



BETRAYING THE BIOS: WHERE THE GUARDIANS OF THE BIOS ARE FAILING

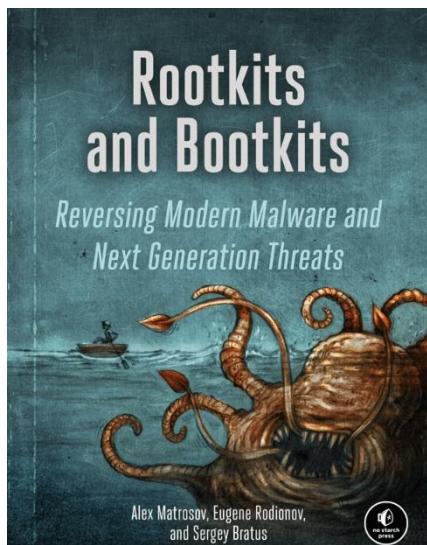
Alex Matrosov
@matrosov

Have a lot of fun with UEFI Security and RE

Former Security Researcher @Intel

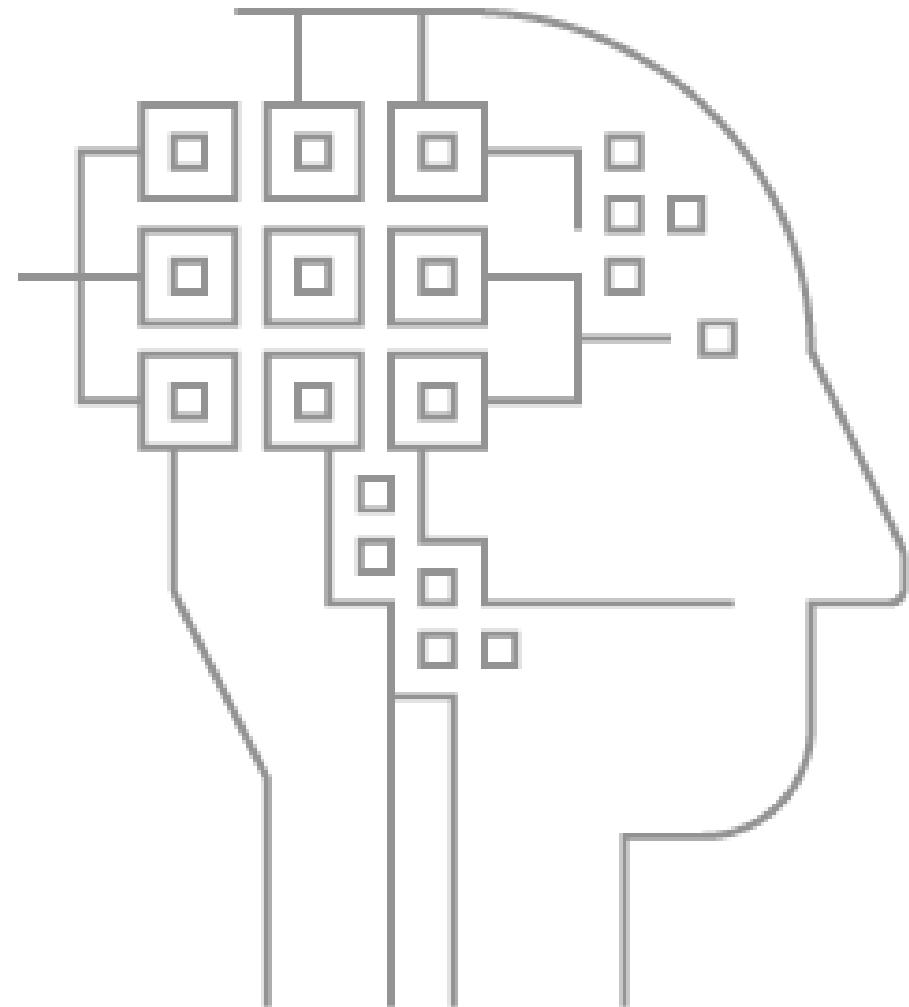
Reverse Engineering since 1997

Book co-author nostarch.com/rootkits

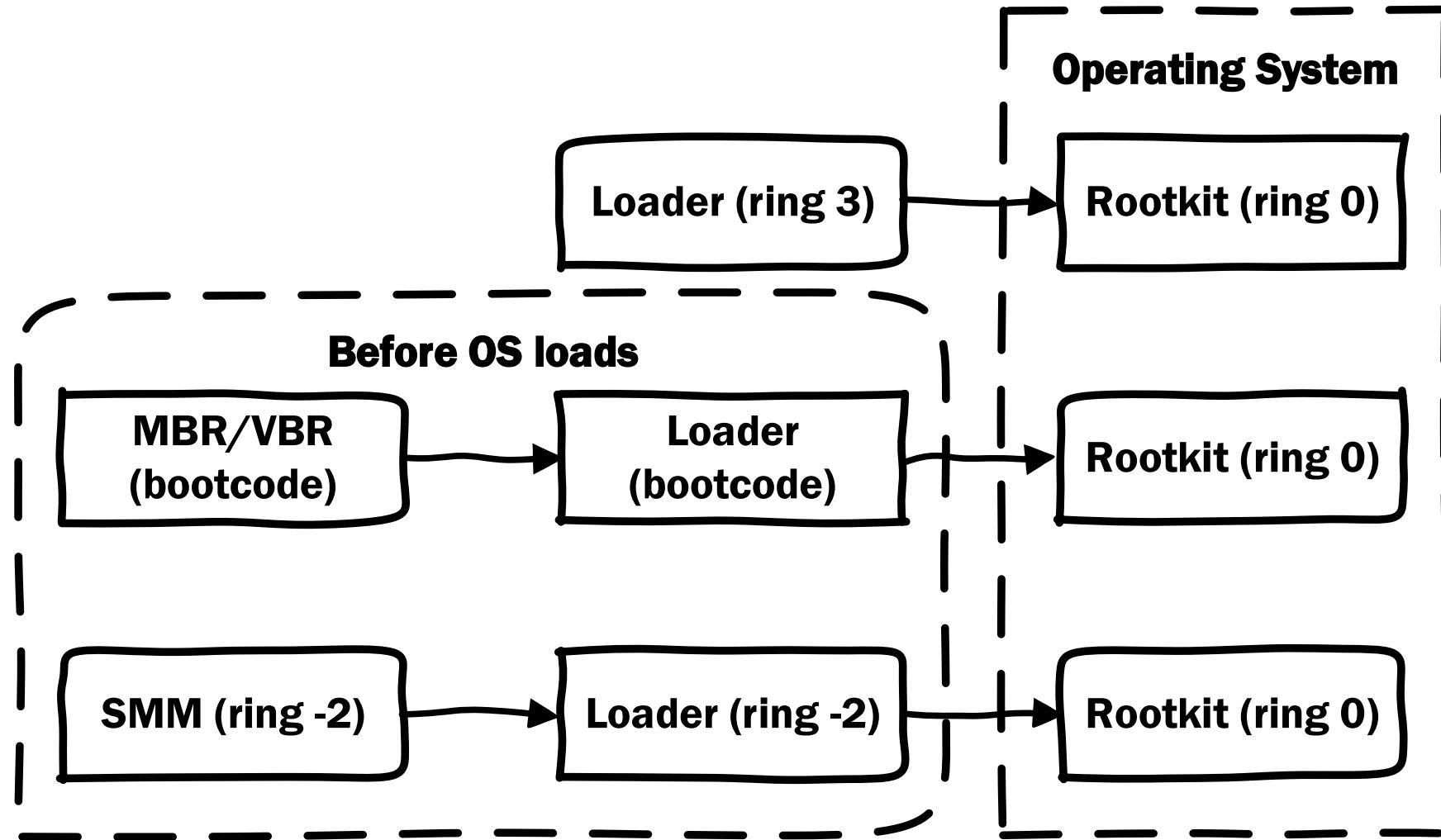


@matrosov

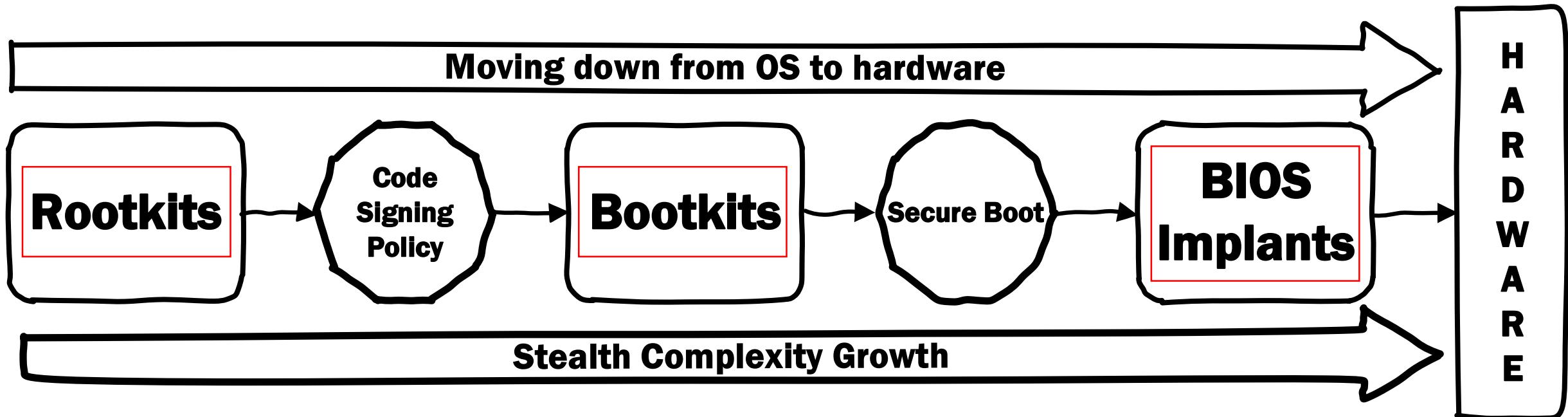
- **Intro**
- **Attacks on BIOS Updates**
 - ✓ Unsigned Updates
 - ✓ BIOS protection bits
 - ✓ SmiFlash and SecSmiFlash
- **Intel Boot Guard**
 - ✓ AMI implementation details
 - ✓ Discover ACM secrets
 - ✓ Vulns
 - ✓ Boot Guard Bypass!
- **Intel BIOS Guard**
 - ✓ AMI implementation details



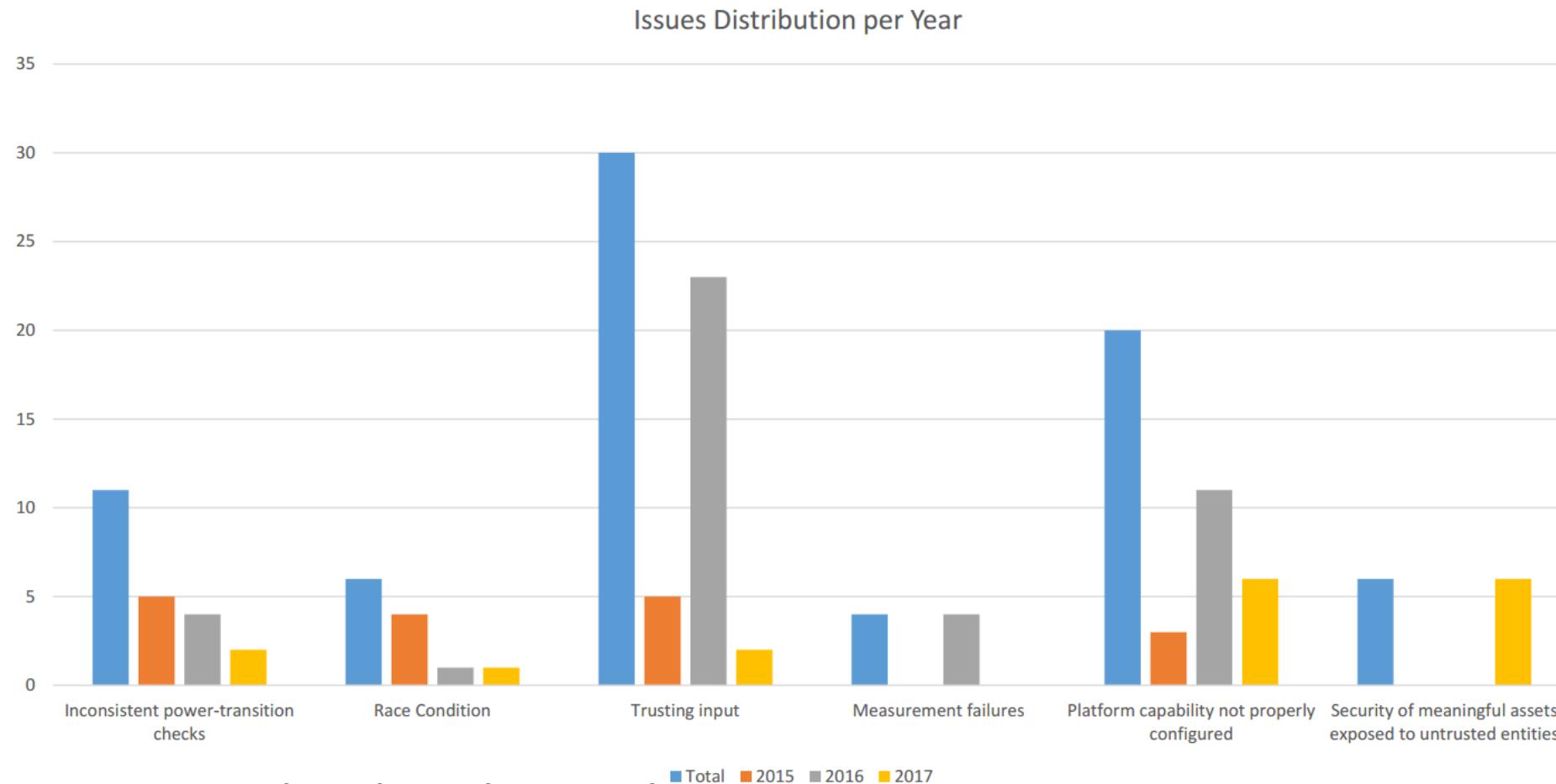
All rootkits want to get into Ring 0



More mitigations, more rootkits complexity

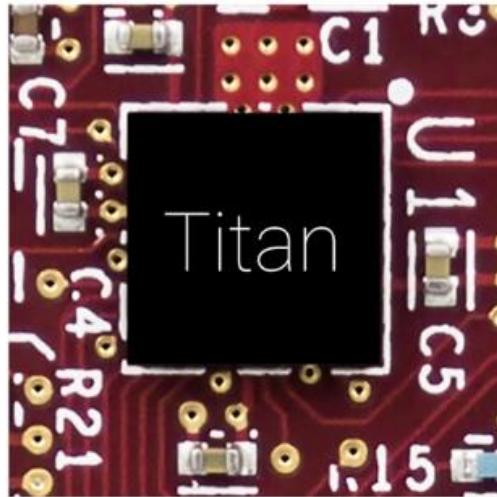


Growths of configuration based vulnerabilities



<https://www.blackhat.com/docs/us-17/thursday/us-17-Branco-Firmware-Is-The-New-Black-Analyzing-Past-Three-Years-Of-BIOS-UEFI-Security-Vulnerabilities.pdf>

Google Titan Chip



Titan

Purpose-built chip to establish hardware root of trust for Google Cloud servers



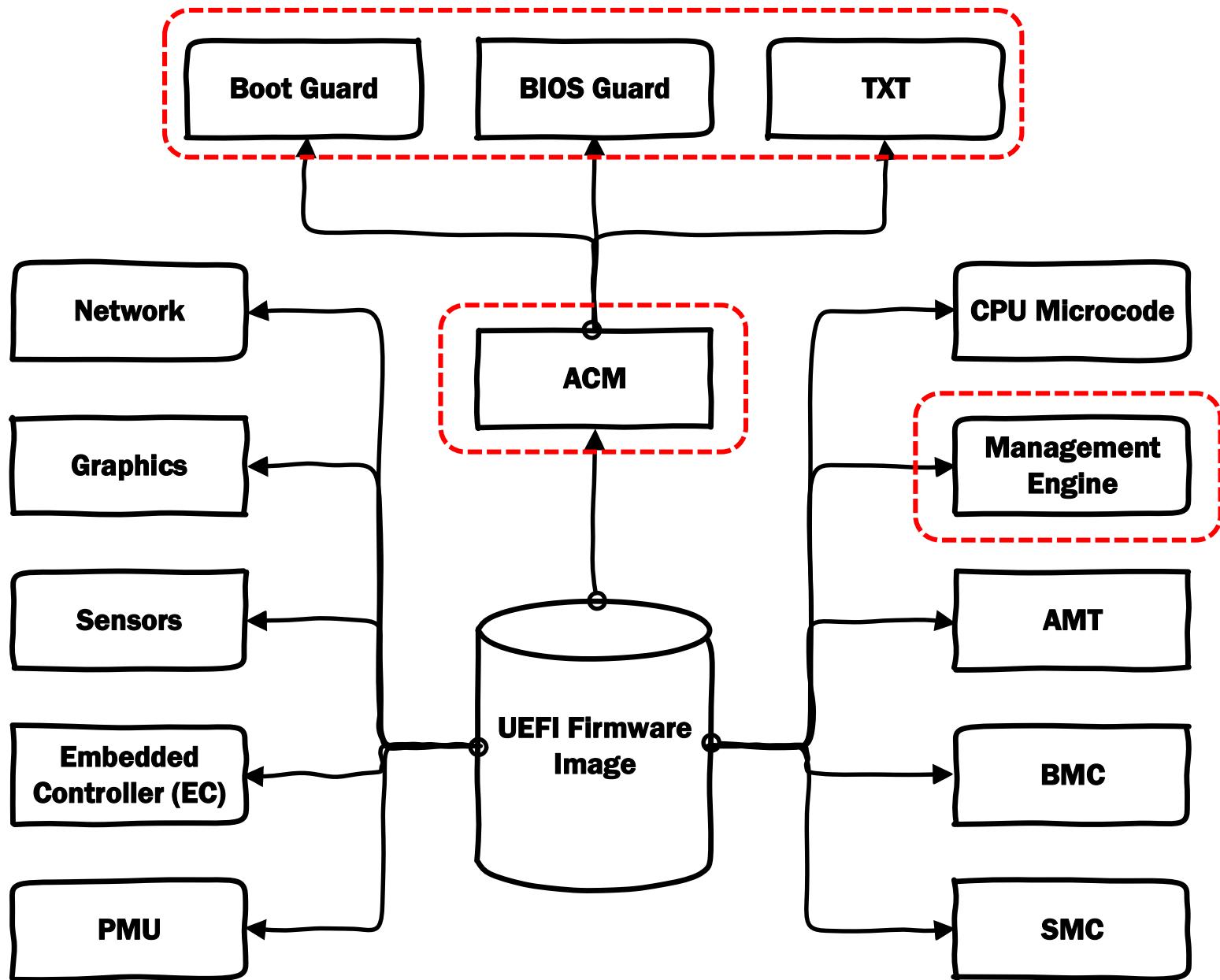
Google's purpose-built server

BIOS Update Issues

No more legacy! UEFI is everywhere!!



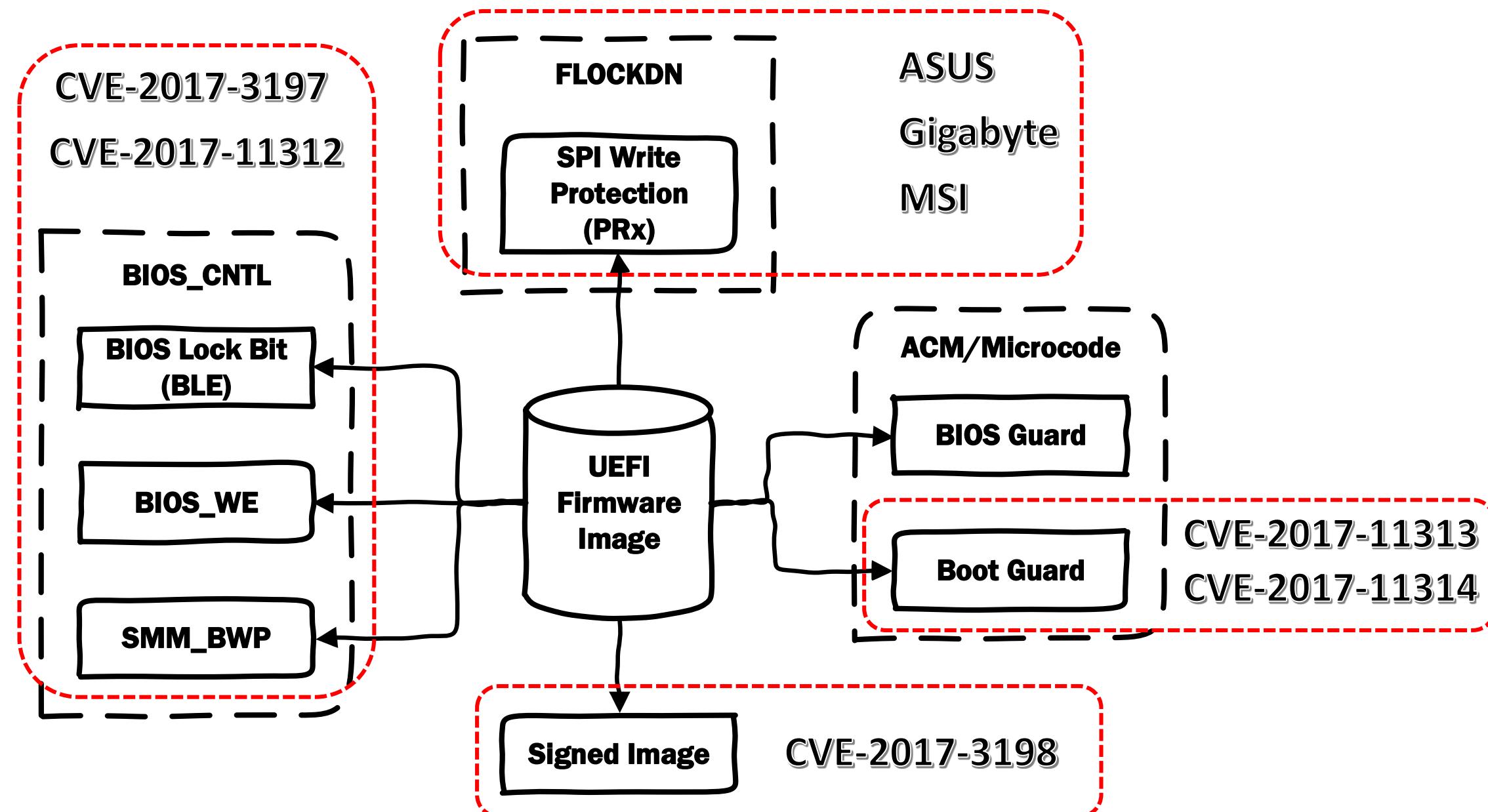
How many different firmware's inside BIOS update?



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.py
[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?
-----
```

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

I DON'T CARE



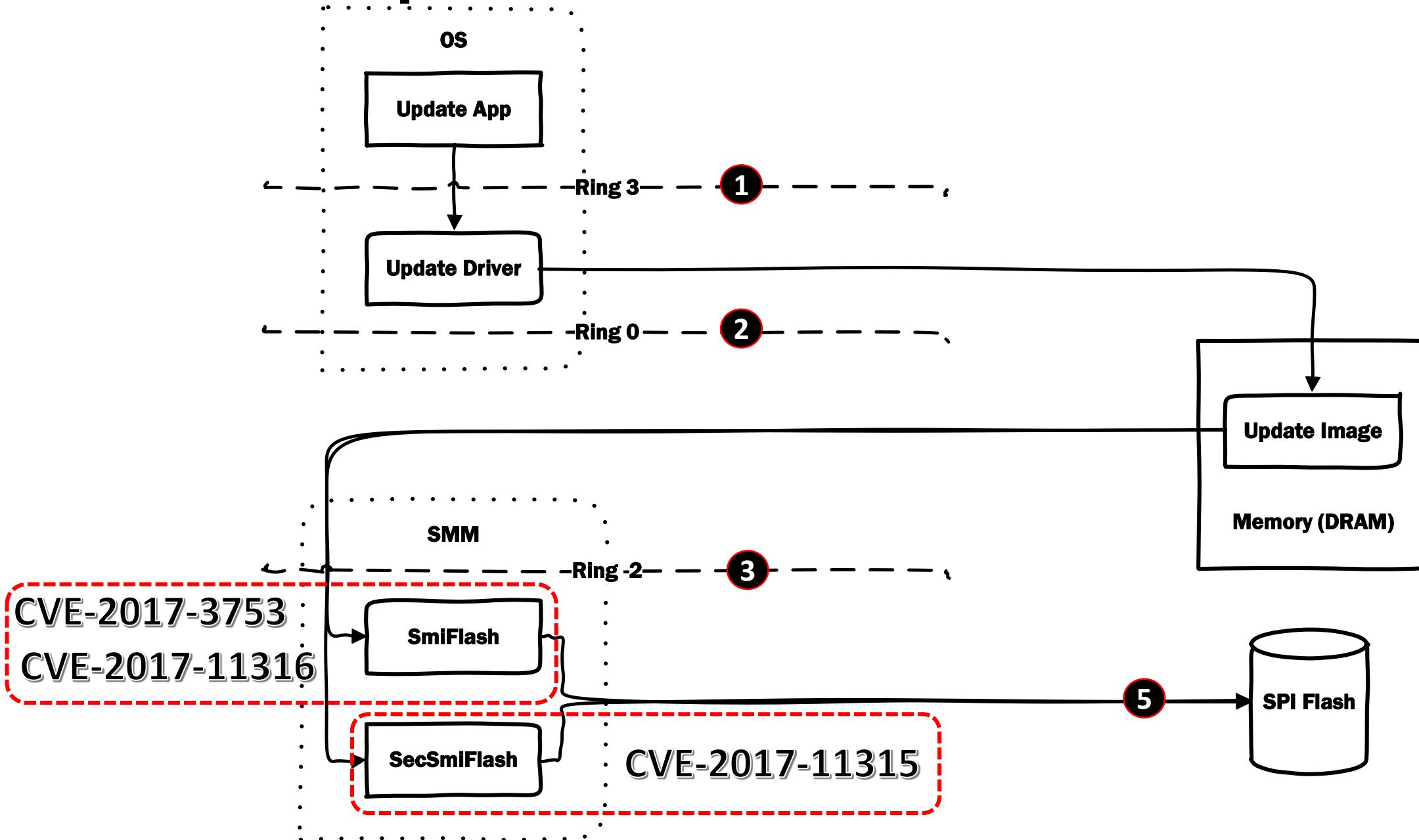


Why so vulnerable?



- 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-A2A2-065FEDE6080]
 - ✓ 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**

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



Replies 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

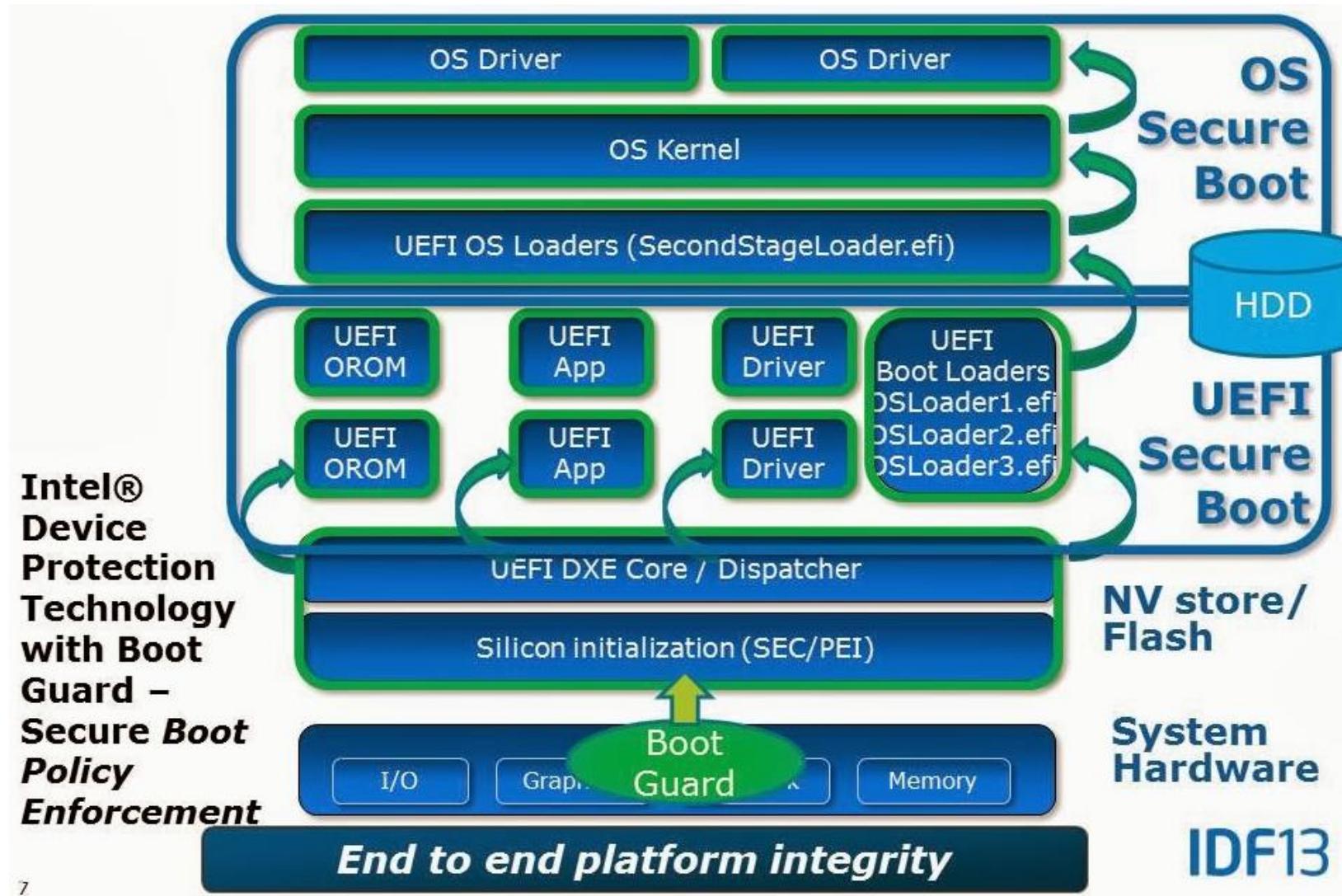
Different shades of Secure Boot

- **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**
- First bypass today?!**

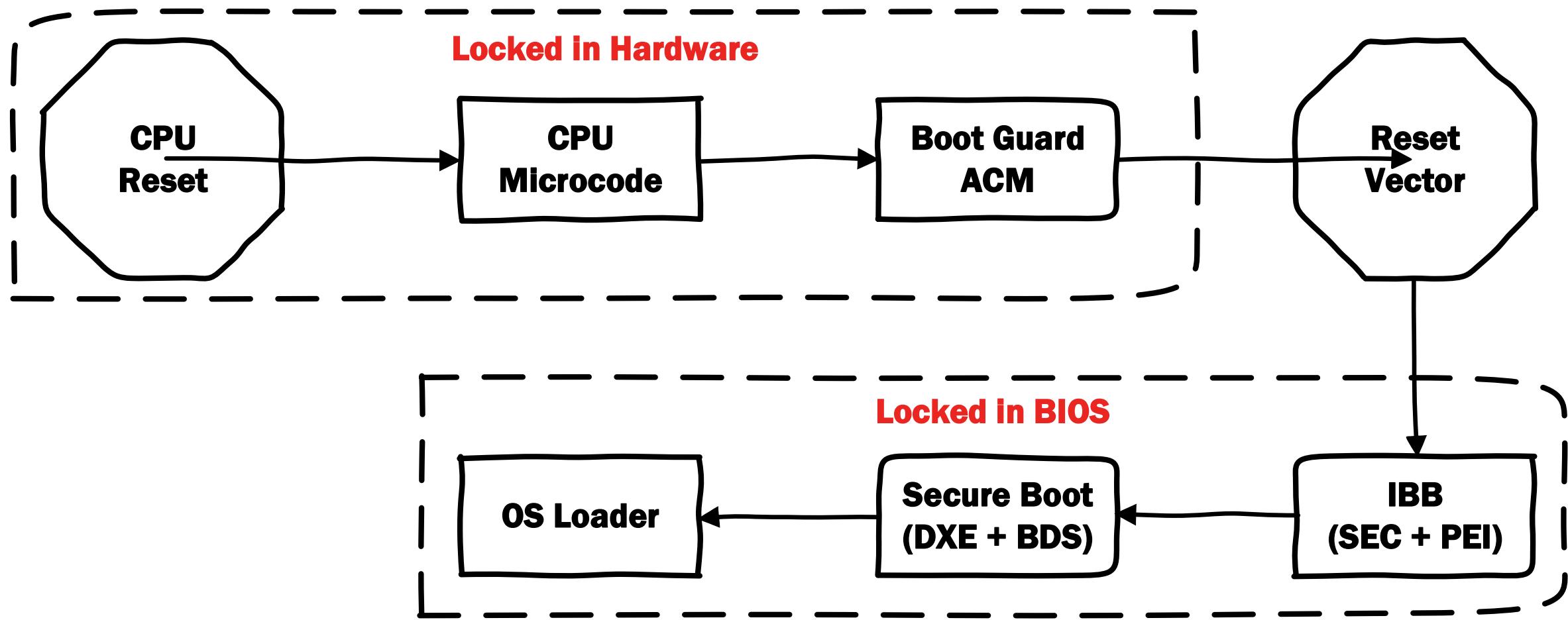
Why Boot Guard has been created?

- **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



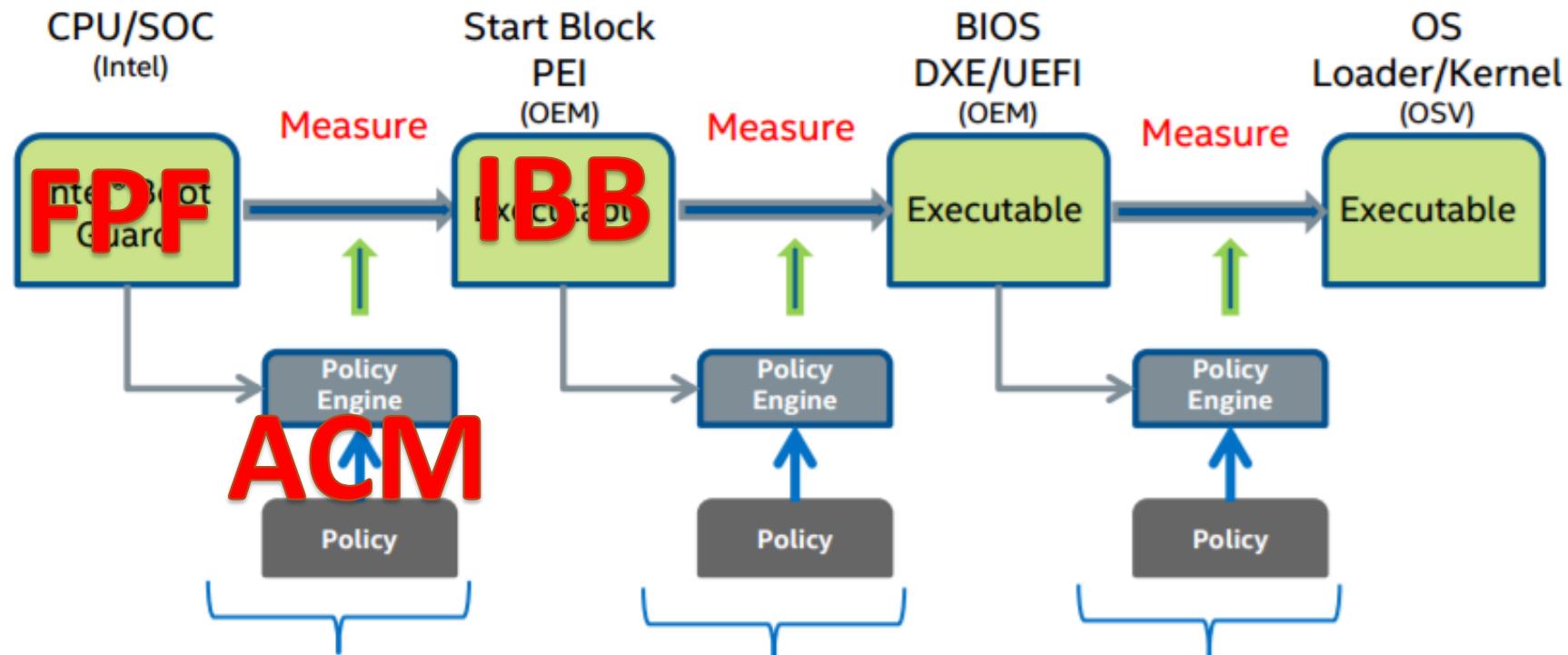
Boot Guard: Boot Flow



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>

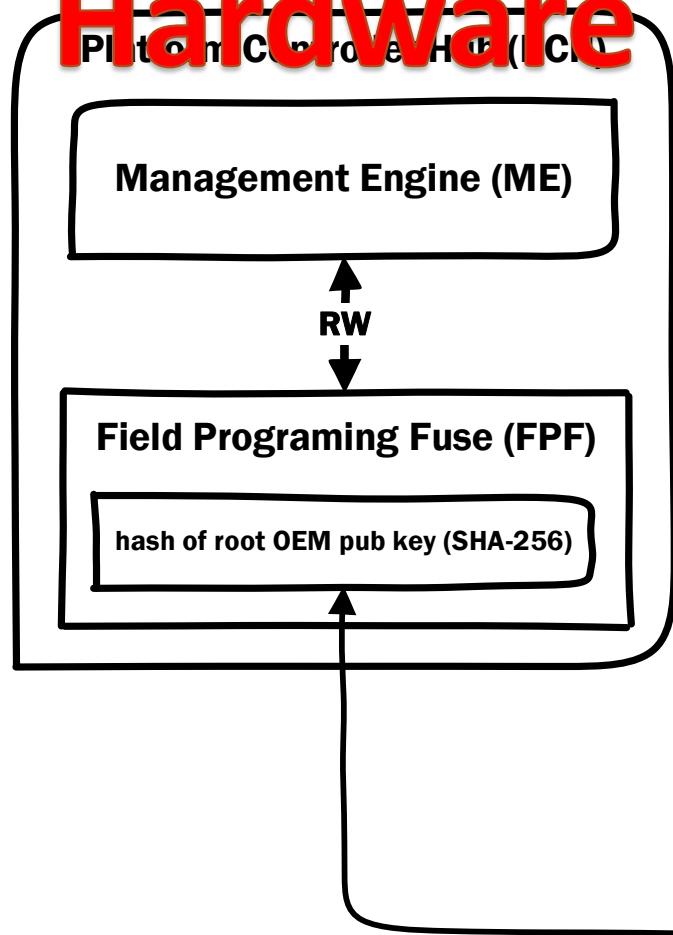
**OEM PI
Verification
Using PI Signed
Firmware Volumes**
Vol 3, section 3.2.1.1
of PI 1.3 Specification

**OEM UEFI 2.4
Secure Boot**

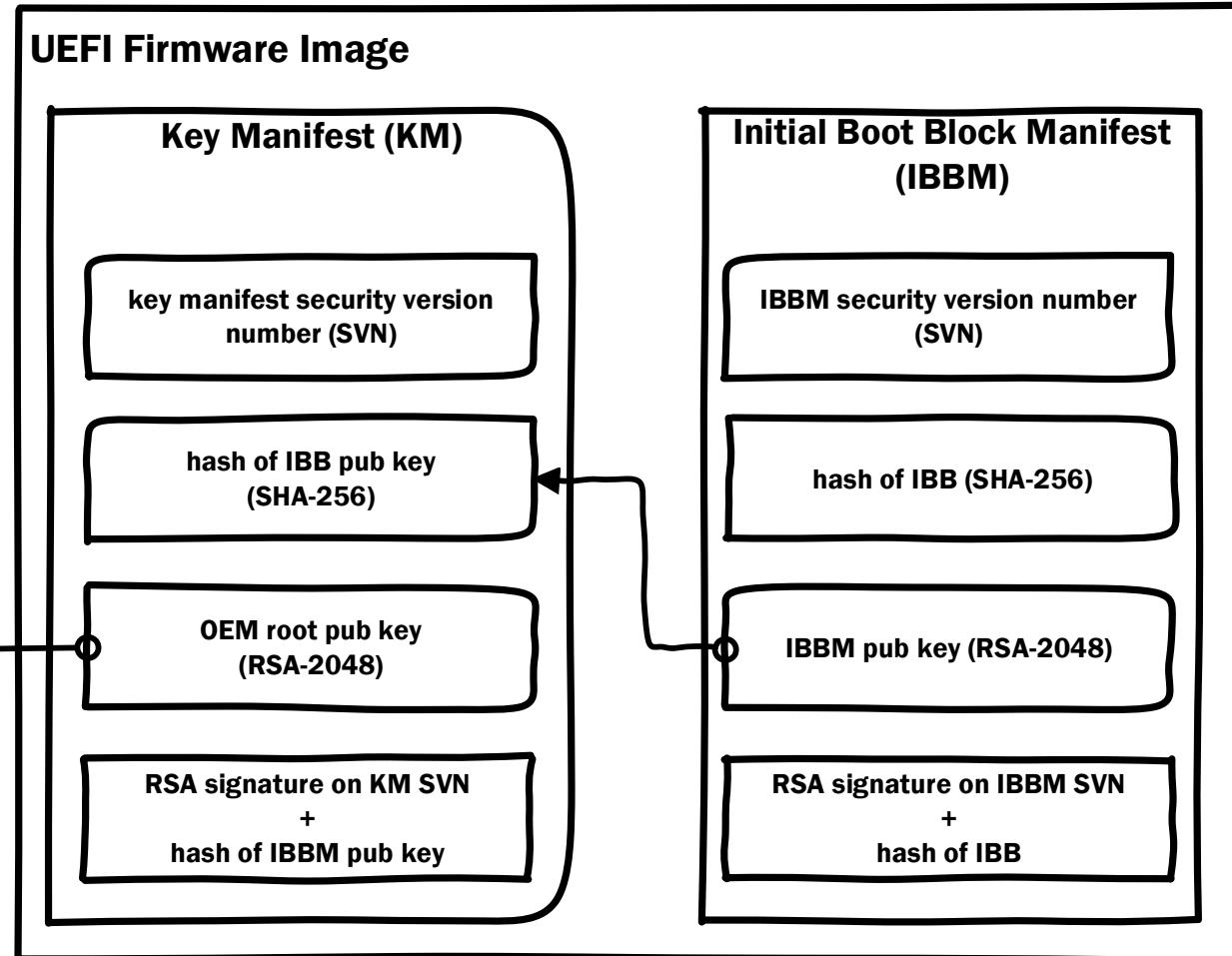
Chapter 27.2 of
The UEFI 2.4
Specification

Boot Guard: Chain of Trust

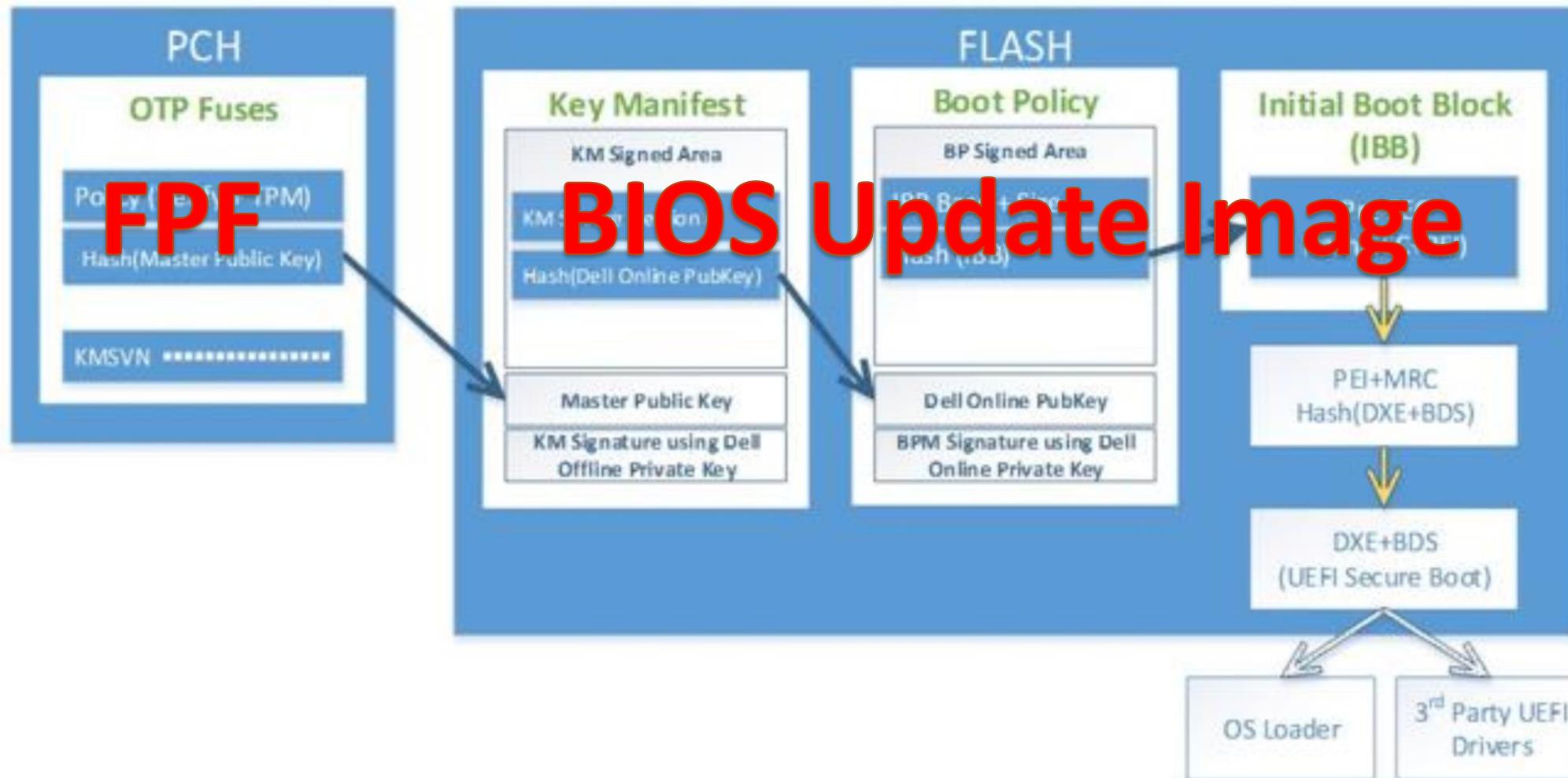
Hardware



Firmware



Demystifying Intel Boot Guard



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

A high-contrast, black and white silhouette of a man from the waist up. He is facing forward, holding a cigarette in his right hand and bringing it to his mouth. A plume of smoke rises from the cigarette. Overlaid on the center of the image is the text "TRUST NO ONE" in a large, bold, sans-serif font.

TRUST
NO
ONE

Safeguard

File Build Help



Intel (R) LP Series Chipset

Premium U

Flash Layout

GuC Encryption Key	00 00 00 00 00 00 00 00 00 00 ...
--------------------	-----------------------------------

Flash Settings

Intel(R) ME Kernel

Intel(R) AMT

Platform Protection

Integrated Clock Controller

Networking & Connectivity

Flex I/O

Internal PCH Buses

GPIO

Power

Integrated Sensor Hub

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

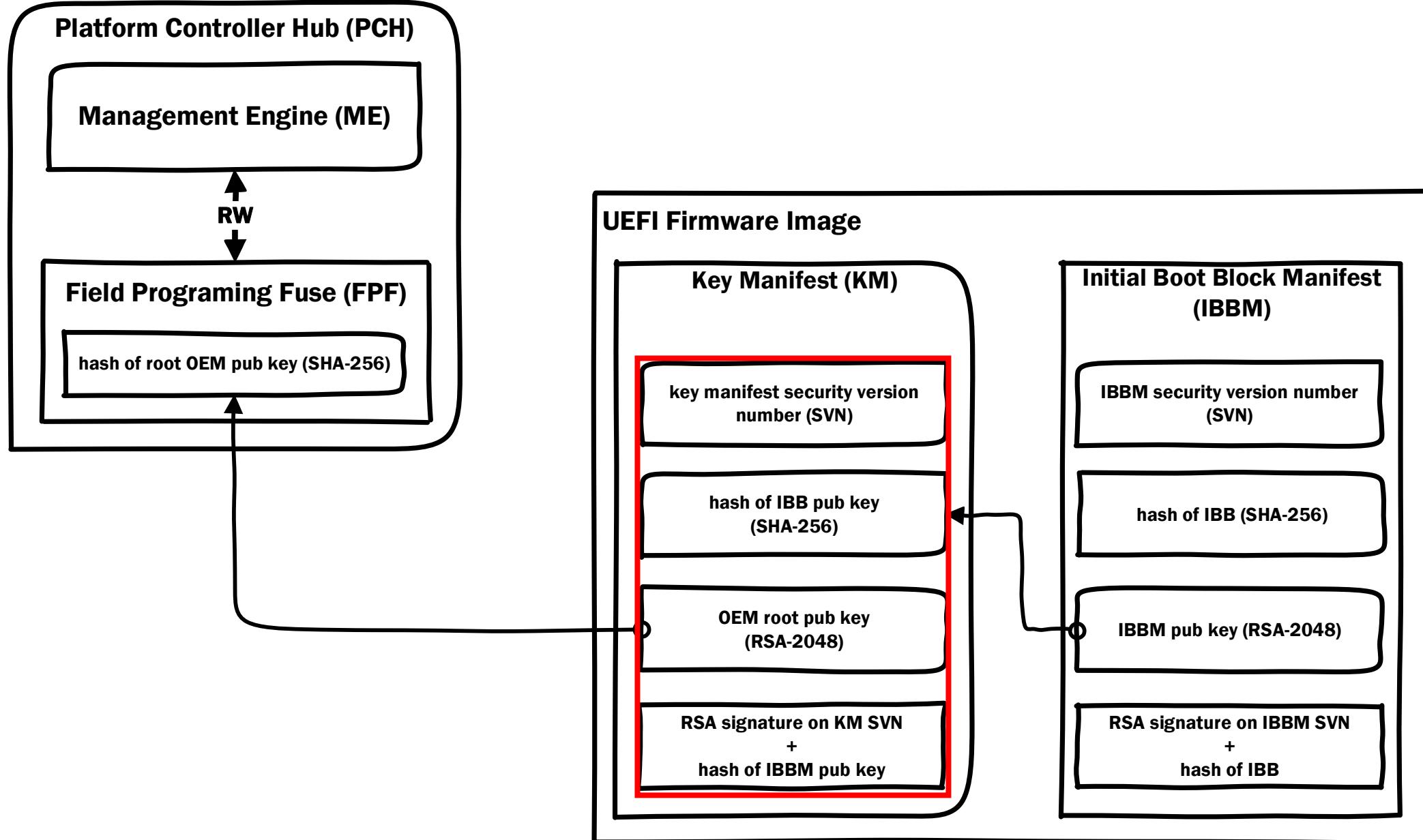
Parameter	Value
Key Manifest ID	0x0
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME
CPU Debugging	Enabled
BSP Initialization	Enabled



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

Grugq

Boot Guard: Chain of Trust



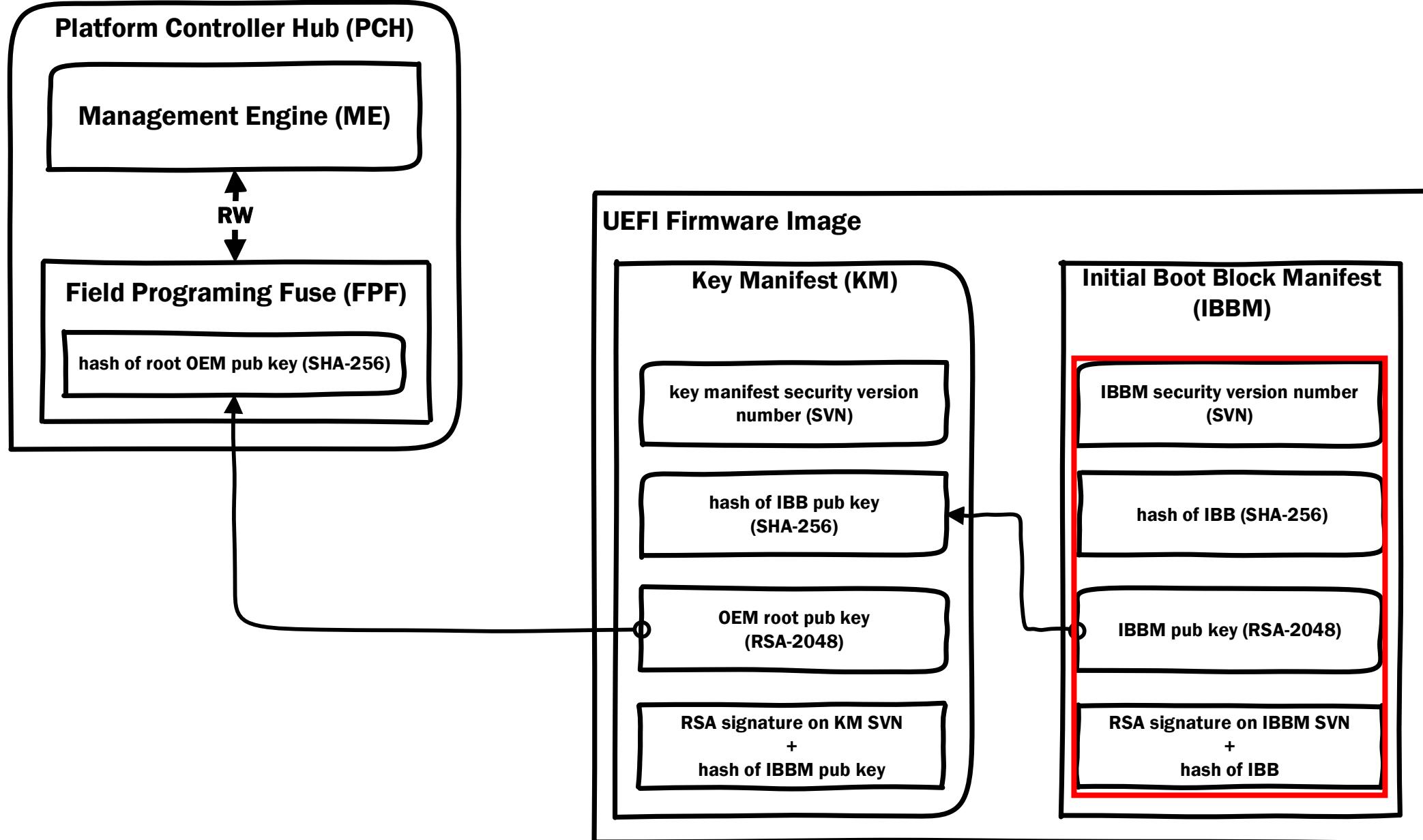
Boot Guard: Key Manifest (KM)

```
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	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000h:	5F	5F	4B	45	59	4D	5F	5F	10	10	00	01	0B	00	20	00	0123456789ABCDEF	KEYM
0010h:	4E	6D	A4	49	D7	69	16	95	7D	6	FE	E5	00	72	CC	IIBM Hash	Nm¤I×ivÖpþoþå€rÌ
0020h:	17	F2	07	55	A5	BB	05	95	8A	00	85	07	85	07	85	07	00
0030h:	10	01	00	10	00	08	01	00	01	00	51	6A	00	AC	10	38	00	
0040h:	AC	A9	E3	3F	05	19	91	83	4F	A2	E7	E7	03	7B	7B	B3	00	
0050h:	45	B7	88	68	F3	D9	27	51	77	2D	F7	F4	BC	67	49	07	00	
0060h:	38	3D	1A	A6	70	4D	87	8F	C8	F5	AF	A4	BC	C5	4C	C2	00	
0070h:	B2	BF	C0	C1	BD	94	42	51	92	9F	00	CF	C0	A0	3B	EA	00	
0080h:	11	E0	F8	E5	E3	EB	46	BF	AD	2B	82	2A	60	34	6D	9D	00	
0090h:	65	E7	DC	28	BA	9A	D3	43	A5	E3	CF	3F	59	36	2C	8A	00	
00A0h:	EA	3C	D3	F2	B3	2A	9F	61	06	F7	81	FC	86	9E	96	6A	00	
00B0h:	08	00	6F	78	1A	20	05	FA	A2	15	4	CD	02	2	FE	00		
00C0h:	20	00	00	25	B	20	23	10	10	10	F0	10	85	5	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00D0h:	17	30	EC	A4	58	2D	93	E4	A8	46	66	99	5D	7F	08	4F	00	
00E0h:	C3	8C	7E	33	C4	D0	59	1B	00	F8	47	B5	0F	4D	B9	4F	00	
00F0h:	84	7F	AF	B7	45	C1	1B	54	66	DA	EF	F0	C0	91	1C	81	00	
0100h:	AE	73	F9	CC	D4	9C	09	C1	FA	7F	E8	7A	7E	39	06	81	00	
0110h:	41	97	89	16	40	93	66	02	8A	3A	20	F1	C3	C4	DE	42	00	
0120h:	B7	5F	5A	9C	02	C7	8F	AC	80	42	8D	8C	7B	40	8C	3F	00	
0130h:	50	39	73	AD	CE	56	93	05	D3	C2	14	00	10	00	08	0B	00	
0140h:	00	52	C7	6B	1F	DB	45	95	F0	F9	37	16	F9	9A	EF	17	00	
0150h:	0B	43	46	B3	E0	94	9D	7D	AD	98	09	87	48	40	5C	4D	00	
0160h:	D2	14	FB	13	4F	B8	95	46	2A	6A	A4	83	2F	93	A2	EB	00	
0170h:	C3	5C	EA	39	43	7E	FD	EC	1B	58	3B	9B	B8	7D	5C	55	00	
0180h:	A8	07	7B	A4	28	C1	43	42	BC	5A	64	CA	EE	3E	54	0E	00	
0190h:	C4	49	42	92	D8	73	0D	0D	C9	00	3D	5F	EC	5C	BC	00	00	
01A0h:	7C	BB	20	FA	20	B8	0F	00										
01B0h:	82	D1	F2	5E	78	C6	24	EF	C1	57	00	6D	53	7B	B0	46	00	
01C0h:	08	A6	90	FF	01	8B	85	EC	49	D3	5E	00	12	0F	77	61	00	
01D0h:	33	F5	0D	70	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01E0h:	0D	84	D4	1E	1F	90	A8	49	95	50	1E	B4	05	82	56	00	00	
01F0h:	92	4C	28	58	1A	CD	A7	16	C5	9A	BF	11	FF	AF	EC	AF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0200h:	FF	24	34	6F	98	CA	0C	F4	A8	AF	C0	BF	8A	C8	B4	56	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0210h:	F6	E6	D4	CA	51	11	9A	20	80	9C	57	33	75	77	59	AA	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0220h:	63	10	55	E0	9F	E9	32	BE	BA	3A	B2	90	D7	62	F1	F4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0230h:	39	00	71	42	3E	65	FE	C1	0A	7D	58	AD	15	B3	C7	34	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0240h:	3C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			

RSA OEM Root Pub Key
RSA Signature
(KM_SVN + hash (IBBM Pub Key))

Boot Guard: Chain of Trust



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
            UBYTE Unknown3
            UNT32 Unknown3
            UNT64 Unknown4
            UNT64 VtdBar
            UNT32 Unknown5
            UNT32 Unknown6
            > UNT64 Unknown7[2]
            UNT16 Unknown8
            struct KEY_HASH IbbHash
                UNT32 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	.Np.....Ùp....
0030h:	00	00	10	00	00	00	F0	00	00	00	00	01	00	00	00	00ð.....
0040h:	00	00	00	00	0F	00	00	00	00	00	00	00	00	00	00	00ðÿÿÿ
0050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00ðÿÿÿ
0060h:	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FFðÿÿÿ
0070h:	OB	00	20	00	01	41	41	41	41	41	41	41	41	41	41	41	IIB Hash
0080h:	B9	42	81	1F	53	5F	IIB Offsets										
0090h:	91	66	5E	C9	04	00	00	00	00	00	00	EA	FF	00	00	12f^É.....êý...
00A0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00éüý.....
00B0h:	00	00	91	FC	FF	80	00	00	00	00	00	00	00	00	80	A1üý€.....€íü
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	BBff...®È"»
00E0h:	D1	01	92	27	A3	59	0A	93	C6	E3	5E	7A	C4	E9	D2	86	Ñ.''fY."Ää^zÄéÖt
00F0h:	E9	3D	19	3C	DE	01	12	A9	29	1B	4F	4F	50	02	57	CA	é=.<Ð..©).OOP.WÉ
0100h:	F3	7E	92	12	5B	7F	8D	F2	D7	18	F9	07	FB	A9	B1	9C	ó~'.[..ð×.ù.û@tæ
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+èŒksÍl"i#
0130h:	C0	9E	70	02	6D	DB	46	77	59	DC	89	CB	AA	93	A3	26	Äžp.mÛFwÝÜ‰Èa"ƒ&
0140h:	B9	68	86	50	35	96	7C	7C	7D	¹h+P5—2+-ÍK©éM!							
0150h:	4B	CF	24	AF	28	02	01	7A	7F	84	07	94	9D	8E	7A	3B	KÍ\$-(..z//,.Žz;
0160h:	29	8E	1B	A8	B4	70	C3	8E	13	29	56	BD	C1	0F	A8	2E)Ž..`pÄž.).VñÄ..”.
0170h:	6A	E4	B5	CB	E5	84	F2	29	28	7F	E3	E6	85	25	08	E4	jäµËå,,ð) (.ãæ..%..ä
0180h:	C8	A6	74	68	B6	66	0B	19	97	12	F8	DA	A9	89	1D	2F	É!tñff..-.øÚC‰../
0190h:	8F	F8	02	A3	FC	A7	6E	3B	63	24	D2	67	7F	49	45	02	.ø..fü\$ñ;c\$Øg.IE.
01A0h:	48	03	B1	A9	69	56	55	12	DD	6D	9B	C5	13	83	74	0E	H..±CiVU.Ým>Å..ft.
01B0h:	9C	57	2B	35	86	71	0B	BF	F8	39	30	7F	61	18	EC	4B	œW+5†q.¿ø90.a.iK
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..!Cä...../
01E0h:	5D	E4	18	BE	0C	62	38	A1	4C	33	5C	C5	57	B7	08	EA	Jä..¾.b8..L3\ÅW..ê
01F0h:	CF	CC	59	34	6F	8A	B6	E0	0E	C3	08	FA	64	BC	04	00	ÍÍY4oŠ¶à.Ã.úd¾..
0200h:	F3	B1	4F	D0	0D	C6	CE	39	F4	FC	CA	90	FE	57	F5	21	ð±OD.ÆÍ9ðüû.þWð!
0210h:	88	A7	D0	F5	28	77	39	FA	70	0C	E5	D6	FC	07	6F	E0	^SDð(w9úp.åÖü.oà
0220h:	F2	58	C7	52	FA	20	DF	CE	17	0D	2D	7D	F3	2E	BB	C2	ðXÇRú.ßI..-}ó.»Â
0230h:	EC	E4	08	4A	BB	20	CC	60	7A	17	C1	39	95	26	27	A4	iä..J» Í-çfÝ} „Ý.ö
0240h:	30	F0	BF	B9	30	3E	1E	9D	7A	17	C1	39	95	26	27	A4	0ð..¹0>.z.íi•&'¤
0250h:	29	8A	85	3C	CD	34	B2	43	C6	7B	09	1C	6C	47	02	þš..Sm4²JE{.L1G.	
0260h:	46	3B	90	51	41	41	E5	51	33	77	17	17	41	41	41	41	ðB:@cç¢.Ð~Ì
0270h:	15	32	FA	30	FD	C5	FO	1F	DB	44	61	7B	E5	16	81	41	.Zú.Àð÷UDa{å..F
0280h:	86	B8	43	BB	C9	44	17	FF	8E	58	27	04	5E	4A	E3	1F	t,C»ED.þžX'.^Jä..
0290h:	52	71	A5	B1	B6	35	54	AA	CE	8E	E6	F6	02	35	1C	9A	Rq¥+¶5T^ÍŽæö..5.š
02A0h:	D2	FC	94	A6	11	FO	EB	63	92	D2	71	98	56	38	51	58	ðü"!..ðëc'ðq~V8QX
02B0h:	3E	D3	1C	76	35	CF	71	37	DB	E9	D6	9C	C0	5E	DA	4B	>Ó.v5Íq7ÛéðœÀ^ÚK
02C0h:	C3	33	E2	62	3A	60	C7	B3	D1	1C	6C	0A	77	73	OC	3D	À3âb:`ç³Ñ.1.ws.=
02D0h:	79	0B	74	36	E1	81	24	71	72	A5	92	9C	C5	40	76	00	y.t6á.\$qr¥'/æÅ@ v.
02E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

((IBBM_SVN + hash (IBB)))

RSA Signature

File Action Help

Structure

Information

Name

```

>10C22623-DB6F-4721-AA30-4C12AF423E 20 // 
>00026AEB-F334-4C15-A7F0-E1E897E9FE 21 // FIT Entry type definitions
>89F06049-F297-4436-8540-E0BF9E92B5 22 //
>9B3F28D5-10A6-46C8-BA72-BD40B847A7 23 #define FIT_TYPE_00_HEADER
77D3DC50-D42B-4916-AC80-8F469035D1
Pad-file
6520F532-2A27-4195-B331-C0854683E0 24 #define FIT_TYPE_01_MICROCODE
>8E295870-D377-4B75-BFDC-9AE2F6DBDE 25 #define FIT_TYPE_02_STARTUP_ACM
>5B85965C-455D-4CC6-9C4C-7F086967D2 26 #define FIT_TYPE_07_BIOS_STARTUP_MODULE
Pad-file
C30FFF4A-10C6-4C0F-A454-FD319BAF6C 27 #define FIT_TYPE_08 TPM_POLICY
Pad-file
7C9A98F8-2B2B-4027-8F16-F7D277D58C 28 #define FIT_TYPE_09 BIOS_POLICY
Pad-file

```

	3h	20F532-2A27-4195-B331-C0854683E0BA
	3h	
	18h (32792)	
	18h (24)	
0x00	30h (32768)	
	(0)	
0x01	Jm: D0h, valid	
0x02	: AAh, valid	
	address: FFFBFFE8h	
0x07	ddress: FFFC0000h	
0x08		
0x09		
0x0A	on	
0x0B		
0x0C	ision 00000074h, Date 01052016h	
0x10	ision 00000028h, Date 04152015h	
0x2D	ision 00000074h, Date 01052016h	
0x2F	ision 0000002Ch, Date 07012015h	
0x7F		

Parser FIT Search Builder

	Address	Size	Version
1	_FIT_	00000080h	0100h
2	00000000FFE10090	00017400h	0100h
3	00000000FFE27490	00015000h	0100h
4	00000000FFE3C490	00017400h	0100h
5	00000000FFE53890	00012C00h	0100h
6	00000000FFFC0000	00000000h	0100h
7	00000000FFFC9180	00000241h	0100h
8	00000000FFFC8100	000002DFh	0100h
	00h		

BootGuard Boot Policy

Boot Guard: Initial Boot Block (IBB)

Hex view: C30FF

0000	5F	5F	41	4	Intel image	Image	Intel
Descriptor region					Descriptor	Region	GbE
GbE region					Region	Region	ME
ME region					Region	Region	BIOS
BIOS region					Volume	Volume	FFSv2
> EfiFirmwareFileSystem2Guid					Padding	Empty (0xFF)	
Padding					Volume	FFSv2	
> F41C52D3-D824-4D2A-A2F0-EC40C23C5916					Volume	FFSv2	
> AFDD39F1-19D7-4501-A730-CF5A27E11548					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-AA49-2EB04F235E09					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-BD88-FCA99F28B011					File	PEI module	AmiTxtPei
A6AEF1F6-F25A-4082-AF39-2229BCF5A6E1					File	PEI module	AmtStatusCodePei
52B3D8A7-9565-48E8-8E13-EC7196721B3C					File	PEI module	PlatformInfoPei
B41956E1-7CA2-42D8-9562-168389F0F066					File	PEI module	BootGuardPei
C776AE42-AA27-4A6E-975B-E0BEA9078BD9					File	PEI module	BiosGuardPeiApRecoveryC...
CAC3FB95-33F5-4596-818B-68E024D0B67B					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-BD8E-6F486A5A9F3C					File	Freeform	
RomLayout					File	Freeform	
CapsuleX64					File	PEI module	CapsuleX64
PcdPeim					File	PEI module	PcdPeim
> A8499E65-A6F6-48B0-96D8-45C266030D83					File	PEI module	SgTpvPei
EEEE611D-F78F-4FB9-B868-5590F7169280					File	PEI module	SiInitPreMem
0C4EEBAC-4BC8-43B4-9F05-E07523A9FC97					File	PEI module	PlatformInitPreMem
654FE61A-2EDA-4749-A76A-56ED7ADE1CBE					File	PEI module	AfterMemoryDummyDriver
E03E6451-297A-4F9E-B1F7-639870327C52					File	PEI module	CmosPei
1068E0ED-5C8E-4724-B011-2C5F95065DF2					File	Freeform	EnhancePeiVariable
CBC91F44-A48C-4A5B-8696-703451D0B053					File	PEI module	
95C89484-DAEC-46E1-8600-3C4C7FC985D6					File	PEI module	BiosGuardRecovery
PeiRamBoot					File	PEI module	PeiRamBootPei
CpuIoPei					File	PEI module	CpuIoPei
> PcatSingleSegmentPciCfg2Pei					File	PEI module	PcatSingleSegmentPciCfg...
> E60A79D5-DC98-47F1-87D3-51BF697B6121					File	PEI module	CpuPei
FAF79E9F-4D40-4F02-8AC9-4B5512708F7F					File	PEI module	BiosGuardCpuPolicyOver...
59ADD620-A1C0-44C5-A90F-A1168770468C					File	PEI module	PlatformInit
Oxe1p1Pei					File	PEI module	Oxe1p1
5AC804F2-7D19-5B5C-A22D-FAF4A8F5178					File	PEI module	AcpivVariableHobOnSmramR...
BD87C542-9CFF-4D4A-A890-0286AF986F34					File	PEI module	PeiOverClock
EFF9400A-AD95-475B-868F-C7AFC313BA72					File	PEI module	AmiPeiCreateDummyRchob
299D6F88-2EC9-4E40-9EC6-DDA7EBF5FD9					File	PEI module	SiInit
B1E9E2CA-B078-4070-BCCD-87449AC7D2A6					File	PEI module	Cpu3Spesi
S3Restore					File	PEI module	S3Restore
988A0C3A-5186-4B55-89F4-CAFDE613DAB1					File	PEI module	BootScriptHidePei
TcgPei					File	PEI module	TcgPei
> 961C19BE-01AC-4B87-87AF-4AE8F090F2A6					File	PEI module	TrEEPei
0D8039FF-49E9-4CC9-A806-BB7C31B0BC80					File	PEI module	AmiTpM20PlatformPei
67451698-1825-4AC5-9990-F350CC7D5D72					File	PEI module	CryptoPPI
AGAA3A962-C591-4701-9025-73D8226089DC					File	PEI module	PeiRamBootCacheRdy
39E8CA1A-7A69-4A73-834A-D6381933286					File	PEI module	UsbPei
BDA7D71A-4C48-4C75-B5BC-D002D17F6397					File	PEI module	AhcRecovery
DACF785C-71DF-497D-AABE-10186B2E1DDE					File	PEI module	Recovery
7ECD9C20-6889-4A6F-B515-D64FF500B109					File	PEI module	FsRecovery
10C22623-D86F-4721-AA30-4C12AF4230A7					File	PEI module	IdeRecovery
00026AEB-F334-4C15-A7F0-E1E897E9FE91					File	PEI module	NvmeRecovery
89F06049-F297-4436-8540-E08F9E92B568					File	PEI module	SdioRecovery
> AmiTcgPlatformPeiAfterMem					File	PEI module	AmiTcgPlatformPeiAfterMem
77D3DC50-D42B-4916-AC80-F8469035D150					File	Raw	
Pad-file					File	Pad	
6520E532-2A27-4195-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]	

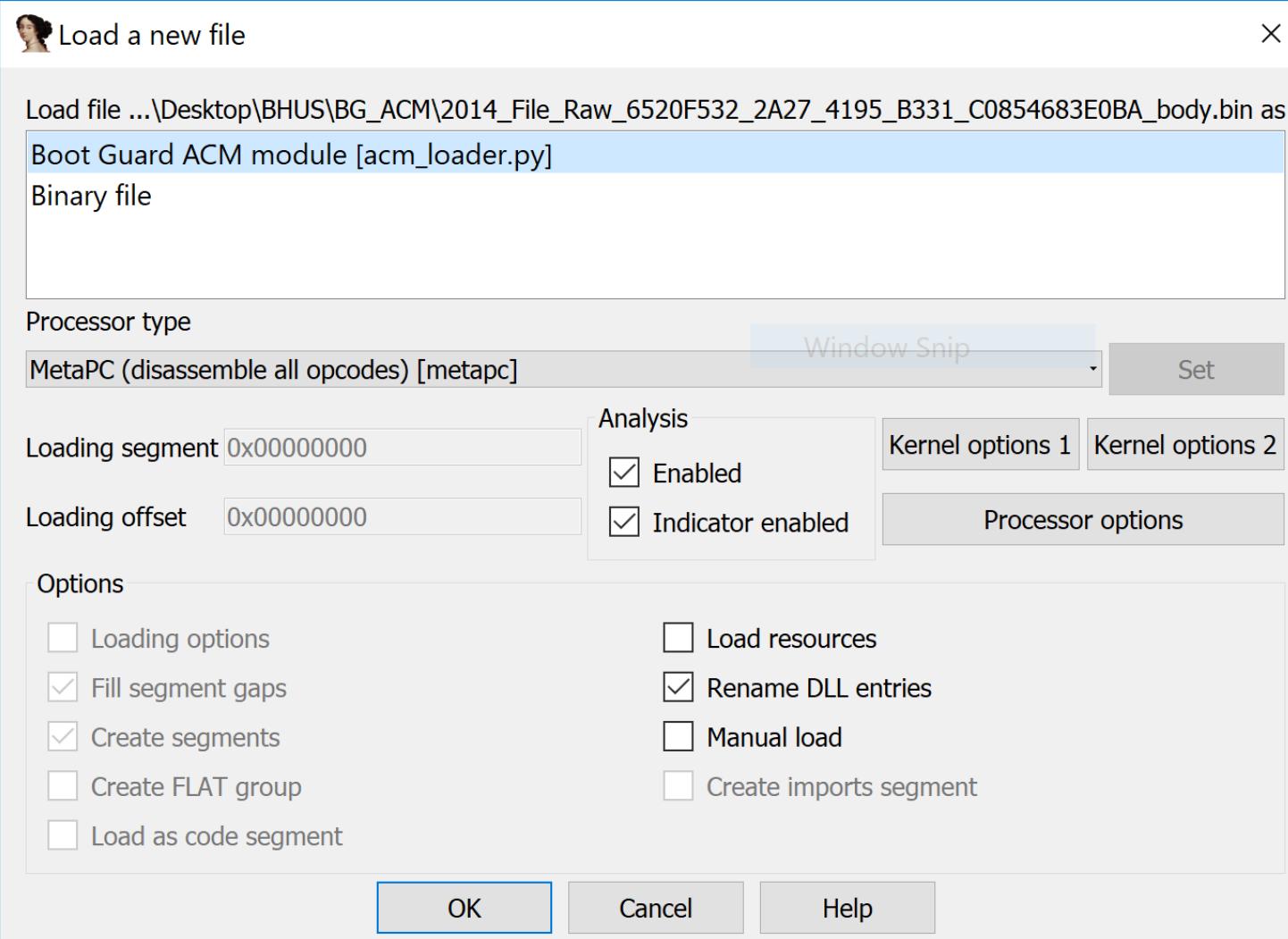
Boot Guard

➤ ACM is x

➤ ACM exec

➤ ACM has

➤ ACM veri

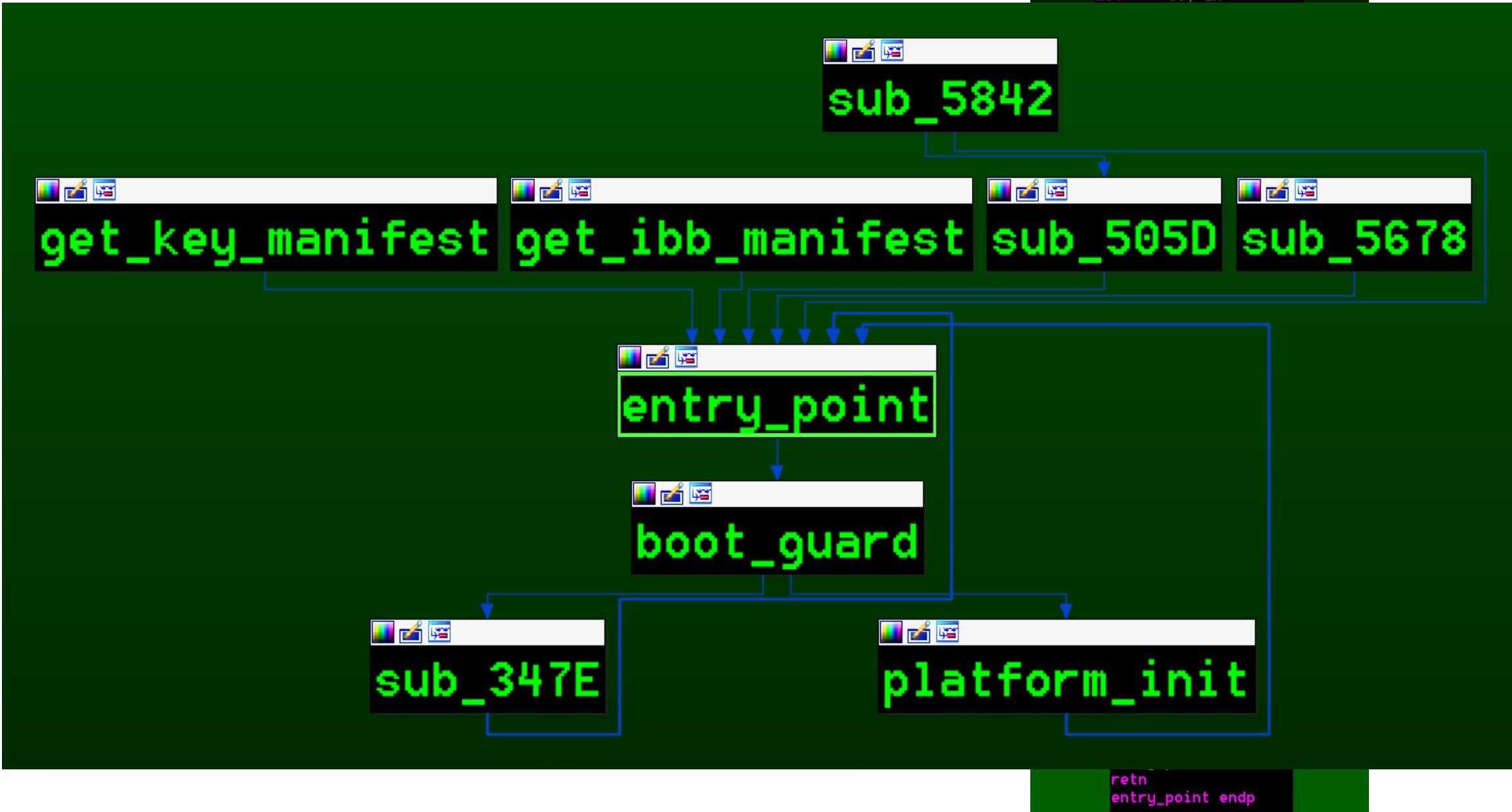


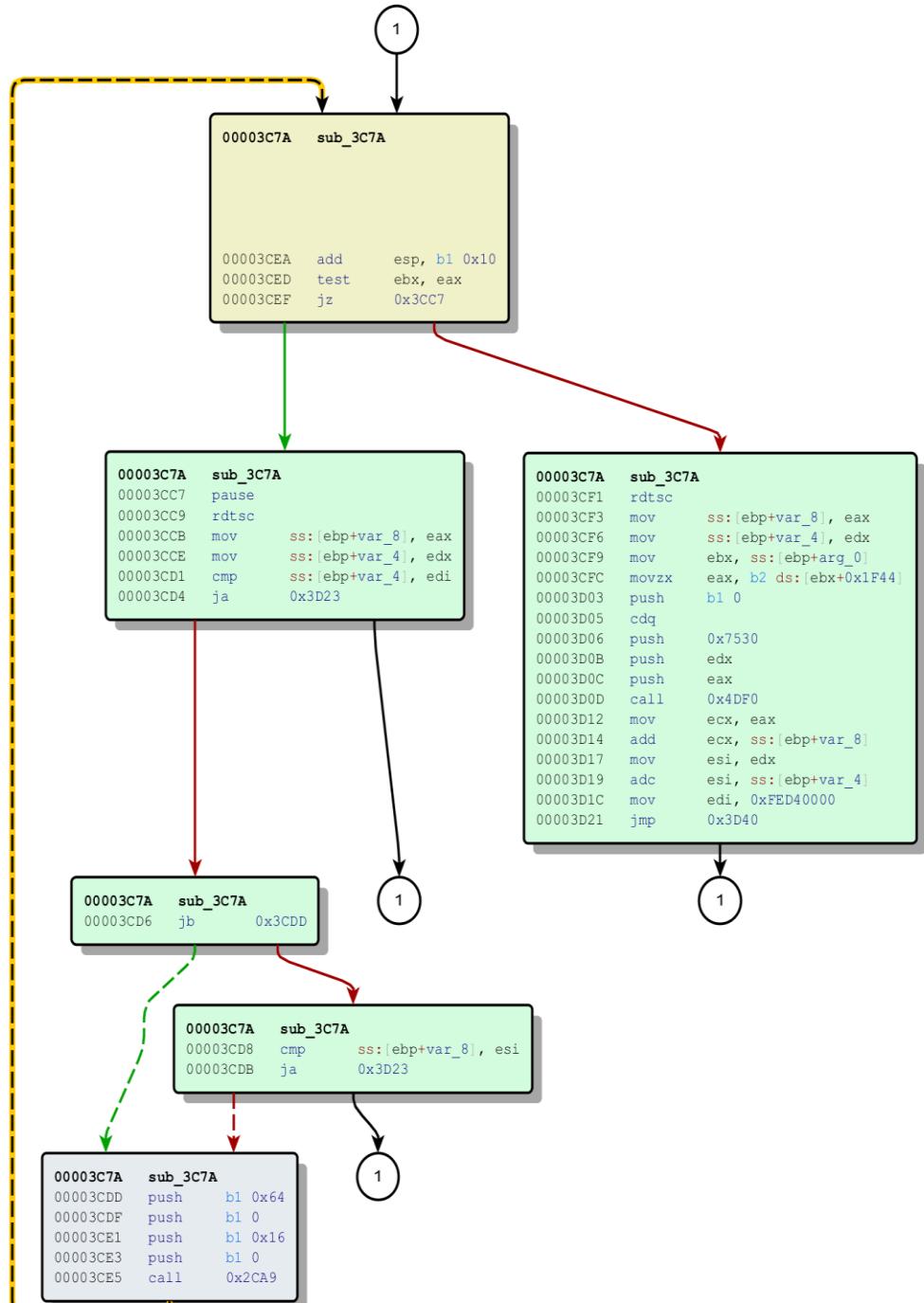
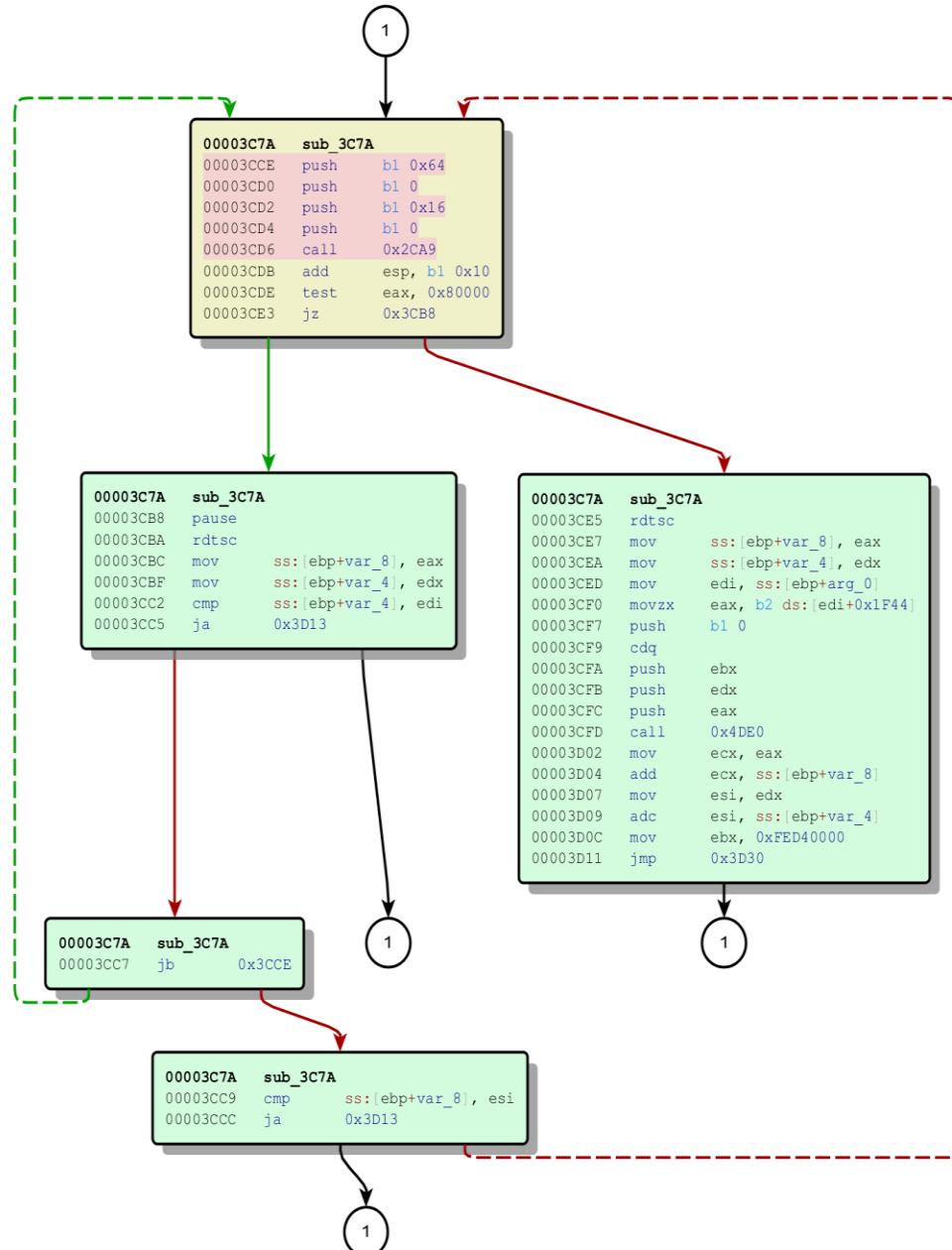
(ACM)
Intel
or NEM)

BB (IBBM)

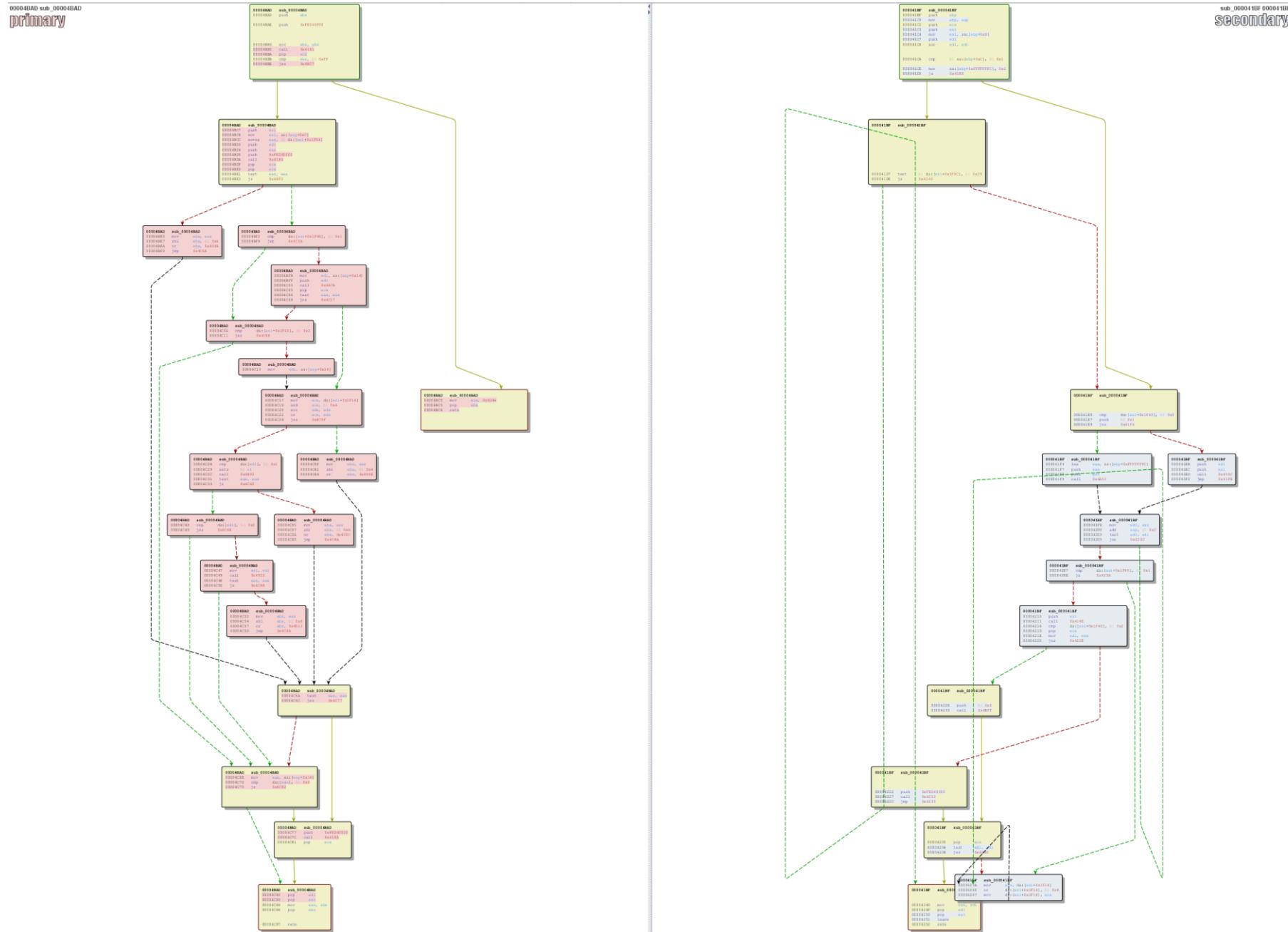
```
c:\Users\matrosov\Desktop\cpu_rec-1.0\cpu_rec-1.0>python cpu_rec.py -v BootGuard_ACM.bin
INFO : Default set of size 11 is read; 8 different CPUs known
INFO : ... MarkovCrossEntropy[2-grams;A] done in 1.294000s
INFO : ... MarkovCrossEntropy[3-grams;A] done in 1.796000s
BootGuard_ACM.bin
INFO : ...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

Boot Guard: Authenticated Code Module (ACM)





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_STATUS BootGuardPei(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

	0	1	2	3	
0000h:	30	B8	5A	2D	C
0010h:	77	20	ED	A0	
0020h:	00	00	A5	FF	
0030h:	76	{43}	3F	BB	
0040h:	7A	DF	BD	A5	
0050h:					

▼ struct
 ► UB
 UIN
 UIN
 ► UB
 UIN
 UIN

Intel image	Image	Intel
Descriptor region	Region	Descriptor
GbE region	Region	GbE
ME region	Region	ME
BIOS region	Region	BIOS
>efiFirmwareFileSystem2Guid	Padding	Empty (0xFF)
Padding	Volume	FFSv2
>AF1C5203-DB24-4D2A-A2F0-E8C423C5916	Volume	FFSv2
>ADDSF39F1-19D7-4501-A730-CESA27E1154B	Volume	FFSv2
>010f5117-0b91-4f94-974f-09d92172c55	Volume	FFSv2
>PeiAprioriFileNameGuid	File	FreeForm PEI apriori file
>7EB7126D-C45E-4B00-9357-7F5075C9CF9	File	PEI module
>PeiCore	File	PEI core
>CapsulePei	File	PEI module
>902F23C3-E1EE-40D1-9382-36D061A63EAA	File	PEI module
>PiSmmCommunicationPei	File	PEI module
>911886FD-2636-4F4B-A4A9-2E804F235E09	File	PEI module
>9962883C-C025-4FBB-B699-4EA4D147CRA8	File	PEI module
>79A608E6-035A-4D49-A89A-A6D5A27F0E2	File	PEI module
>C1FB0624-27EA-40D1-AM48-94C3DC5C7E0D	File	PEI module
>C7D4B8C1-E80A-4C91-B08E-FC9A99-28B011	File	PEI module
>A6AF1F6F-F524-4B82-AE93-22929FC5A6E1	File	PEI module
>52B3D0A7-9565-48E8-BE13-E7C19672183C	File	PEI module
>B41956E7-7CA2-4D2B-9562-186389P0F866	File	PEI module
>C776AE2A-M27-446E-975B-E08EA90780D9	File	PEI module
>CAC39B95-33F5-4596-8188-68E2D0B687B	File	PEI module
>0FE0FAD3-043D-4C65-A94D-FF77FDFF0F2B4	File	PEI module
>E9312938-E56B-4614-A252-CF7D27377E26	File	PEI module
>688445C6-6B75-42CA-8E8E-1CB94421B59B	File	PEI module
>0D1EDF27-E928-4562-92D0-5C82E9C197EAE	File	PEI module
>E9D07F62-25EC-4F9D-MAAB-AAD20B59A10	File	PEI module
>0FD1D3A2-99F7-428B-BC69-8881D429A332	File	FreeForm
>838DCF34-9087-4D55-8A94-A0E71675BF4	File	PEI module
>C91C3C17-FC47-4E65-BD8E-6F486A594F3C	File	FreeForm
>0DCA793A-EA96-4D2B-BD7B-DC7F684E38C1	File	FreeForm
>CapsuleX64	File	PEI module
>PcdPeim	File	CapsuleX64
>0E2DAFG3-8A4F-4026-A899-DE2D7F46E5C	File	PEI module
>A8499E65-A6F6-48B0-96D8-45C266030D83	File	PEI module
>EEEE1161-F78F-4F91-B868-55907169280	File	PEI module
>9C4E8ABC-4B8C-4A9A-9F05-E87523AFC97	File	PEI module
>654F61A-2EDA-4749-A76A-56ED7A0F1CBE	File	PEI module
>F03E6451-297A-4F91-E717-63987327C52	File	PEI module
>1068E0ED-5C8E-4724-B011-2C595965DF2	File	PEI module
>CBC914A-4ABC-A45B-8696-703451D0B653	File	FreeForm
>C95C9849A-D4EC-4E61-8690-3C47C985D6	File	PEI module
>08EF015D-EC55-4B23-B648-7BA40F0FD85D	File	PEI module
>cpuIoPei	File	PcdPeim
>PcatSingleSegmentPciCfg2Pei	File	SgtPvPei
>E60@7905-DC9B-4F71-87D3-51BF67986121	File	SiInitPreMem
>F7E9L9E9-4D40-4F02-8AC9-4B5512708F7F	File	PlatformInitPreMem
>59AD062D-A1C0-44C5-A90F-A1168770468C	File	AfterMemoryDummyDriver
>0xe0Tp1	File	CmosPei
>5AC804F2-7D19-5B5C-A22D-FAF4A8F5178	File	BiosGuardRecovery
>D87C524-C9CF-4D4A-8909-02B6A986F34	File	PeiRamBootPei
>EFF940A0-A095-4758-868F-C7AF313A872	File	CpuIoPei
>29906f8B-2E93-4E40-9E6C-0DA47E8BF5D9	File	PcatSingleSegmentPciCfg2Pei
>B1E9E2CA-8078-4070-BCD-87449AC7D2A6	File	CpuPei
>EF6D52CC-0E99-4F09-96C0-E808089078FC	File	SiInit
>988A03CA-5186-4B55-8949-CADF613DAB1	File	PlatformInit
>349980B6-930A-495-AB04-2E6CFDFF631	File	DxeTp1
>961C198C-1D1C-4B47-87AF-4AE0PF90FD2A6	File	AcpiVariableHobOnSmmramReserveHob
>608039F7-49E9-C9A8-B08G-B78C31B08C80	File	PeiOverClock
>67451698-1825-4AC5-9990-5805C0D75D72	File	AmIPeiCreateDummyRchob
>A6A3A962-C591-4701-9E05-7D30226089DC	File	CryptoPPi
>39E8C1A7-7A69-4A73-83DA-06381932386	File	PeiRambootCacheRdy
>B0D701A4-4C8A-4C75-BCEB-D002D17E6397	File	UsbPei
>D4CF785C-71D9-47D9-AB0E-10186B821D0E	File	Ahcirecovery
>7EDC9C20-6889-4A6F-B515-D647F500B109	File	Recovery
>10C22236-D6F7-4721-AA30-4C12A4238A7	File	FsRecovery
>00026ABF-F334-A1C5-1F70-11E897E9F91	File	IdeRecovery
>89F08649-F297-4436-8548-E08F9e92B8568	File	NvmeRecovery
>998F2BD8-10A6-4C6C-B872-BD04B847A71A	File	SdiorRecovery
>7703DC50-D42B-4916-AC80-8F469035D150	File	AmITcgPlatformPeiAfterMem
>Pad-file	File	Raw
>6520F532-2A27-4195-B331-C0854683E0BA	File	Pad
>BE295870-D377-4B75-BFDC-9AE2F0B0DE22	File	Raw
>5885965C-455D-4CC6-9C4C-7F086967D2B0	File	FreeForm
>Pad-file	File	FreeForm
C30FF4A-10C6-4C0F-A5A4-FD319BAF6CE6	File	Raw
>Pad-file	File	Pad
7C9A098F-2B2B-4B27-8F16-F7D277D58025	File	Raw
>Pad-file	File	Pad
D1E59F50-E8C3-4545-BF61-11F00223C97	File	Raw
>Non-empty pad-file	File	Pad
Free space	Free sp...	

451D0B053]

0123456789ABCDE
0, Z-Ç~•¶..(„.Ò@ž
w í —Ûšýí Q€<.) }
. . ¥ÿ¤ . . . ĐA . E. °MÝ
vC?»V ! Óp ÓÖè. CMe1
z ßž¥* . èD¤ . ¥ÿ\ s¤.

H_KEY HK

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;
    }

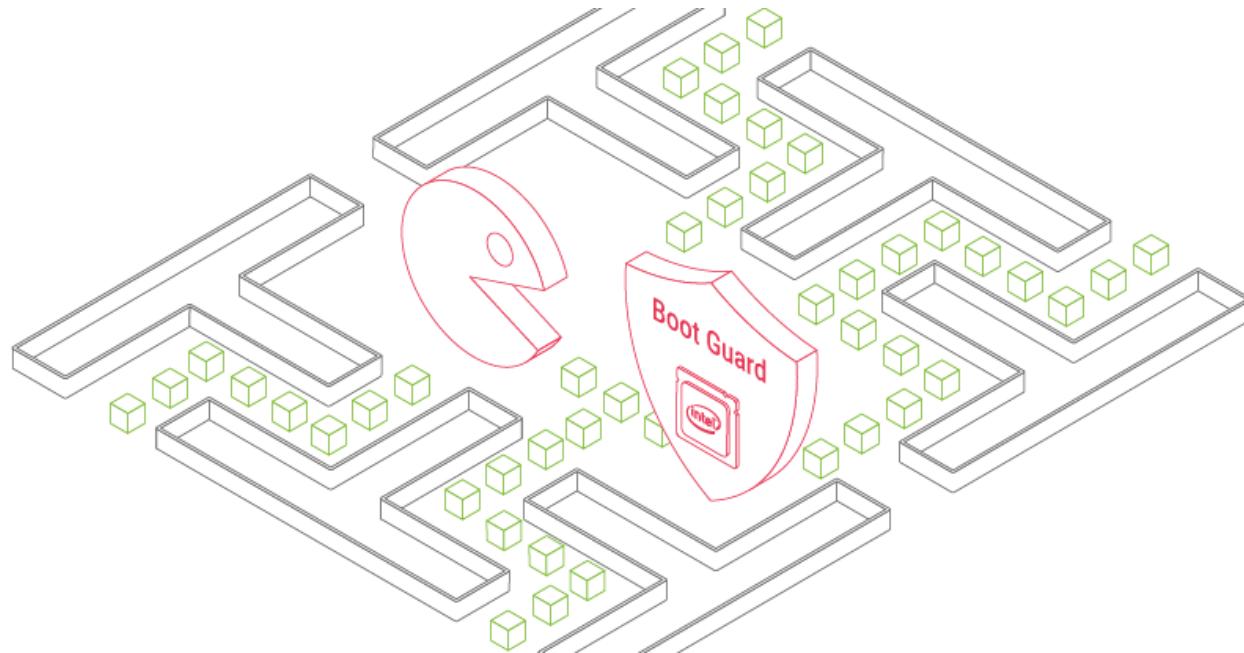
    ...

    return EFI_SUCCESS;
}
```

S3 rootkits coming :-)

← one more 0-day bug?

BootGuardDxe Validation Flow



- <https://embedi.com/blog/bypassing-intel-boot-guard>
- Intel NUC Boot Guard Bypass CVE-2017-5722 kudos to Alex Ermolov
- <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00084>

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:
Localized Language:

Independent Firmware Recovery:
Enabled

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

Root Guard Configuration

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

14)

(CVE-2017-11313)



copy from Gigabyte official website



Vertical Markets

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



Powerful Commercial Applications

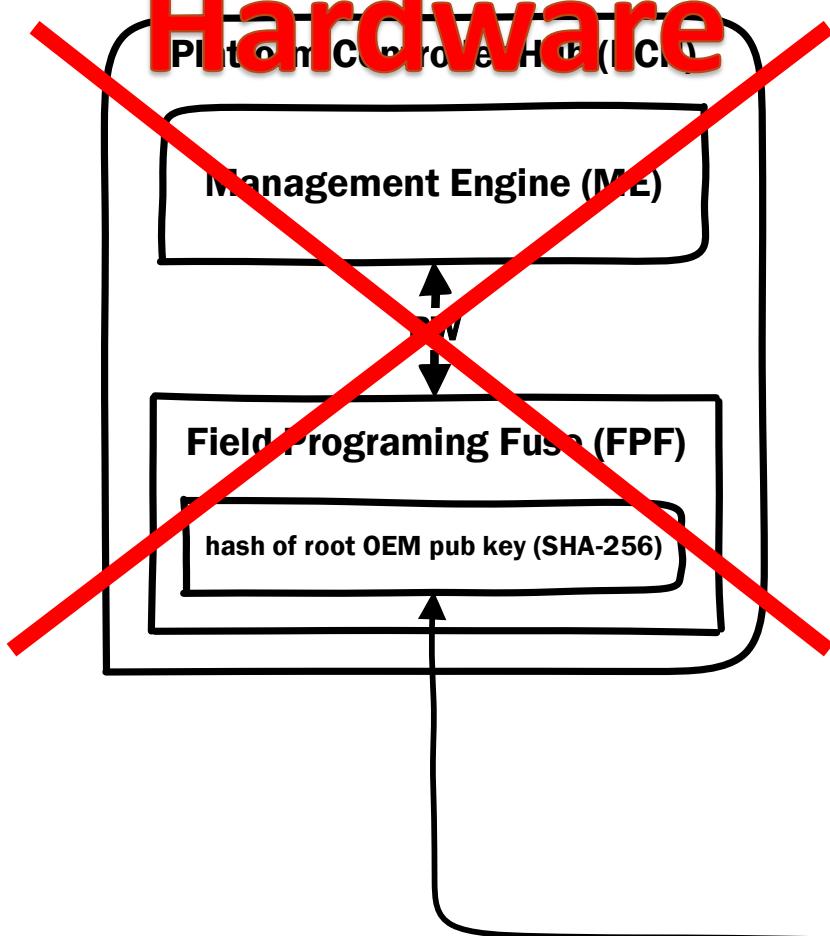
- Factory testing machine
- Bank ATM system
- Gaming equipment
- Vending machine
- Security system

Five steps to bypass Boot Guard

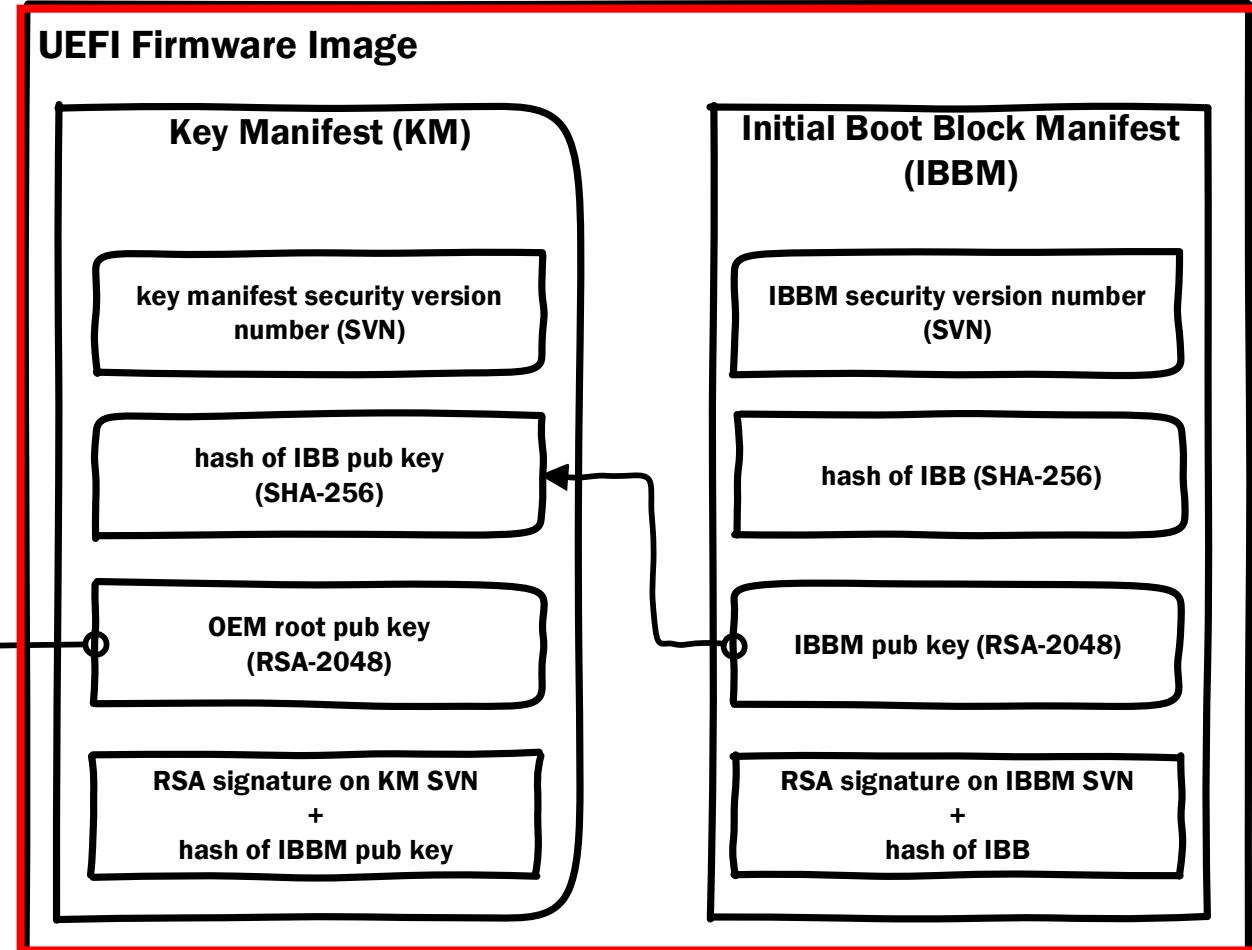
- 1) **Modify UEFI firmware update image with rootkit/implant
or
Disable Intel Boot Guard**
- 2) **Initial Boot Block (IBB)**
 - ✓ Recalculate signature on 2048-bit RSA key pair for IBB
 - ✓ Modify IBB manifest inside UEFI firmware update file
 - ✓ Recalculate signature for IBB manifest with different 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



Firmware



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

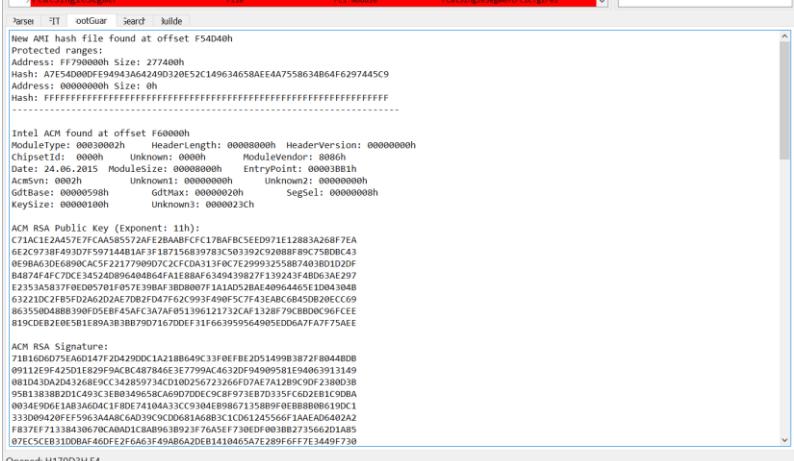
“For FPF issue, we discuss with internal the BIOS don’t need any update but we will add ME Lock tool to our production process soon, the new production ship will include ME Lock.”

UEFITool for Intel Boot Guard visual validation



<https://github.com/LongSoft/UEFITool/releases/tag/A43>

<https://medium.com/@matrosov/bypass-intel-boot-guard-cc05edfca3a9>



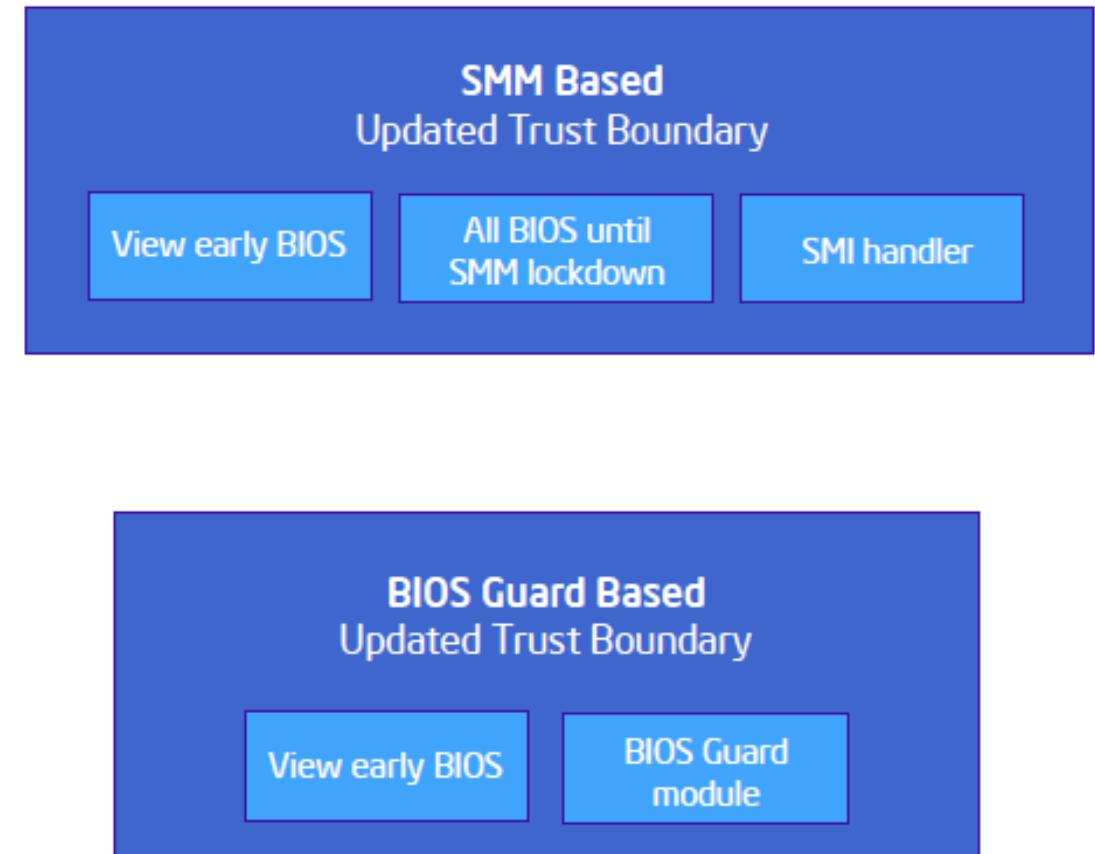
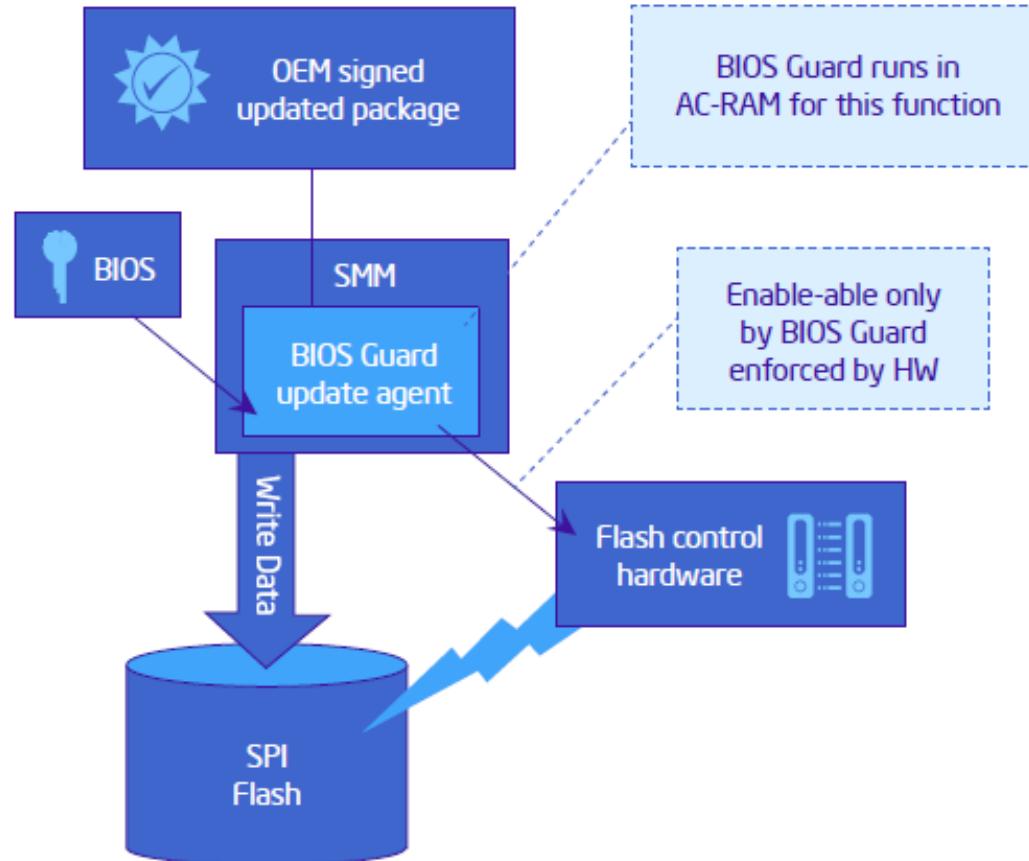
Opened: H170D3H.F4

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



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

ZeroNights HackQuest starting at 10/23



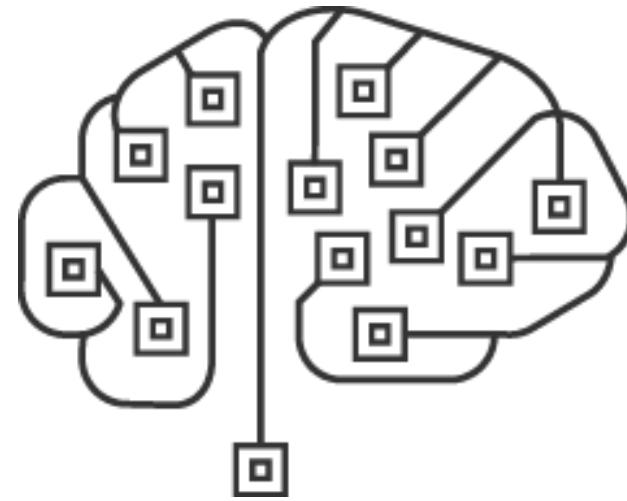
<http://hackquest.zeronights.org/>

16-17 NOVEMBER 2017

ZERO NIGHTS



All the stuff will be released on public
save the link:



https://github.com/REhints/BlackHat_2017

Thank you for your attention!

Alex Matrosov
@matrosov