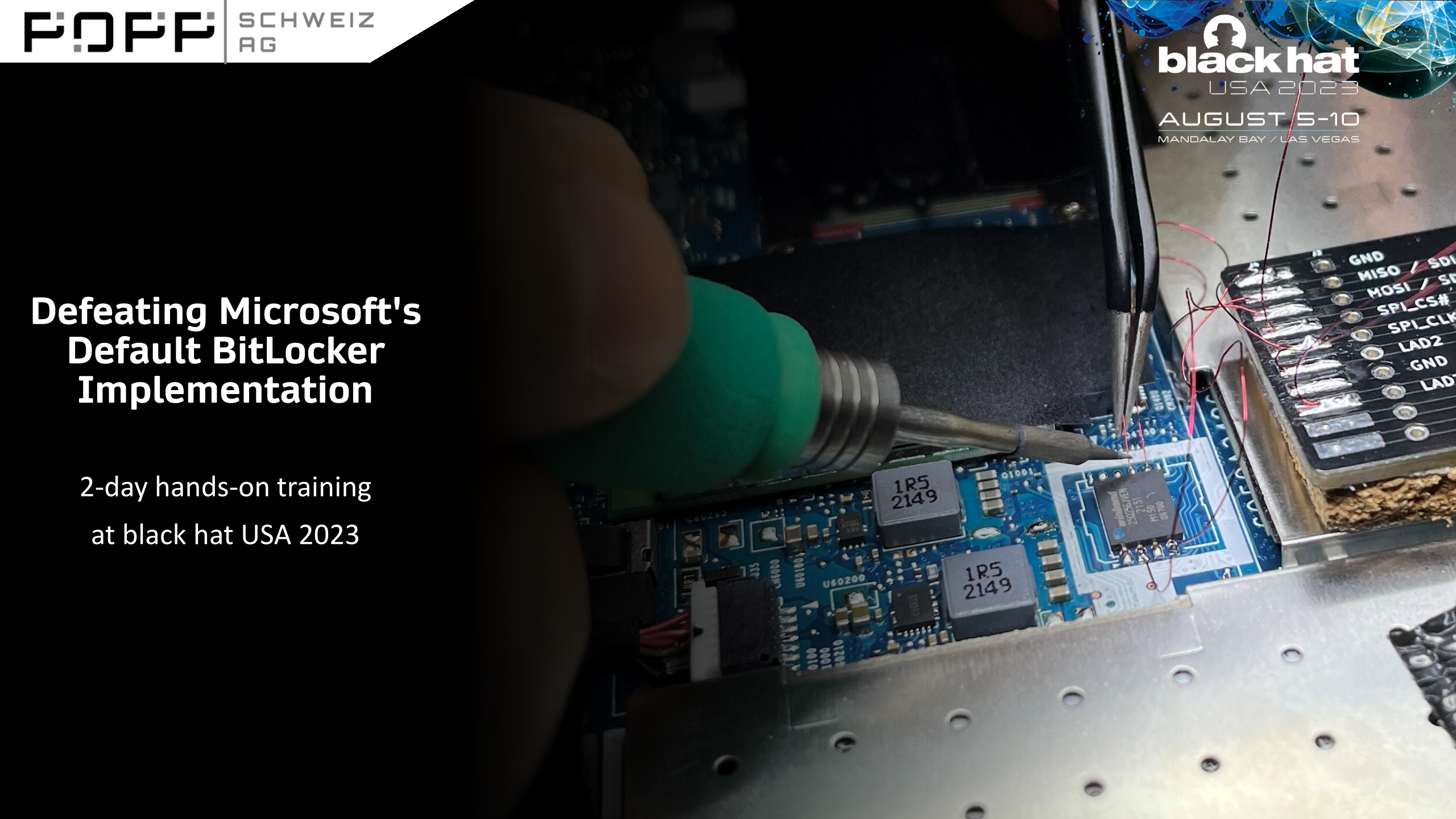
POFP SCHWEIZ AG



Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023

Disclaimer

The material presented in this hardware hacking course is intended solely for educational purposes. It is important to understand that the techniques and knowledge acquired here must be used responsibly and within the boundaries of the law. By participating in this course, you acknowledge and agree to the following:

1. The information and skills obtained in this course should only be applied to devices that you own or have obtained legal consent to test.
2. Unauthorized access, disruption, or tampering with any device without appropriate legal consent is strictly prohibited and may result in criminal or civil liability.
3. The instructors and organizers of this course do not condone any illegal or unethical activities, including hacking, that violate the rights and privacy of others.
4. You are solely responsible for any actions you take based on the knowledge gained from this course. The instructors and organizers shall not be held liable for any damages or consequences arising from the misuse or unauthorized application of this knowledge.
5. Always respect the privacy and security of others. Do not attempt to exploit vulnerabilities or compromise the integrity of any device or network without proper authorization.

Remember, hacking can have legal implications, and it is essential to adhere to ethical guidelines and the laws of your jurisdiction.

Agenda Day 1

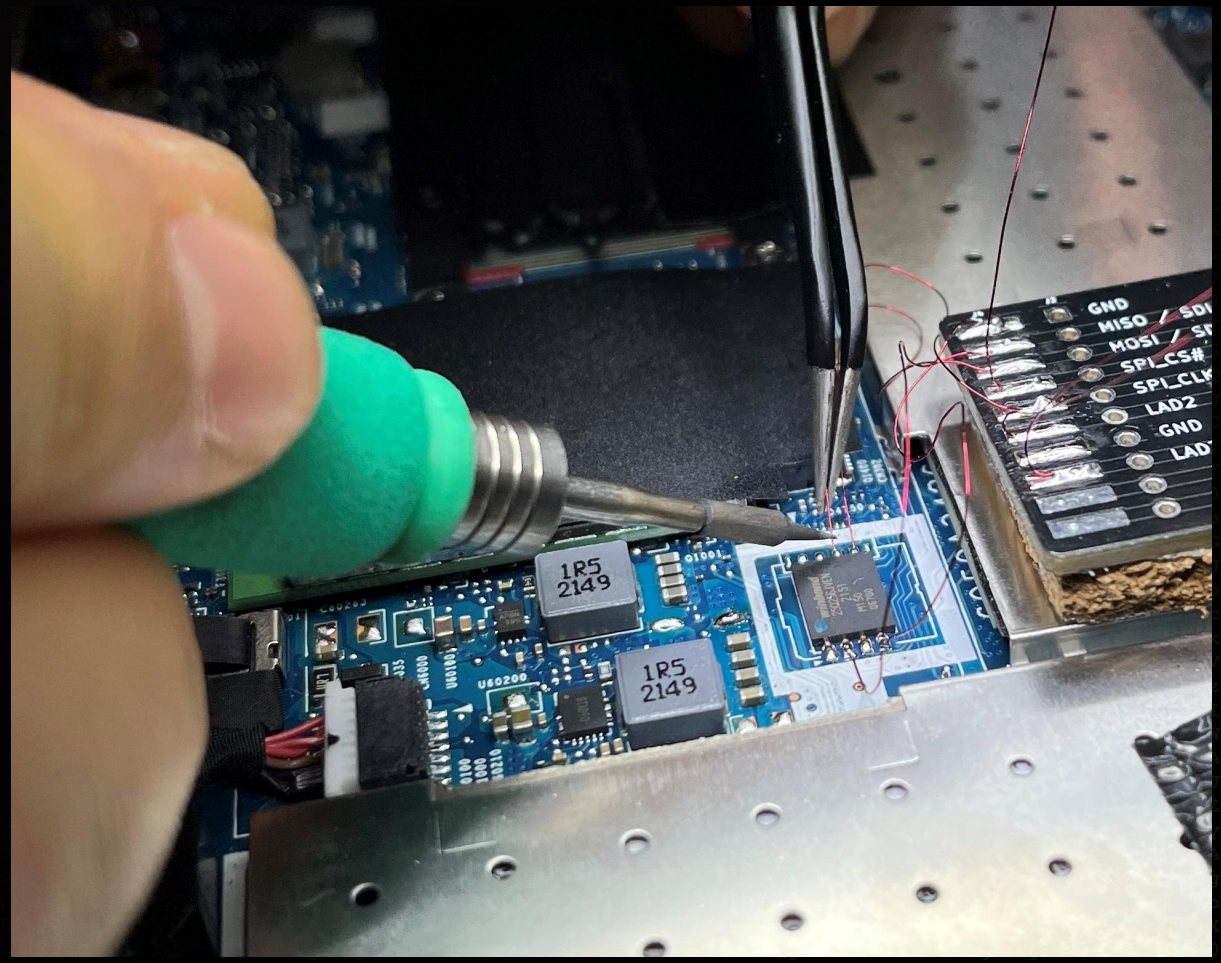
- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
- Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

Welcome to Day 2

- Review
- Open questions?



Agenda Day 2

- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

BitLocker Theory

- Operating Modes
- Protectors
- Key Handling
- Protector Related Threat Model

Operating Modes

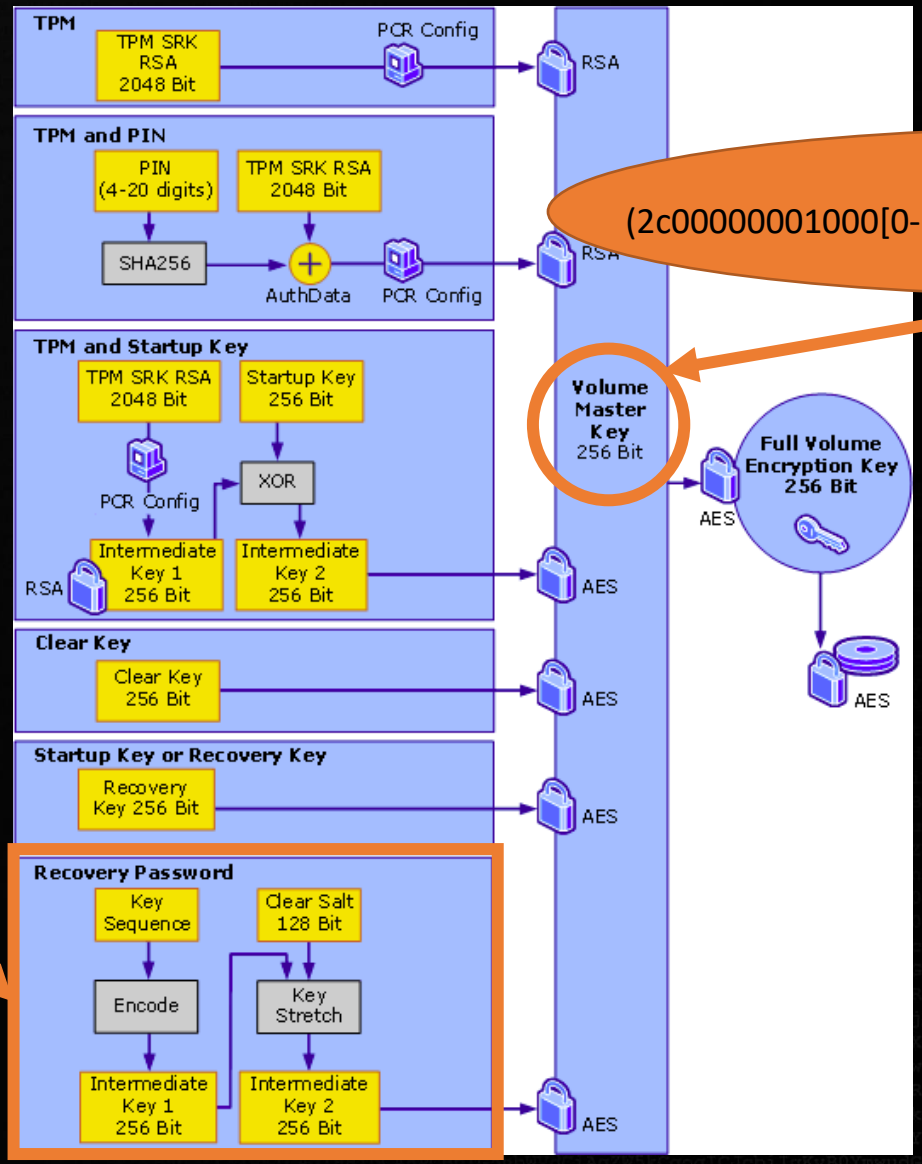
BitLocker Theory

- BitLocker to Go
  - Removable data drives
  - USB flash drives
  - SD cards
  - External hard disk drives
  - … any drives NTFS, FAT16, FAT32 or exFAT formatted
- BitLocker System Drive Encryption
  - Only for Windows operating systems
  - Enforced with Windows 11

BitLocker Protectors

BitLocker Theory

manage-bde.exe -protectors -get <drive>:

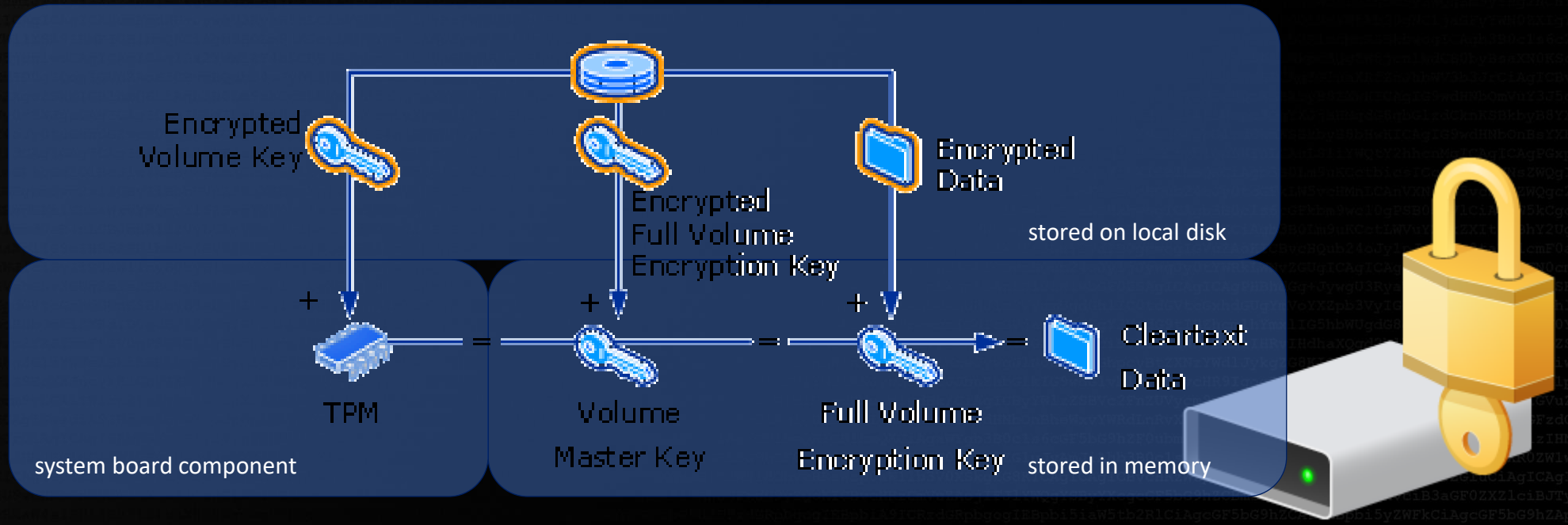


(2c00000001000[0-1]000[0-5]200000)([0-9a-f]{64})

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732774(v=ws.10)

BitLocker Key Handling

BitLocker Theory

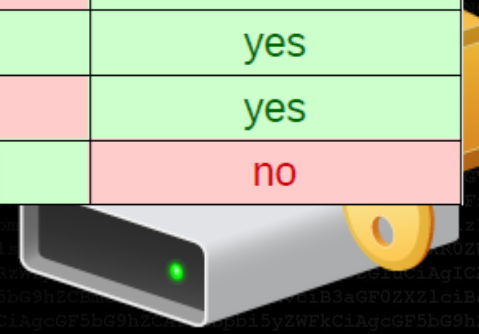


https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732774(v=ws.10)

Protector related Threat Model

BitLocker Theory

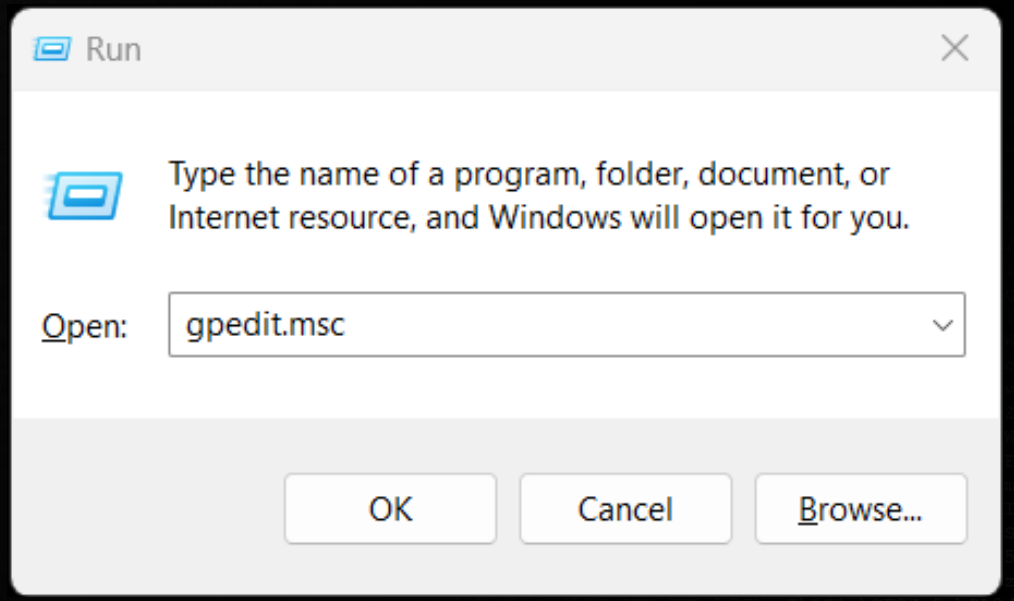
	Protectors	Brute Force Resistant	System Integrity Guaranteed	Key Material Physically Present	Human Input Required	Additional Hardware Required
1	TPM-only	yes	yes	yes	no	no
2	TPM + PIN	yes	yes	no	yes	no
3	TPM + USB key	yes	yes	no	no	yes
4	TPM + PIN + USB Key	yes	yes	no	yes	yes
5	USB Key only	yes	no	no	no	yes
6	Password only	no	no	no	yes	no



GPO Options for BitLocker

BitLocker Theory

- Win + R → gpedit.msc



GPO Options for BitLocker

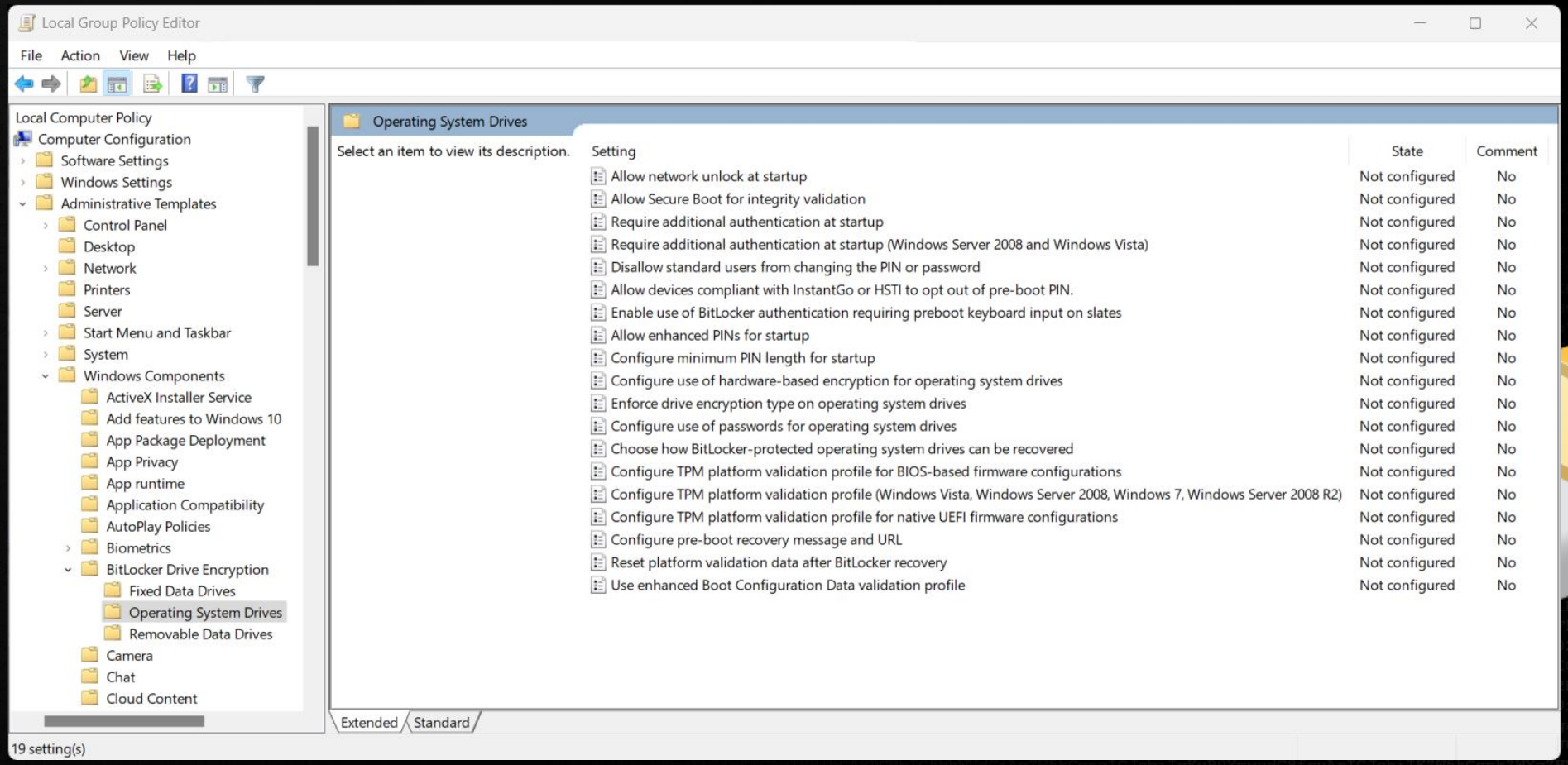
BitLocker Theory

- Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives

- German: Computer Konfiguration > Administrative Vorlagen > Windows-Komponenten > BitLocker Laufwerkverschlüsselung > Betriebssystemlaufwerke

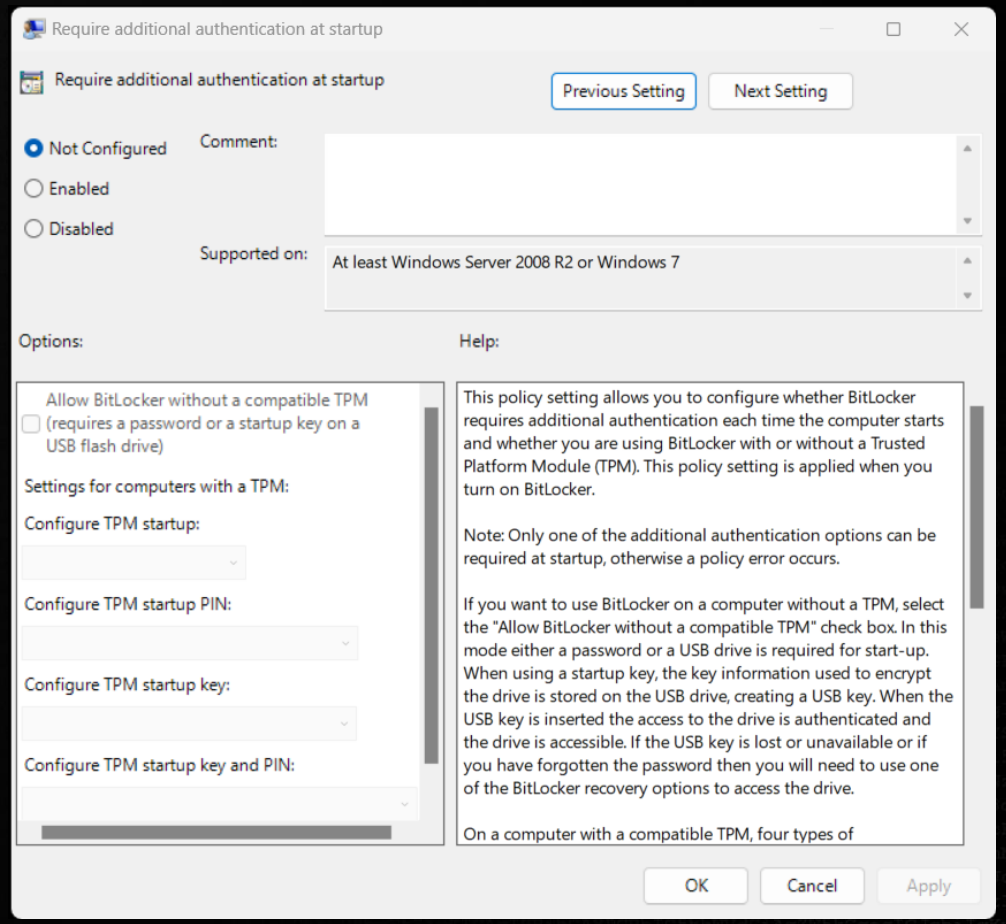
GPO Options for BitLocker

BitLocker Theory



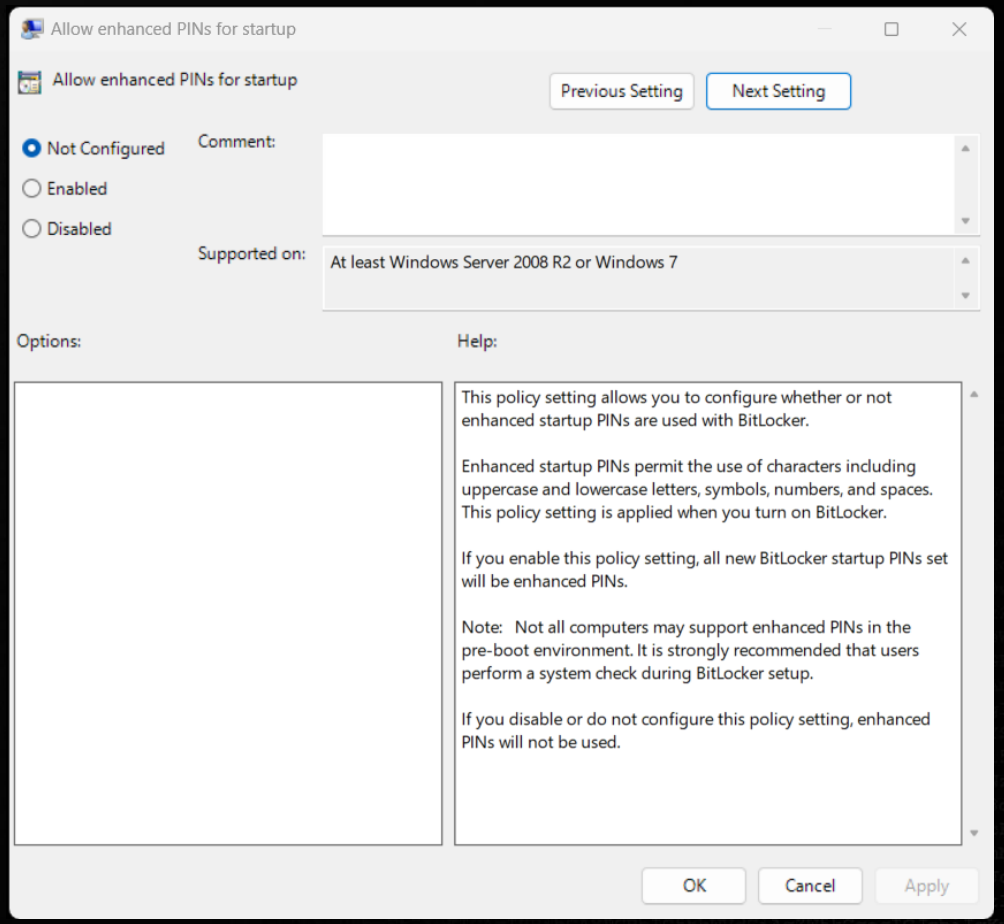
GPO Options for BitLocker

BitLocker Theory



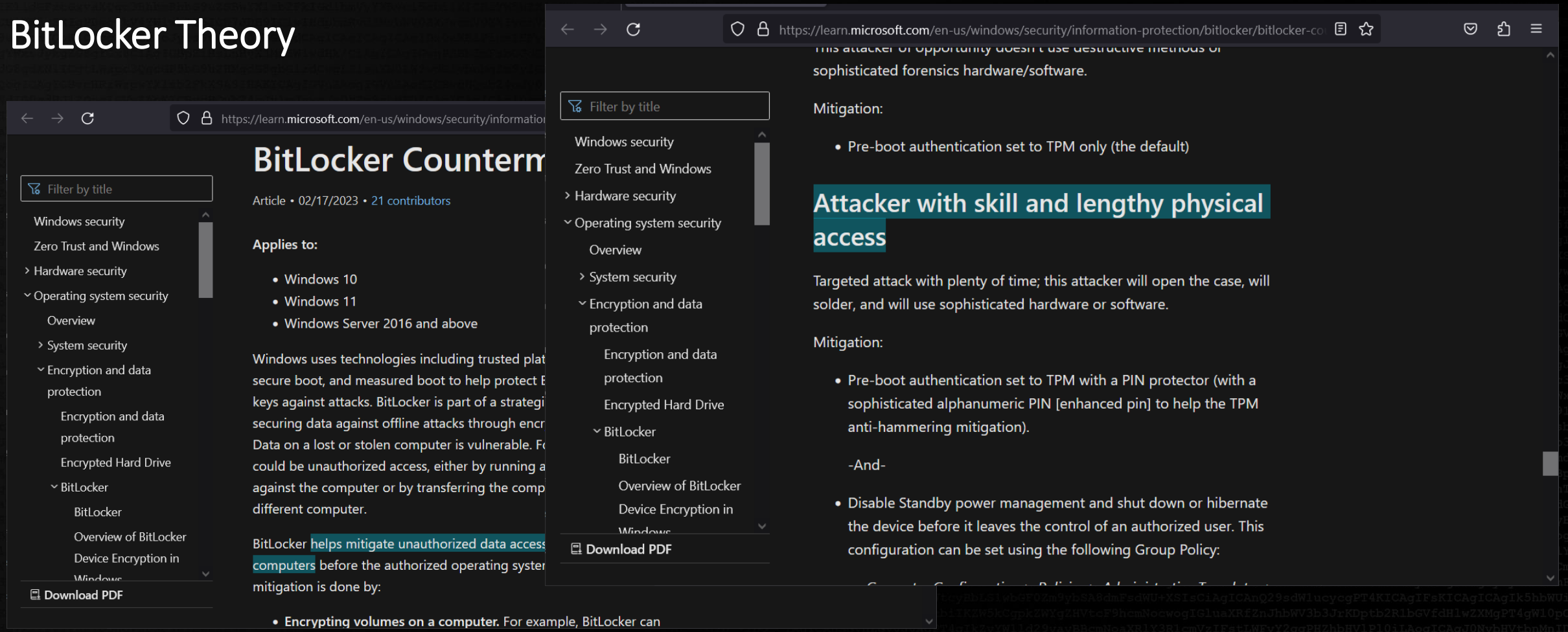
GPO Options for BitLocker

BitLocker Theory



Wait! What?

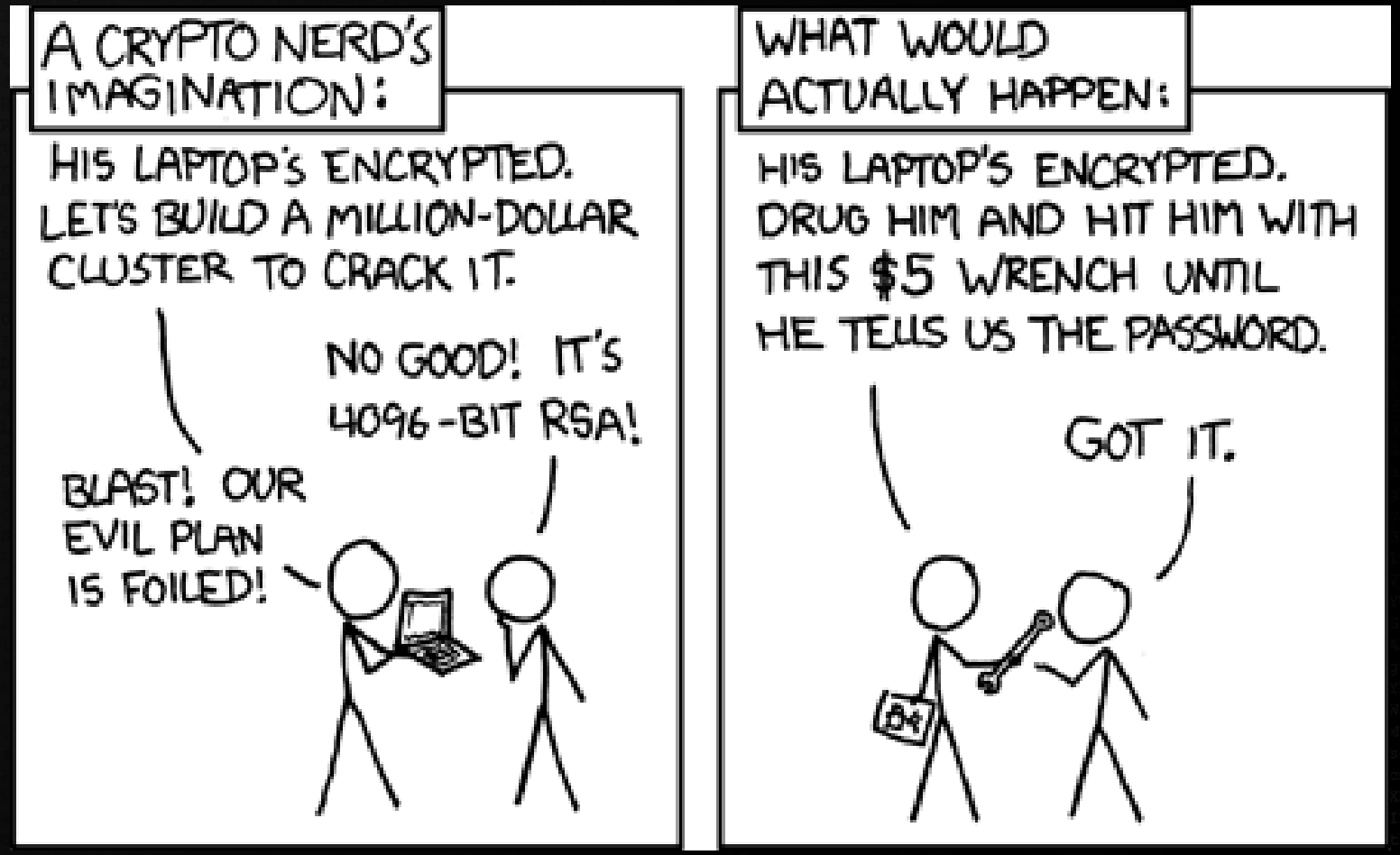
BitLocker Theory



https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures

Reality

BitLocker Theory



https://xkcd.com/538/

Agenda Day 2

- ✅ BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

TPM Theory

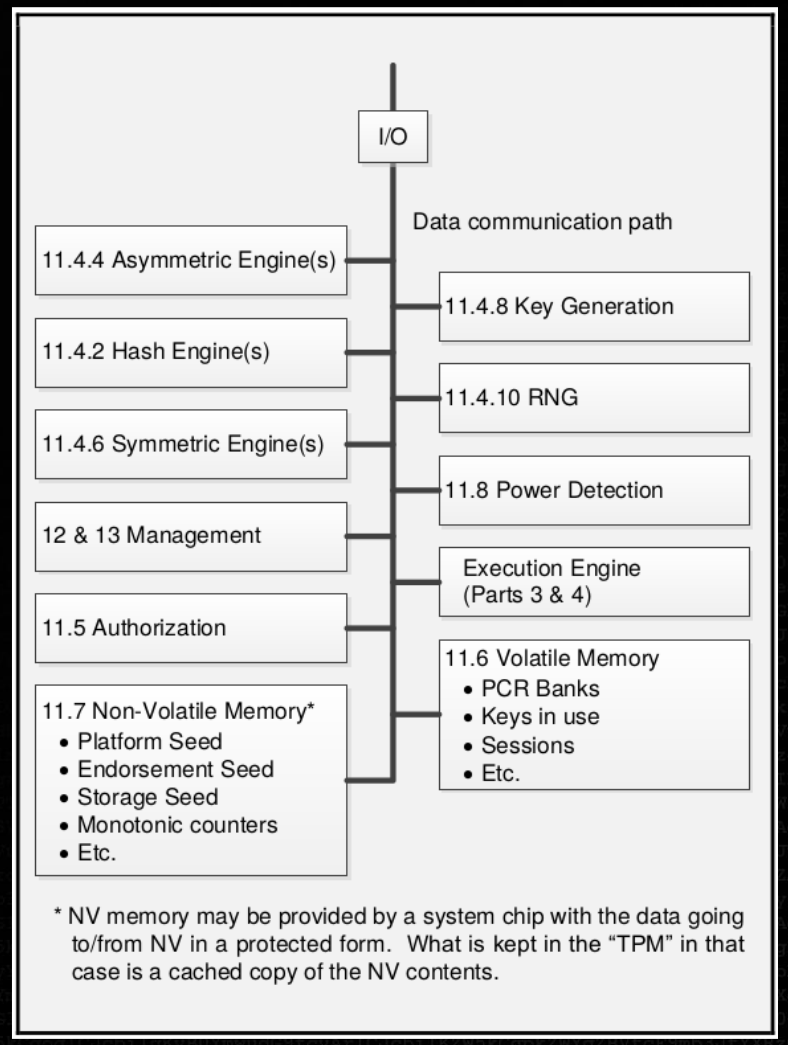
- Trusted Platform Module (TPM)
- TPM Implementations
- TPM Dependent Technologies (Windows)
- Use Case BitLocker
- TPM Hardware Implementation
- Bus Protocols
  - SPI
  - LPC
  - I2C

Trusted Platform Module

TPM Theory

- Not an HSM
- Smartcard equivalent for systems

- Random number generator (RNG)



TPM Implementations

TPM Theory

Trust Element	Security Level	Security Features	Typical Application
Discrete TPM	+++	Tamper Resistant Hardware	Critical Systems
Integrated TPM	++	Hardware	Gateways
Firmware TPM	+	TEE	Entertainment Systems
Software TPM	n/a	n/a	Testing & Prototyping
Virtual TPM	+	Hypervisor	Cloud Environment

TPM Dependent Technologies (Windows)

TPM Theory

- Measured Boot with support for attestation
- TPM-based virtual smart card
- TPM-based certificate storage
- TPM cmdlets
- Physical presence interface
- Endorsement keys
- TPM key attestation
- Anti-hammering

Use Case BitLocker

TPM Theory

1. Measured Boot - to ensure the platforms integrity and unseal the TPM
2. Obtaining PIN / Startup Key if enabled
3. Sending the encrypted VMK to the TPM for unwrapping
4. Decrypting the FVEK with the unwrapped and unsealed VMK
5. Decrypt the drive with the obtained FVEK and continue

Use Case BitLocker

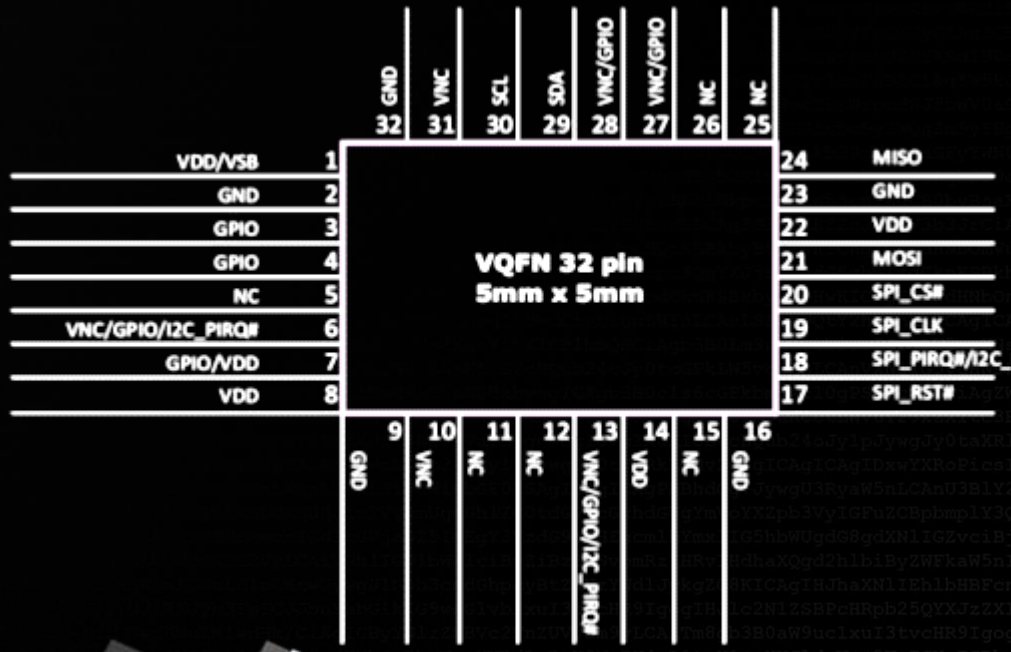
TPM Theory

- **Sending the encrypted VMK to the TPM for unwrapping**
- TPM 2.0 specification "6.5.2.2.2 Data Availability“: any result of every command is put into the TPM_DATA_FIFO_X registers
- X stands for a locality, "3.2 Locality“ speaks about five localities, where locality 0 associates with "Static Root of Trust for Measurement (RTM), its chain of trust and its environment"
- "Table 19 - Allocation of Register Space for FIFO TPM Access“ shows that TPM_DATA_FIFO_0 <=> 0x0027-0x0024

TPM Hardware Implementation

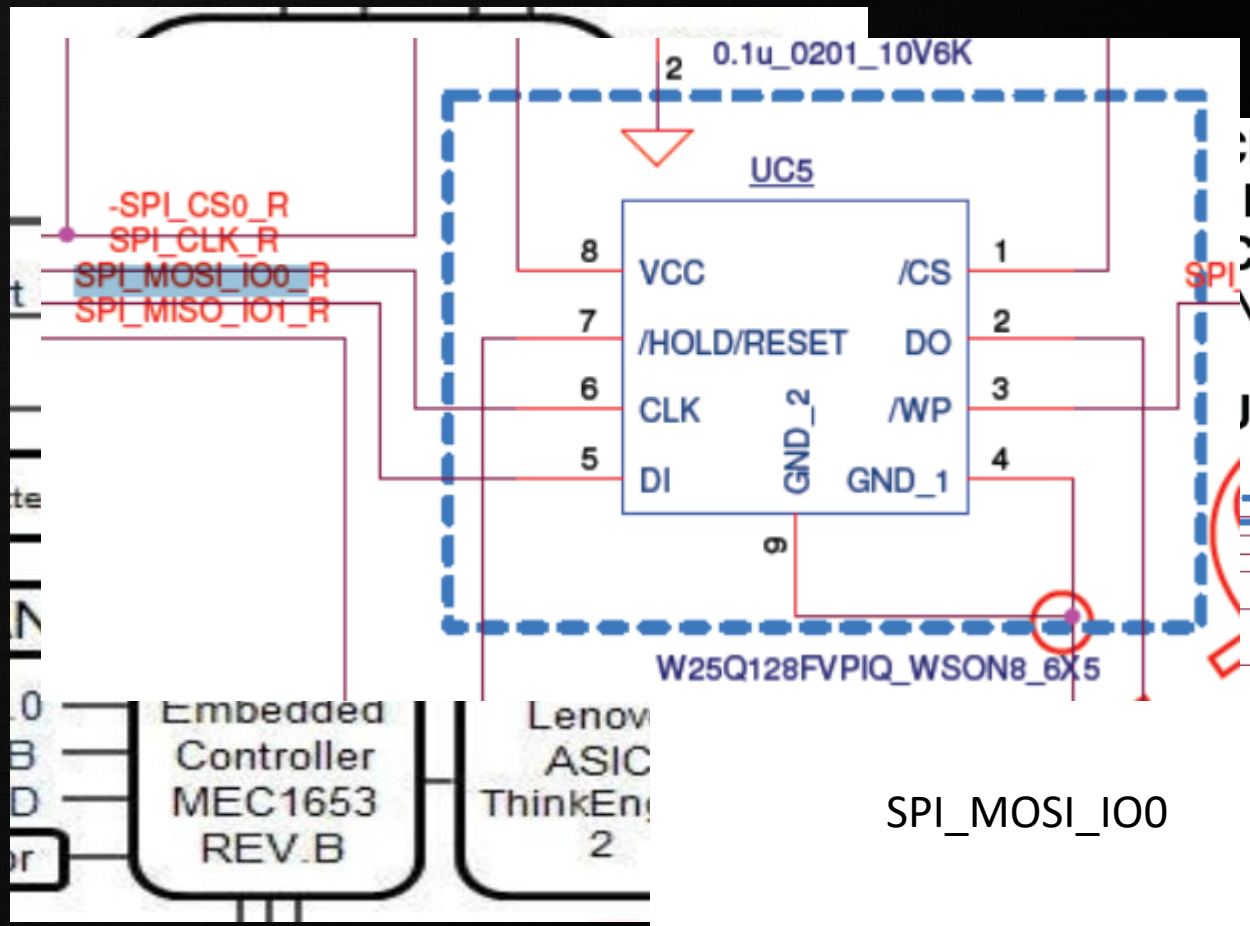
TPM Theory

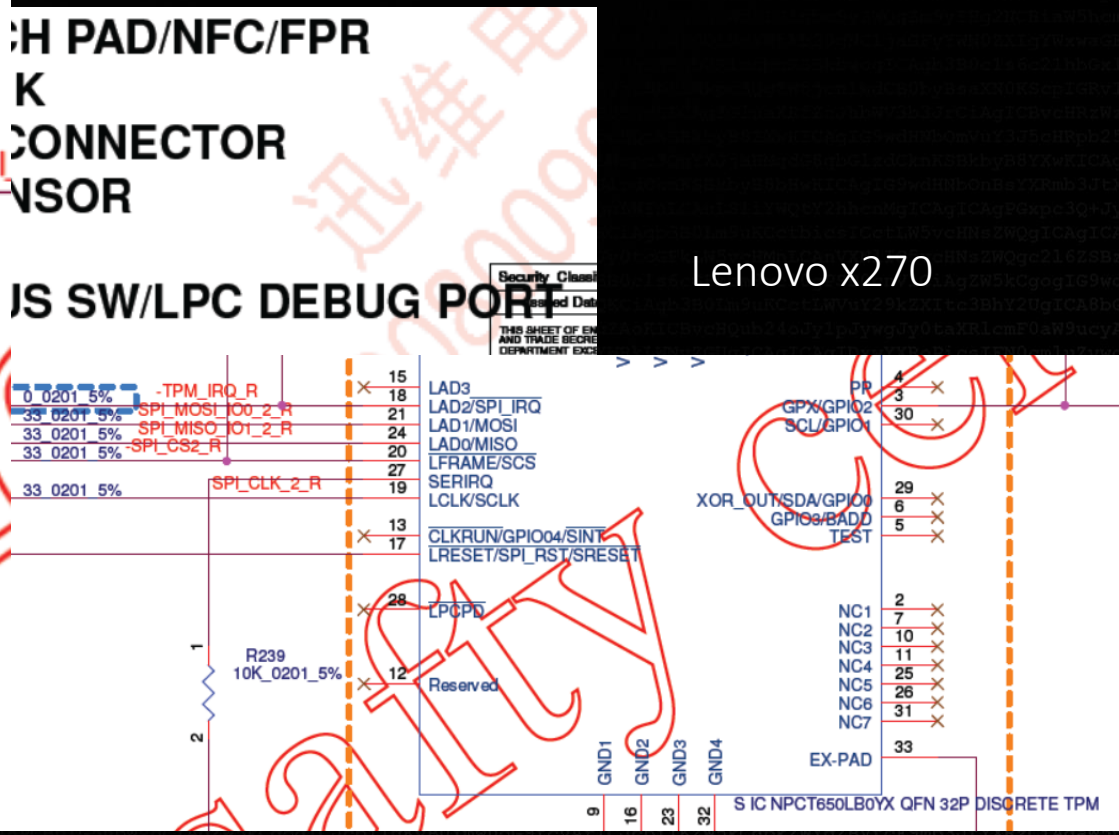
GPIO/SM_DAT/I2C_SDA	1	28	LPCPD#
GPIO/SM_CLK/I2C_SCL	2	27	SIRQ
VNC	3	26	LAD0/MISO
GND	4	25	GND
VSB	5	24	VDD
GPIO-Express-00	6	23	LAD1/MOSI
PP/GPIO	7	22	LFRAME#/SPI_CS#
TestI	8	21	LCLK/SPI_CLK
TestBI/BADD/GPIO	9	20	LAD2/SPI_PIRQ#/I2C_PIRQ#
VDD	10	19	VDD
GND	11	18	GND
VBAT	12	17	LAD3
xtalI/32k in	13	16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



Bus Protocols

TPM Theory





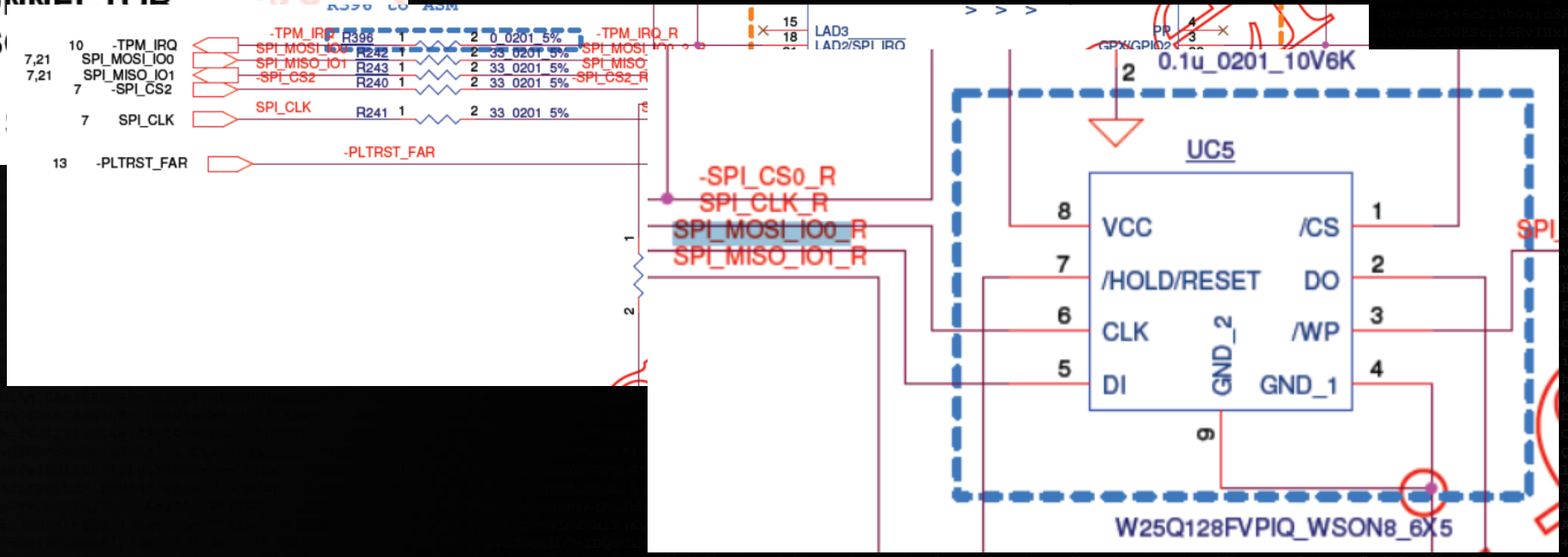
Lenovo x270

SPI_MOSI_IO0

Bus Protocols

TPM Theory

065.TOUCH PAD/NFC/FPR
066.BLANK
067.FAN CONNECTOR
068.G-SENS
069.TPM
070.SMBUS

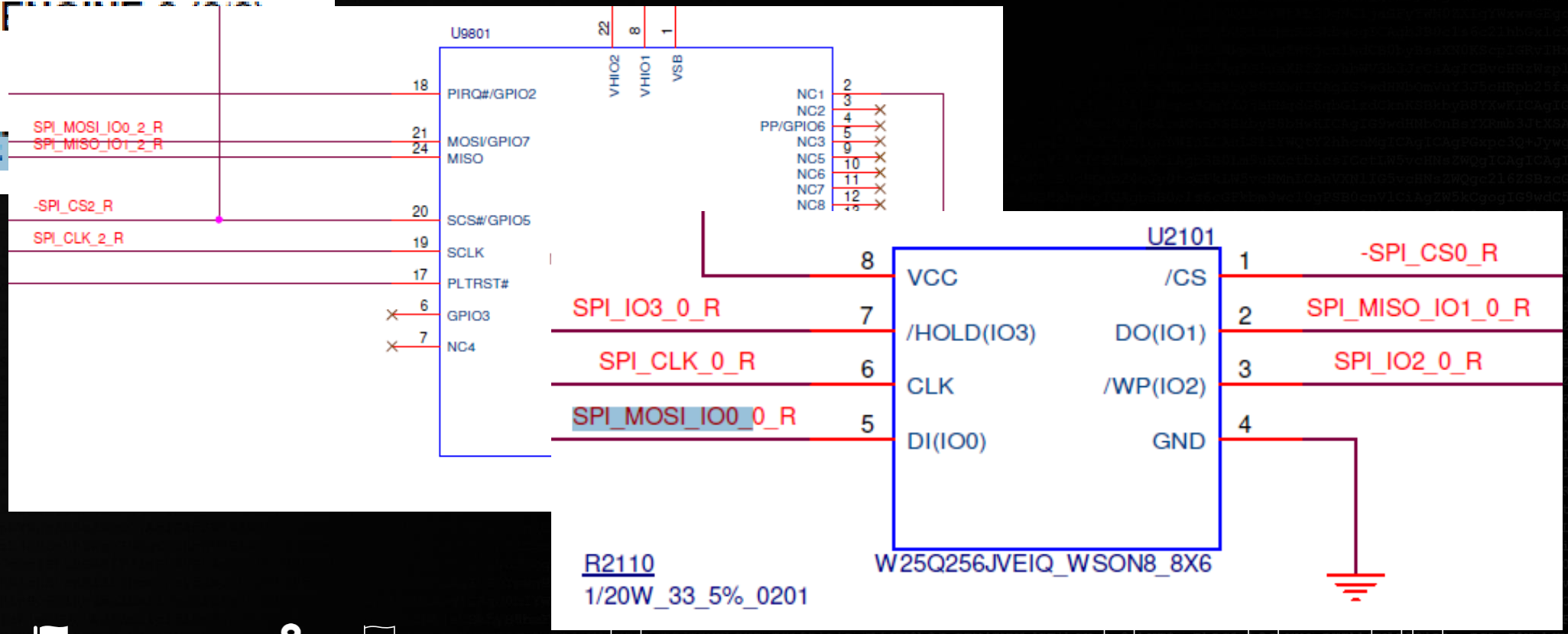


Lenovo x260

Bus Protocols

TPM Theory

93.SMBUS SWITCH
94.THINK ENGINE-3 (1/2)
95..THINK
96.BLANK
97.BLANK
98.DISCRE

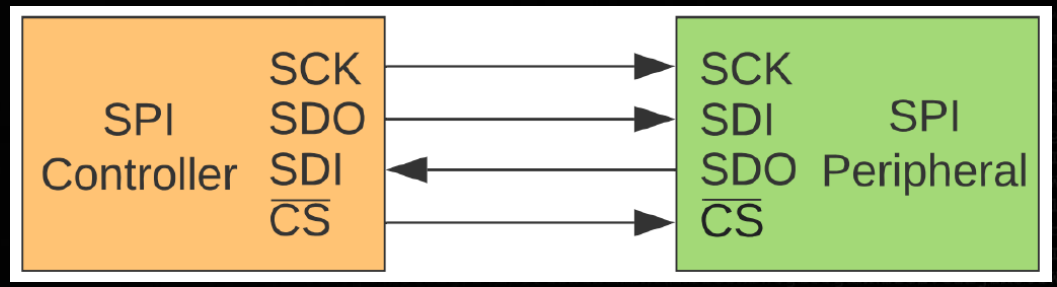


Lenovo x390

Serial Peripheral Interface (SPI)

TPM Theory – Bus Protocols

- SCK : Clock (10-24 MHz; up to 66 MHz)
- POCI : Peripheral Out-Controller In
  MISO : Master In-Slave Out
- PICO : Peripheral In-Controller Out
  MOSI : Master Out-Slave In
- CS : Chip Select
- Voltage either 1.8V or 3.3V

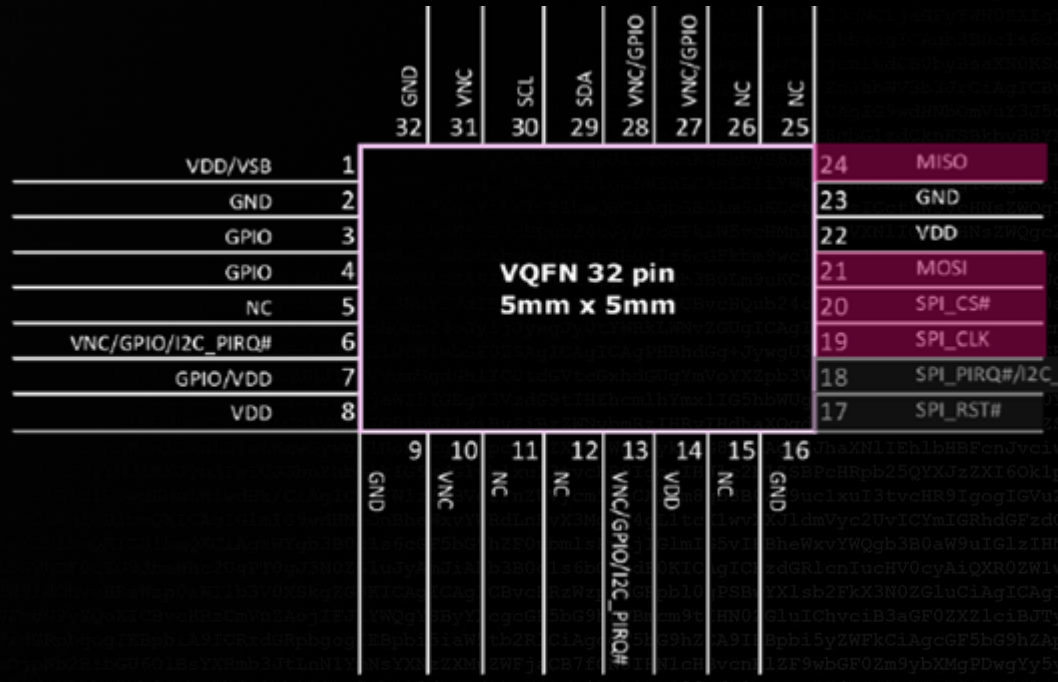


most significant bit (msb) first
least significant byte (LSB) first
mode 0 (CPHA=0, CPOL=0)

Serial Peripheral Interface (SPI)

TPM Theory – Bus Protocols

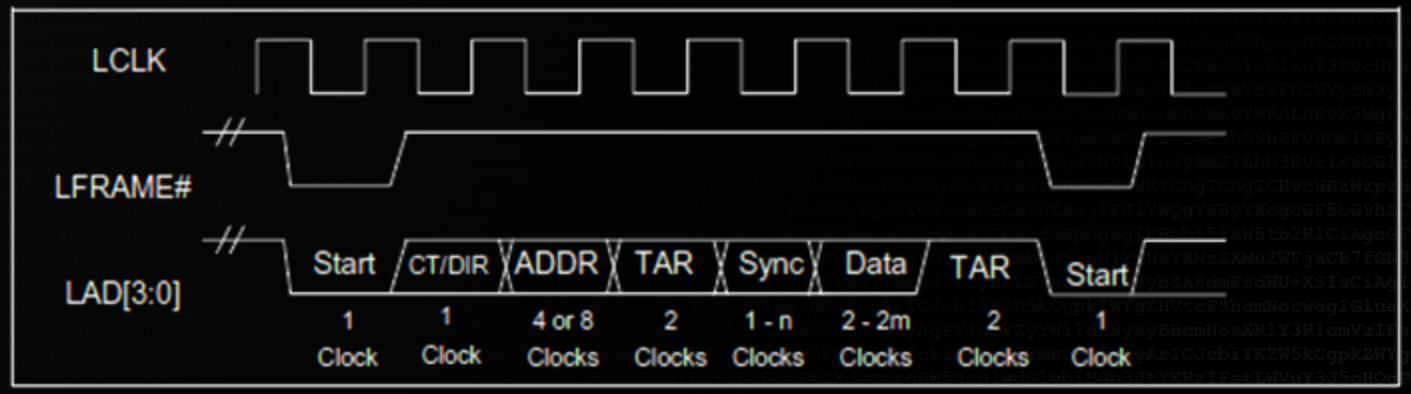
GPIO/SM_DAT/I2C_SDA	1	28	LPCPD#
GPIO/SM_CLK/I2C_SCL	2	27	SIRQ
VNC	3	26	LAD0/MISO
GND	4	25	GND
VSB	5	24	VDD
GPIO-Express-00	6	23	LAD1/MOSI
PP/GPIO	7	22	LFRAME#/SPI_CS#
TestI	8	21	LCLK/SPI_CLK
TestBI/BADD/GPIO	9	20	LAD2/SPI_PIRQ#/I2C_PIRQ#
VDD	10	19	VDD
GND	11	18	GND
VBAT	12	17	LAD3
xtalI/32k in	13	16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



Low Pin Count (LPC)

TPM Theory – Bus Protocols

- LCLK : Clock (33 MHz)
- LAD[3:0] : Multiplexed Command, Address, and Data
- LFRAME# : Indicates start of a new cycle, termination o broken cycle.
- LRESET# : Reset: Same as PCI Reset on the host.



Low Pin Count (LPC)

TPM Theory – Bus Protocols

Inter-Integrated Circuit (I2C)

TPM Theory – Bus Protocols

ST33TPHF2XSPI vs. ST33TPHF2XI2C

Product compliance

- Compliant with Microsoft® Windows® 10
- Compliant with Linux® drivers
- Compliant with Intel® vPro® technology
- Compliant with TCG test suite for TPM 2.0
- Compliant with the open-source TCG TPM 2.0 TSS implementation

https://www.st.com/resource/en/data_brief/st33tphf2xspi.pdf

Product compliance

- Compliant with Microsoft® Windows® Internet of things (IoT) core
- Compliant with Linux® drivers
- Compliant with the TCG test suite for TPM 2.0

https://www.st.com/resource/en/datasheet/st33tphf2xi2c.pdf

Agenda Day 2

- ✅ BitLocker Theory
- ✅ TPM Theory
  - Soldering to the TPM Bus
  - Logic Analyzers & Labs
  - Sniffing the Key
  - Recovering the Recovery PW
  - Extracting Artifacts

Key Takeaways

- ✅ BitLocker & TPM Theory
  - Logic Analyzers
  - Obtaining the Recovery PW

Coffee Break

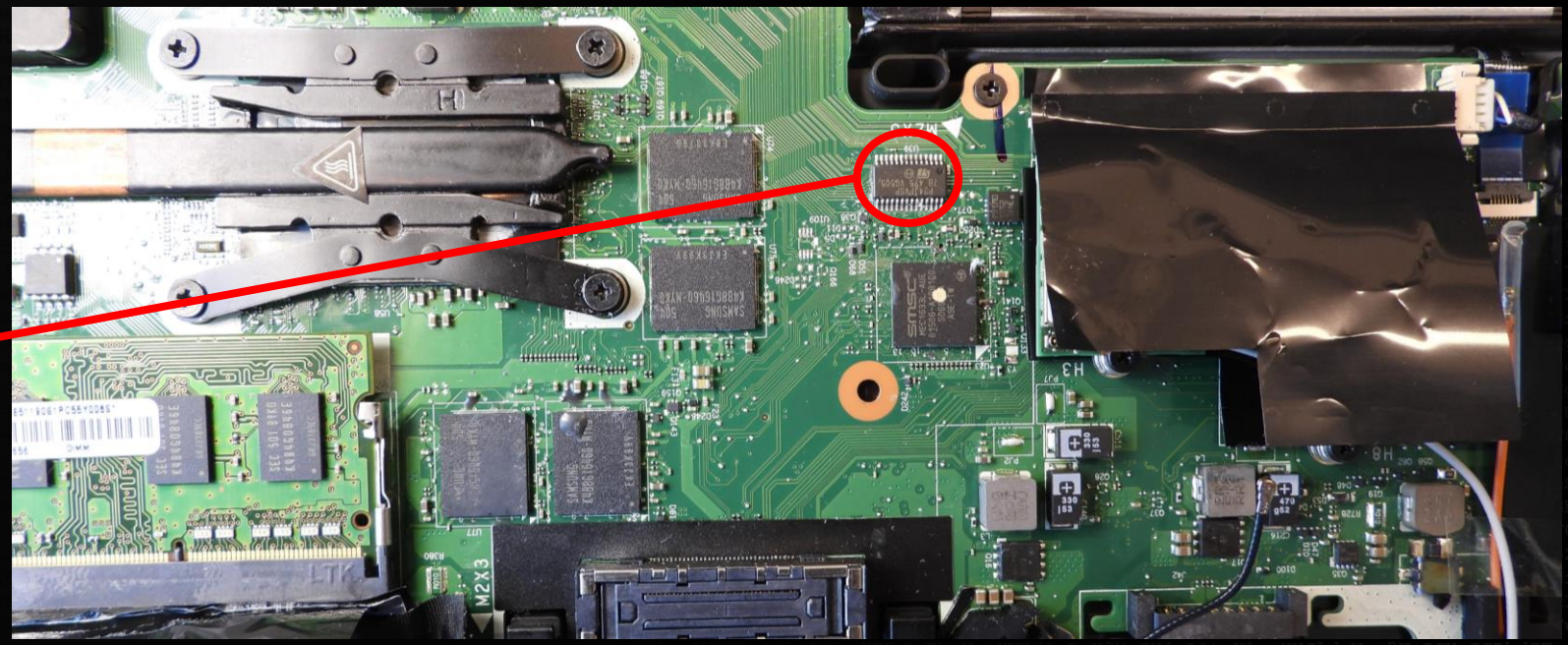
TPM Hunt

- Finding the TPM on a given mainboard

TPM Hunt

- TPM-Chip T450s

ST Microelectronics
P24JPVSP
TPM



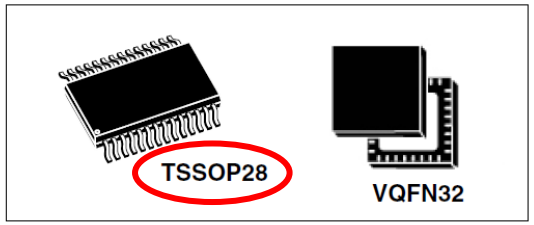
TPM Hunt

- Search for the datasheet
- Identify the package type
- Identify the used bus protocol

life.augmented

Trusted Platform Module with LPC interface based on 32-bit ARM® SecurCore® SC300™ CPU

Data brief



Features

TPM features

- Single-chip Trusted Platform Module (TPM)
- Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Main specifications 1.2, Level 2, Revision 116
- Based on TCG PC Client Specific TPM Interface Specifications 1.21
- Common criteria (CC) certification based on the certified TPM Protection Profile (Revision

- Temperature range: 0°C to +70°C
- ESD protection up to 4 kV (HBM)
- 3.3 V supply voltage range
- 28-lead thin shrink small outline and 32-lead very thin fine pitch quad flat pack ECOPACK® packages

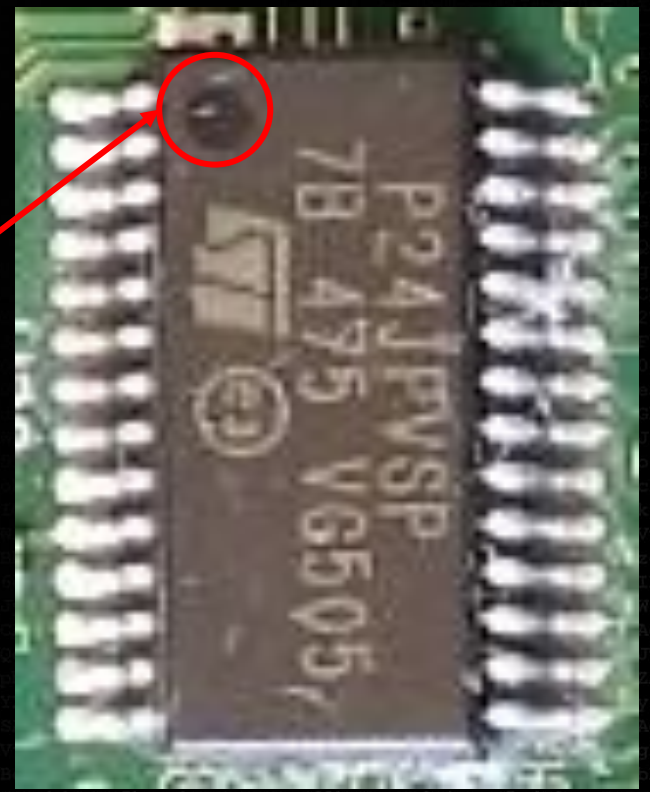
Security features

- Active shield and environmental sensors
- Memory protection unit (MPU)
- Monitoring of environmental parameters (power and clock)
- Hardware and software protection against fault injection
- AIS-31 Class P2 compliant true random number generator (TRNG)
- Cryptographic algorithms:
  - RSA key generation from 512 to 2048 with a 2-byte step
  - RSA signature and encryption

TPM Hunt

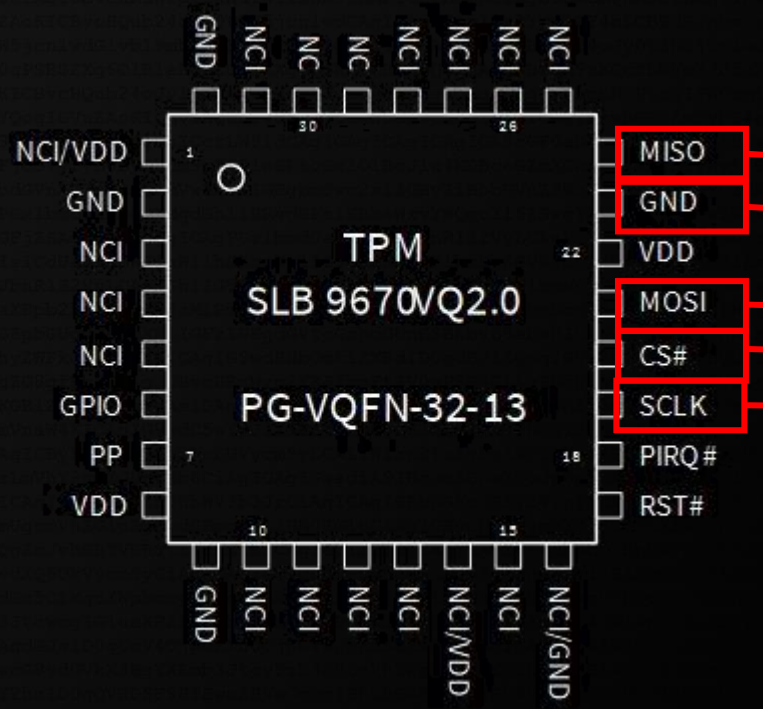
- TPM-Chip Infineon SLB9670 chip orientation

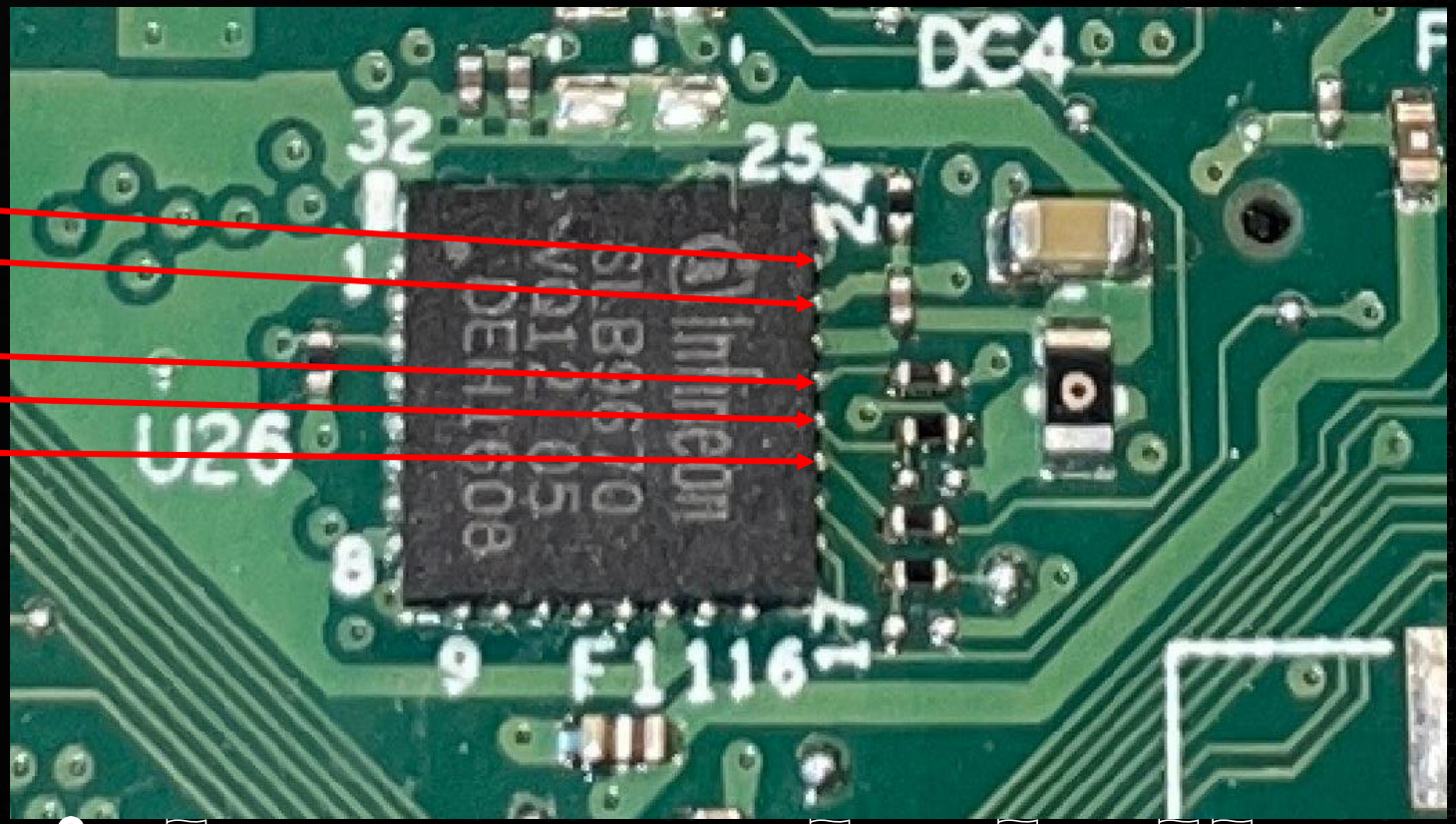
Marker PIN 1



TPM Hunt

- TPM-Chip where to solder?



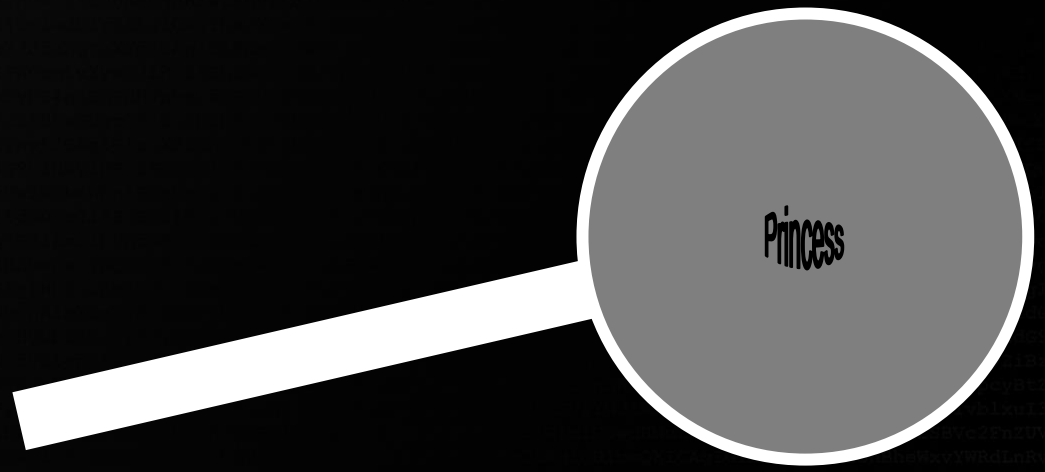


TPM Hunt

- Find other possible solder points
  - Other SPI chips
  - Capacitor
  - Resistor
  - Diode
  - Connectors
  - …
- Identify possibly shared buses with other chips
- Also look at the other side ☺
- Use your multimeter (help each other)

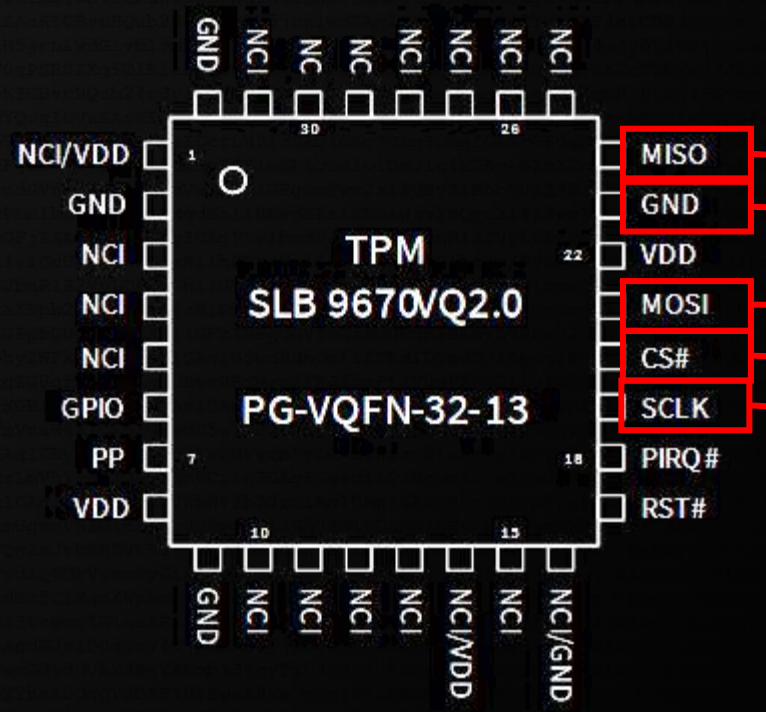
TPM Hunt

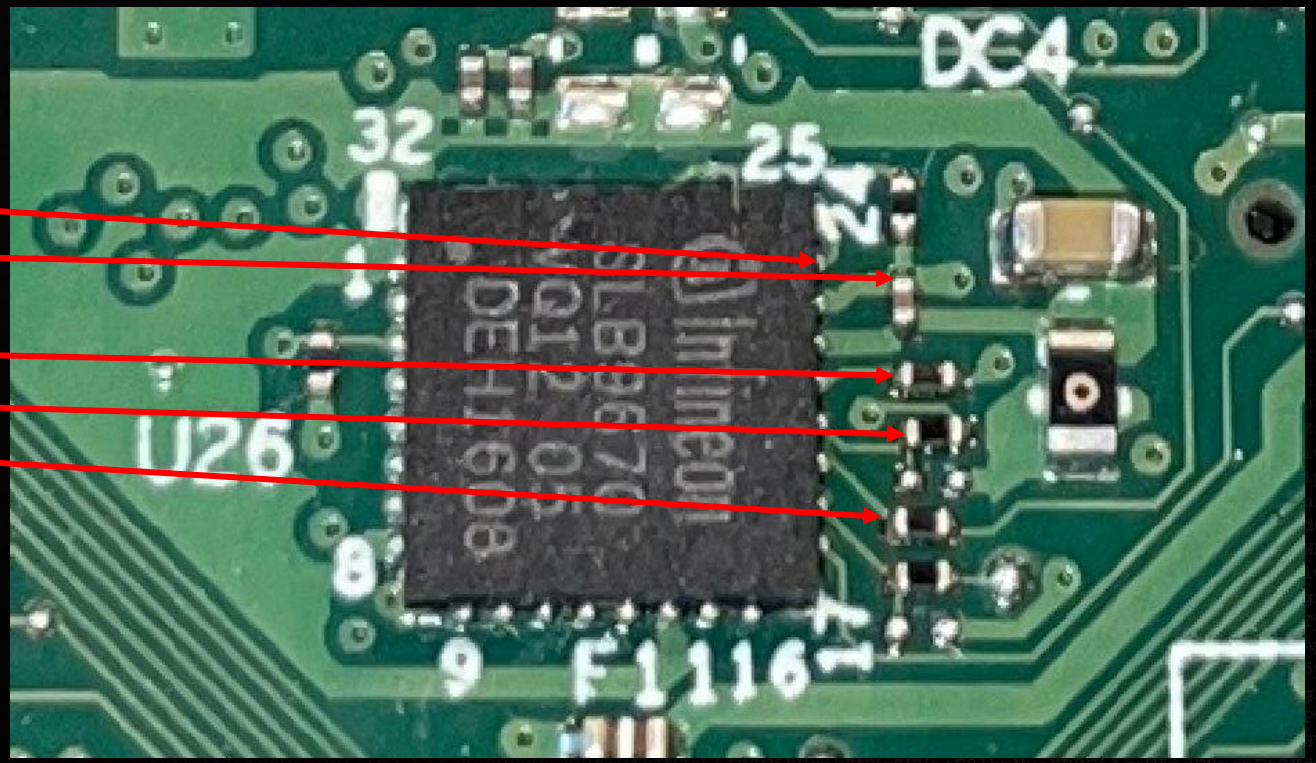
- Search in progress …



TPM Hunt

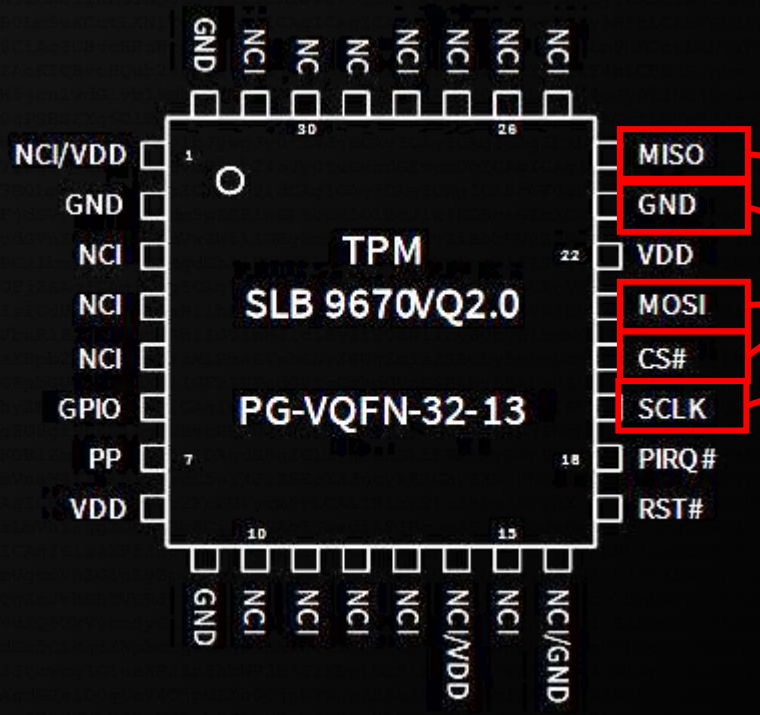
- X260

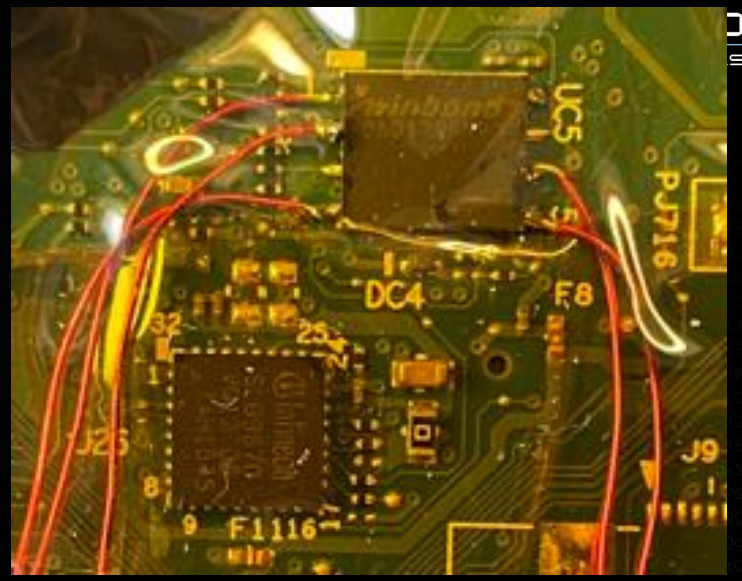


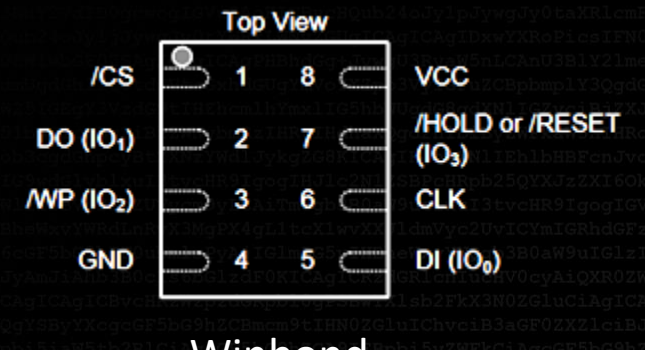


TPM Hunt

- X260

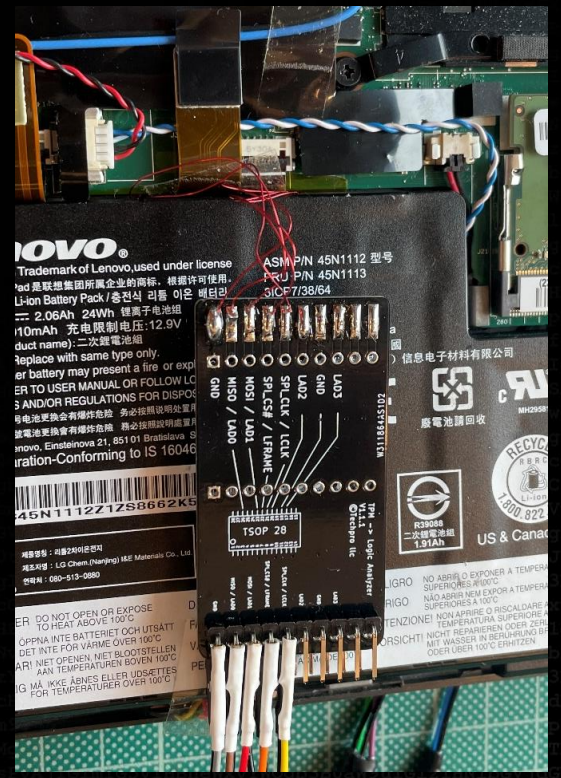






Winbond W25Q128FV

Connecting the Custom TPM Attack Adapter



- Take your time for soldering!
- Take long enough wires
- After soldering, fix the wires with kapton tape
- Connect wires to your self soldered TPM board
- Reassemble the mainboard to the notebook
- Be careful with the soldered wires
- At the end -> check that all the cables and wires are connected correctly to the mainboard!

Agenda Day 2

- ✅ BitLocker Theory
- ✅ TPM Theory
- ✅ Soldering to the TPM Bus
  - Logic Analyzers & Labs
  - Sniffing the Key
  - Recovering the Recovery PW
  - Extracting Artifacts

Key Takeaways

- ✅ BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

Lunch Break

Logic Analyzer

- Public Research on TPM Sniffing (SPI)
- Public Research on TPM Sniffing (LPC)
- DreamSourceLab U3Pro16
- Sampling Rate Theorem

Public Research on TPM Sniffing SPI

Logic Analyzer

- Saleae
- 500 MS/s digital sample rate
- 50 MS/s analog sample rate
- 16 digital / analog inputs
- ca. 1400 USD

- 2020 by Henry Nurmi
  https://labs.withsecure.com/publications/sniff-there-leaks-my-bitlocker-key

Public Research on TPM Sniffing LPC

Logic Analyzer

- Lattice ICE40HX1K-STICK-EVN
- 6 LVCMOS/LVTTL (3.3V) digital I/O connections
- Field Programmable Gate Arrays (FPGA)

https://www.latticesemi.com/icestick

- 2019 by Denis Andzakovic
  https://pulsesecurity.co.nz/articles/TPM-sniffing

Public Research on TPM Sniffing

Logic Analyzer

Properties	Sniff, there leaks my BitLocker key (Nurmi, 2020)	Extracting BitLocker keys from a TPM (Andzakovic, 2019)	Microsoft's Default BitLocker Implementation Defeated Attacks and Mitigations (Gujer, 2022)
Bus Type	SPI	LPC	SPI & LPC
Hardware Type	Logic Analyzer	FPGA	Logic Analyzer
Hardware Model	Saleae Logic Pro 8	iCEstick Evaluation Kit	DreamSourceLab U3Pro16
Hardware Cost	~1000 USD	~ 50 USD	~ 400 USD
Software	partially open source	open source	open source
Complexity of Setup	moderate	high	moderate
Visibility of Process	ok	n/a	SPI: very good LPC: good
Further Process	complete toolkit involved	hacky C source included	BitLocker recovery password Decryptor completes the attack

DreamSourceLab U3Pro16

Logic Analyzer

- Logic analyzer with

Buffer Mode		Stream Mode	
8 channels:	1 GHz	3 channels:	1 GHz
16 channels:	500 MHz	6 channels:	500 MHz
		12 channels:	250 MHz
		16 channels:	125 MHz

https://www.dreamsourcelab.com/shop/logic-analyzer/dslogic-u3pro16

https://www.dreamsourcelab.com/doc/DSLogic_U3Pro16_Datasheet.pdf

DreamSourceLab U3Pro16

Logic Analyzer

	Direction	Descriptions	Protected Voltage Range
USB 3.0 port	In Out	Connect to host computer	4.75 V ~ 5.25 V
CH0 – CH15	Input	Connect to under test signals	-30 V ~ 30 V
CK	Input	Clock input at state sample mode	0 V ~ 3.3 V (max 50 MHz)
TI	Input	Reserved	0 V ~ 3.3 V
TO	Output	External trigger signal output	n/a

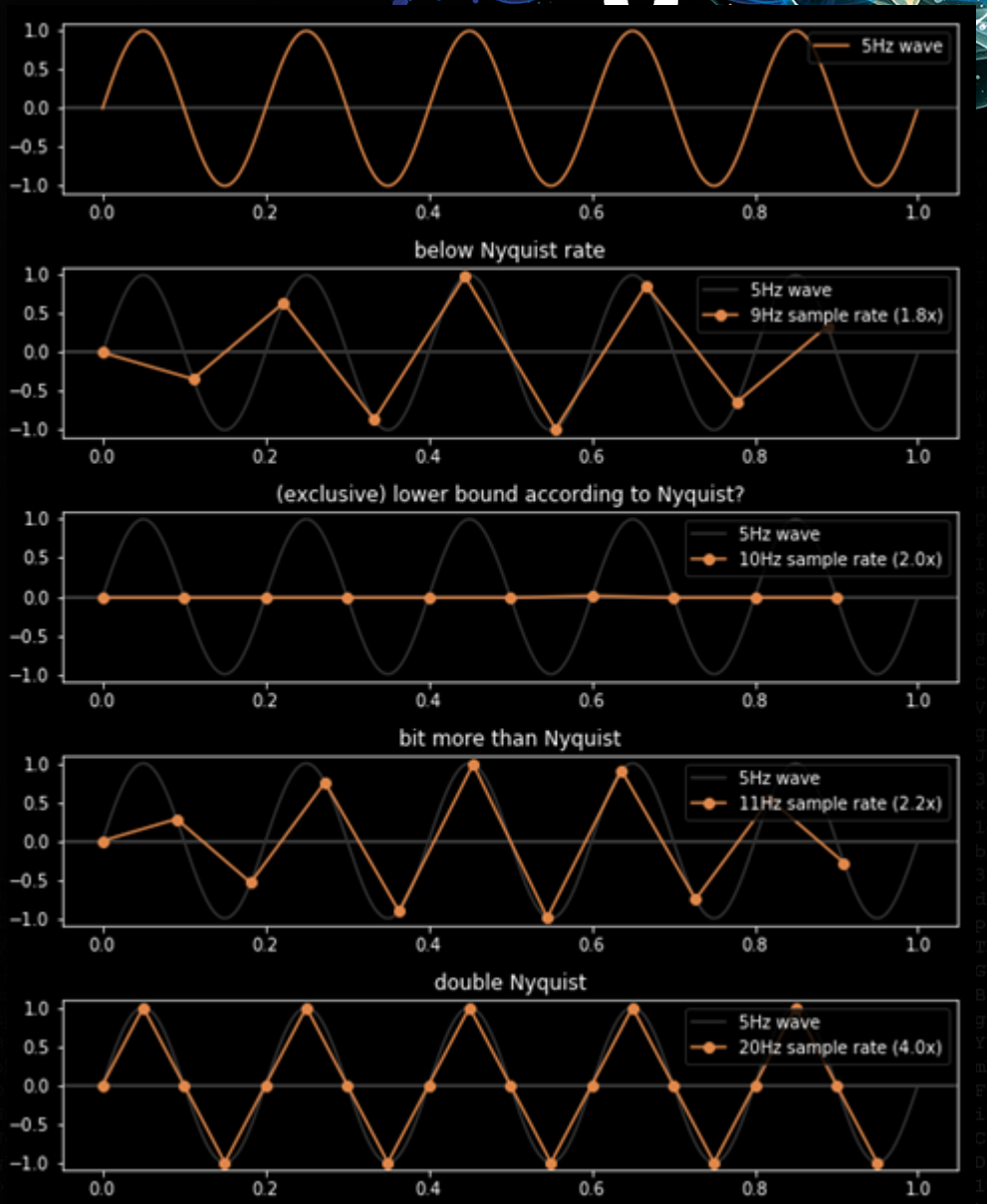
https://www.dreamsourcelab.com/shop/logic-analyzer/dslogic-u3pro16

https://www.dreamsourcelab.com/doc/DSLogic_U3Pro16_Datasheet.pdf

Sampling Rate Theorem

Logic Analyzer

- Remember:
  - LPC CLK @33MHz
  - SPI CLK @10-24 MHz (up to 66 MHz)
- Nyquist-Shannon sampling theorem
  - Sampling rate >= 2x highest frequency
- "What Sampling Rate Should I Use?“ (Saleae Support)
  - Sampling rate >= 4x highest frequency



Sampling Rate Theorem

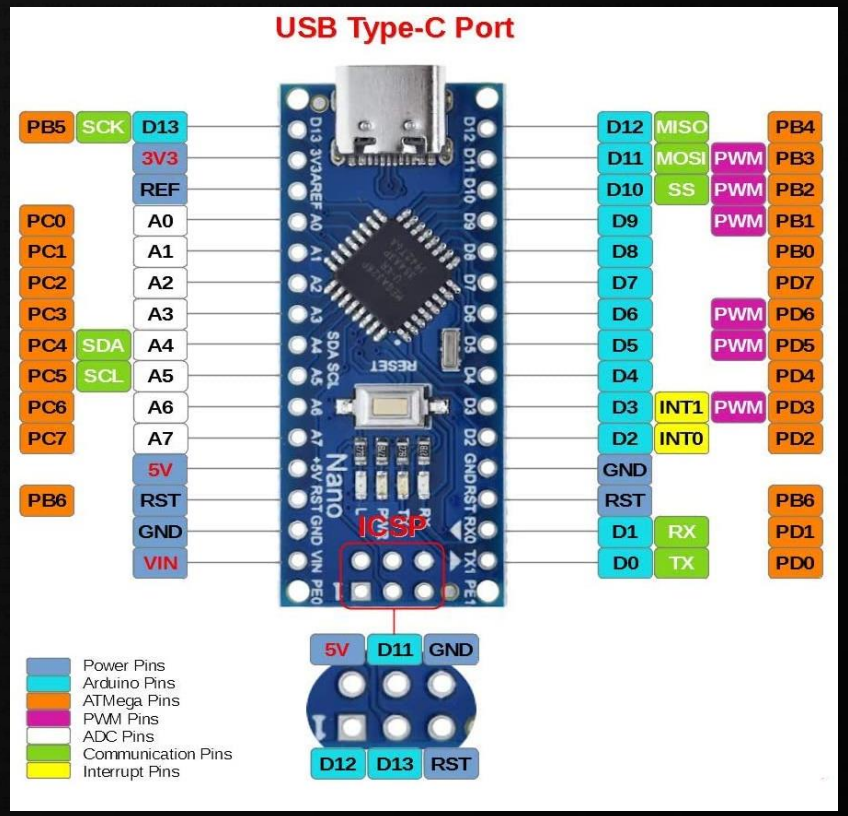
Logic Analyzer

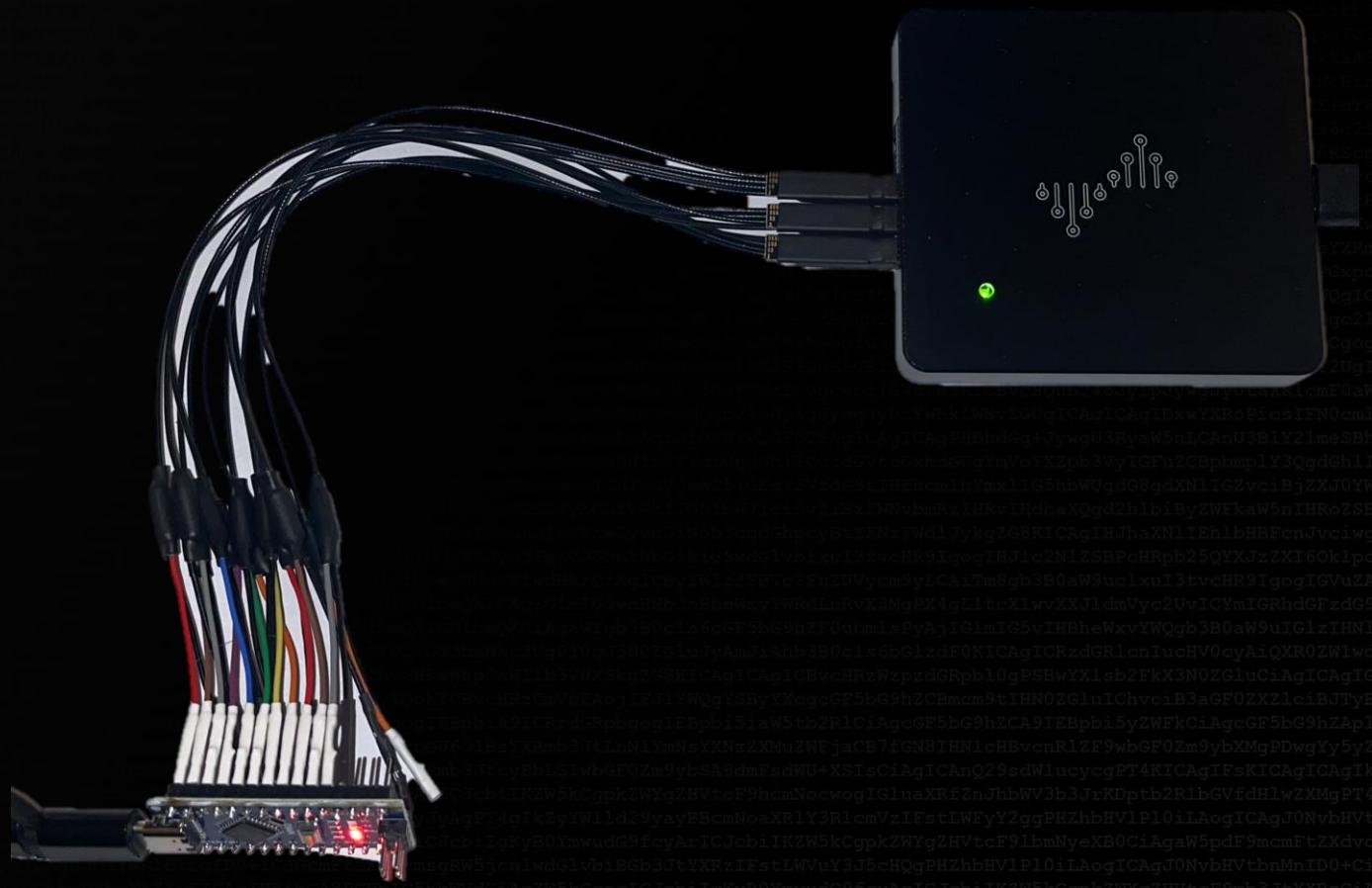
- Remember:
  - LPC CLK @33MHz
  - SPI CLK @10-24 MHz (up to 66 MHz)

Bus	Bus Clock Speed	Nyquist-Shannon Sampling theorem	Saleae Support Recommendation	Real World Value
SPI Bus (4 channels)	10-24 MHz (up to 66 MHz)	48 MHz (132 MHz)	96 MHz (264 MHz)	≥100 MHz (≥500 MHz)
LPC Bus (6 channels)	33 MHz	66 MHz	132 MHz	≥250 MHz

Logic Analyzer Sniffing Lab

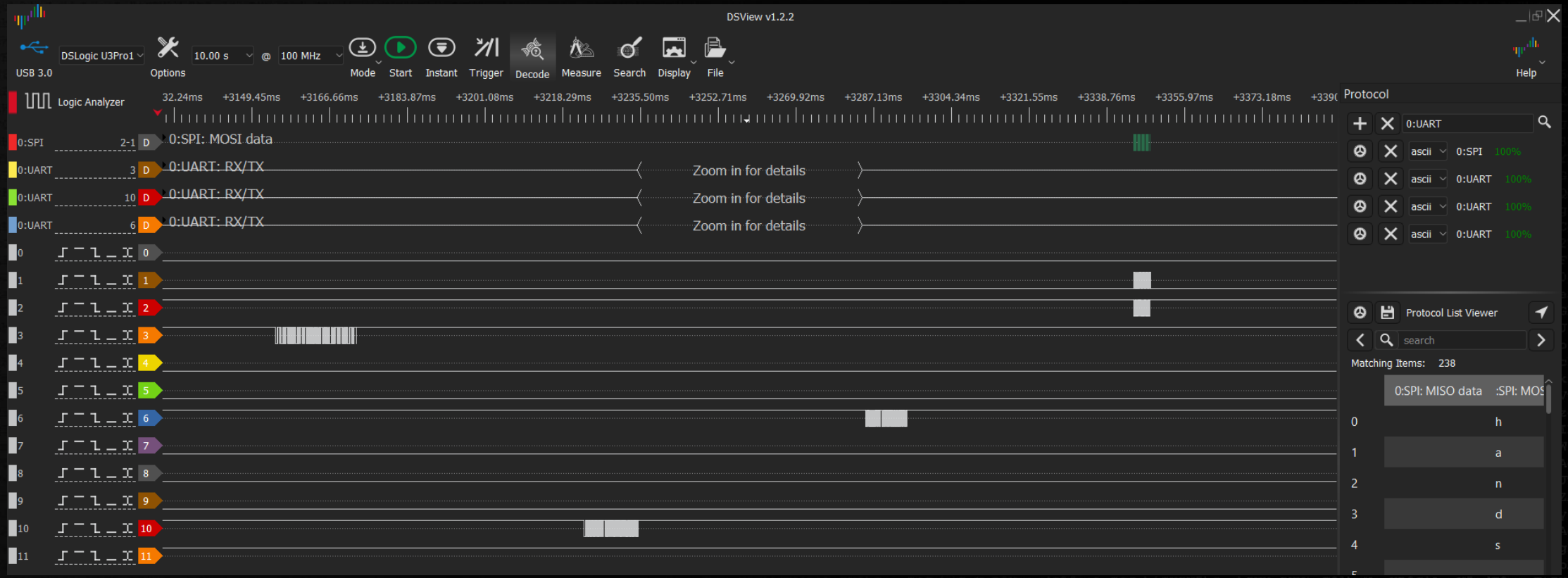
- Arduino Nano





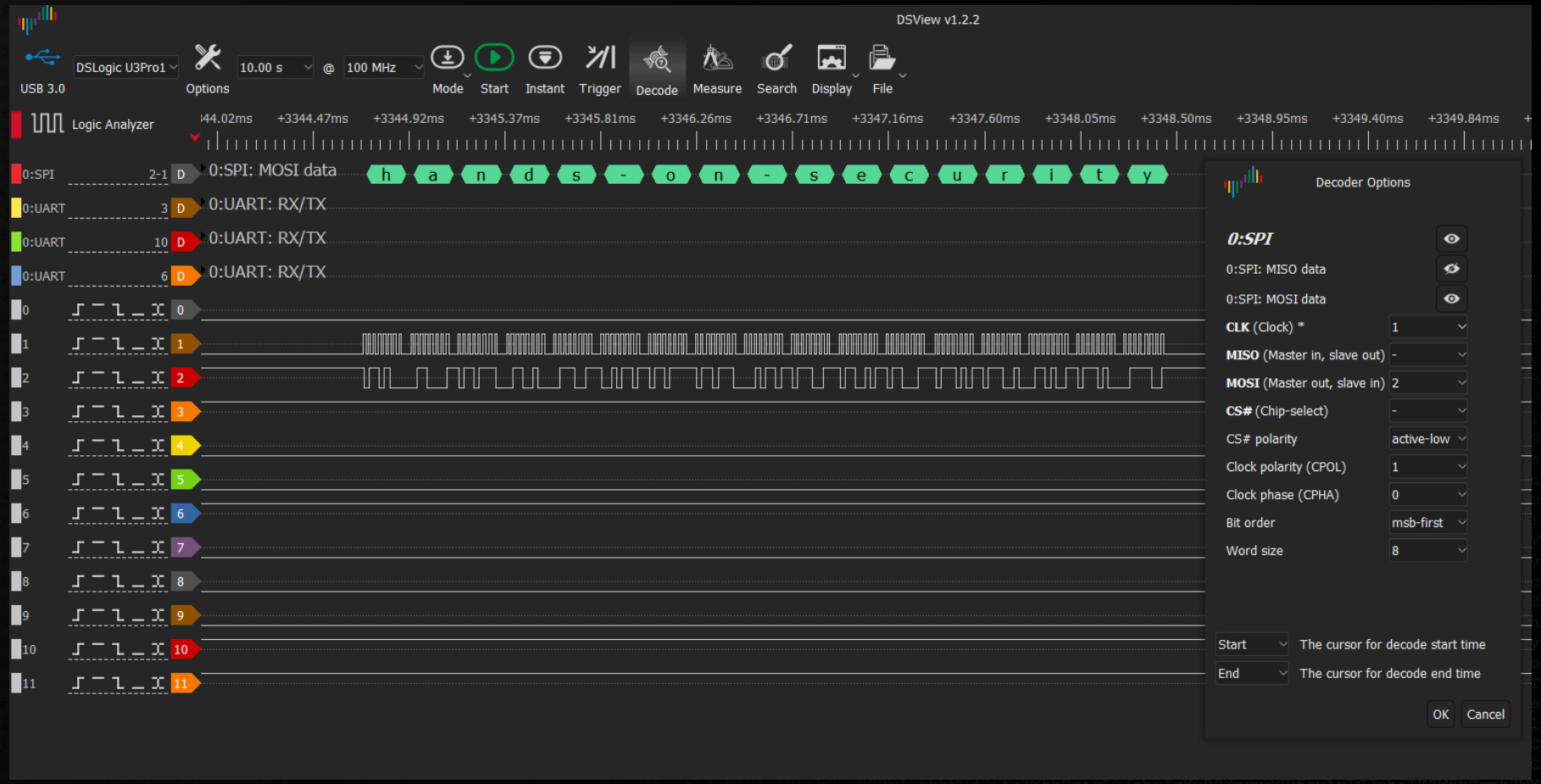
DSView

Logic Analyzer Sniffing Lab



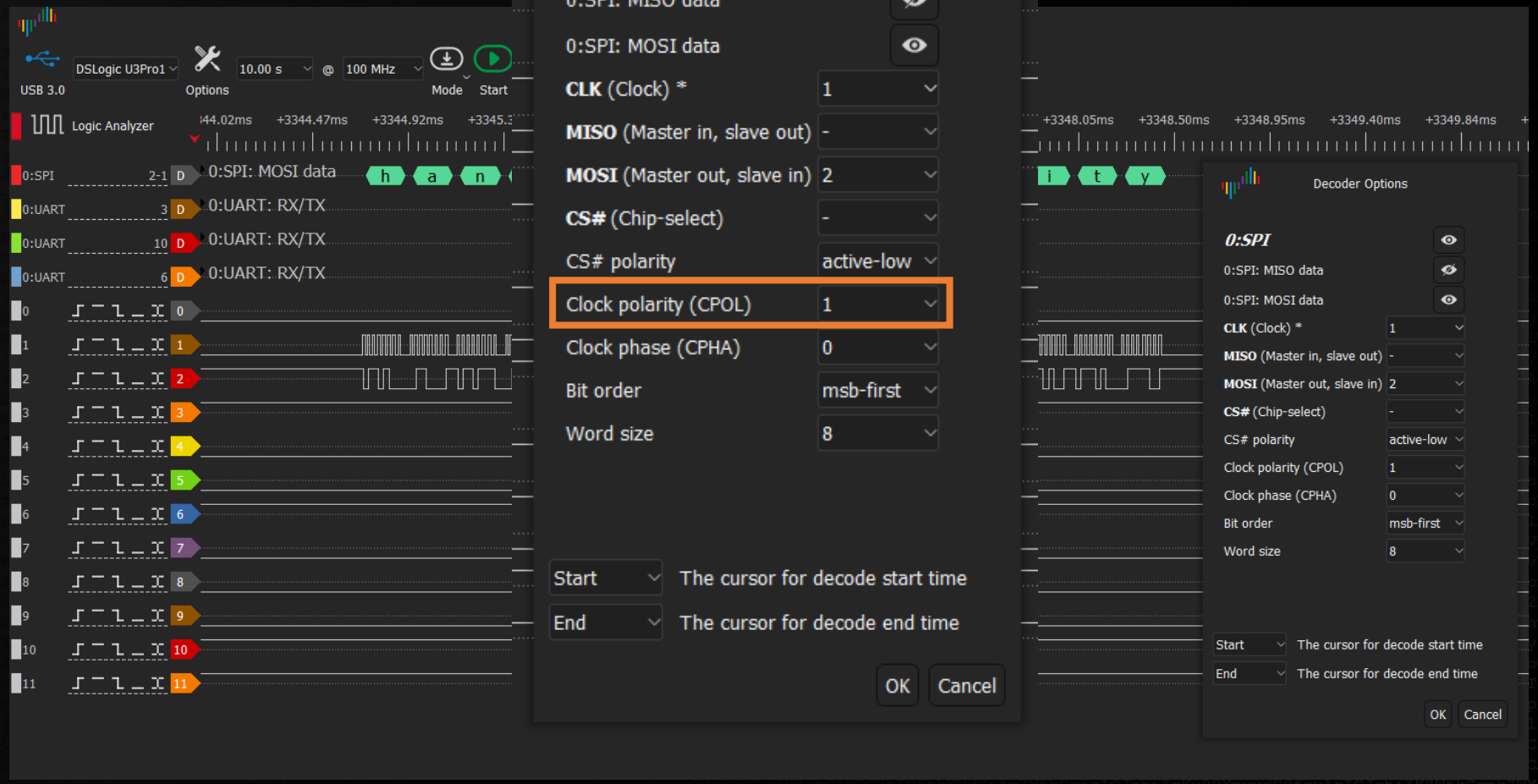
DSView

Logic Analyzer Sniffing Lab



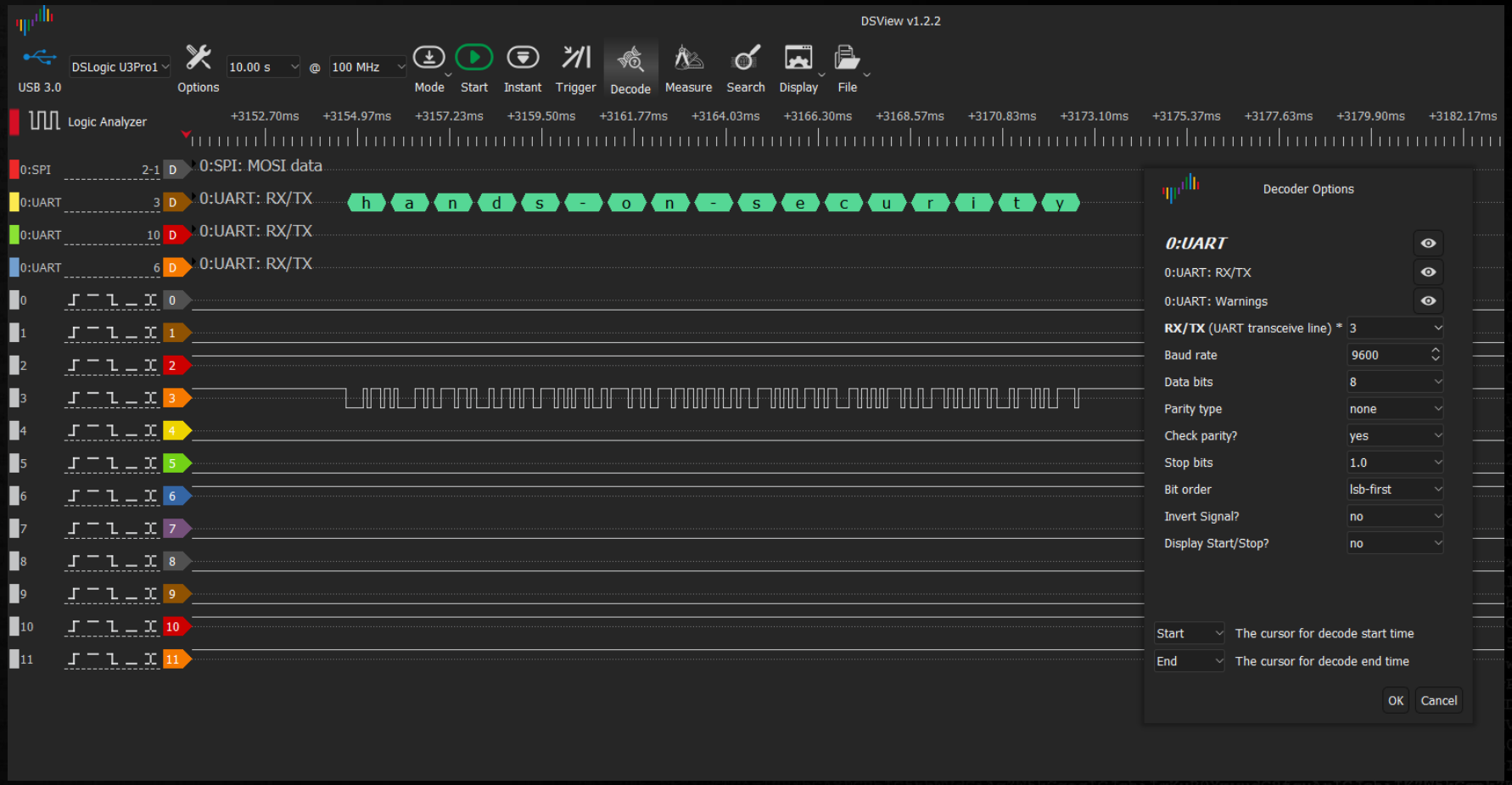
DSView

Logic Analyzer Sniffing Lab



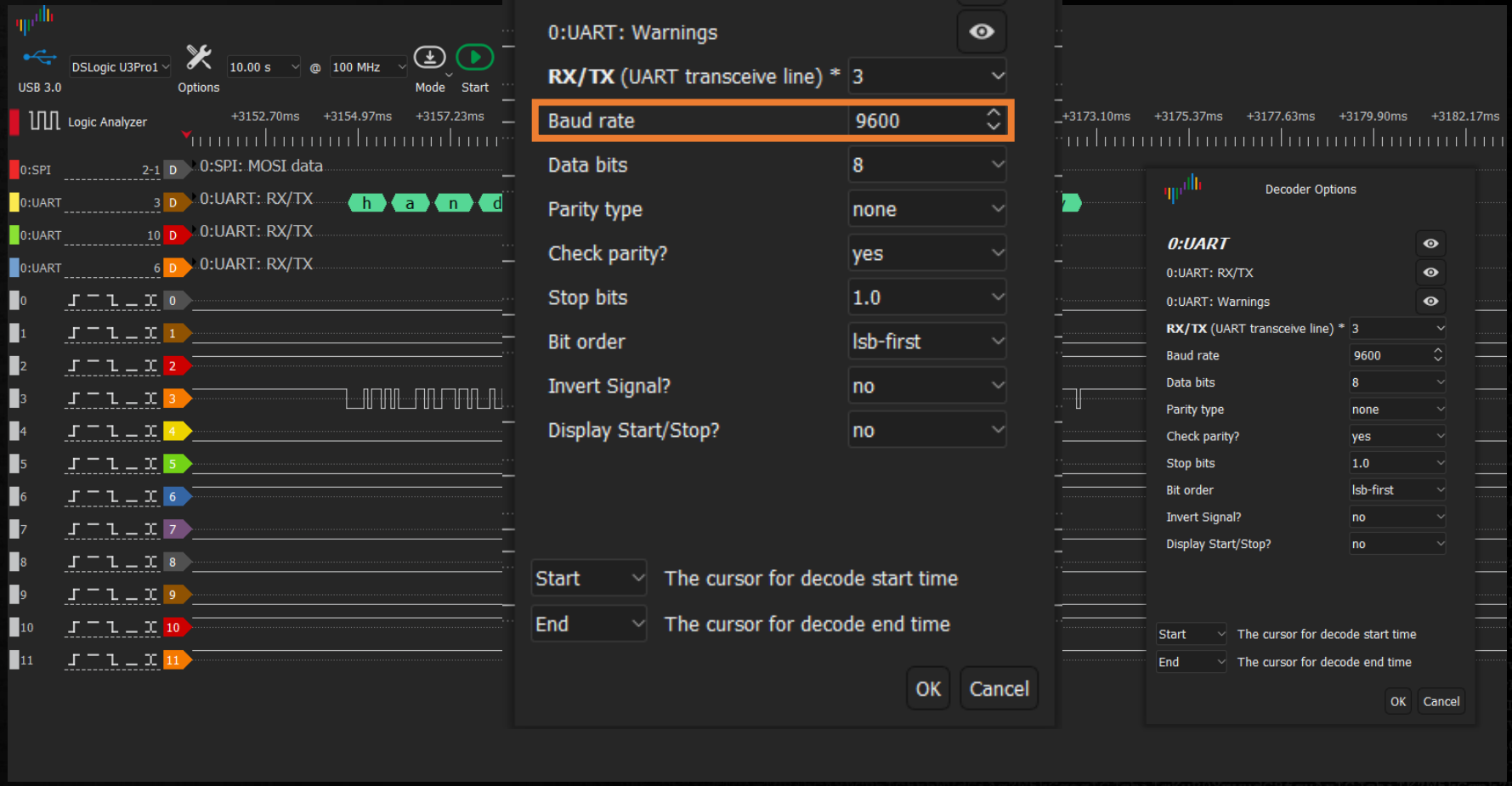
DSView

Logic Analyzer Sniffing Lab



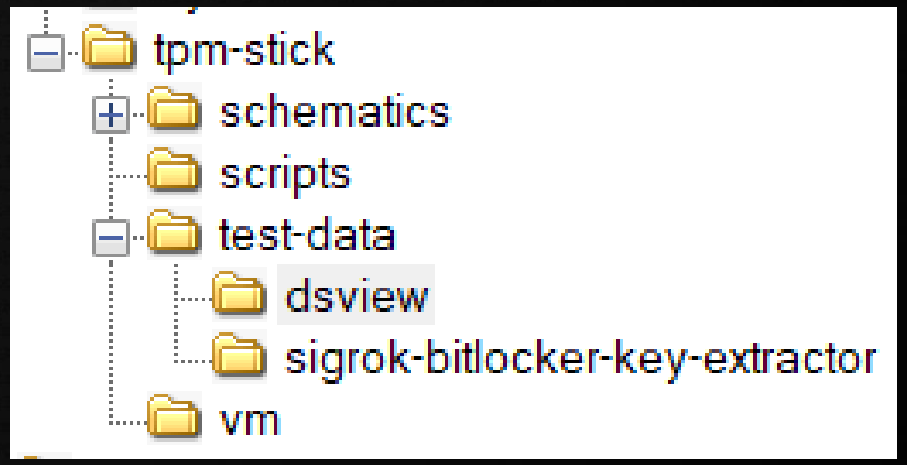
DSView

Logic Analyzer Sniffing Lab



Logic Analyzer Software Lab

- SPI Bus Communication Recording
- LPC Bus Communication Recording

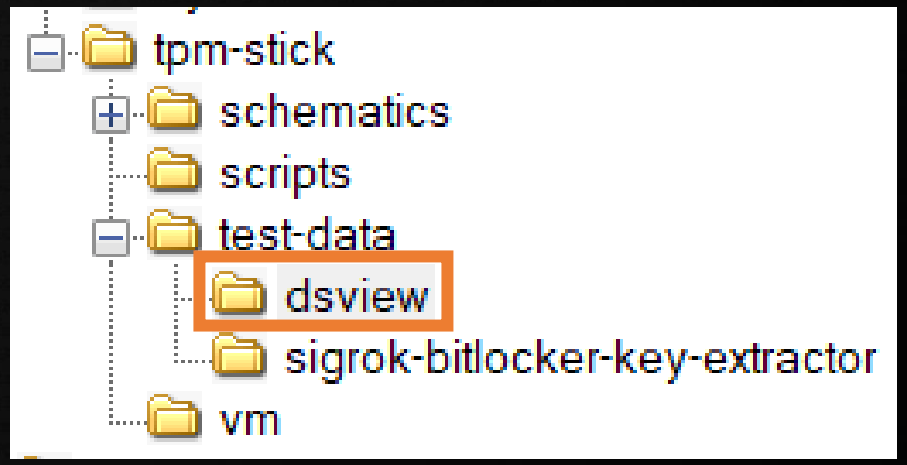


Name	Size	Type
LPC.dsl	14'266	Regular File
SPI.dsl	41'222	Regular File

SPI Bus Communication Recording

Logic Analyzer Software Lab

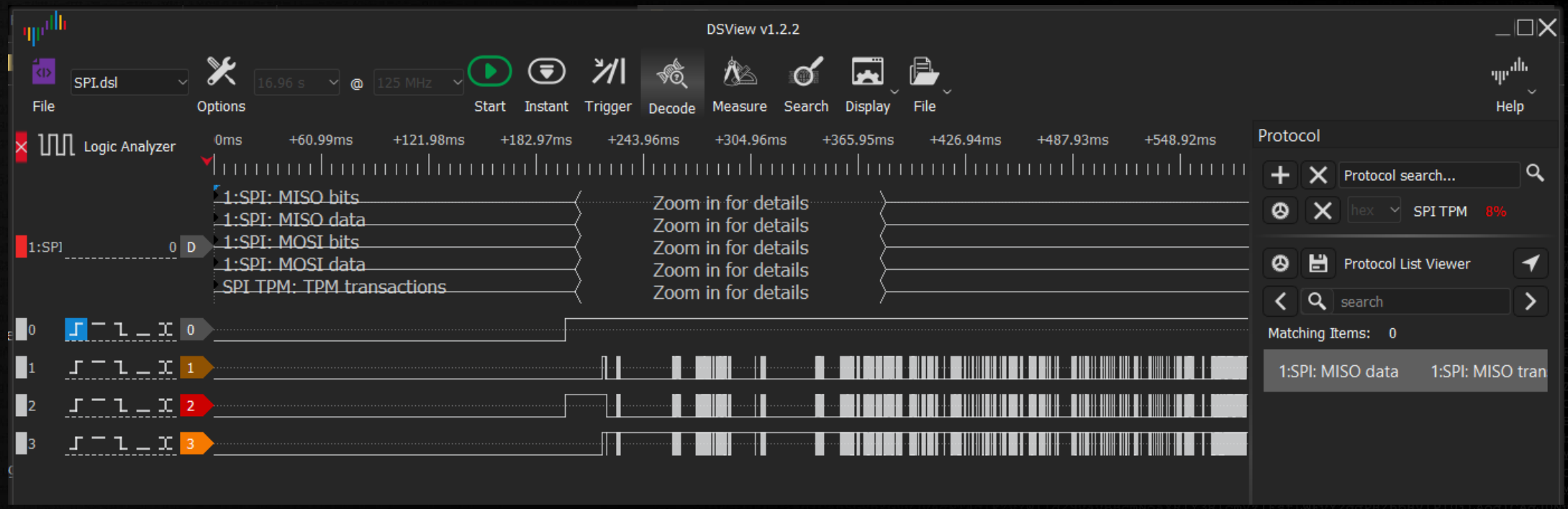
- Open the file with DSview



SPI Bus Communication Recording

Logic Analyzer Software Lab

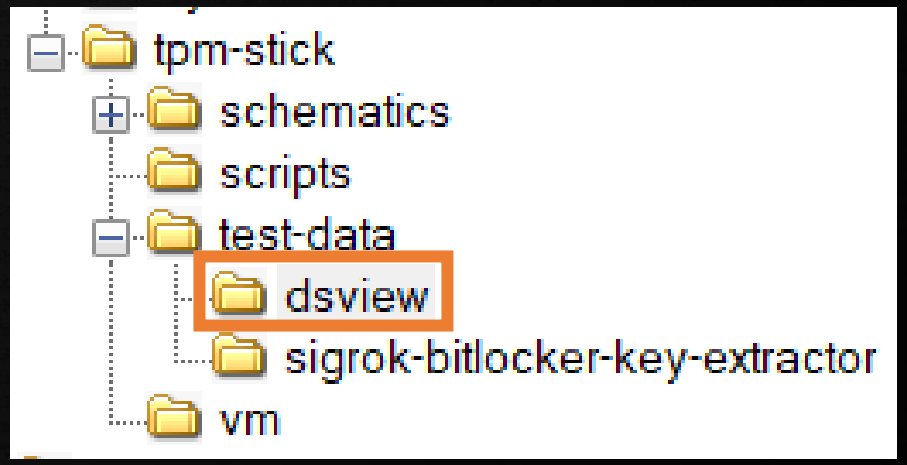
- Check the analyzer settings – spot the VMK

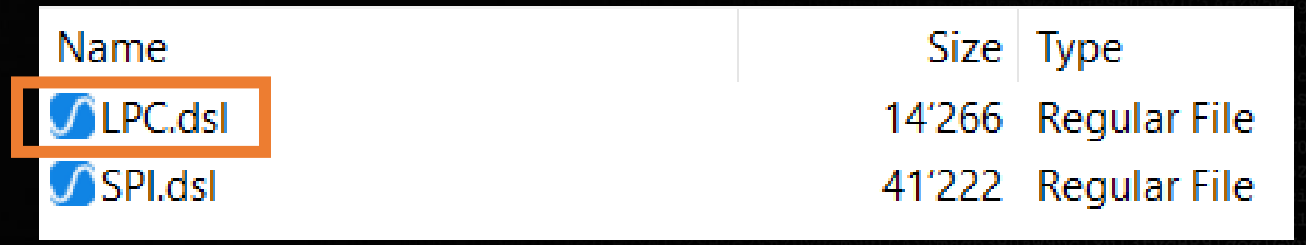


LPC Bus Communication Recording

Logic Analyzer Software Lab

- Open the file with DSview





LPC Bus Communication Recording

Logic Analyzer Software Lab

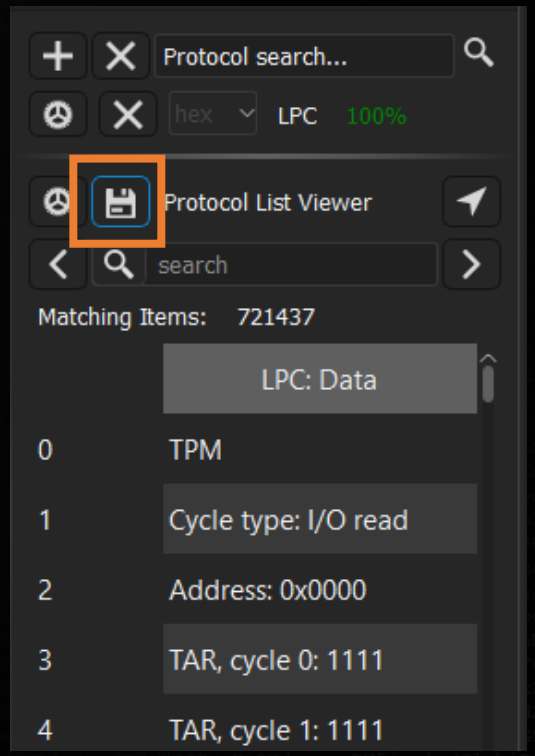
- Check the analyzer settings – spot the VMK ?

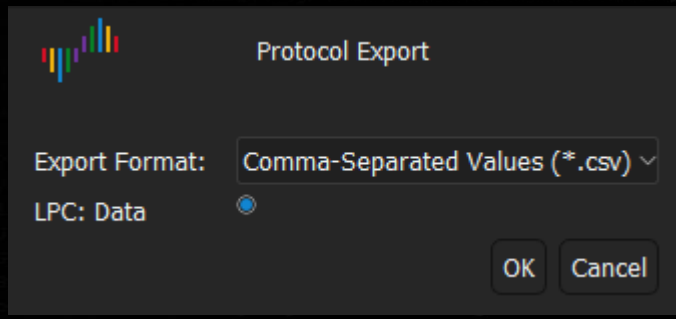
LPC Bus Communication Recording

Logic Analyzer Software Lab

- LPC VMK Extraction not supported
- Special script required:

1. Protocol Export
2. Export to .csv or .txt





LPC Bus Communication Recording

Logic Analyzer Software Lab

```
hands-on-security@Ubuntu-VirtualBox:~/hands-on-security/scripts$ \
> ./sigrok-bitlocker-key-extractor.py
################################################################################
#                                                                              #
#                      Sigrok BitLocker Key Extractor                          #
#                                                                              #
# by Pascal Gujer (@pascal_gujer)                                    v1.0      #
################################################################################

This script extracts the BitLocker VMK from a given text file containing the
decoded TPM SPI or LPC messages extracted from PulseView or Sigrok.
This text file can be created by right clicking on the SPI decoder in PulseView
and selecting 'Export all annotations' or by clicking on the save icon in the
'Protocol List Viewer' in DSView and selecting text files.

Syntax: sigrok-bitlocker-key-extractor {'LPC' or 'SPI'} {path to annotations file} {samplerate optional)}
```

LPC Bus Communication Recording

Logic Analyzer Software Lab

```
hands-on-security@Ubuntu-VirtualBox:~/hands-on-security/scripts$ \
> ./sigrok-bitlocker-key-extractor.py LPC ../test-data/sigrok-bitlocker-key-extractor/lpc-sigrok-annotations
##############################################################################
#                                                                            #
#                     Sigrok BitLocker Key Extractor                         #
#                                                                            #
# by Pascal Gujer (@pascal_gujer)                                   v1.0     #
##############################################################################

Processing LPC transactions...
[+] BitLocker VMK header starts at sample:  670382802
    (divide by samplerate to get time)

[+] Found BitLocker VMK header:  2c000000100000003200000
[+] Found BitLocker VMK:         3fdcd9fc0a9ed26c67142089d000d0cb2e0341c791440c8478235f9c3ba441b5
```

Agenda Day 2

- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
  - Sniffing the Key
  - Recovering the Recovery PW
  - Extracting Artifacts

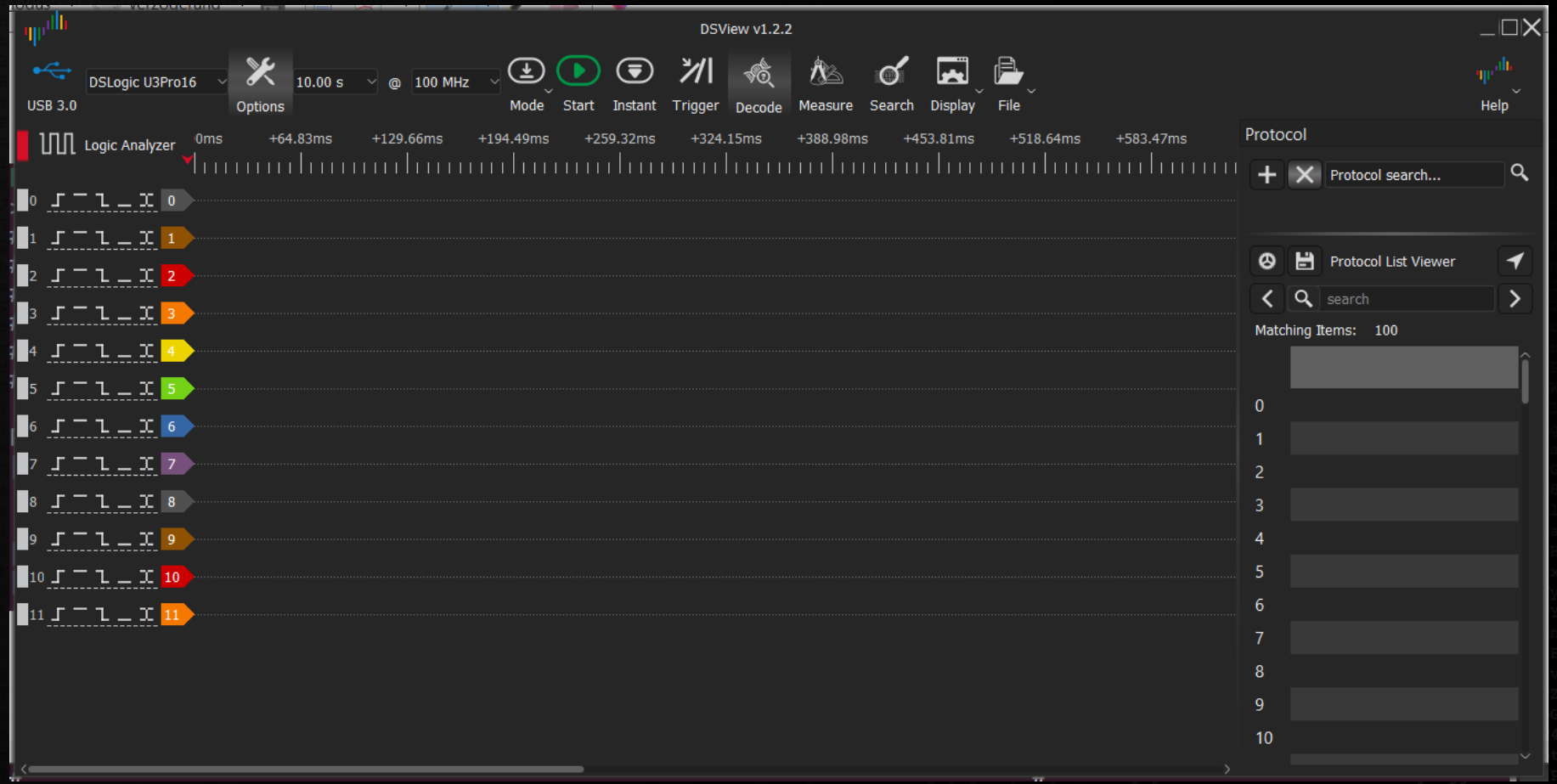
Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
  - Obtaining the Recovery PW

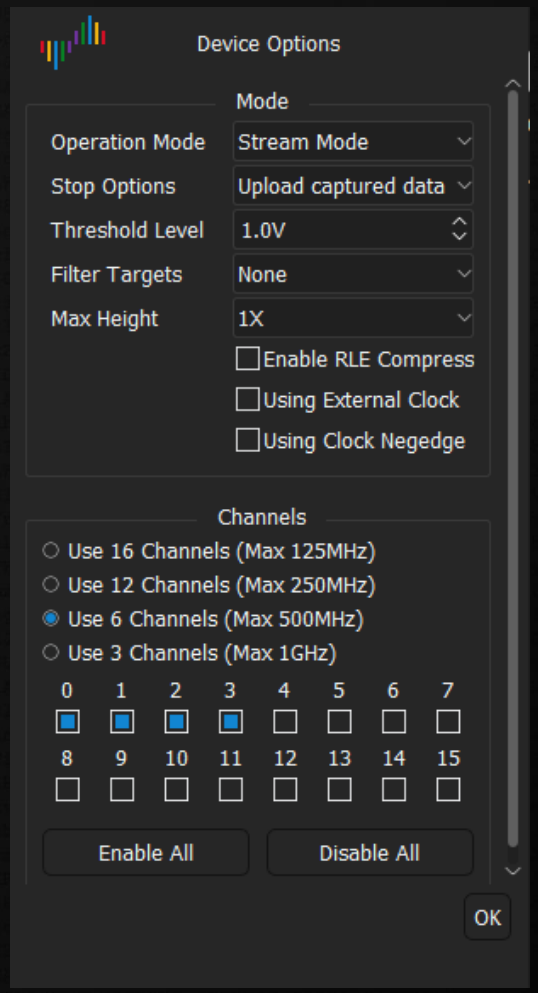
TPM Sniffing

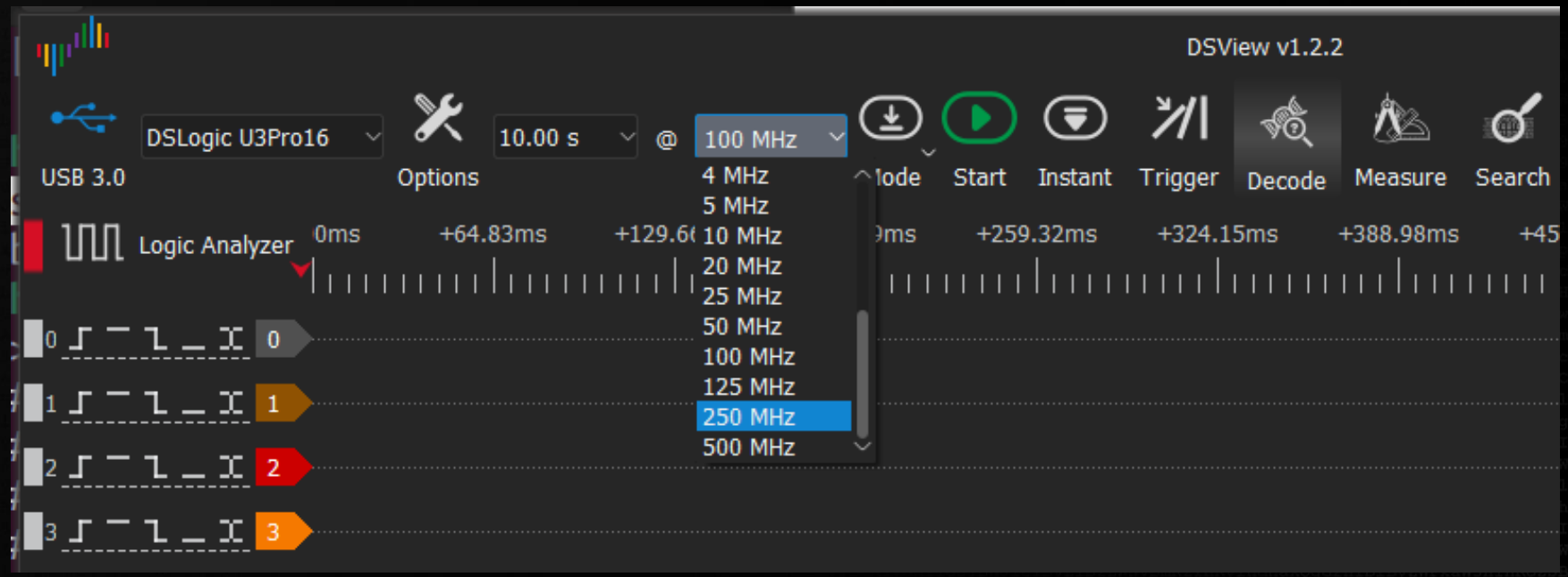
1. Connect the logic analyzer's signal pins
2. Connect at least one GND
3. Setup DSView to record the correct pins at the correct sampling rate
4. Start a measurement for ~20 sec && boot Windows
5. Save the capture – **NO CTRL+S (!!!)**
6. Add and configure SPI Decoder
7. Wait for the magic to happen…

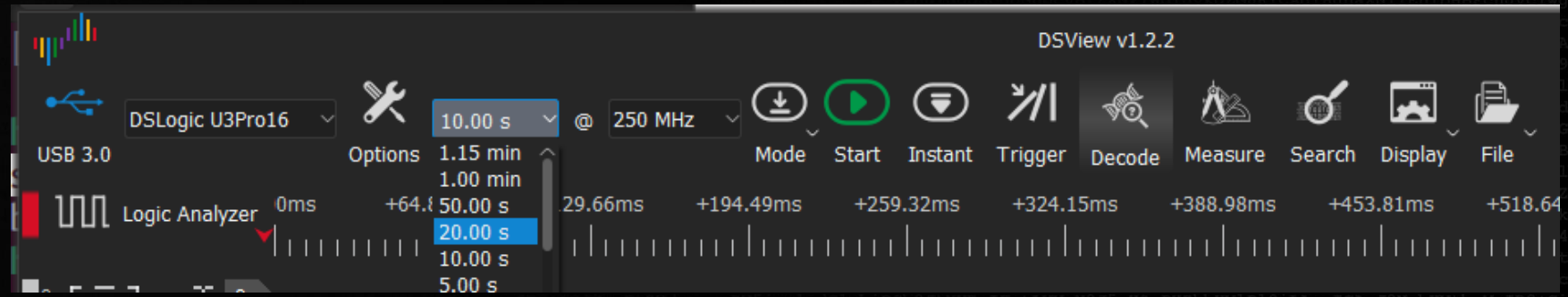
TPM Sniffing



TPM Sniffing





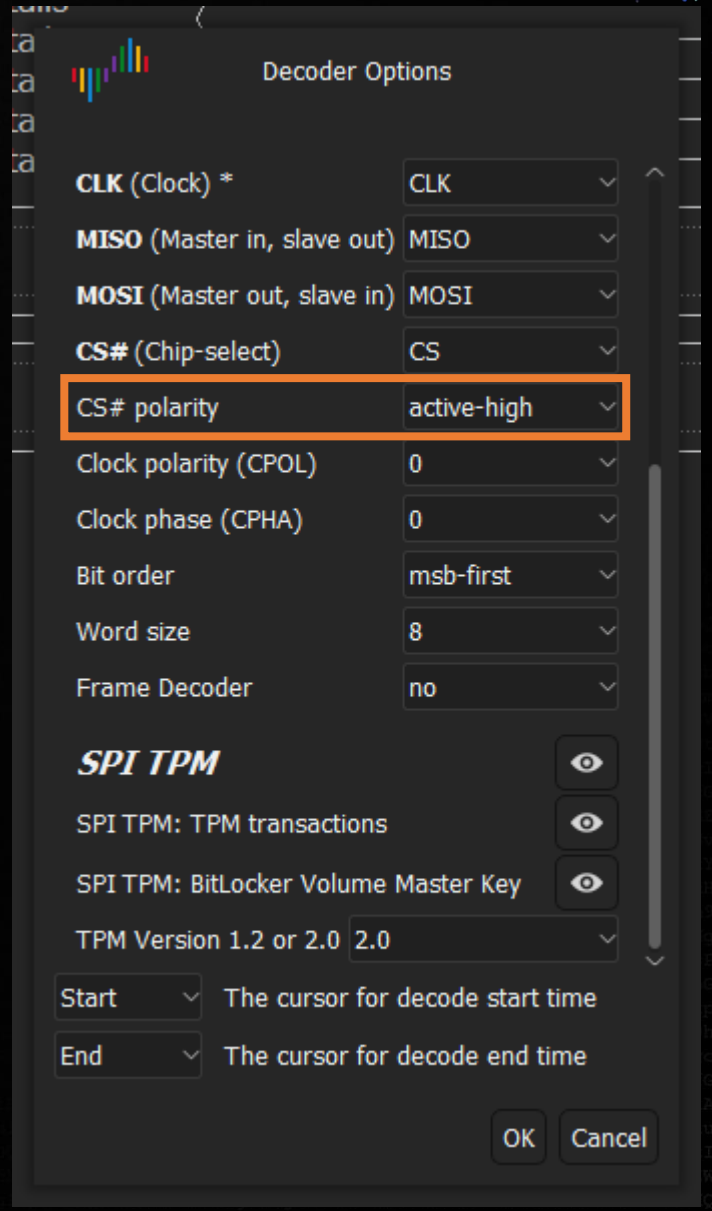


TPM Sniffing

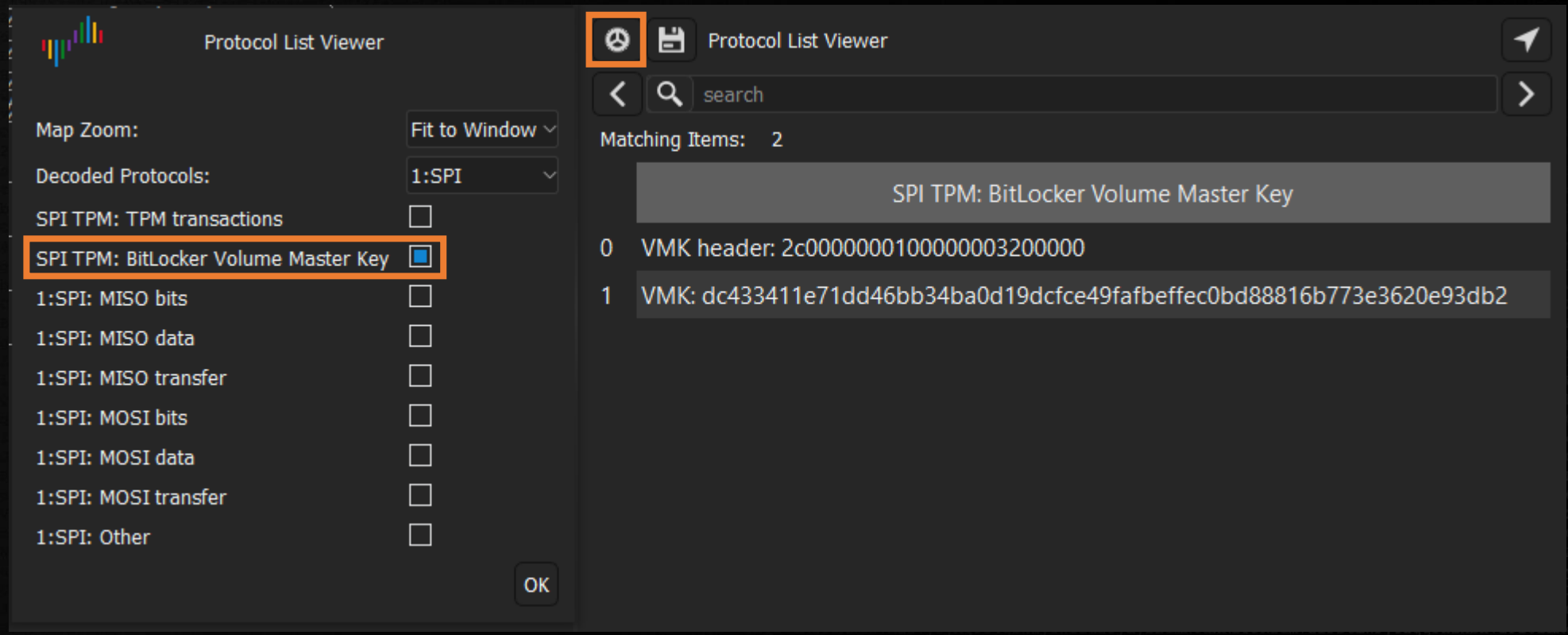
1. Connect the logic analyzer's signal pins
2. Connect at least one GND
3. Setup DSView to record the correct pins at the correct sampling rate
4. Start a measurement for ~20 sec && boot Windows
5. Save the capture – **NO CTRL+S (!!!)**
6. Add and configure SPI Decoder
7. Wait for the magic to happen…

TPM Sniffing

- Default decoder settings
- CS# (Chip-select) must be **active- high** when sniffing on a non TPM chip-select line



TPM Sniffing



Agenda Day 2

- ✅ BitLocker Theory
- ✅ TPM Theory
- ✅ Soldering to the TPM Bus
- ✅ Logic Analyzers & Labs
- ✅ Sniffing the Key
  - Recovering the Recovery PW
  - Extracting Artifacts

Key Takeaways

- ✅ BitLocker & TPM Theory
- ✅ Logic Analyzers
  - Obtaining the Recovery PW

Coffee Break

Recovering Recovery Password

1. Extract BitLocker metadata from a given partition by parsing the output of dislocker-metadata
2. Decrypt the recovery password entry by using the (nonce, mac,payload) from the BitLocker metadata entry with "Datum value type: 3“ and your VMK
3. Remove the header from the decrypted recovery password

1c 00 00 00 01 00 00 00 00 10 00 00 **fc 2f 86 ef 46 9d 99 02 22 1a f8 6b 56 82 d0 4b**

4. Split the binary data in chunks of two bytes

fc 2f|86 ef|46 9d|99 02|22 1a|f8 6b|56 82|d0 4b

Recovering Recovery Password

1. Swap the endianness of each chunk

   fc 2f|86 ef|46 9d|99 02|22 1a|f8 6b|56 82|d0 4b

2. Convert chunks to decimal number

   12284 61318 40262 665 6690 27640 33366 19408

3. Multiply decimal number by 11

   135124 674498 442882 7315 73590 304040 367026 213488

4. Pad each number with leading zeroes to 6 digits

   135124 674498 442882 007315 073590 304040 367026 213488

5. Concat to BitLocker recovery password

   135124-674498-442882-007315-073590-304040-367026-213488

Recovering Recovery Password

```
user@user-Precision-7510:~/tpm/Data/software/bitlocker-recovery-key-decryptor$ sudo ./bitlocker-recovery-key-decryptor.py
3fdcd9fc0a9ed26c67142089d000d0cb2e0341c791440c8478235f9c3ba441b5 /dev/loop10
#############################################################################
#                                                                           #
#                     Bitlocker Recovery Password Decryptor                 #
#                                                                           #
# by Pascal Gujer (@pascal_gujer)                                           #
#############################################################################

Extracting Bitlocker key material with dislocker-metadata...
Parsing output...

Nonce:                  e0ec9ed5e184d80103000000
MAC:                    e03b0c4e34bc03c212121af7f961945a
Encrypted Recovery Password: 5e49a1757a27eaabaa059431dfa98782f0b8b167784056b428074728

VMK:                    3fdcd9fc0a9ed26c67142089d000d0cb2e0341c791440c8478235f9c3ba441b5

Decrypting recovery password...
The decrypted recovery password is authentic:
1c000000100000000100000fc2f86ef469d9902221af86b5682d04b

[+] Sucessfully retrieved the BitLocker Recovery Password in human readable format:

           135124-674498-442882-007315-073590-304040-367026-213488
```

Recovering Recovery Password

LAB TIME!

```
hands-on-security@Ubuntu-VirtualBox:~/hands-on-security/scripts$ \
> ./bitlocker-recovery-password-decryptor.py
#############################################################################
#                                                                           #
#                      BitLocker Recovery Password Decryptor                #
#                                                                           #
# by Pascal Gujer (@pascal_gujer)                                  v1.0     #
#############################################################################

This script decrypts the encrypted recovery password from a given BitLocker drive
with the given Volume Master Key (VMK) and prints the result in the official
recovery password format.

'dislocker-metadata' is required to be in path

Syntax: bitlocker-recovery-password-decryptor {VMK as hex} {path to BitLocker partition}
```

black hat USA 2023
AUGUST 5-10
MANDALAY BAY / LAS VEGAS

Agenda Day 2

- ✓ BitLocker Theory
- ✓ TPM Theory
- ✓ Soldering to the TPM Bus
- ✓ Logic Analyzers & Labs
- ✓ Sniffing the Key
- ✓ Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- ✓ BitLocker & TPM Theory
- ✓ Logic Analyzers
- ✓ Obtaining the Recovery PW

Unlocking BitLocker

- WinFE

Windows Forensic Environment

- manage-bde.exe -unlock <drive>: -recoverypassword xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx
- Additional challenge:
  - Get the Windows password – you're the experts ☺

Agenda Day 2

- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW

End of Day 2

- Questions?

Agenda Day 1

- Equipment Inspection
- Soldering Theory & Lab
- Tamper Protection Switches
- Forensic Data Acquisition
- Notebook Internals
- Notebook Disassembly

Key Takeaways

- Ability to Solder
- Tamper Protection Switches
- Basic Forensic Data Acquisition

Agenda Day 2

- BitLocker Theory
- TPM Theory
- Soldering to the TPM Bus
- Logic Analyzers & Labs
- Sniffing the Key
- Recovering the Recovery PW
- Extracting Artifacts

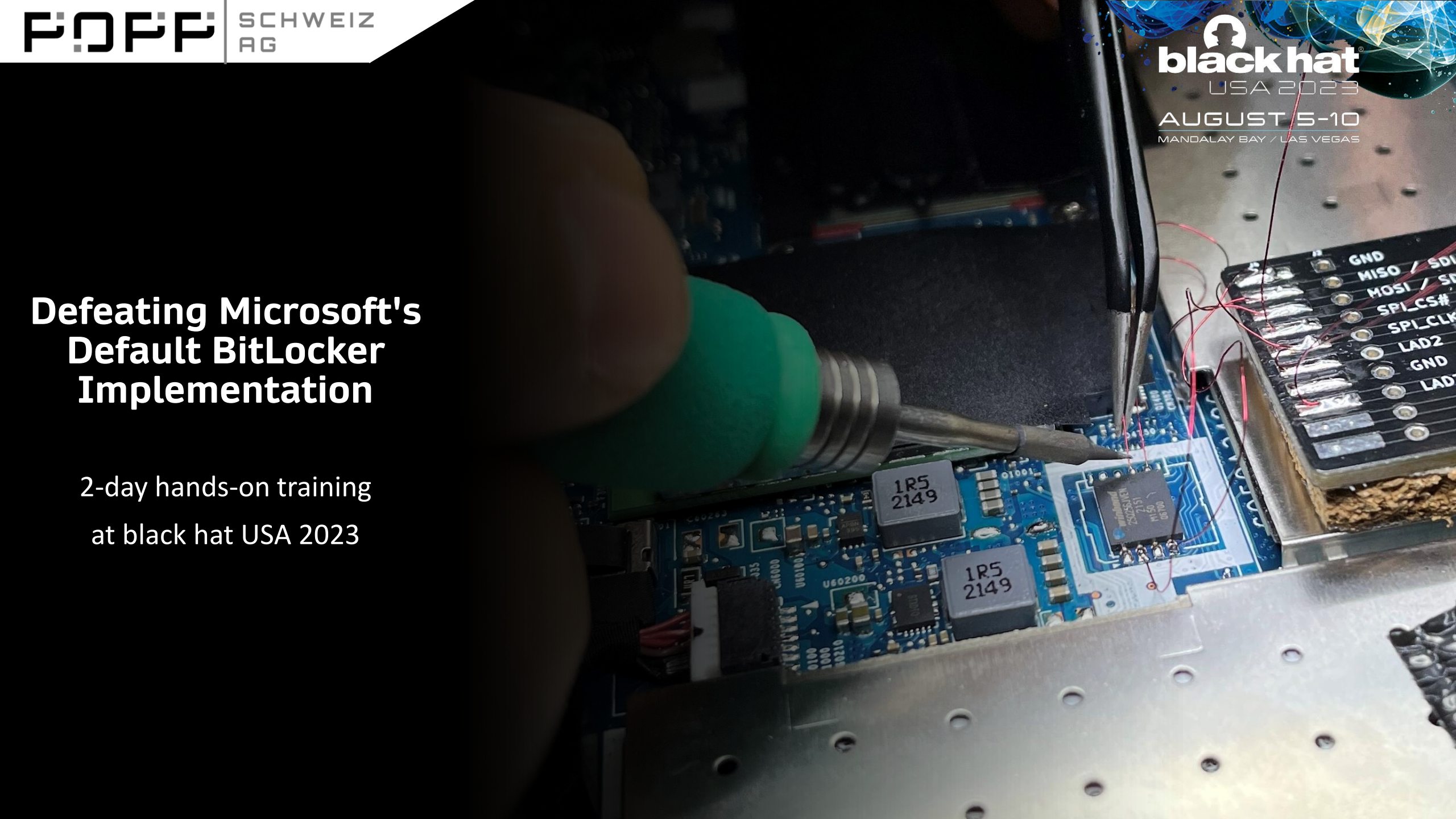
Key Takeaways

- BitLocker & TPM Theory
- Logic Analyzers
- Obtaining the Recovery PW


Corona
Extra
BEER
355 ml
CERVECERIA MODELO, S. DE R.L. DE C.V.
MEXICO, D.F.

You rocked!

POFP SCHWEIZ AG



Defeating Microsoft's Default BitLocker Implementation

2-day hands-on training

at black hat USA 2023