax
```

```
retn
entry_point endp
```

Boot Guard ACM BinDiff: Haswell vs Skylake





```
00003C7A    sub_3C7A
00003CCE    push      bl 0x64
00003CD0    push      bl 0
00003CD2    push      bl 0x16
00003CD4    push      bl 0
00003CD6    call      0x2CA9
00003CDB    add       esp, bl 0x10
00003CDE    test      eax, 0x80000
00003CE3    jz        0x3CB8
```

```
00003C7A    sub_3C7A
00003CB8    pause
00003CBA    rdtsc
00003CBC    mov       ss:[ebp+var_8], eax
00003CBF    mov       ss:[ebp+var_4], edx
00003CC2    cmp       ss:[ebp+var_4], edi
00003CC5    ja        0x3D13
```

```
00003C7A    sub_3C7A
00003CE5    rdtsc
00003CE7    mov       ss:[ebp+var_8], eax
00003CEA    mov       ss:[ebp+var_4], edx
00003CED    mov       edi, ss:[ebp+arg_0]
00003CF0    movzx     eax, b2 ds:[edi+0x1F44]
00003CF7    push      bl 0
00003CF9    cdq
00003CFA    push      ebx
00003CFB    push      edx
00003CFC    push      eax
00003CFD    call      0x4DE0
00003D02    mov       ecx, eax
00003D04    add       ecx, ss:[ebp+var_8]
00003D07    mov       esi, edx
00003D09    adc       esi, ss:[ebp+var_4]
00003D0C    mov       ebx, 0xFED40000
00003D11    jmp       0x3D30
```

```
00003C7A    sub_3C7A
00003CC7    jb        0x3CCE
```

```
00003C7A    sub_3C7A
00003CC9    cmp       ss:[ebp+var_8], esi
00003CCC    ja        0x3D13
```

```
00003C7A    sub_3C7A
00003CEA    add       esp, bl 0x10
00003CED    test      ebx, eax
00003CEF    jz        0x3CC7
```

```
00003C7A    sub_3C7A
00003CC7    pause
00003CC9    rdtsc
00003CCB    mov       ss:[ebp+var_8], eax
00003CCE    mov       ss:[ebp+var_4], edx
00003CD1    cmp       ss:[ebp+var_4], edi
00003CD4    ja        0x3D23
```

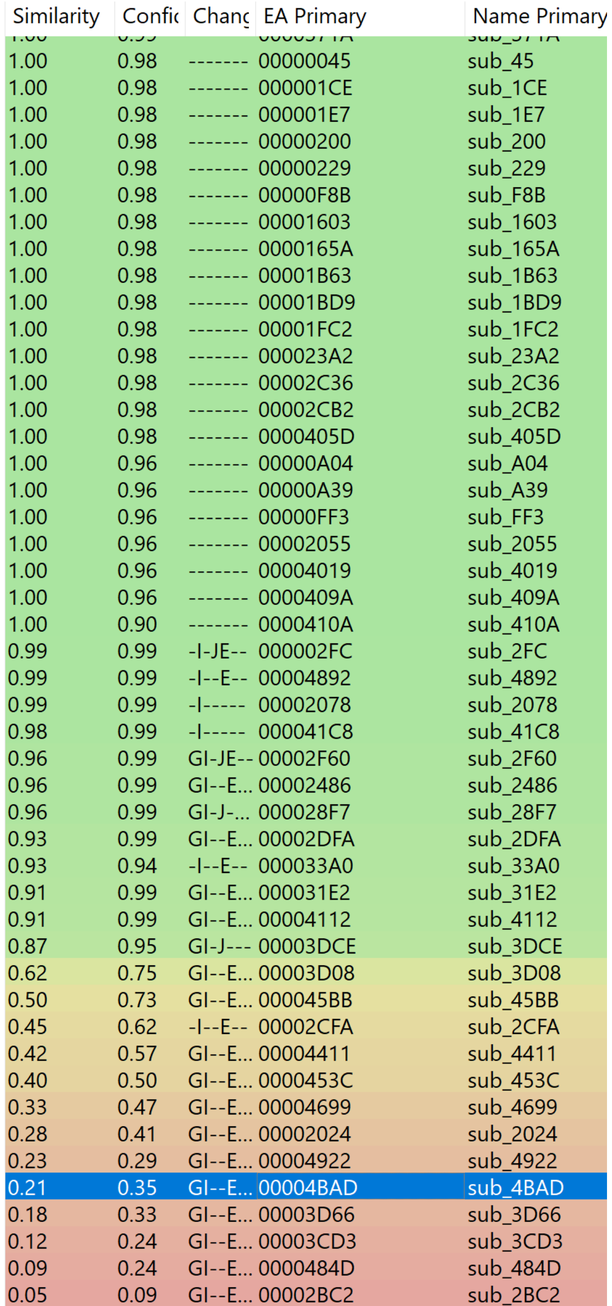
```
00003C7A    sub_3C7A
00003CF1    rdtsc
00003CF3    mov       ss:[ebp+var_8], eax
00003CF6    mov       ss:[ebp+var_4], edx
00003CF9    mov       ebx, ss:[ebp+arg_0]
00003CFC    movzx     eax, b2 ds:[ebx+0x1F44]
00003D03    push      bl 0
00003D05    cdq
00003D06    push      0x7530
00003D0B    push      edx
00003D0C    push      eax
00003D0D    call      0x4DF0
00003D12    mov       ecx, eax
00003D14    add       ecx, ss:[ebp+var_8]
00003D17    mov       esi, edx
00003D19    adc       esi, ss:[ebp+var_4]
00003D1C    mov       edi, 0xFED40000
00003D21    jmp       0x3D40
```

```
00003C7A    sub_3C7A
00003CD6    jb        0x3CDD
```

```
00003C7A    sub_3C7A
00003CD8    cmp       ss:[ebp+var_8], esi
00003CDB    ja        0x3D23
```

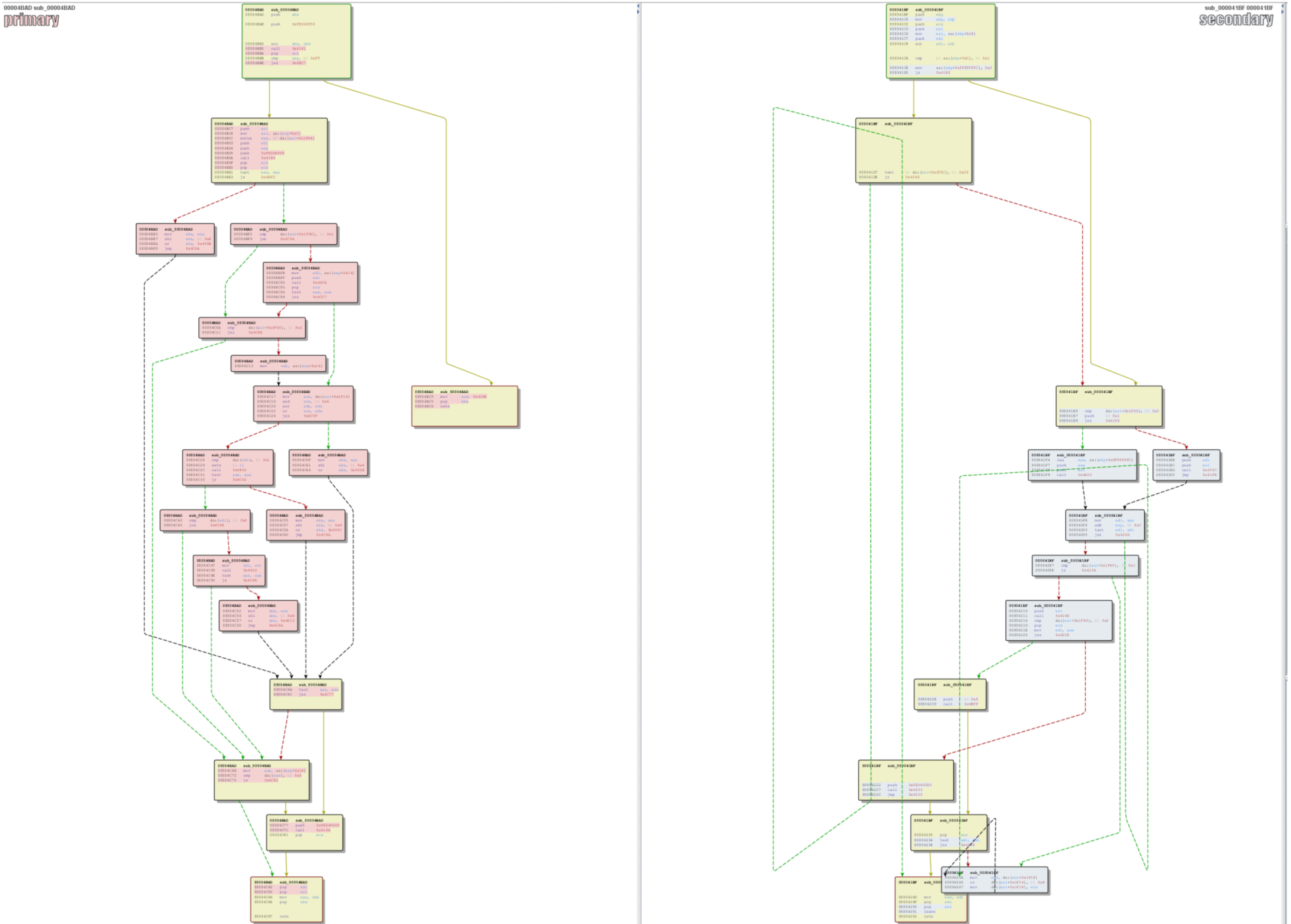
```
00003C7A    sub_3C7A
00003CDD    push      bl 0x64
00003CDF    push      bl 0
00003CE1    push      bl 0x16
00003CE3    push      bl 0
00003CE5    call      0x2CA9
```

Boot Guard ACM BinDiff: Broadwell vs Skylake



Similarity	Confic	Chang	EA Primary	Name Primary
1.00	0.99		0000371A	sub_371A
1.00	0.98	-------	00000045	sub_45
1.00	0.98	-------	000001CE	sub_1CE
1.00	0.98	-------	000001E7	sub_1E7
1.00	0.98	-------	00000200	sub_200
1.00	0.98	-------	00000229	sub_229
1.00	0.98	-------	00000F8B	sub_F8B
1.00	0.98	-------	00001603	sub_1603
1.00	0.98	-------	0000165A	sub_165A
1.00	0.98	-------	00001B63	sub_1B63
1.00	0.98	-------	00001BD9	sub_1BD9
1.00	0.98	-------	00001FC2	sub_1FC2
1.00	0.98	-------	000023A2	sub_23A2
1.00	0.98	-------	00002C36	sub_2C36
1.00	0.98	-------	00002CB2	sub_2CB2
1.00	0.98	-------	0000405D	sub_405D
1.00	0.96	-------	00000A04	sub_A04
1.00	0.96	-------	00000A39	sub_A39
1.00	0.96	-------	00000FF3	sub_FF3
1.00	0.96	-------	00002055	sub_2055
1.00	0.96	-------	00004019	sub_4019
1.00	0.96	-------	0000409A	sub_409A
1.00	0.90	-------	0000410A	sub_410A
0.99	0.99	-I-JE--	000002FC	sub_2FC
0.99	0.99	-I--E--	00004892	sub_4892
0.99	0.99	-I-----	00002078	sub_2078
0.98	0.99	-I-----	000041C8	sub_41C8
0.96	0.99	GI-JE--	00002F60	sub_2F60
0.96	0.99	GI--E...	00002486	sub_2486
0.96	0.99	GI-J-...	000028F7	sub_28F7
0.93	0.99	GI--E...	00002DFA	sub_2DFA
0.93	0.94	-I--E--	000033A0	sub_33A0
0.91	0.99	GI--E...	000031E2	sub_31E2
0.91	0.99	GI--E...	00004112	sub_4112
0.87	0.95	GI-J---	00003DCE	sub_3DCE
0.62	0.75	GI--E...	00003D08	sub_3D08
0.50	0.73	GI--E...	000045BB	sub_45BB
0.45	0.62	-I--E--	00002CFA	sub_2CFA
0.42	0.57	GI--E...	00004411	sub_4411
0.40	0.50	GI--E...	0000453C	sub_453C
0.33	0.47	GI--E...	00004699	sub_4699
0.28	0.41	GI--E...	00002024	sub_2024
0.23	0.29	GI--E...	00004922	sub_4922
0.21	0.35	GI--E...	00004BAD	sub_4BAD
0.18	0.33	GI--E...	00003D66	sub_3D66
0.12	0.24	GI--E...	00003CD3	sub_3CD3
0.09	0.24	GI--E...	0000484D	sub_484D
0.05	0.09	GI--E...	00002BC2	sub_2BC2

Boot Guard ACM BinDiff: Broadwell vs Skylake



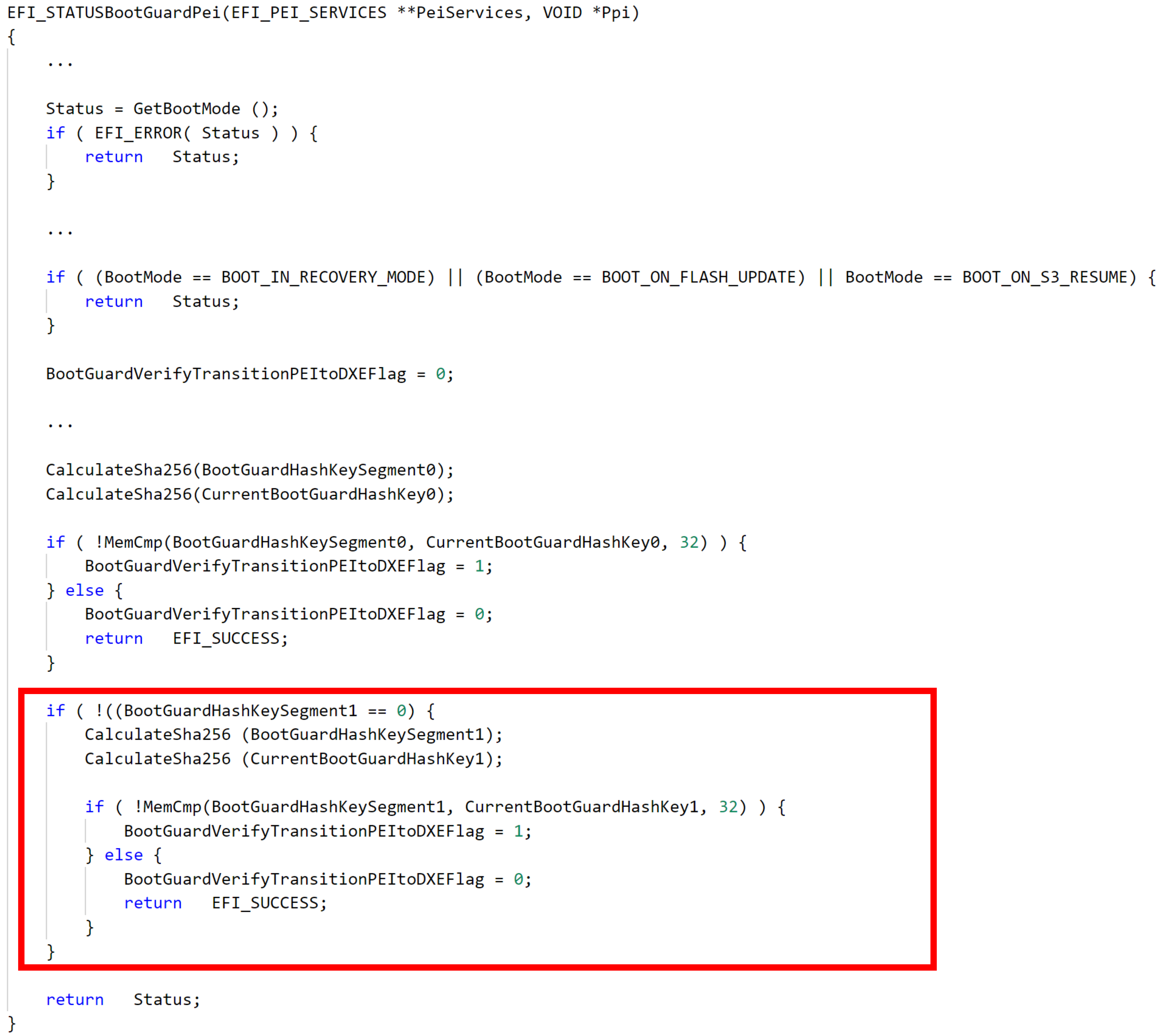
Boot Guard BIOS Components (AMI)

- **PEI**
  - **BootGuardPei** [B41956E1-7CA2-42db-9562-168389F0F066]

- **SMM**
  - **VerifyFwBootGuard** [EE89F590-A816-4ac5-B3A9-1BC759B12439]

- **DXE**
  - **BootGuardDxe** [1DB43EC9-DF5F-4cf5-AAF0-0E85DB4E149A]

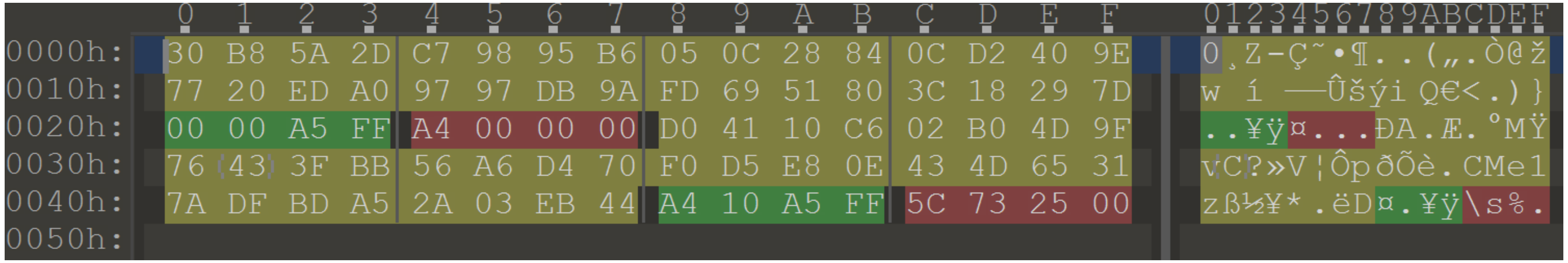
BootGuardPei Validation Flow



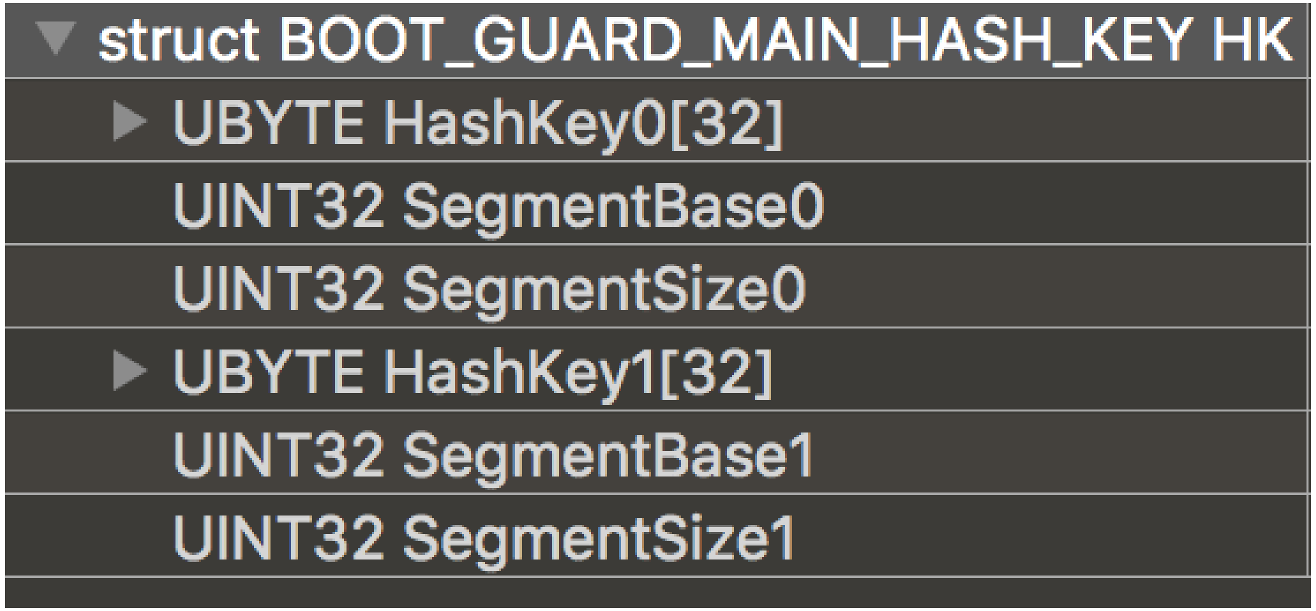
```
EFI_STATUSBootGuardPei(EFI_PEI_SERVICES **PeiServices, VOID *Ppi)
{
    ...

    Status = GetBootMode ();
    if ( EFI_ERROR( Status ) ) {
        return   Status;
    }

    ...

    if ( (BootMode == BOOT_IN_RECOVERY_MODE) || (BootMode == BOOT_ON_FLASH_UPDATE) || BootMode == BOOT_ON_S3_RESUME) {
        return   Status;
    }

    BootGuardVerifyTransitionPEItoDXEFlag = 0;

    ...

    CalculateSha256(BootGuardHashKeySegment0);
    CalculateSha256(CurrentBootGuardHashKey0);

    if ( !MemCmp(BootGuardHashKeySegment0, CurrentBootGuardHashKey0, 32) ) {
        BootGuardVerifyTransitionPEItoDXEFlag = 1;
    } else {
        BootGuardVerifyTransitionPEItoDXEFlag = 0;
        return   EFI_SUCCESS;
    }

    if ( !((BootGuardHashKeySegment1 == 0) {
        CalculateSha256 (BootGuardHashKeySegment1);
        CalculateSha256 (CurrentBootGuardHashKey1);

        if ( !MemCmp(BootGuardHashKeySegment1, CurrentBootGuardHashKey1, 32) ) {
            BootGuardVerifyTransitionPEItoDXEFlag = 1;
        } else {
            BootGuardVerifyTransitionPEItoDXEFlag = 0;
            return   EFI_SUCCESS;
        }
    }

    return   Status;
}
```

Boot Guard: PEI FV_HASH

- FV_HASH_KEY [CBC91F44-A4BC-4A5B-8696-703451D0B053]

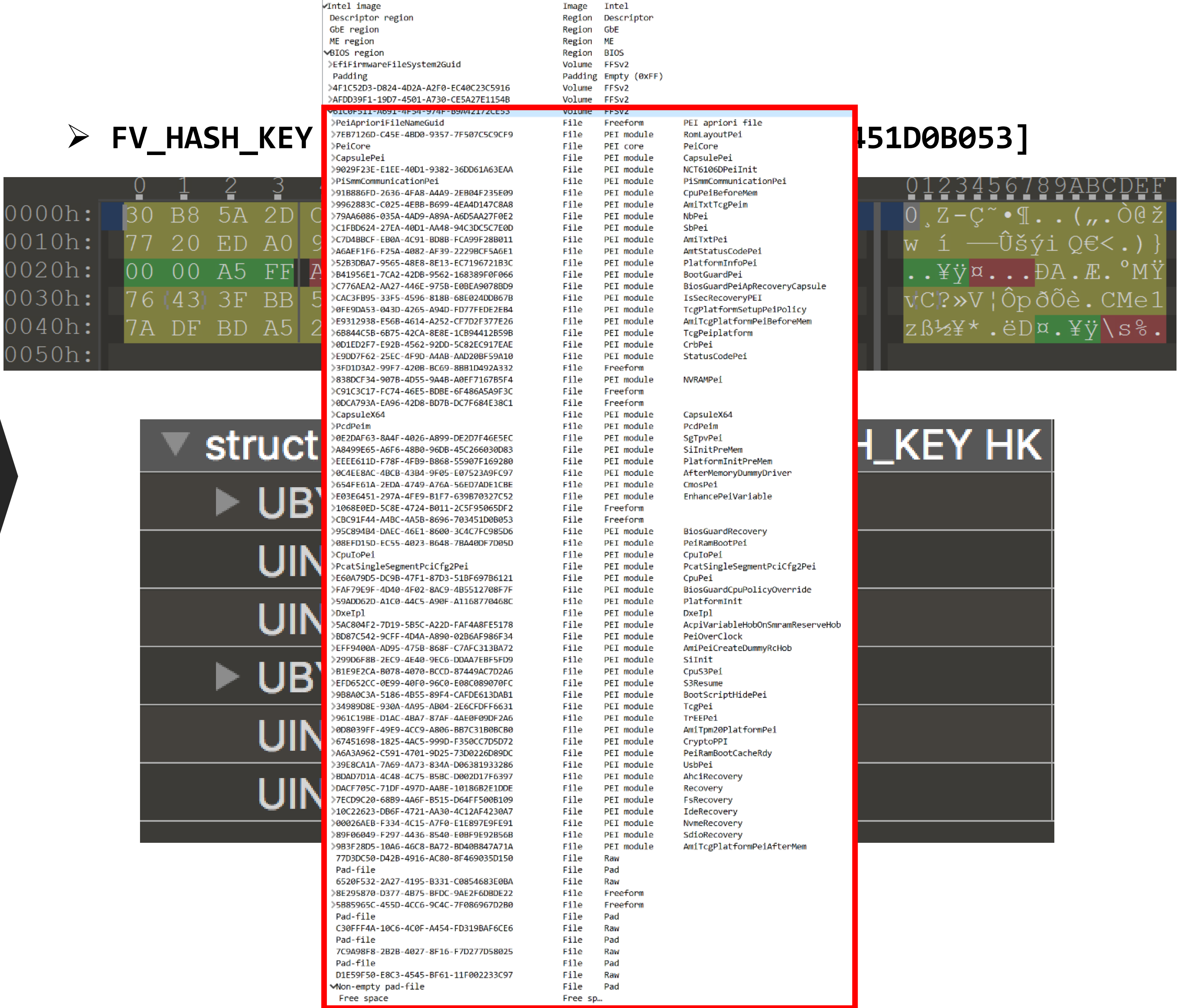


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 30 B8 5A 2D C7 98 95 B6 05 0C 28 84 0C D2 40 9E   0¸Z-Ç˜•¶..(„.Ò@ž
0010h: 77 20 ED A0 97 97 DB 9A FD 69 51 80 3C 18 29 7D   w í ——Ûšýi Q€<.)}
0020h: 00 00 A5 FF A4 00 00 00 D0 41 10 C6 02 B0 4D 9F   ..¥ÿ¤...ÐA.Æ.°MŸ
0030h: 76 43 3F BB 56 A6 D4 70 F0 D5 E8 0E 43 4D 65 31   vC?»V¦ÔpðÕè.CMe1
0040h: 7A DF BD A5 2A 03 EB 44 A4 10 A5 FF 5C 73 25 00   zß½¥*.ëD¤.¥ÿ\s%.
0050h:
```



```
▼ struct BOOT_GUARD_MAIN_HASH_KEY HK
    ▶ UBYTE HashKey0[32]
      UINT32 SegmentBase0
      UINT32 SegmentSize0
    ▶ UBYTE HashKey1[32]
      UINT32 SegmentBase1
      UINT32 SegmentSize1
```

Boot Guard: PEI FV_HASH



➢ FV_HASH_KEY 451D0B053]

```
     0  1  2  3  4                                   0123456789ABCDEF
0000h: 30 B8 5A 2D C                                 0¸Z−Ç˜•¶..(„.Ò@ž
0010h: 77 20 ED A0 9                                 w í —Ûšýi Q€<.)}
0020h: 00 00 A5 FF A                                 ..¥ÿ¤...ÐA.Æ.°MŸ
0030h: 76 43 3F BB 5                                 vC?»V¦Ôpðõè.CMe1
0040h: 7A DF BD A5 2                                 zß½¥*.ëD¤.¥ÿ\s%.
0050h:
```

```
struct                                   H_KEY HK
  UBY
  UIN
  UIN
  UBY
  UIN
  UIN
```

```
˅Intel image                                  Image    Intel
  Descriptor region                           Region   Descriptor
  GbE region                                  Region   GbE
  ME region                                   Region   ME
 ˅BIOS region                                 Region   BIOS
  >EfiFirmwareFileSystem2Guid                 Volume   FFSv2
   Padding                                    Padding  Empty (0xFF)
  >4F1C52D3-D824-4D2A-A2F0-EC40C23C5916       Volume   FFSv2
  >AFDD39F1-19D7-4501-A730-CE5A27E1154B       Volume   FFSv2
  ˅61C0F511-A691-4F54-974F-B9A42172CE53       Volume   FFSv2
   >PeiAprioriFileNameGuid                    File     Freeform      PEI apriori file
   >7EB7126D-C45E-4BD0-9357-7F507C5C9CF9      File     PEI module    RomLayoutPei
   >PeiCore                                   File     PEI core      PeiCore
   >CapsulePei                                File     PEI module    CapsulePei
   >9029F23E-E1EE-40D1-9382-36DD61A63EAA      File     PEI module    NCT6106DPeiInit
   >PiSmmCommunicationPei                     File     PEI module    PiSmmCommunicationPei
   >91B886FD-2636-4FA8-A4A9-2EB04F235E09      File     PEI module    CpuPeiBeforeMem
   >9962883C-C025-4EBB-B699-4EA4D147C8A8      File     PEI module    AmiTxtTcgPeim
   >79AA6086-035A-4AD9-A89A-A6D5AA27F0E2      File     PEI module    NbPei
   >C1FBD624-27EA-40D1-AA48-94C3DC5C7E0D      File     PEI module    SbPei
   >C7D4BBCF-EB0A-4C91-BD8B-FCA99F28B011      File     PEI module    AmiTxtPei
   >A6AEF1F6-F25A-4082-AF39-2229BCF5A6E1      File     PEI module    AmtStatusCodePei
   >52B3DBA7-9565-48E8-8E13-EC7196721B3C      File     PEI module    PlatformInfoPei
   >B41956E1-7CA2-42DB-9562-168389F0F066      File     PEI module    BootGuardPei
   >C776AEA2-AA27-446E-975B-E0BEA9078BD9      File     PEI module    BiosGuardPeiApRecoveryCapsule
   >CAC3FB95-33F5-4596-818B-68E024DDB67B      File     PEI module    IsSecRecoveryPEI
   >0FE9DA53-043D-4265-A94D-FD77FEDE2EB4      File     PEI module    TcgPlatformSetupPeiPolicy
   >E9312938-E56B-4614-A252-CF7D2F377E26      File     PEI module    AmiTcgPlatformPeiBeforeMem
   >6B844C5B-6B75-42CA-8E8E-1CB94412B59B      File     PEI module    TcgPeiplatform
   >0D1ED2F7-E92B-4562-92DD-5C82EC917EAE      File     PEI module    CrbPei
   >E9DD7F62-25EC-4F9D-A4AB-AAD20BF59A10      File     PEI module    StatusCodePei
   >3FD1D3A2-99F7-420B-BC69-8BB1D492A332      File     Freeform
   >838DCF34-907B-4D55-9A4B-A0EF7167B5F4      File     PEI module    NVRAMPei
   >C91C3C17-FC74-46E5-BDBE-6F486A5A9F3C      File     Freeform
   >0DCA793A-EA96-42D8-BD7B-DC7F684E38C1      File     Freeform
   >CapsuleX64                                File     PEI module    CapsuleX64
   >PcdPeim                                   File     PEI module    PcdPeim
   >0E2DAF63-8A4F-4026-A899-DE2D7F46E5EC      File     PEI module    SgTpvPei
   >A8499E65-A6F6-48B0-96DB-45C266030D83      File     PEI module    SiInitPreMem
   >EEEE611D-F78F-4FB9-B868-55907F169280      File     PEI module    PlatformInitPreMem
   >0C4EE8AC-4BCB-43B4-9F05-E07523A9FC97      File     PEI module    AfterMemoryDummyDriver
   >654FE61A-2EDA-4749-A76A-56ED7ADE1CBE      File     PEI module    CmosPei
   >E03E6451-297A-4FE9-B1F7-639B70327C52      File     PEI module    EnhancePeiVariable
   >1068E0ED-5C8E-4724-B011-2C5F95065DF2      File     Freeform
   >CBC91F44-A4BC-4A5B-8696-703451D0B053      File     Freeform
   >95C894B4-DAEC-46E1-8600-3C4C7FC985D6      File     PEI module    BiosGuardRecovery
   >08EFD15D-EC55-4023-B648-7BA40DF7D05D      File     PEI module    PeiRamBootPei
   >CpuIoPei                                  File     PEI module    CpuIoPei
   >PcatSingleSegmentPciCfg2Pei               File     PEI module    PcatSingleSegmentPciCfg2Pei
   >E60A79D5-DC9B-47F1-87D3-51BF697B6121      File     PEI module    CpuPei
   >FAF79E9F-4D40-4F02-8AC9-4B5512708F7F      File     PEI module    BiosGuardCpuPolicyOverride
   >59ADD62D-A1C0-44C5-A90F-A1168770468C      File     PEI module    PlatformInit
   >DxeIpl                                    File     PEI module    DxeIpl
   >5AC804F2-7D19-5B5C-A22D-FAF4A8FE5178      File     PEI module    AcpiVariableHobOnSmramReserveHob
   >BD87C542-9CFF-4D4A-A890-02B6AF986F34      File     PEI module    PeiOverClock
   >EFF9400A-AD95-475B-868F-C7AFC313BA72      File     PEI module    AmiPeiCreateDummyRcHob
   >299D6F8B-2EC9-4E40-9EC6-DDAA7EBF5FD9      File     PEI module    SiInit
   >B1E9E2CA-B078-4070-BCCD-87449AC7D2A6      File     PEI module    CpuS3Pei
   >EFD652CC-0E99-40F0-96C0-E08C089070FC      File     PEI module    S3Resume
   >9B8A0C3A-5186-4B55-89F4-CAFDE613DAB1      File     PEI module    BootScriptHidePei
   >34989D8E-930A-4A95-AB04-2E6CFDFF6631      File     PEI module    TcgPei
   >961C19BE-D1AC-4BA7-87AF-4AE0F09DF2A6      File     PEI module    TrEEPei
   >0D8039FF-49E9-4CC9-A806-BB7C31B0BCB0      File     PEI module    AmiTpm20PlatformPei
   >67451698-1825-4AC5-999D-F350CC7D5D72      File     PEI module    CryptoPPI
   >A6A3A962-C591-4701-9D25-73D0226D89DC      File     PEI module    PeiRamBootCacheRdy
   >39E8CA1A-7A69-4A73-834A-D06381933286      File     PEI module    UsbPei
   >BDAD7D1A-4C48-4C75-B5BC-D002D17F6397      File     PEI module    AhciRecovery
   >DACF705C-71DF-497D-AABE-10186B2E1DDE      File     PEI module    Recovery
   >7ECD9C20-68B9-4A6F-B515-D64FF500B109      File     PEI module    FsRecovery
   >10C22623-DB6F-4721-AA30-4C12AF4230A7      File     PEI module    IdeRecovery
   >00026AEB-F334-4C15-A7F0-E1E897E9FE91      File     PEI module    NvmeRecovery
   >89F06049-F297-4436-8540-E0BF9E92B56B      File     PEI module    SdioRecovery
   >9B3F28D5-10A6-46C8-BA72-BD40B847A71A      File     PEI module    AmiTcgPlatformPeiAfterMem
    77D3DC50-D42B-4916-AC80-8F469035D150      File     Raw
    Pad-file                                  File     Pad
    6520F532-2A27-4195-B331-C0854683E0BA      File     Raw
   >8E295870-D377-4B75-BFDC-9AE2F6DBDE22      File     Freeform
   >5B85965C-455D-4CC6-9C4C-7F086967D2B0      File     Freeform
    Pad-file                                  File     Pad
    C30FFF4A-10C6-4C0F-A454-FD319BAF6CE6      File     Raw
    Pad-file                                  File     Pad
    7C9A98F8-2B2B-4027-8F16-F7D277D58025      File     Raw
    Pad-file                                  File     Pad
    D1E59F50-E8C3-4545-BF61-11F002233C97      File     Raw
   ˅Non-empty pad-file                        File     Pad
     Free space                               Free sp…
```

VerifyFwBootGuard SMM Validation Flow
(Intel ME communications over HECI)

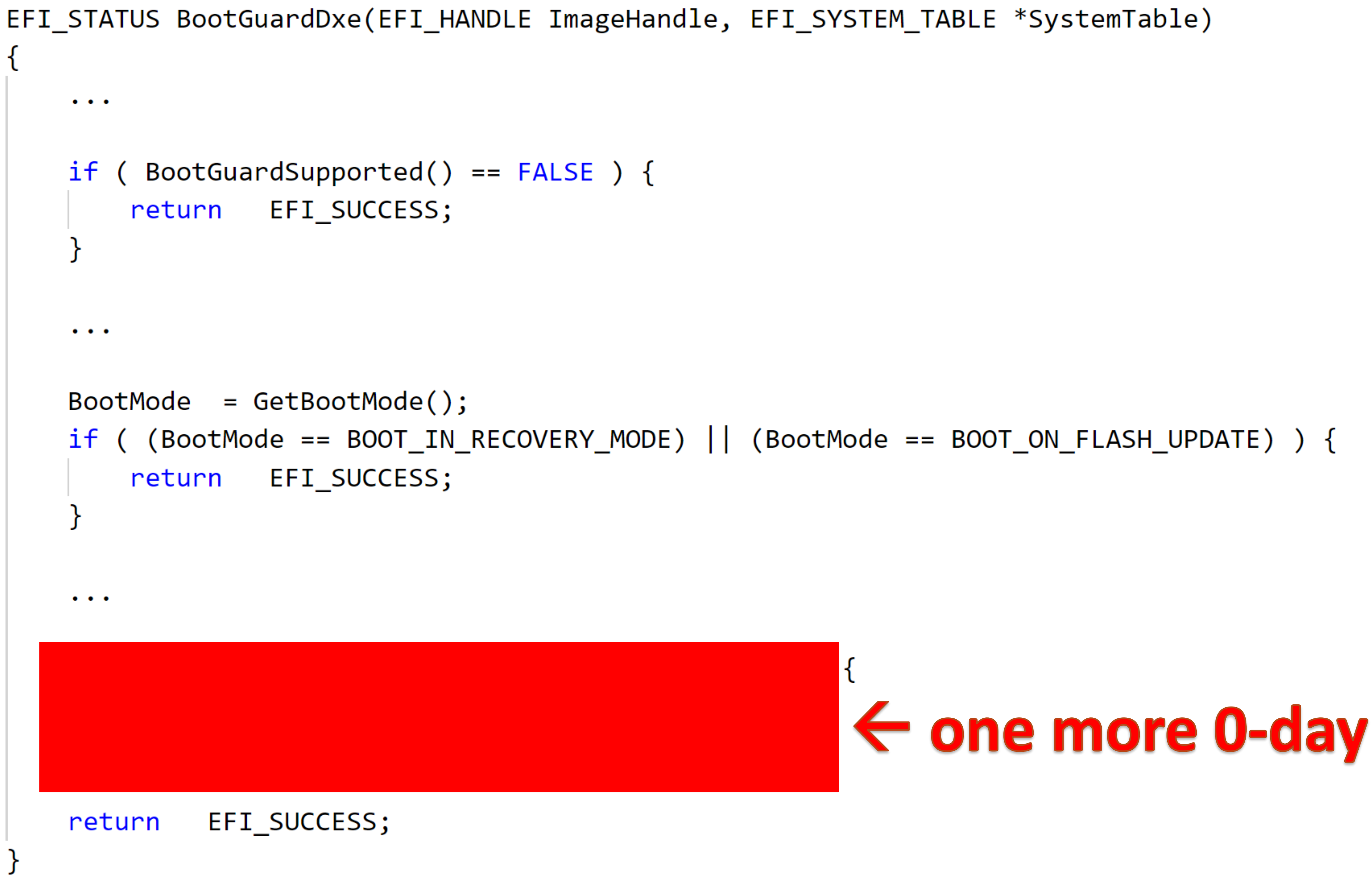
- Find and Verify ACM
  - Verify ACM SVN

- Find and Verify Key Manifest (KM)
  - Verify KM SVN

- Find and Verify Boot Policy Manifest (BPM)
  - Verify BPM SVN

- If something wrong return EFI_SECURITY_VIOLATION

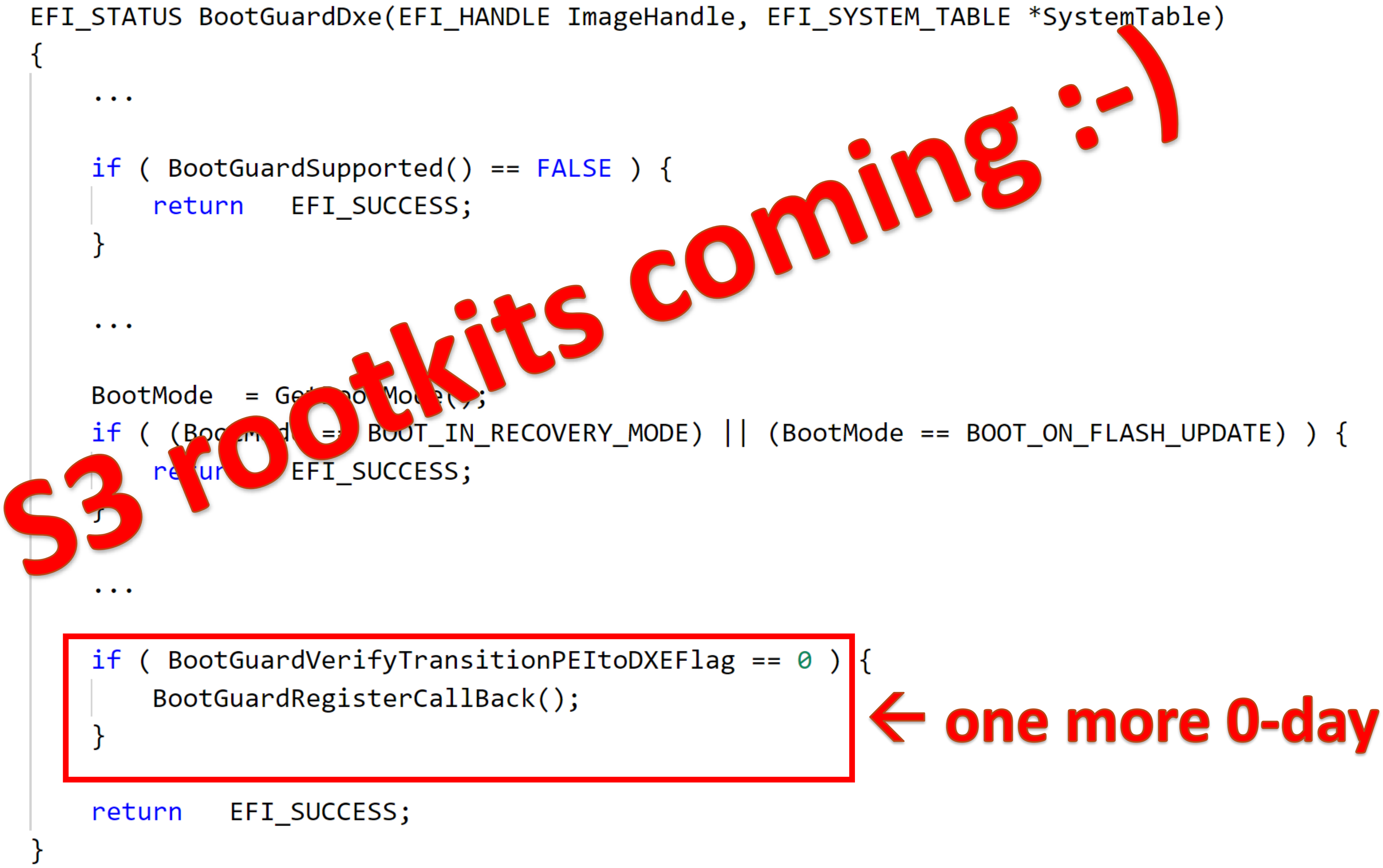
BootGuardDxe Validation Flow



```
EFI_STATUS BootGuardDxe(EFI_HANDLE ImageHandle, EFI_SYSTEM_TABLE *SystemTable)
{
    ...

    if ( BootGuardSupported() == FALSE ) {
        return   EFI_SUCCESS;
    }

    ...

    BootMode  = GetBootMode();
    if ( (BootMode == BOOT_IN_RECOVERY_MODE) || (BootMode == BOOT_ON_FLASH_UPDATE) ) {
        return   EFI_SUCCESS;
    }

    ...

   [redacted] {

    return   EFI_SUCCESS;
}
```

← one more 0-day bug?

BootGuardDxe Validation Flow



```
EFI_STATUS BootGuardDxe(EFI_HANDLE ImageHandle, EFI_SYSTEM_TABLE *SystemTable)
{
    ...

    if ( BootGuardSupported() == FALSE ) {
        return   EFI_SUCCESS;
    }

    ...

    BootMode   = GetBootMode();
    if ( (BootMode == BOOT_IN_RECOVERY_MODE) || (BootMode == BOOT_ON_FLASH_UPDATE) ) {
        return   EFI_SUCCESS;
    }

    ...

    if ( BootGuardVerifyTransitionPEItoDXEFlag == 0 ) {
        BootGuardRegisterCallBack();
    }

    return   EFI_SUCCESS;
}
```

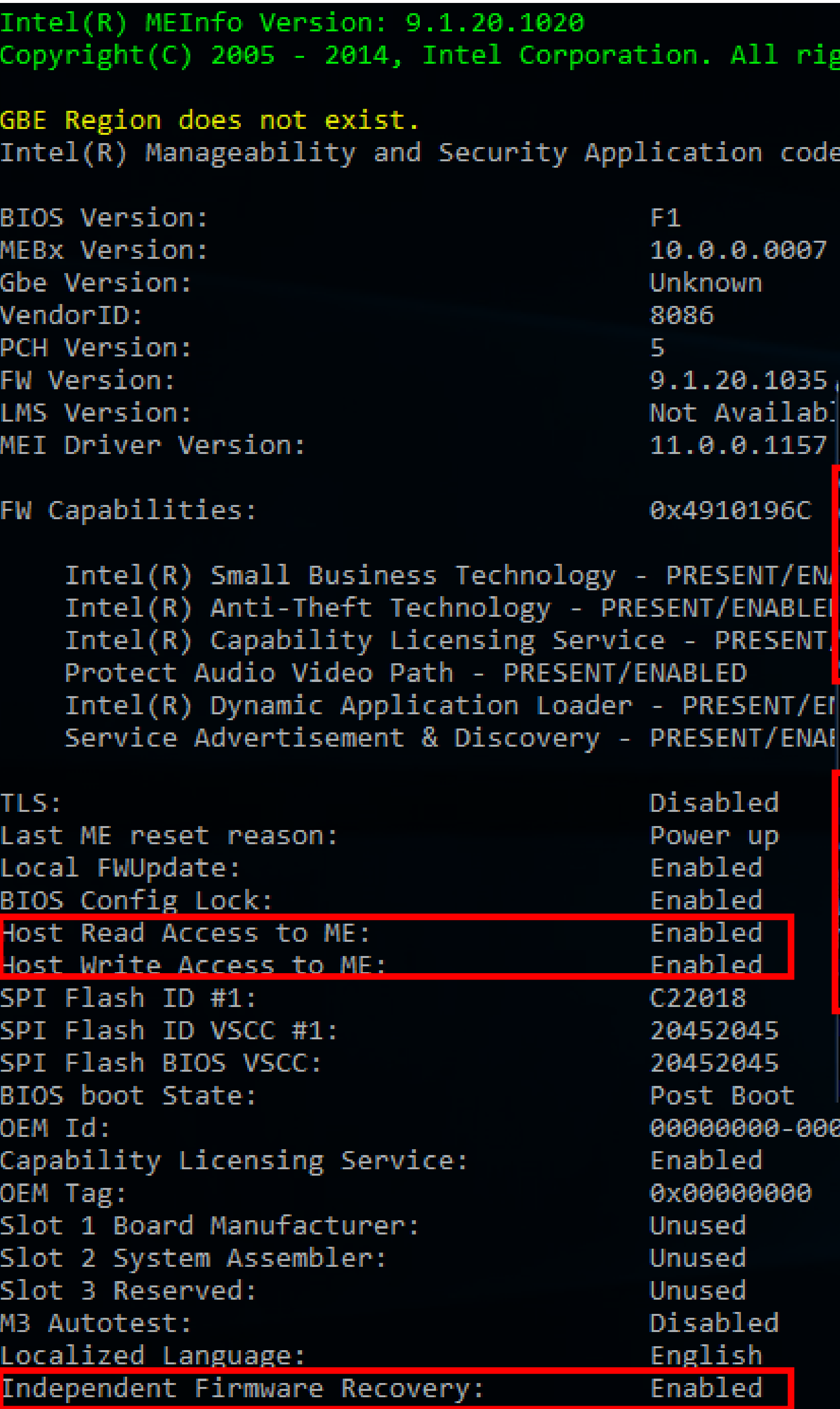
S3 rootkits coming :-)

← one more 0-day bug?

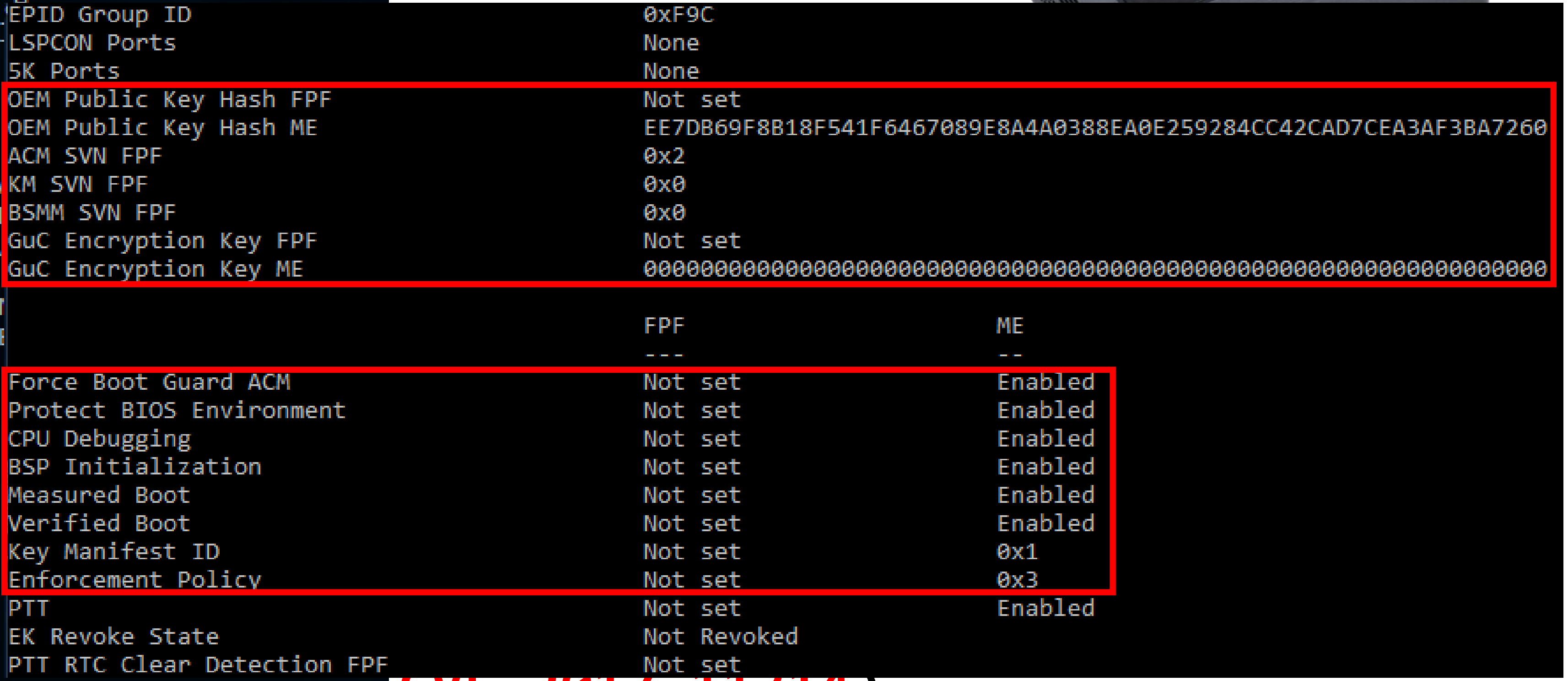
Target Platform

- Gigabyte (GB-BSi7HA-6500)
  - ✓ Intel 6th generation Core i7 CPU (Skylake) with vPro
  - ✓ Intel Boot Guard – ENABLED
  - ✓ Intel BIOS Guard – NOT ENABLED

- Vulnerabilities
  - ✓ Host Write/Read Access to ME (CVE-2017-11314)
  - ✓ Intel Boot Guard Configuration not Locked (CVE-2017-11313)



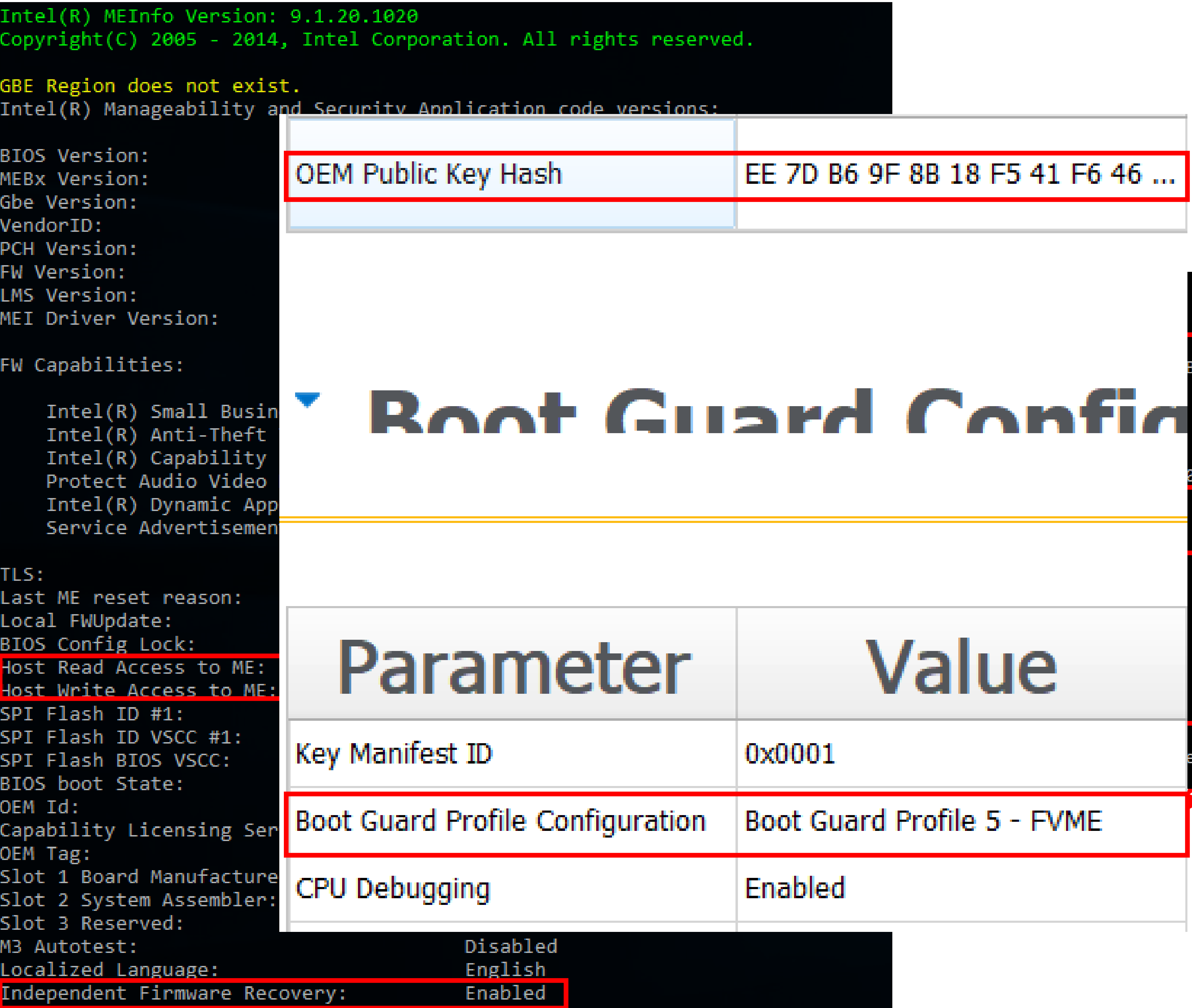
```
Intel(R) MEInfo Version: 9.1.20.1020
Copyright(C) 2005 - 2014, Intel Corporation. All rights reserved.

GBE Region does not exist.
Intel(R) Manageability and Security Application code versions:

BIOS Version:                           F1
MEBx Version:                           10.0.0.0007
Gbe Version:                            Unknown
VendorID:                               8086
PCH Version:                            5
FW Version:                             9.1.20.1035 H
LMS Version:                            Not Availab
MEI Driver Version:                     11.0.0.1157

FW Capabilities:                        0x4910196C

    Intel(R) Small Business Technology - PRESENT/EN
    Intel(R) Anti-Theft Technology - PRESENT/ENABLE
    Intel(R) Capability Licensing Service - PRESENT
    Protect Audio Video Path - PRESENT/ENABLED
    Intel(R) Dynamic Application Loader - PRESENT/E
    Service Advertisement & Discovery - PRESENT/ENA

TLS:                                    Disabled
Last ME reset reason:                   Power up
Local FWUpdate:                         Enabled
BIOS Config Lock:                       Enabled
Host Read Access to ME:                 Enabled
Host Write Access to ME:                Enabled
SPI Flash ID #1:                        C22018
SPI Flash ID VSCC #1:                   20452045
SPI Flash BIOS VSCC:                    20452045
BIOS boot State:                        Post Boot
OEM Id:                                 00000000-0000-0000-0000-000000000000
Capability Licensing Service:           Enabled
OEM Tag:                                0x00000000
Slot 1 Board Manufacturer:              Unused
Slot 2 System Assembler:                Unused
Slot 3 Reserved:                        Unused
M3 Autotest:                            Disabled
Localized Language:                     English
Independent Firmware Recovery:          Enabled
```



```
EPID Group ID                             0xF9C
LSPCON Ports                              None
5K Ports                                  None
OEM Public Key Hash FPF                   Not set
OEM Public Key Hash ME                    EE7DB69F8B18F541F6467089E8A4A0388EA0E259284CC42CAD7CEA3AF3BA7260
ACM SVN FPF                               0x2
KM SVN FPF                                0x0
BSMM SVN FPF                              0x0
GuC Encryption Key FPF                    Not set
GuC Encryption Key ME                     0000000000000000000000000000000000000000000000000000000000000000

                                          FPF                       ME
                                          ---                       --
Force Boot Guard ACM                      Not set                   Enabled
Protect BIOS Environment                  Not set                   Enabled
CPU Debugging                             Not set                   Enabled
BSP Initialization                        Not set                   Enabled
Measured Boot                             Not set                   Enabled
Verified Boot                             Not set                   Enabled
Key Manifest ID                           Not set                   0x1
Enforcement Policy                        Not set                   0x3
PTT                                       Not set                   Enabled
EK Revoke State                           Not Revoked
PTT RTC Clear Detection FPF               Not set
```

CVE-2017-11314)

not Locked (CVE-2017-11313)

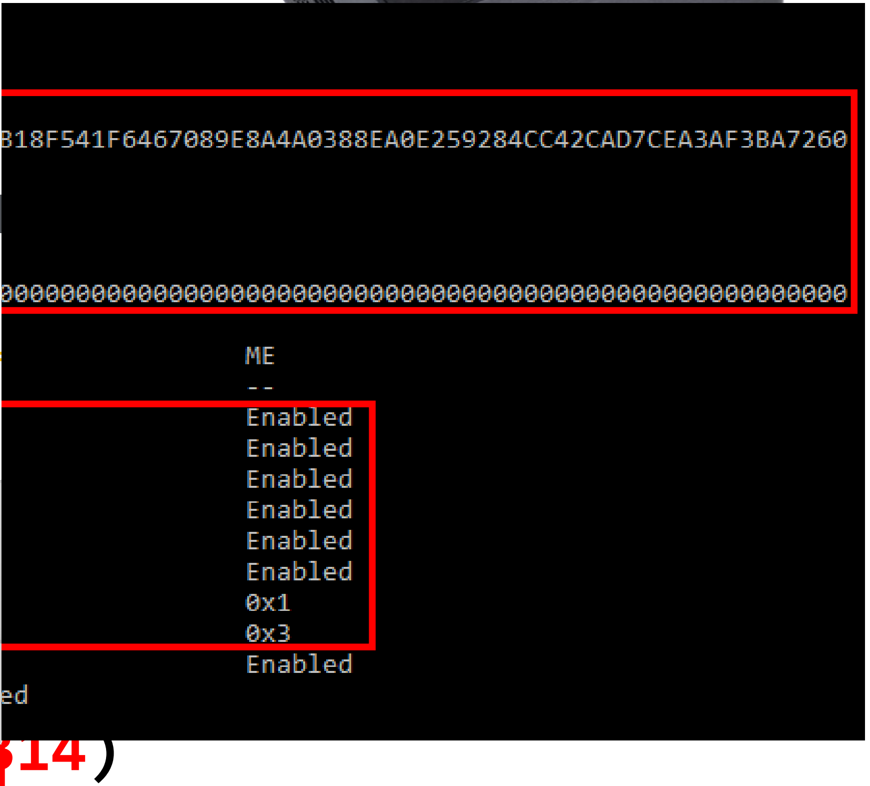


```
Intel(R) MEInfo Version: 9.1.20.1020
Copyright(C) 2005 - 2014, Intel Corporation. All rights reserved.

GBE Region does not exist.
Intel(R) Manageability and Security Application code versions:

BIOS Version:
MEBx Version:
Gbe Version:
VendorID:
PCH Version:
FW Version:
LMS Version:
MEI Driver Version:

FW Capabilities:

    Intel(R) Small Busin
    Intel(R) Anti-Theft
    Intel(R) Capability
    Protect Audio Video
    Intel(R) Dynamic App
    Service Advertisemen

TLS:
Last ME reset reason:
Local FWUpdate:
BIOS Config Lock:
Host Read Access to ME:
Host Write Access to ME:
SPI Flash ID #1:
SPI Flash ID VSCC #1:
SPI Flash BIOS VSCC:
BIOS boot State:
OEM Id:
Capability Licensing Ser
OEM Tag:
Slot 1 Board Manufacture
Slot 2 System Assembler:
Slot 3 Reserved:
M3 Autotest:                            Disabled
Localized Language:                     English
Independent Firmware Recovery:          Enabled
```

OEM Public Key Hash	EE 7D B6 9F 8B 18 F5 41 F6 46 ...

Boot Guard Config

Parameter	Value
Key Manifest ID	0x0001
Boot Guard Profile Configuration	Boot Guard Profile 5 - FVME
CPU Debugging	Enabled

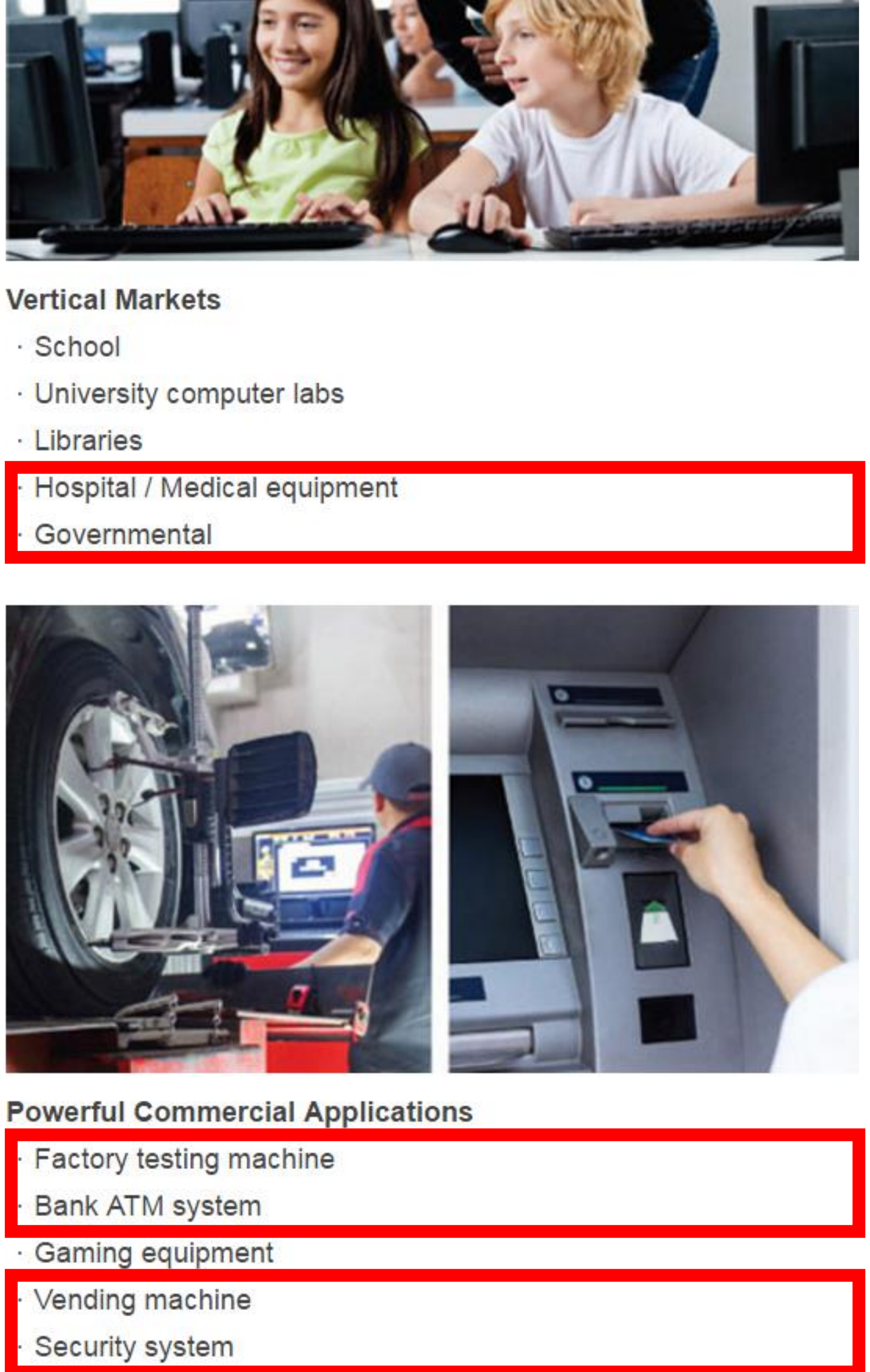


```
B18F541F6467089E8A4A0388EA0E259284CC42CAD7CEA3AF3BA7260


0000000000000000000000000000000000000000000000000000000

              ME
              --
              Enabled
              Enabled
              Enabled
              Enabled
              Enabled
              Enabled
              0x1
              0x3
              Enabled
ed
```

314)

(CVE-2017-11313)

copy from Gigabyte official website



Vertical Markets

- School
- University computer labs
- Libraries
- Hospital / Medical equipment
- Governmental

Powerful Commercial Applications

- Factory testing machine
- Bank ATM system
- Gaming equipment
- Vending machine
- Security system

Five steps to bypass Boot Guard

1) **Modify UEFI firmware update image with rootkit/implant**

   or

   Disable Intel Boot Guard

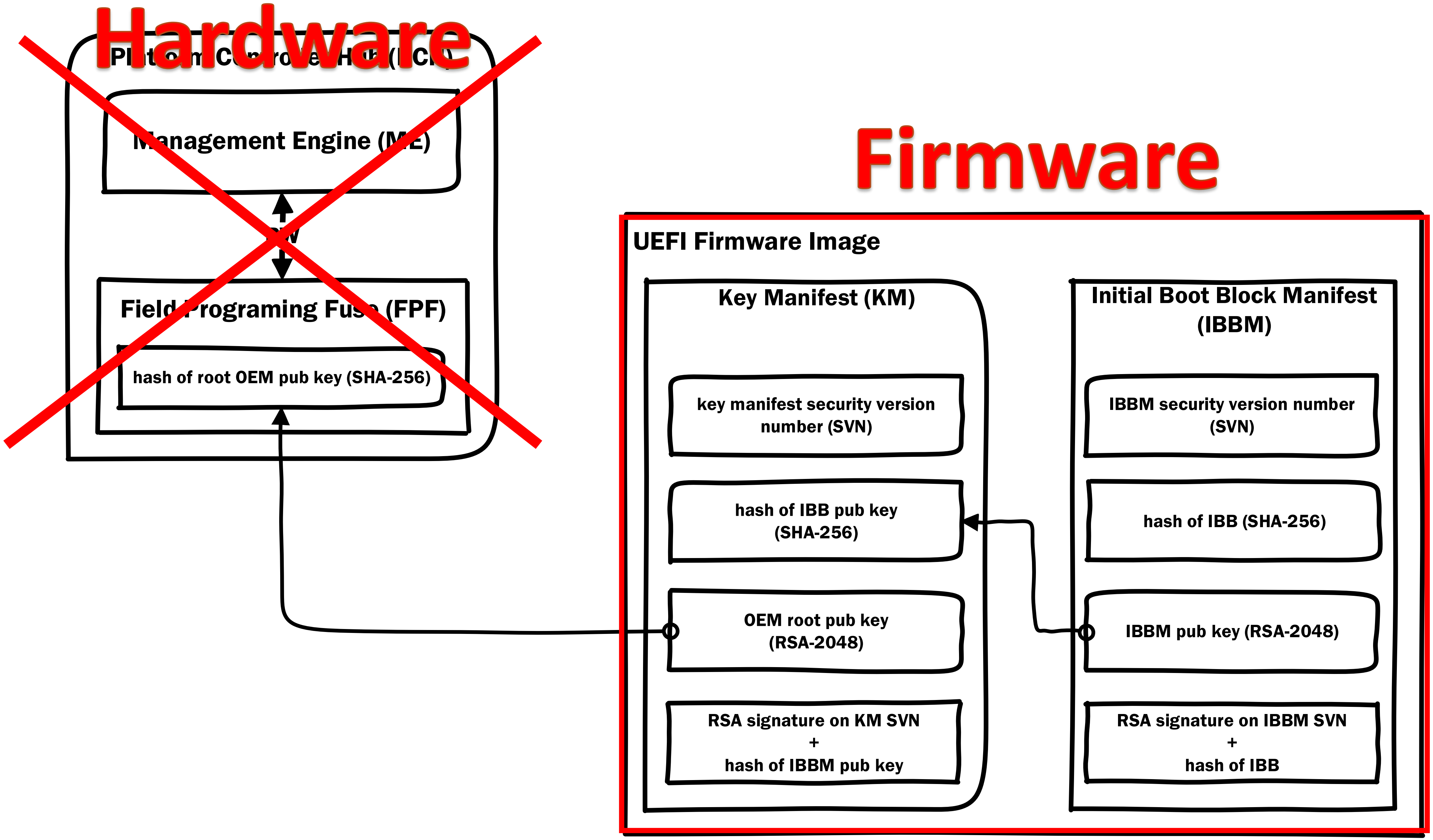
2) **Initial Boot Block (IBB)**
   - ✓ Recalculate signature on 2048-bit RSA key pair for IBB
   - ✓ Modify IBB manifest inside UEFI firmware update file
   - ✓ Recalculate signature for IBB manifest with different 2048-bit RSA key pair

3) **Modify Root Key manifest**
   - ✓ Recalculate SHA256 hash of the public key from Root Key Manifest

4) **Modify ME region with new key (CVE-2017-11314)**
   - ✓ Modify Boot Guard configuration with active verified boot policy

5) **Lock Boot Guard configuration with by FPF (CVE-2017-11313)**

Boot Guard: Chain of Trust



Hardware

Platform Controller Hub (PCH)

Management Engine (ME)

Field Programing Fuse (FPF)

hash of root OEM pub key (SHA-256)

Firmware

UEFI Firmware Image

Key Manifest (KM)

key manifest security version number (SVN)

hash of IBB pub key (SHA-256)

OEM root pub key (RSA-2048)

RSA signature on KM SVN + hash of IBBM pub key

Initial Boot Block Manifest (IBBM)

IBBM security version number (SVN)

hash of IBB (SHA-256)

IBBM pub key (RSA-2048)

RSA signature on IBBM SVN + hash of IBB

Intel Statement

“Intel provides a 6th and 7th generation Core Platforms Secure Configuration Specification, which covers how to securely configure the platform. Additionally, Intel makes available a utility that our ecosystem partners can use to test and identify potential configuration issues.”

Gigabyte Statement

“For FPF issue, we discuss with internal the BIOS don’t need any update but we will add ME Lock tool to our production process soon, the new production ship will include ME Lock.”

Intel BIOS Guard

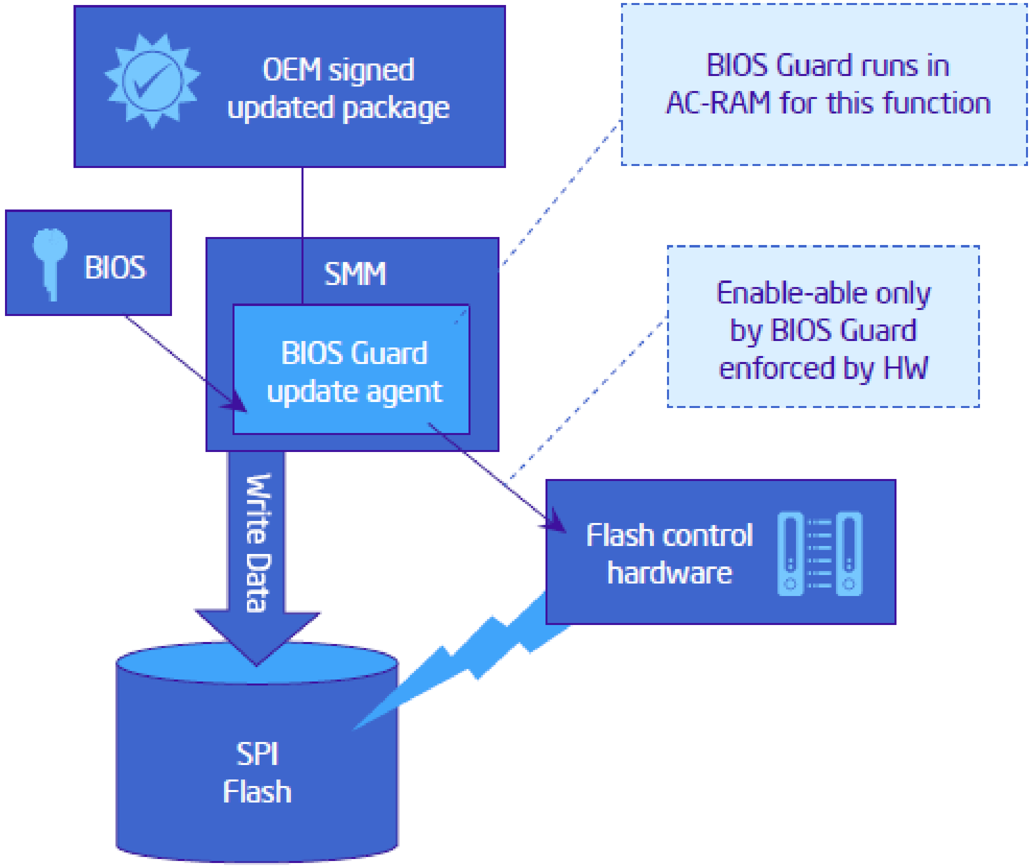
Intel BIOS Guard

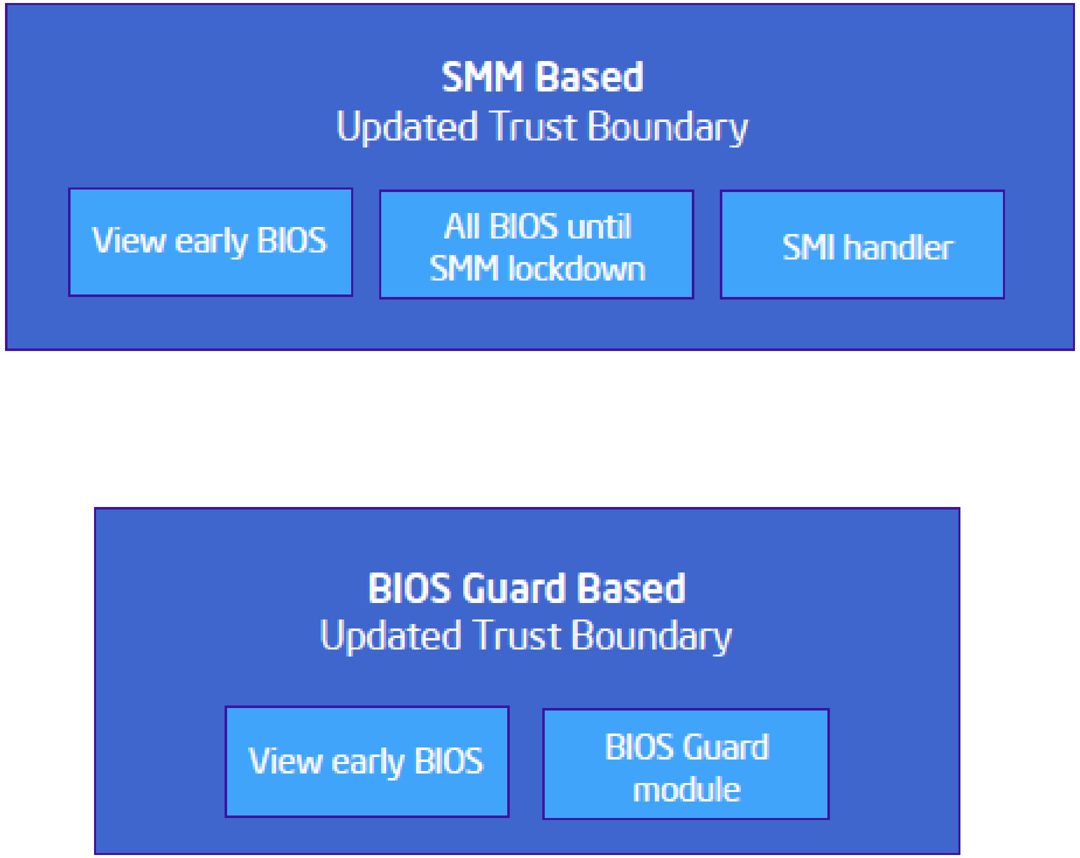
- ➢ **Armoring SPI Flash access**
  - ✓ Access controlled by BIOS Guard ACM
  - ✓ Attack Surface = Firmware

- ➢ **BIOS update authentication**
  - ✓ Root of Trust = Hardware -> Trusted Platform Module (TPM)
  - ✓ Attack Surface = Firmware

- ➢ **Verified Boot -> since 2013**
  - ✓ Root of Trust = Hardware -> Field Programming Fuse (FPF)->Locked
  - ✓ Attack Surface = Firmware + Hardware

Demystifying Intel BIOS Guard


OEM signed updated package
BIOS Guard runs in AC-RAM for this function
BIOS
SMM
BIOS Guard update agent
Enable-able only by BIOS Guard enforced by HW
Write Data
Flash control hardware
SPI Flash



http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/security-technologies-4th-gen-core-retail-paper.pdf

Boot Guard BIOS Components (AMI)

- **PEI**
  - **BiosGuardPeiApRecoveryCapsule** [C776AEA2-AA27-446e-975B-E0BEA9078BD9]
  - **BiosGuardRecovery** [95C894B4-DAEC-46E1-8600-3C4C7FC985D6]
  - **BiosGuardCpuPolicyOverride** [FAF79E9F-4D40-4F02-8AC9-4B5512708F7F]

- **SMM**
  - **BiosGuardSmm** [44FE07D3-C312-4ad4-B892-269AB069C8E1]
  - **BiosGuardServices** [6D4BAA0B-F431-4370-AF19-99D6209239F6]

- **DXE**
  - **BiosGuardDxe** [6D1D13B3-8874-4e92-AED5-22FC7C4F7391]
  - **BiosGuardNvs** [17565311-4B71-4340-88AA-DC9F4422E53A]

Boot Guard BIOS Components (AMI)

- **PEI**
  - **BiosGuardPeiApRecoveryCapsule – AMI Capsule Update Validation**
  - **BiosGuardRecovery – Recovery Update Image parser**
  - **BiosGuardCpuPolicyOverride**
    - ✓ **Find Public Key**
    - ✓ **Find and Load BIOS Guard ACM**
- **SMM**
  - **BiosGuardSmm - Recovery SMI Handlers**
- **DXE**
  - **BiosGuardDxe - Recovery helper for update process**
    - ✓ **UEFI variable cleanup**
  - **BiosGuardNvs – ACPI helper for update process**
    - ✓ **AMI Capsule validation**

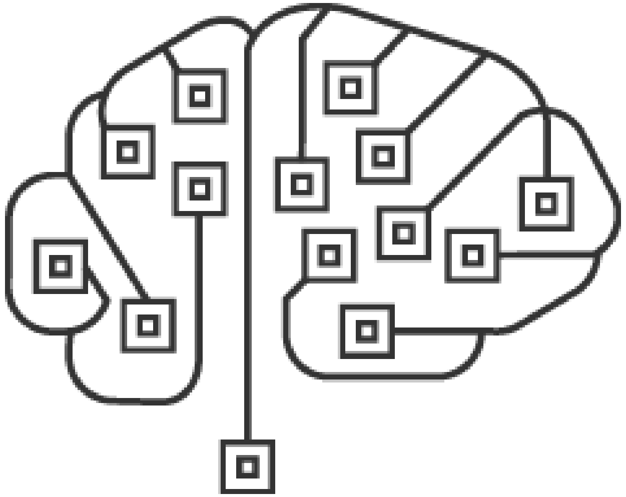
BIOS Guard Commands (AMI)

- PEI
  - BG_READ
  - BG_WRITE
  - BG_ERASE
  - BG_WRITE_ENABLE
  - BG_WRITE_DISABLE

- SMM
  - BG_READ
  - BG_WRITE
  - BG_ERASE

All the stuff will be released on public

save the link:



https://github.com/REhints/BlackHat_2015

Thank you for your attention!

Alex Matrosov

@matrosov