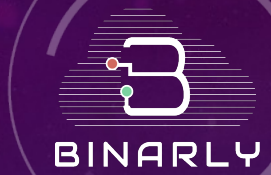
AVAR 2021 VIRTUAL



THE EVOLUTION OF THREAT ACTORS: FIRMWARE IS THE NEXT FRONTIER

ALEX MATROSOV

@MATROSOV

A FEW WORDS ABOUT ME

- Founder and CEO at BINARLY

- 20+ years doing all shades of cyber
- Break a few times CPU’s and GPU’s
- Dedicating all my free time to surfing

AVAR2012
Best Speaker Award

is hereby granted to:

Aleksandr Matrosov

Eugene Rodionov

for being selected and recognized as the most excellent speaker among all AVAR2012 participants.

Date: November 14, 2012

Zhang Jian
AVAR2012 Conference Chairman

AVAR2012
最優秀スピーカー賞

アレクサンダー マトロソフ
ユージン ロディオノフ 殿

AVAR 2012でおこなわれたあなたの講演はすべての講演のなかにおいてもっとも優秀であったという評価を参加者より得られました　よってここにその栄誉を讃えこれを賞します

2012 年 11 月 14 日

AVAR2012　実行委員長
Zhang Jian

Festi Botnet Analysis & Investigation

Alex Matrosov

Eugene Rodionov

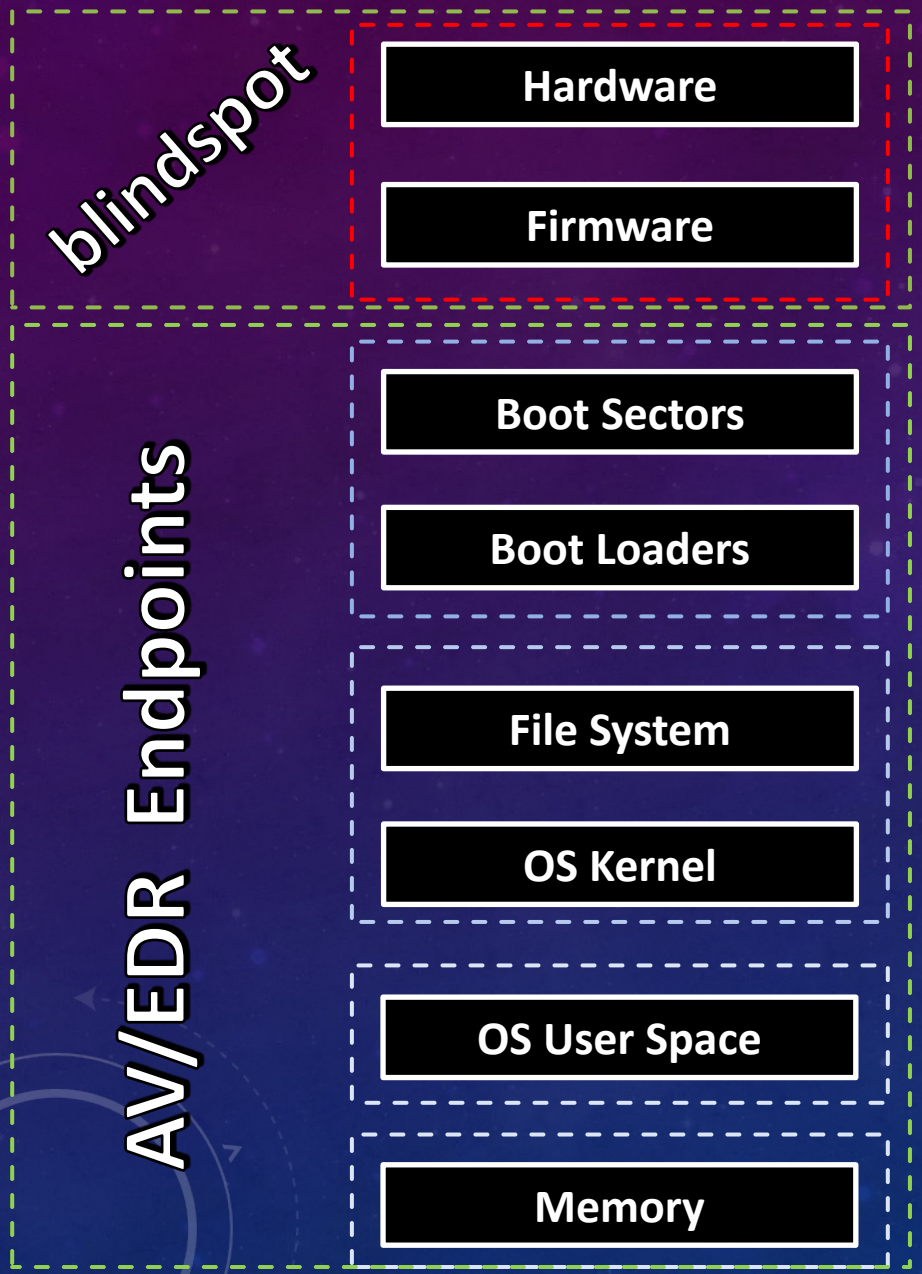
eset

AVAR 2012
HANG ZHOU

Security Industry Visibility Point

Modern Persistence Techniques

Types of Persistence

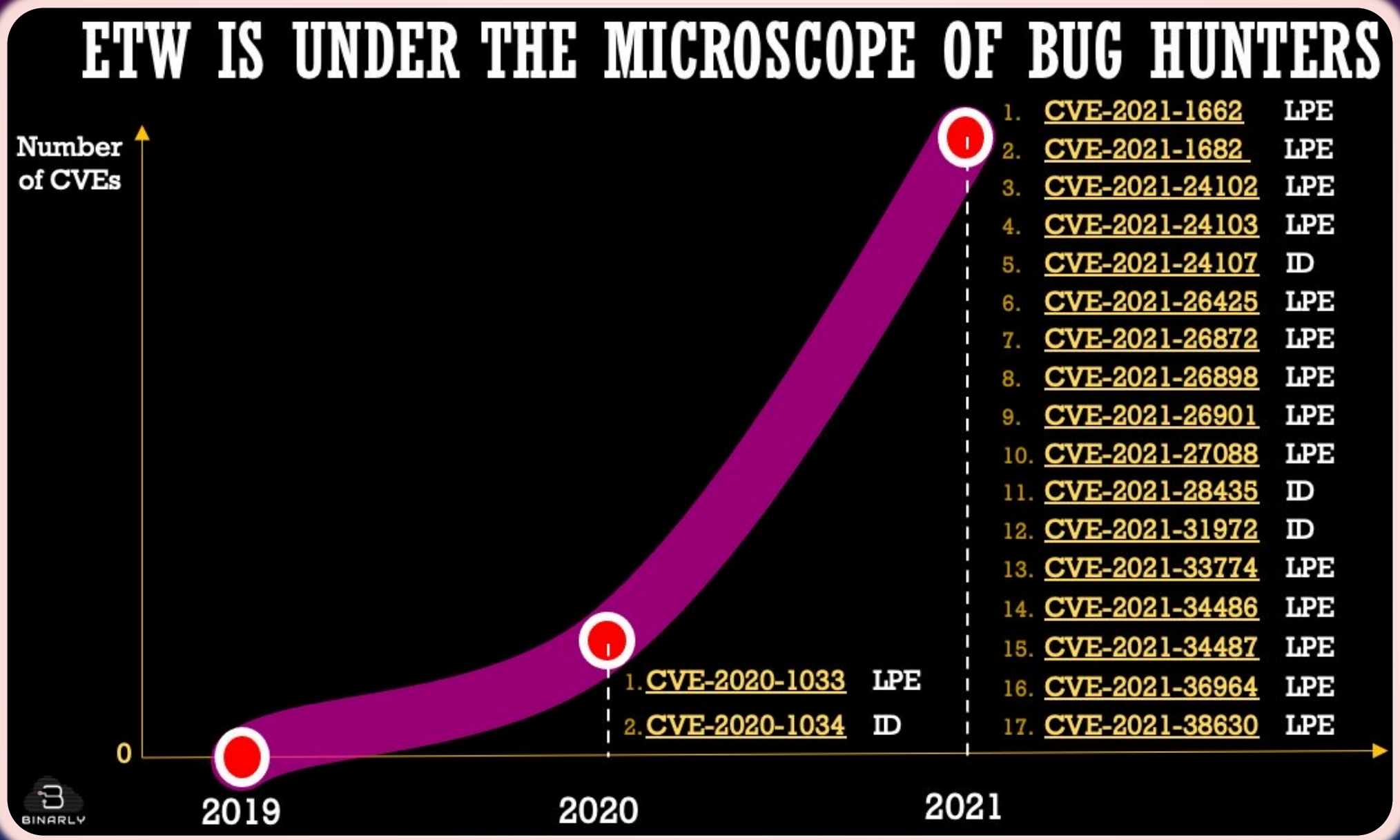


HW/FW Persistence

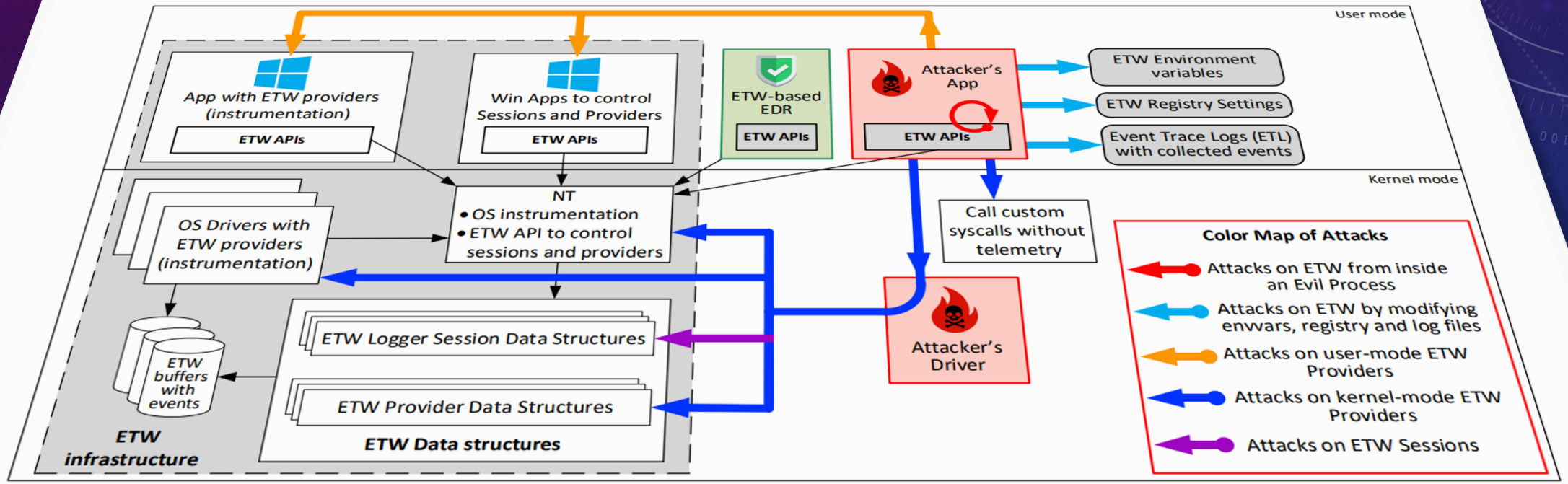
Reboot/Shutdown Persistence

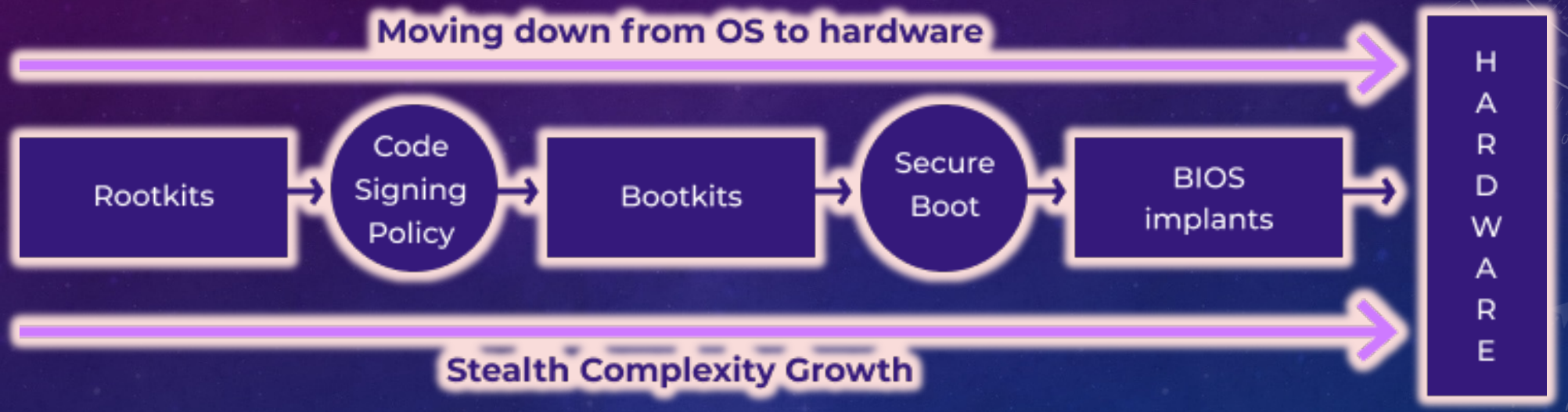
Sleep/Hibernate Persistence

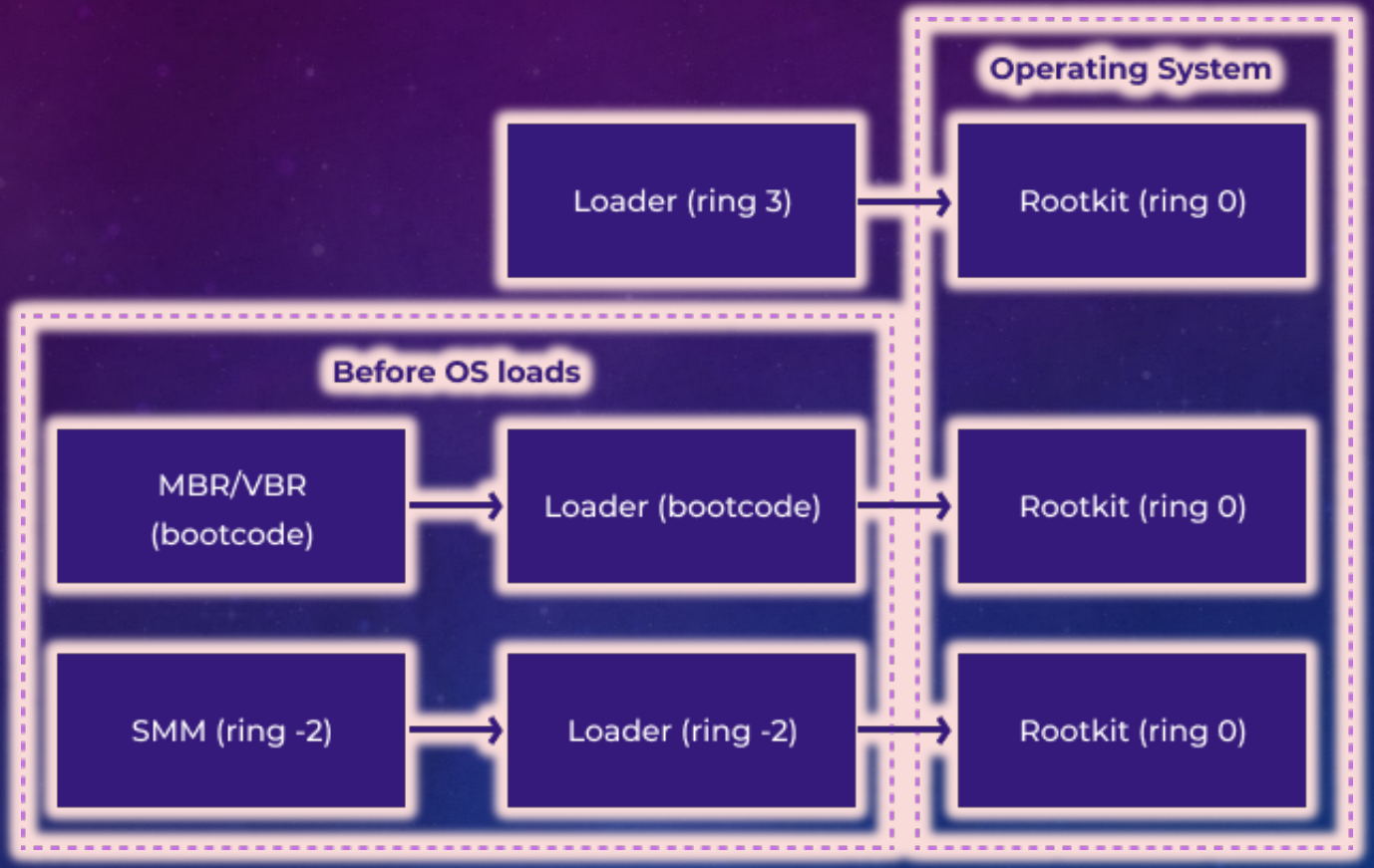
ETW IS UNDER THE MICROSCOPE OF BUG HUNTERS



Threat Modeling ETW

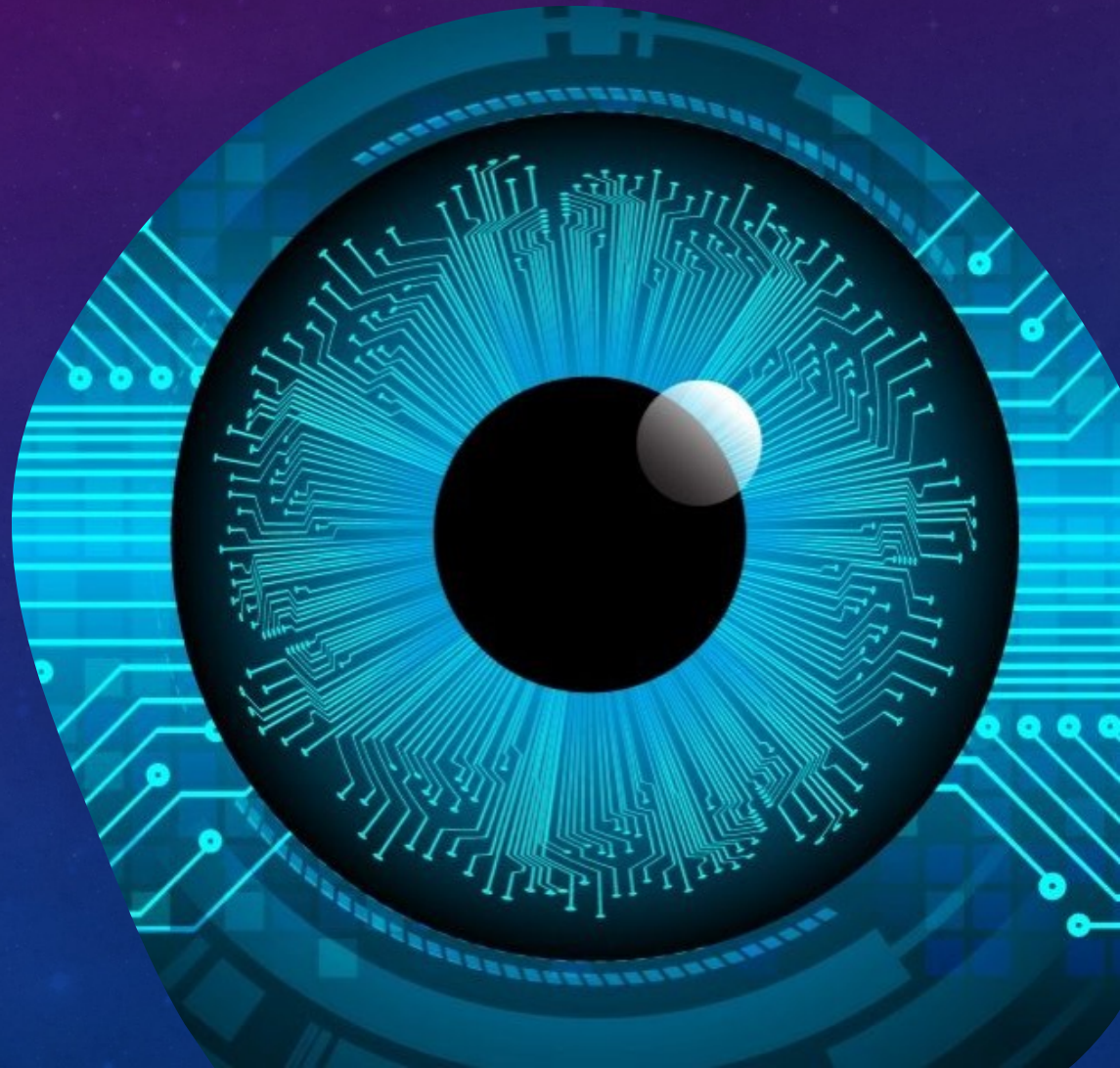



Moving down from OS to hardware
Rootkits
Code Signing Policy
Bootkits
Secure Boot
BIOS implants
HARDWARE
Stealth Complexity Growth


Operating System
Loader (ring 3)
Rootkit (ring 0)
Before OS loads
MBR/VBR
(bootcode)
Loader (bootcode)
Rootkit (ring 0)
SMM (ring -2)
Loader (ring -2)
Rootkit (ring 0)

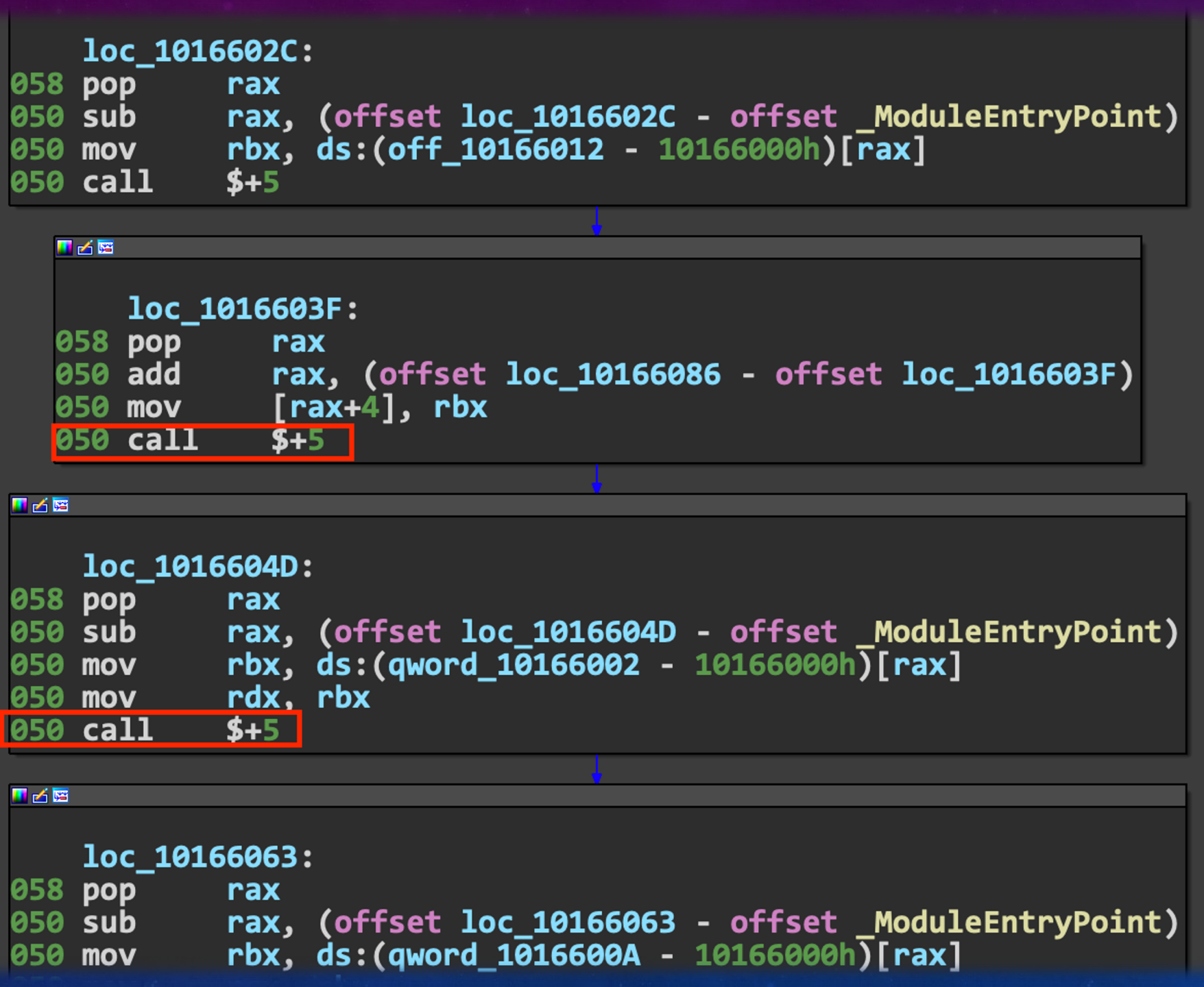
```
.text:00000000000002BD                mov     r9d, 1          ; DataSize
.text:00000000000002C3                lea     rdx, VendorGuid ; VendorGuid
.text:00000000000002CA                mov     [rsp+38h+Data], rax ; Data
.text:00000000000002CF                mov     rax, cs:gRT_368
.text:00000000000002D6                lea     rcx, VariableName ; "fTA"
.text:00000000000002DD                lea     r8d, [r9+6]     ; Attributes
.text:00000000000002E1                mov     [rsp+38h+arg_8], 0
.text:00000000000002E6                call    [rax+EFI_RUNTIME_SERVICES.SetVariable] ; gRT->SetVariable()
.text:00000000000002E6                                        ; EFI_STATUS(EFIAPI * EFI_SET_VARIABLE) (IN CHAR16 *VariableName
.text:00000000000002E6                                        ; VariableName   A Null-terminated string that is the name of th
.text:00000000000002E6                                        ; VendorGuid     A unique identifier for the vendor.
.text:00000000000002E6                                        ; Attributes     Attributes bitmask to set for the variable.
.text:00000000000002E6                                        ; DataSize       The size in bytes of the Data buffer. Unless th
.text:00000000000002E6                                        ; then a SetVariable() call with a DataSize of zero will not cau
.text:00000000000002E9                xor     eax, eax
.text:00000000000002EB                add     rsp, 38h
.text:00000000000002EF                retn
text:00000000000002EF _ModuleEntryPoint endp
```

5-year old indicator




BIOS
UEFI
BIOS boot code
MBR (Master Boot Record)
VBR/IPL
(Volume Boot Record/ Initial Program Loader)
bootmgr
winload.efi
Load kernel and boot start drivers
UEFI boot code
UEFI boot loader (bootmgfw.efi)
winload.efi
Load kernel and boot start drivers
Isn't Secure Boot supposed to keep us all safe?

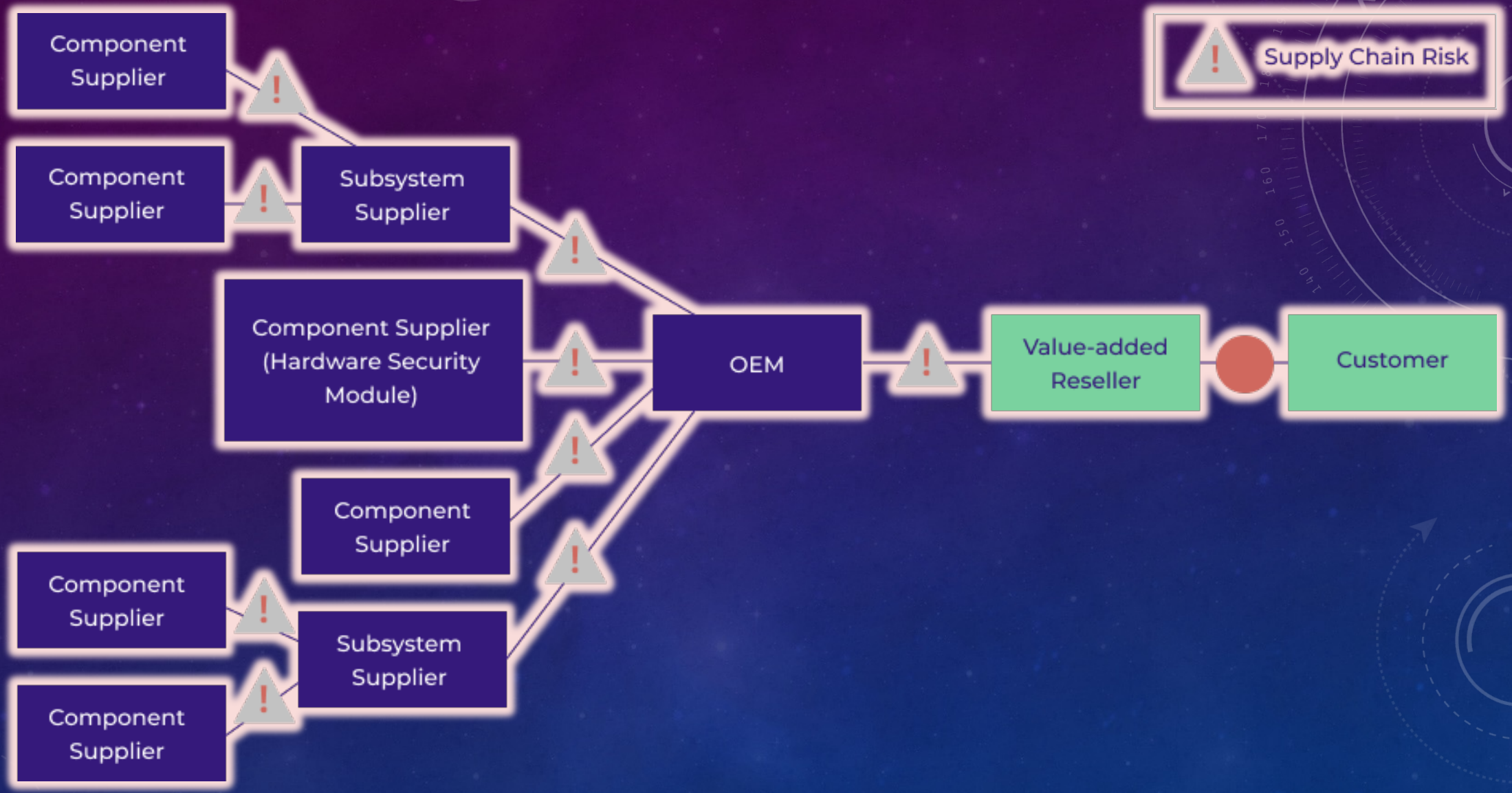
Reversing Modern Malware and Next Generation Threats


loc_1016602C:
058 pop rax
050 sub rax, (offset loc_1016602C - offset _ModuleEntryPoint)
050 mov rbx, ds:(off_10166012 - 10166000h)[rax]
050 call $+5
loc_1016603F:
058 pop rax
050 add rax, (offset loc_10166086 - offset loc_1016603F)
050 mov [rax+4], rbx
050 call $+5
loc_1016604D:
058 pop rax
050 sub rax, (offset loc_1016604D - offset _ModuleEntryPoint)
050 mov rbx, ds:(qword_10166002 - 10166000h)[rax]
050 mov rdx, rbx
050 call $+5
loc_10166063:
058 pop rax
050 sub rax, (offset loc_10166063 - offset _ModuleEntryPoint)
050 mov rbx, ds:(qword_1016600A - 10166000h)[rax]

```
Verifying: ..\..\resources\kaspersky_bl_1.efi
Signature Index: 0 (Primary Signature)
Hash of file (sha256): 81D8FB4C9E2E7A8225656B4B8273B7CBA4B03EF2E9EB20E0A0291624ECA1BA86

Signing Certificate Chain:
    Issued to: Microsoft Corporation Third Party Marketplace Root
    Issued by: Microsoft Corporation Third Party Marketplace Root
    Expires:   Sat Oct 06 05:09:33 2035
    SHA1 hash: 05861FDE0CCACD6EEC8D91DB6E0F22C257748532

        Issued to: Microsoft Corporation UEFI CA 2011
        Issued by: Microsoft Corporation Third Party Marketplace Root
        Expires:   Sun Jun 28 04:32:45 2026
        SHA1 hash: 46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3

            Issued to: Microsoft Windows UEFI Driver Publisher
            Issued by: Microsoft Corporation UEFI CA 2011
            Expires:   Sun Aug 12 03:20:00 2018
            SHA1 hash: B86A405A7958003D441423D2726930D4B0424350

The signature is timestamped: Thu Feb 08 02:46:56 2018
Timestamp Verified by:
    Issued to: Microsoft Root Certificate Authority 2010
    Issued by: Microsoft Root Certificate Authority 2010
    Expires:   Sun Jun 24 05:04:01 2035
    SHA1 hash: 3B1EFD3A66EA28B16697394703A72CA340A05BD5

        Issued to: Microsoft Time-Stamp PCA 2010
        Issued by: Microsoft Root Certificate Authority 2010
        Expires:   Wed Jul 02 04:46:55 2025
        SHA1 hash: 2AA752FE64C49ABE82913C463529CF10FF2F04EE

            Issued to: Microsoft Time-Stamp Service
            Issued by: Microsoft Time-Stamp PCA 2010
            Expires:   Sat Sep 08 00:56:54 2018
            SHA1 hash: C9ECBB482D35D994BEB68EF726A9316E8A878E32
```

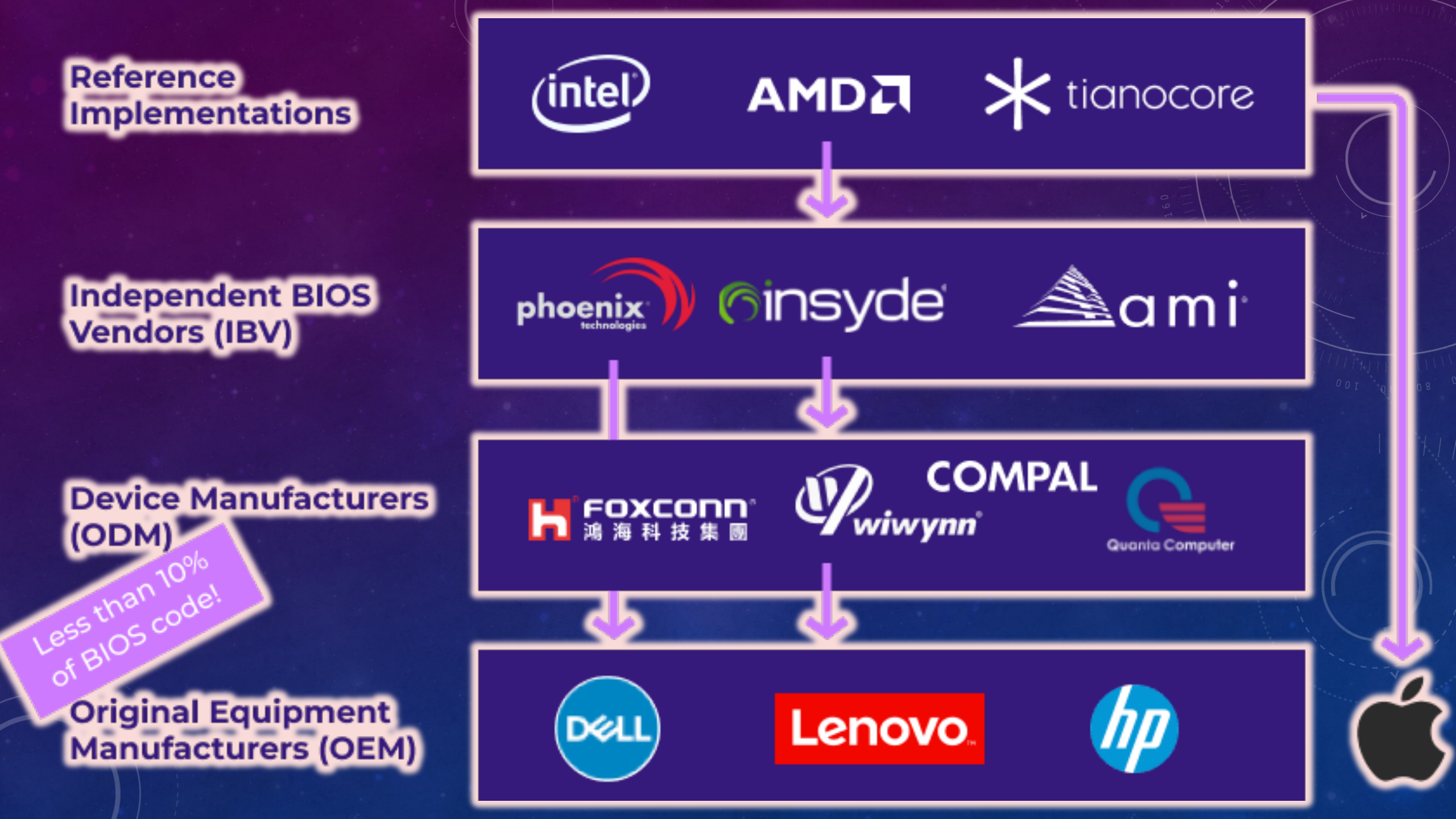
SIGNED != TRUSTED

WE BLINDLY TRUST ANY SIGNED CODE COMING FROM TRUSTED SOURCE

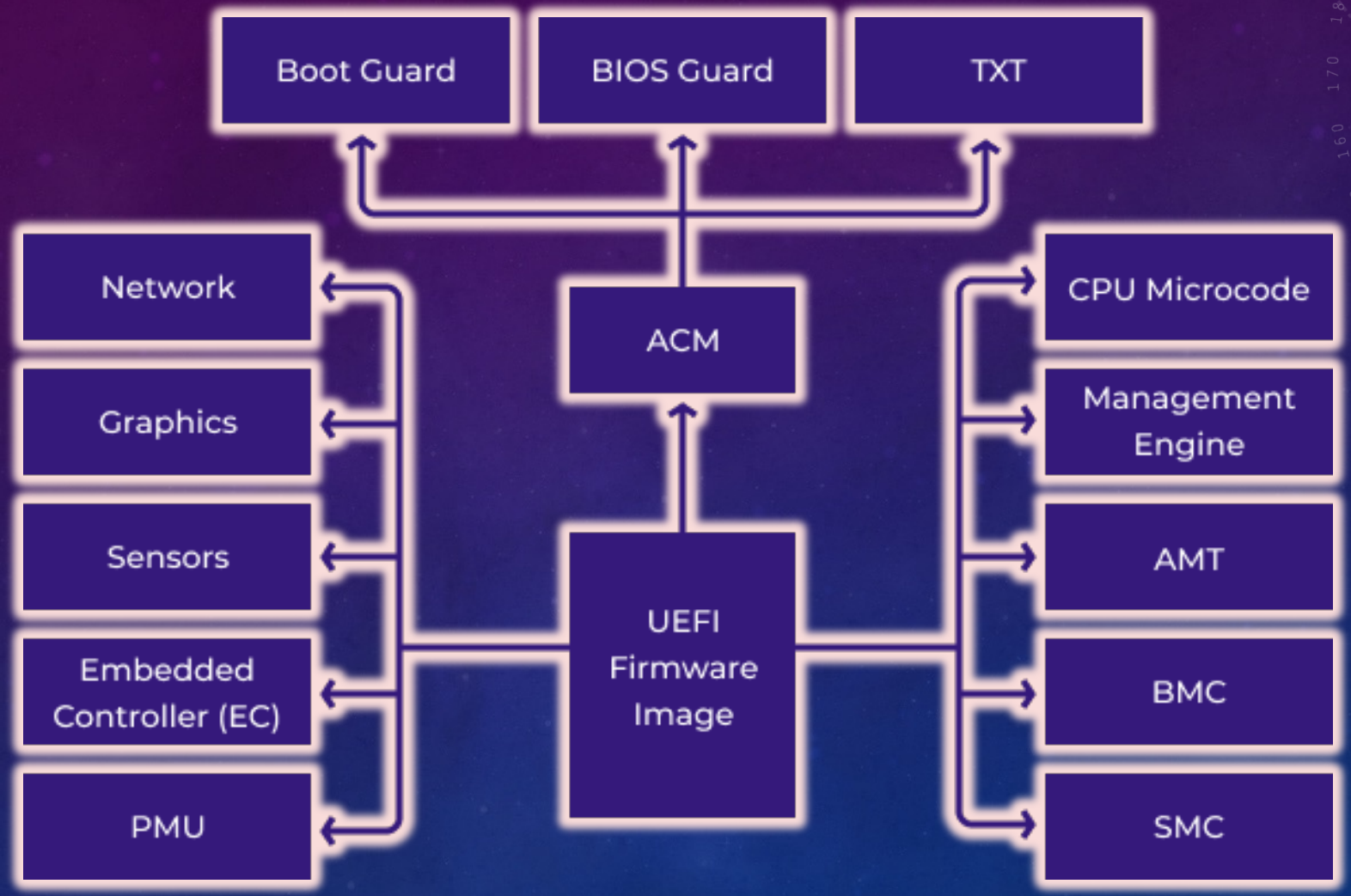

Supply Chain Risk
Component Supplier
Component Supplier
Subsystem Supplier
Component Supplier (Hardware Security Module)
Component Supplier
Component Supplier
Subsystem Supplier
Component Supplier
OEM
Value-added Reseller
Customer

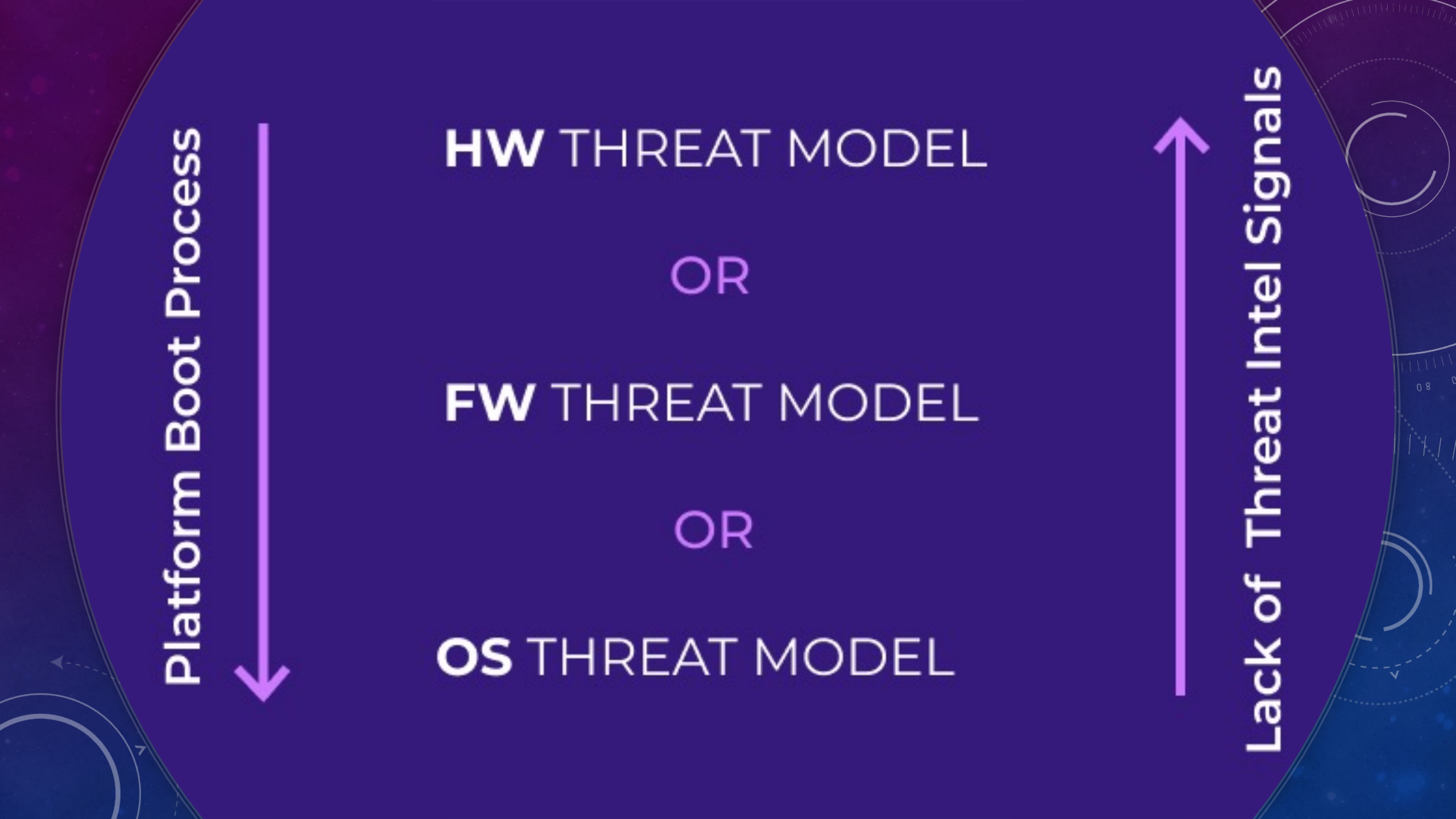
Vendor Name	Vendor Advisory	CVE	URL
Intel	INTEL-SA-00525	CVE-2021-0144	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00525.html
Dell	DSA-2021-146	CVE-2021-0144	https://www.dell.com/support/kbdoc/en-us/000189473/dsa-2021-146-dell-client-platform-security-update-for-intel-bssa-vulnerability
Nvidia	NV-5213	CVE-2021-0144	https://nvidia.custhelp.com/app/answers/detail/a_id/5213
Lenovo	LEN-61893	CVE-2021-0144	https://support.lenovo.com/eg/en/product_security/ps500424-intel-bssa-dft-advisory
HP	HPSBHF03736	CVE-2021-0144	https://support.hp.com/za-en/document/ish_4168405-4168434-16/hpsbhf03736
HPE	HPESBHF04171	CVE-2021-0144	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04171en_us
Supermicro	no vendor ID	CVE-2021-0144	https://www.supermicro.com/en/support/security_Intel-SA-00525
F5	K08593253	CVE-2021-0144	https://support.f5.com/csp/article/K08593253

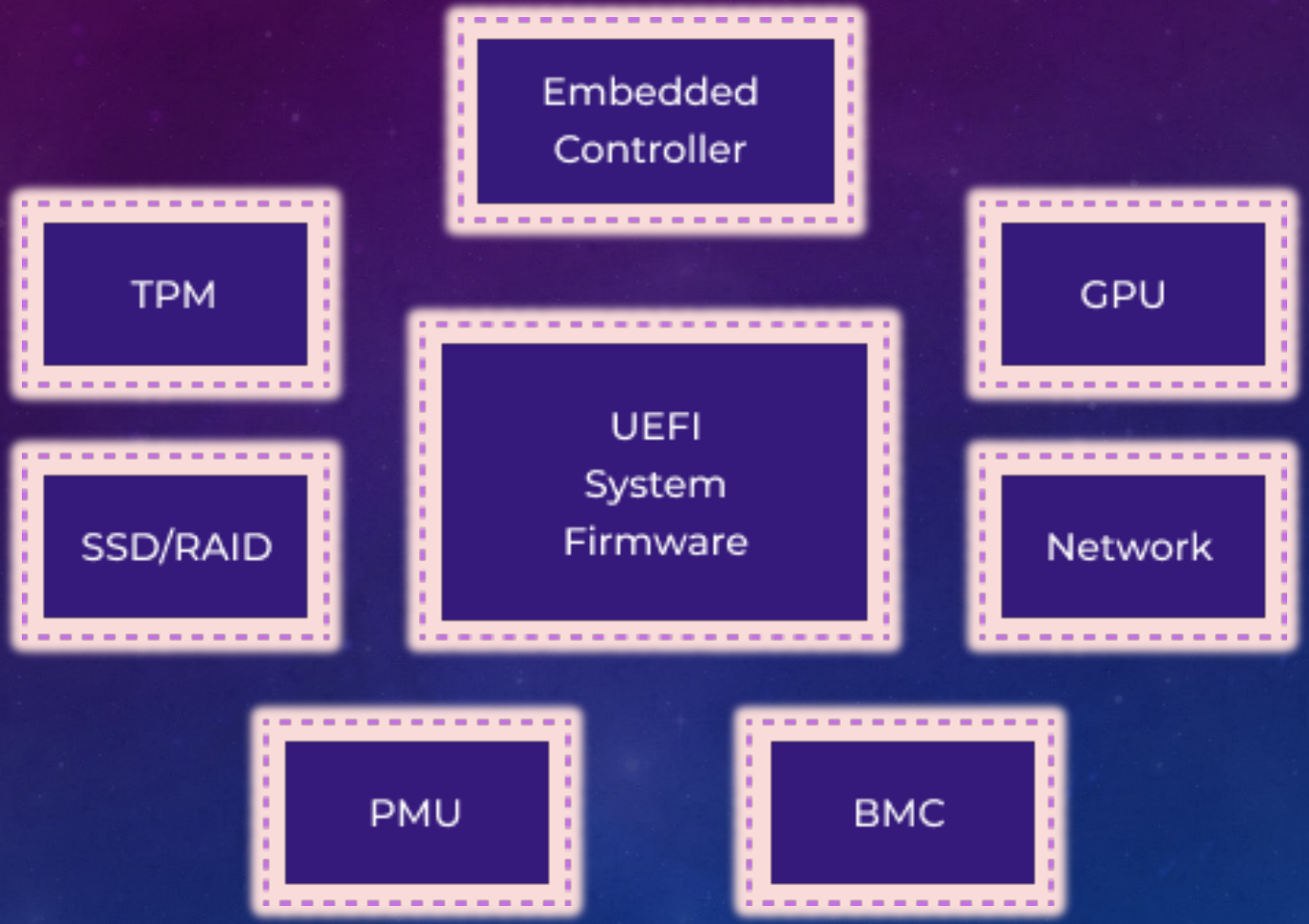
FROM REPORTING THE FIRMWARE VULNERABILITY TO THE FIX USUALLY TAKES AROUND 6-9 MONTHS OR MORE


Reference Implementations
intel
AMD
tianocore
Independent BIOS Vendors (IBV)
phoenix technologies
insyde
ami
Device Manufacturers (ODM)
FOXCONN 鴻海科技集團
COMPAL
wiwynn
Quanta Computer
Less than 10% of BIOS code!
Original Equipment Manufacturers (OEM)
DELL
Lenovo
hp

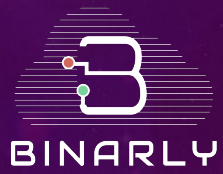
FIRMWARE SUPPLY CHAIN IS VERY COMPLEX AND NOT 100% CONTROLLED BY A SINGLE VENDOR.


Boot Guard
BIOS Guard
TXT
Network
Graphics
Sensors
Embedded Controller (EC)
PMU
ACM
UEFI Firmware Image
CPU Microcode
Management Engine
AMT
BMC
SMC


Platform Boot Process
HW THREAT MODEL
OR
FW THREAT MODEL
OR
OS THREAT MODEL
Lack of Threat Intel Signals


Embedded Controller
TPM
GPU
UEFI System Firmware
SSD/RAID
Network
PMU
BMC

WE BLINDLY TRUST EVERYTHING IS BAKED IN SILICON



AVAR 2021 VIRTUAL

THANK YOU!

@MATROSOV