Umgehung von Festplattenverschlüsselung mit Trusted Platform Module am Beispiel von BitLocker

Professionelle Textsatzsysteme

0xffd700

17. Dezember 2021

Inhaltsverzeichnis

Festplattenverschlüsselung

Festplattenverschlüsselung

Methode zum Schutz von Daten gegen physikalische Angriffe durch Verschlüsselung des gesamten Datenträgers oder einzelner Sektoren.

[9]

Trusted Platform Module (TPM)

- Krypto-Prozessor zur Erweiterung von grundlegenden Sicherheitsfunktionen

Abbildung 1: TPM Chip [1]

[10]

Trusted Platform Module (TPM)

- Krypto-Prozessor zur Erweiterung von grundlegenden Sicherheitsfunktionen
  - Generiert, speichert und limitiert den Einsatz von kryptografischen Schlüsseln

Abbildung 1: TPM Chip [1]

[10]

Trusted Platform Module (TPM)

- Krypto-Prozessor zur Erweiterung von grundlegenden Sicherheitsfunktionen
  - Generiert, speichert und limitiert den Einsatz von kryptografischen Schlüsseln
  - Authentifiziert Geräte

Abbildung 1: TPM Chip [1]

[10]

Trusted Platform Module (TPM)

- Krypto-Prozessor zur Erweiterung von grundlegenden Sicherheitsfunktionen
  - Generiert, speichert und limitiert den Einsatz von kryptografischen Schlüsseln
  - Authentifiziert Geräte
  - Sicherstellung der Plattformintegrität

Abbildung 1: TPM Chip [1]

[10]

BitLocker

- Sicherheitsfunktion von Microsoft

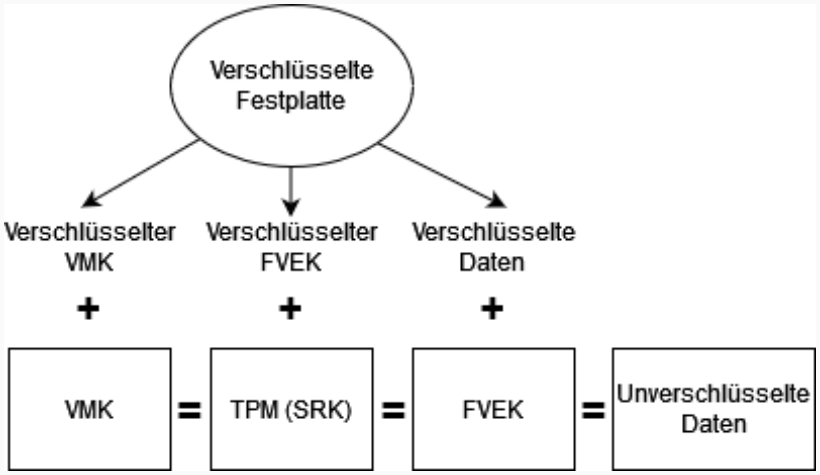

Abbildung 2: BitLocker Entschlüsselung

[5]

BitLocker

- Sicherheitsfunktion von Microsoft
- Plattformvalidierung durch Sealed Storage

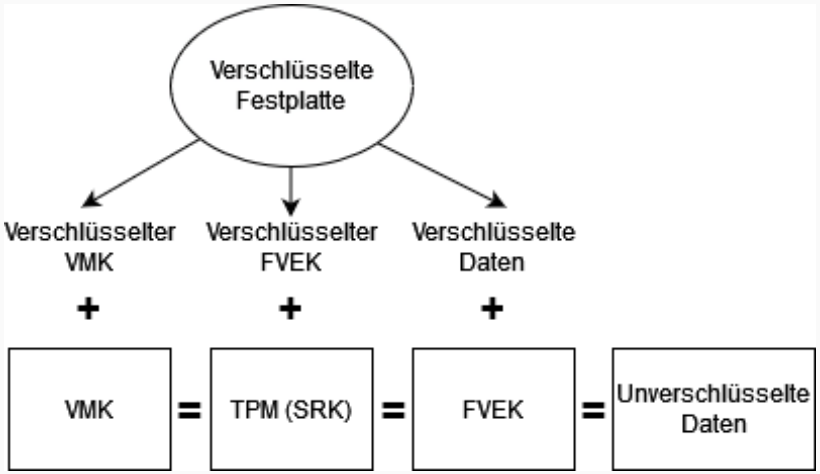

Abbildung 2: BitLocker Entschlüsselung

[5]

BitLocker

- Sicherheitsfunktion von Microsoft
- Plattformvalidierung durch Sealed Storage
- Entschlüsselung mit BitLocker:

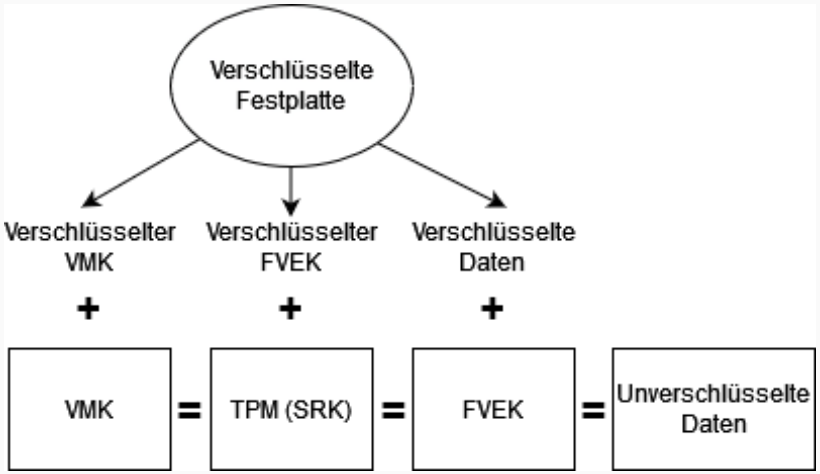

Abbildung 2: BitLocker Entschlüsselung

[5]

BitLocker

- Sicherheitsfunktion von Microsoft
- Plattformvalidierung durch Sealed Storage
- Entschlüsselung mit BitLocker:
  - Volume Master Key (VMK)

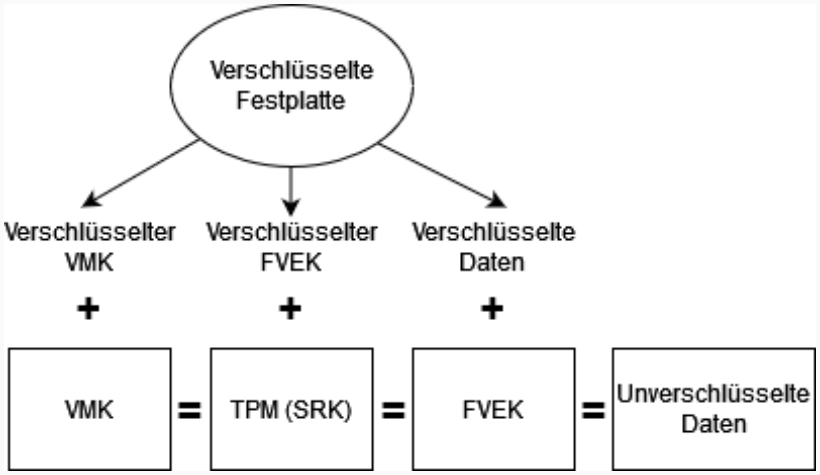

Abbildung 2: BitLocker Entschlüsselung

[5]

BitLocker

- Sicherheitsfunktion von Microsoft
- Plattformvalidierung durch Sealed Storage
- Entschlüsselung mit BitLocker:
  - Volume Master Key (VMK)
  - Storage Root Key (SRK)

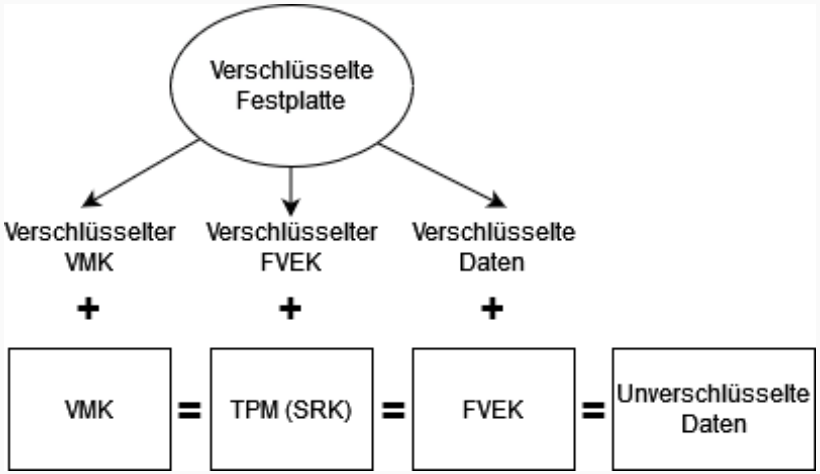

Abbildung 2: BitLocker Entschlüsselung

[5]

BitLocker

- Sicherheitsfunktion von Microsoft
- Plattformvalidierung durch Sealed Storage
- Entschlüsselung mit BitLocker:
  - Volume Master Key (VMK)
  - Storage Root Key (SRK)
  - Full Volume Encryption Key (FVEK)

[5]

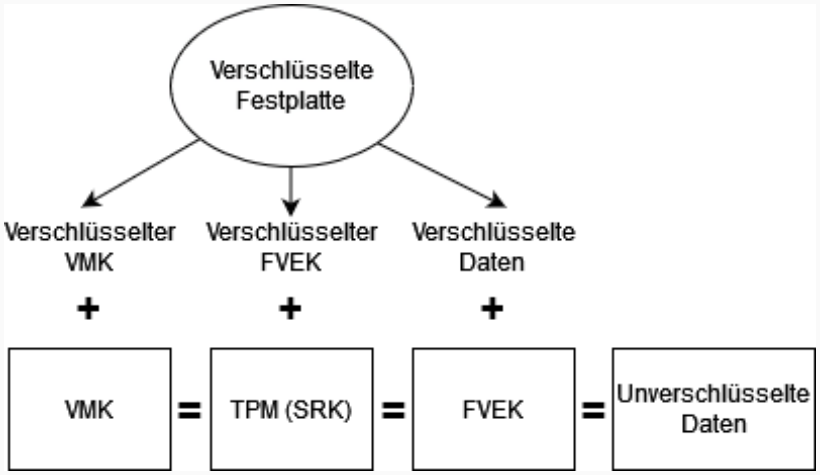

Abbildung 2: BitLocker Entschlüsselung

Umgehung von Festplattenverschlüsselung

Bekannte Angriffe

- Evil Maid Angriff

[7]

Bekannte Angriffe

- Evil Maid Angriff
- Cold Boot Angriff

[7]

Bekannte Angriffe

- Evil Maid Angriff
- Cold Boot Angriff
- Direkt Memory Access Angriff

[7]

Bekannte Angriffe

- Evil Maid Angriff
- Cold Boot Angriff
- Direkt Memory Access Angriff
- Hotplug Angriff

[7]

Serial Peripheral Interface (SPI) Angriff

- FVEK wird beim Bootvorgang vom TPM zu Windows gesendet

Serial Peripheral Interface (SPI) Angriff

- FVEK wird beim Bootvorgang vom TPM zu Windows gesendet
- Unverschlüsselte Kommunikation zwischen TPM und CPU

Serial Peripheral Interface (SPI) Angriff

- FVEK wird beim Bootvorgang vom TPM zu Windows gesendet
- Unverschlüsselte Kommunikation zwischen TPM und CPU
- Auslesen der Daten über den SPI-Bus

Praxisversuch

Versuchsaufbau

- Physikalischer Zugriff

Versuchsaufbau

- Physikalischer Zugriff
- Windows 10 Professional

Versuchsaufbau

- Physikalischer Zugriff
- Windows 10 Professional
- Vollständige Verschlüsselung mit BitLocker

Versuchsaufbau

- Physikalischer Zugriff
- Windows 10 Professional
- Vollständige Verschlüsselung mit BitLocker
- TPM 2.0 mit Serial Peripheral Interface

Trusted Platform Module abhören

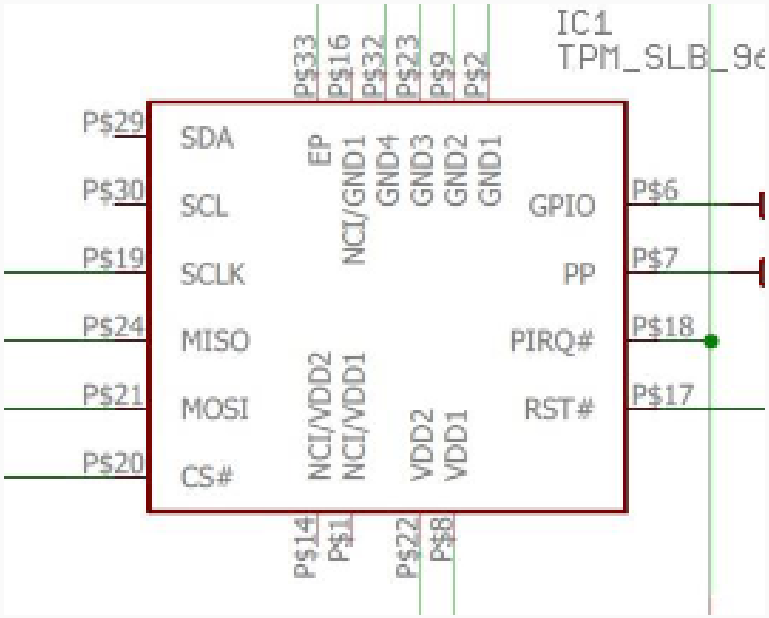

Abbildung 3: Infineon TPM [2]

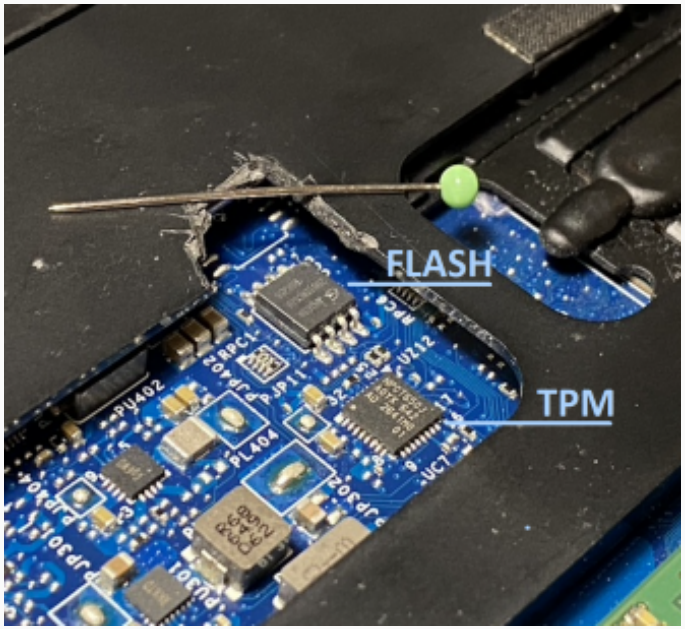

Abbildung 4: BIOS und TPM [3]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip

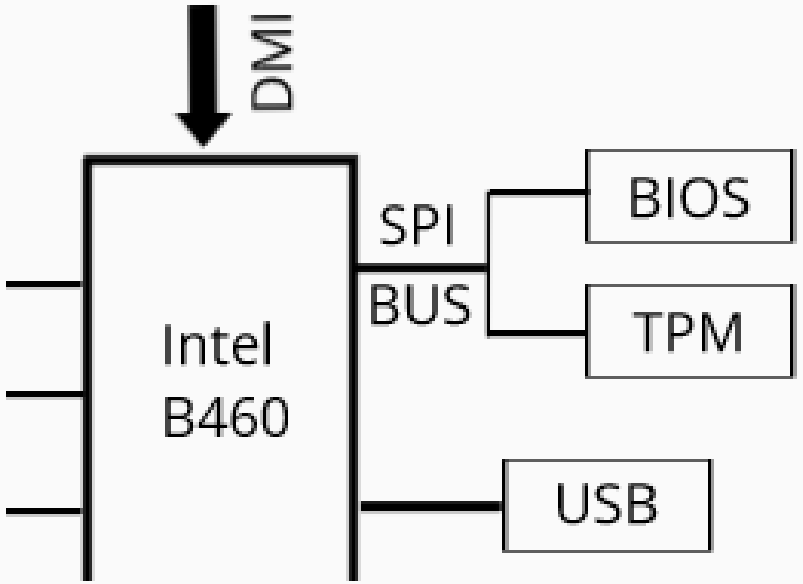

Abbildung 5: SPI-Bus [6]

[11, S. 335-349]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip
- SPI-Bus:

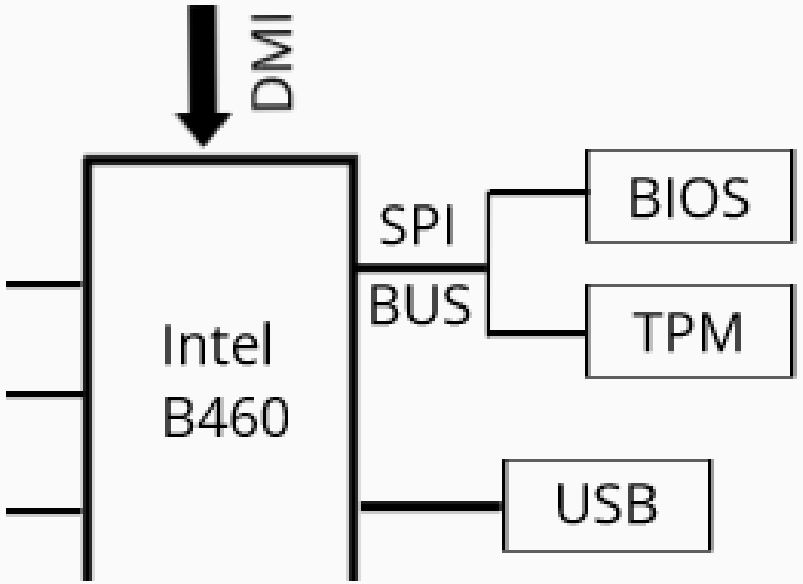

Abbildung 5: SPI-Bus [6]

[11, S. 335-349]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip
- SPI-Bus:
  - Master Out Slave In (MOSI)

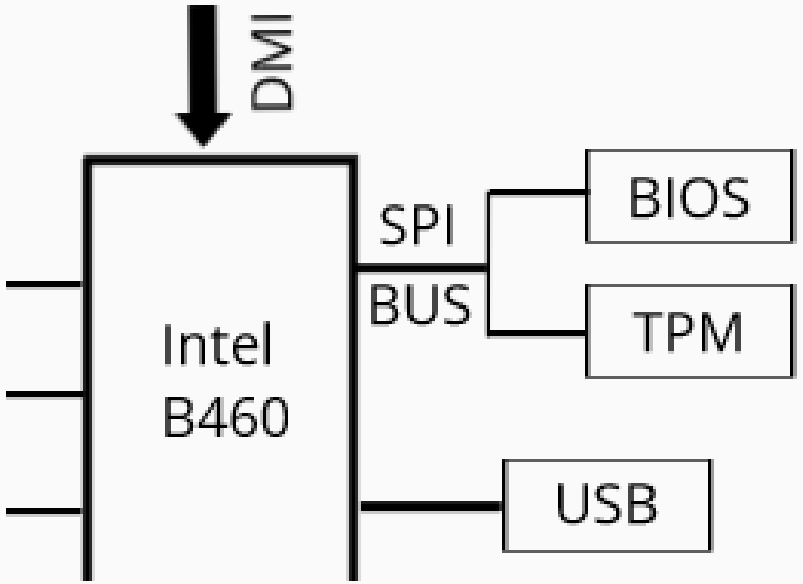

Abbildung 5: SPI-Bus [6]

[11, S. 335-349]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip
- SPI-Bus:
  - Master Out Slave In (MOSI)
  - Master In Slave Out (MISO)

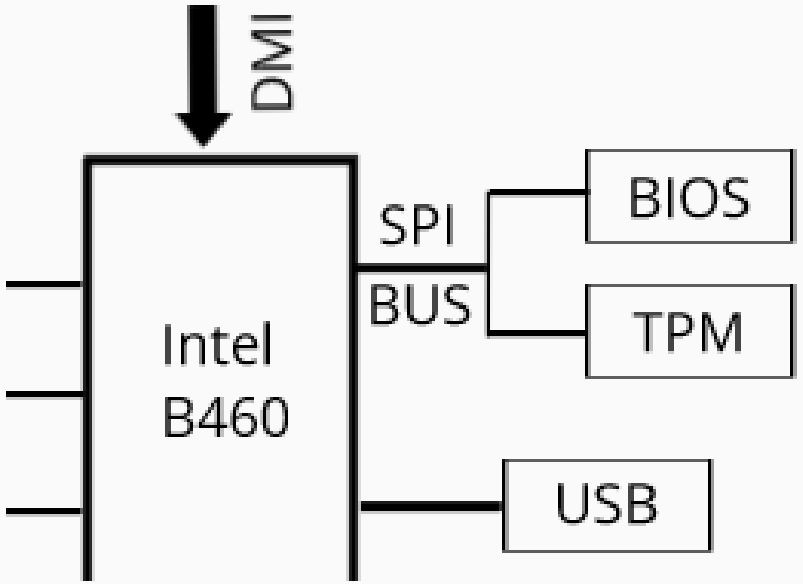

Abbildung 5: SPI-Bus [6]

[11, S. 335-349]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip
- SPI-Bus:
  - Master Out Slave In (MOSI)
  - Master In Slave Out (MISO)
  - Schiebetakt (CLK)

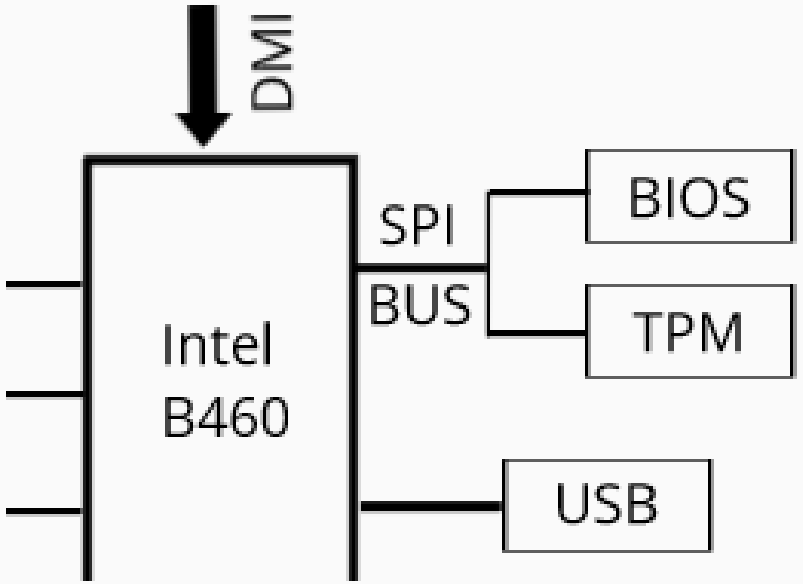

Abbildung 5: SPI-Bus [6]

[11, S. 335-349]

Serial Peripheral Interface

- Synchroner und serieller Datenbus mit Master-Slave-Prinzip
- SPI-Bus:
  - Master Out Slave In (MOSI)
  - Master In Slave Out (MISO)
  - Schiebetakt (CLK)
  - Chip Select (CS)

[11, S. 335-349]

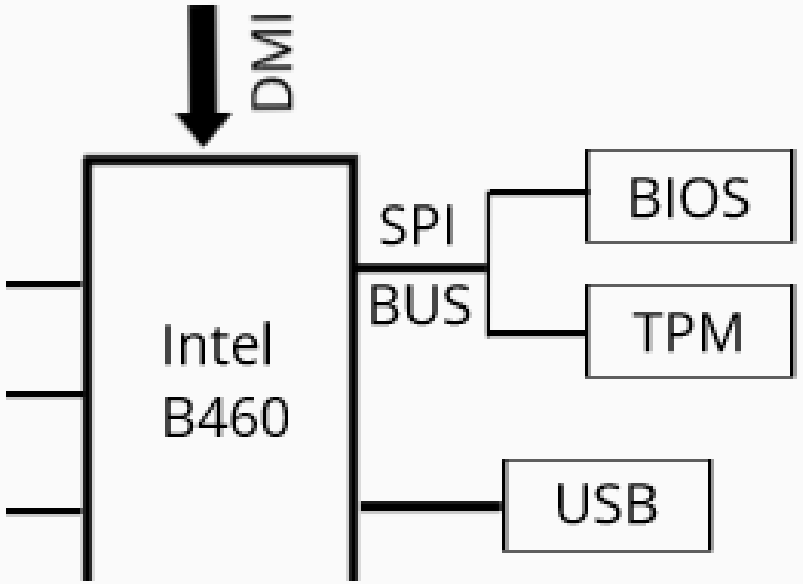

Abbildung 5: SPI-Bus [6]

SPI-Bus abhören

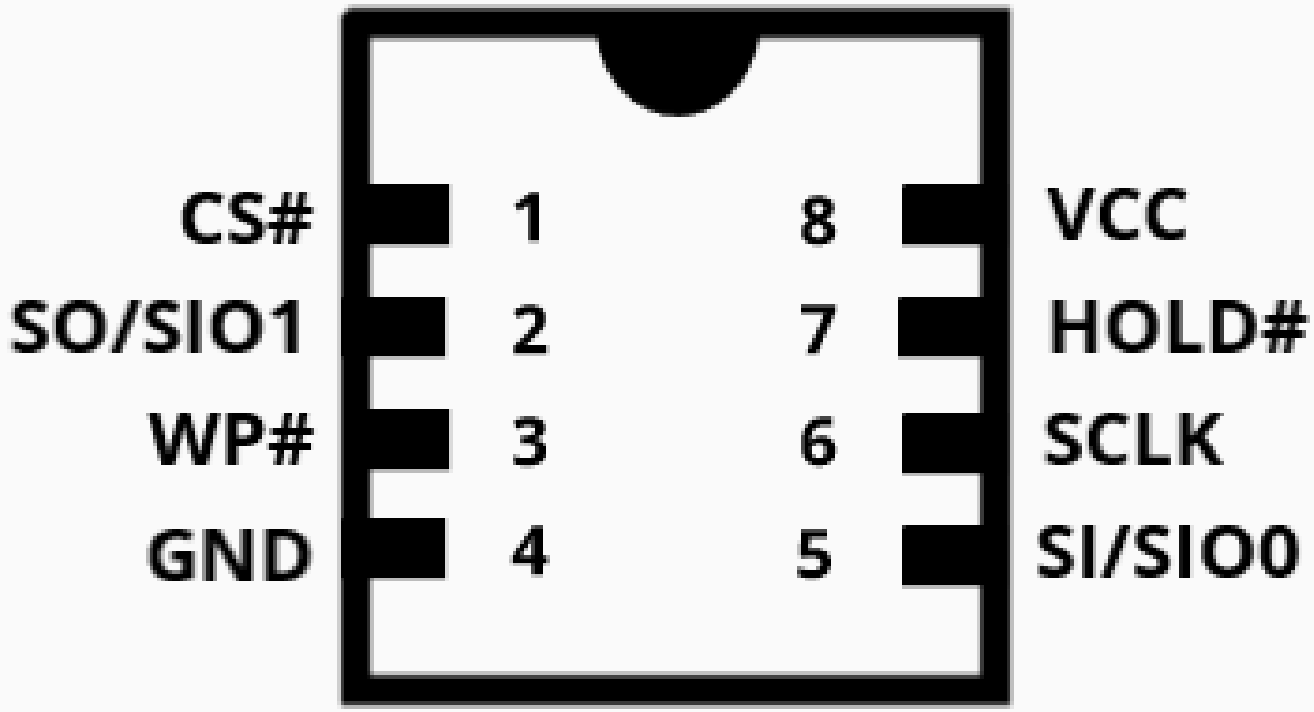

Abbildung 6: BIOS Blockdiagramm [8]

Logik Analyzer

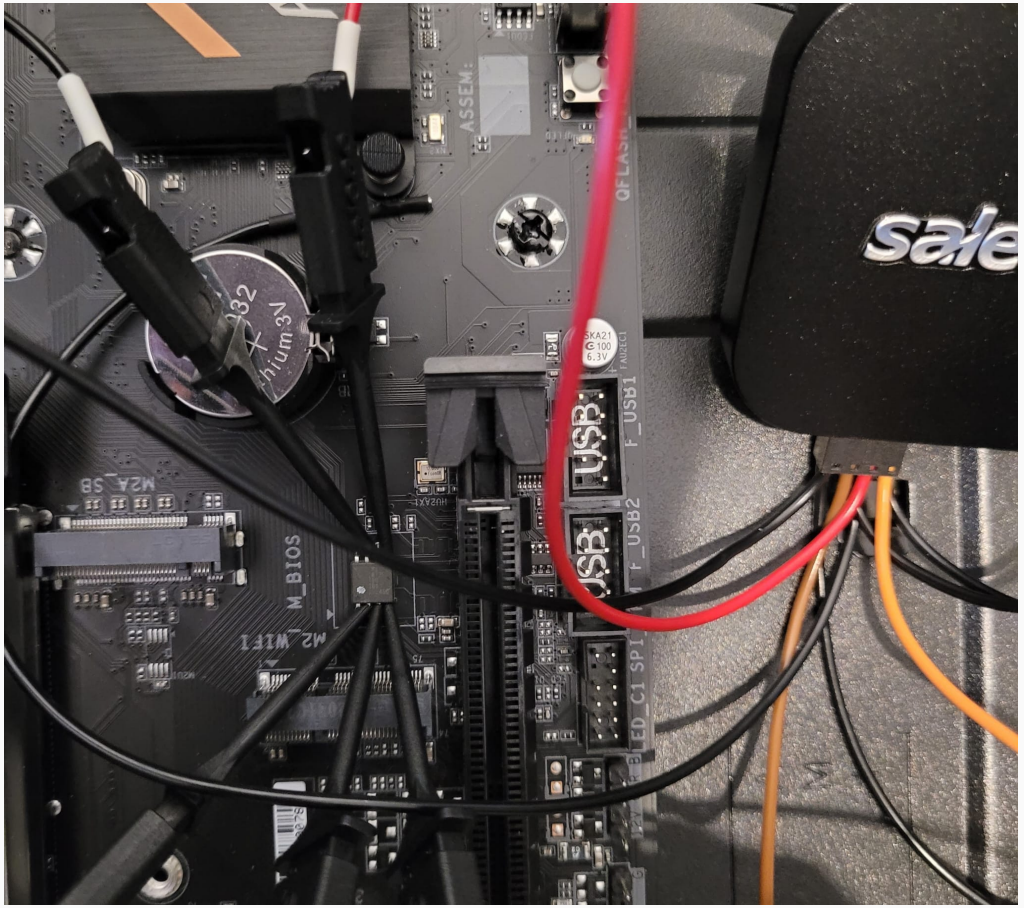

Abbildung 7: Saleae Logik Analyzer

BitLocker Key Extractor

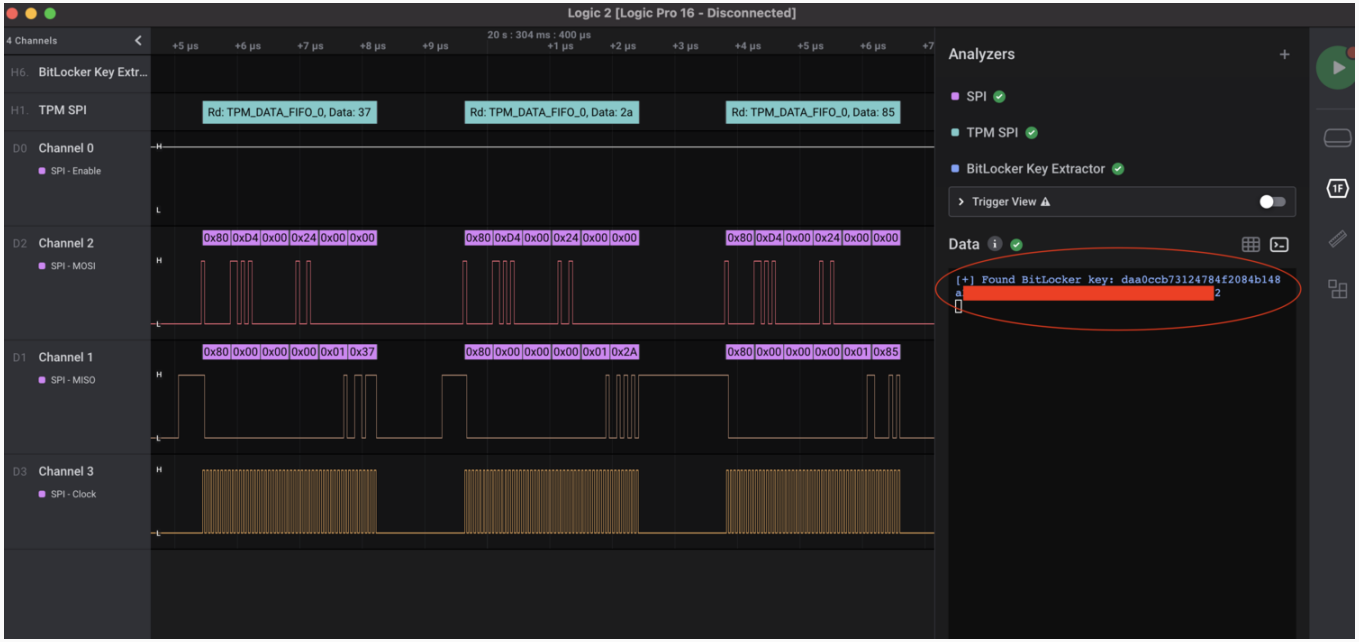

Abbildung 8: Saleae Logic Pro [2]

Speichermedium entschlüsseln

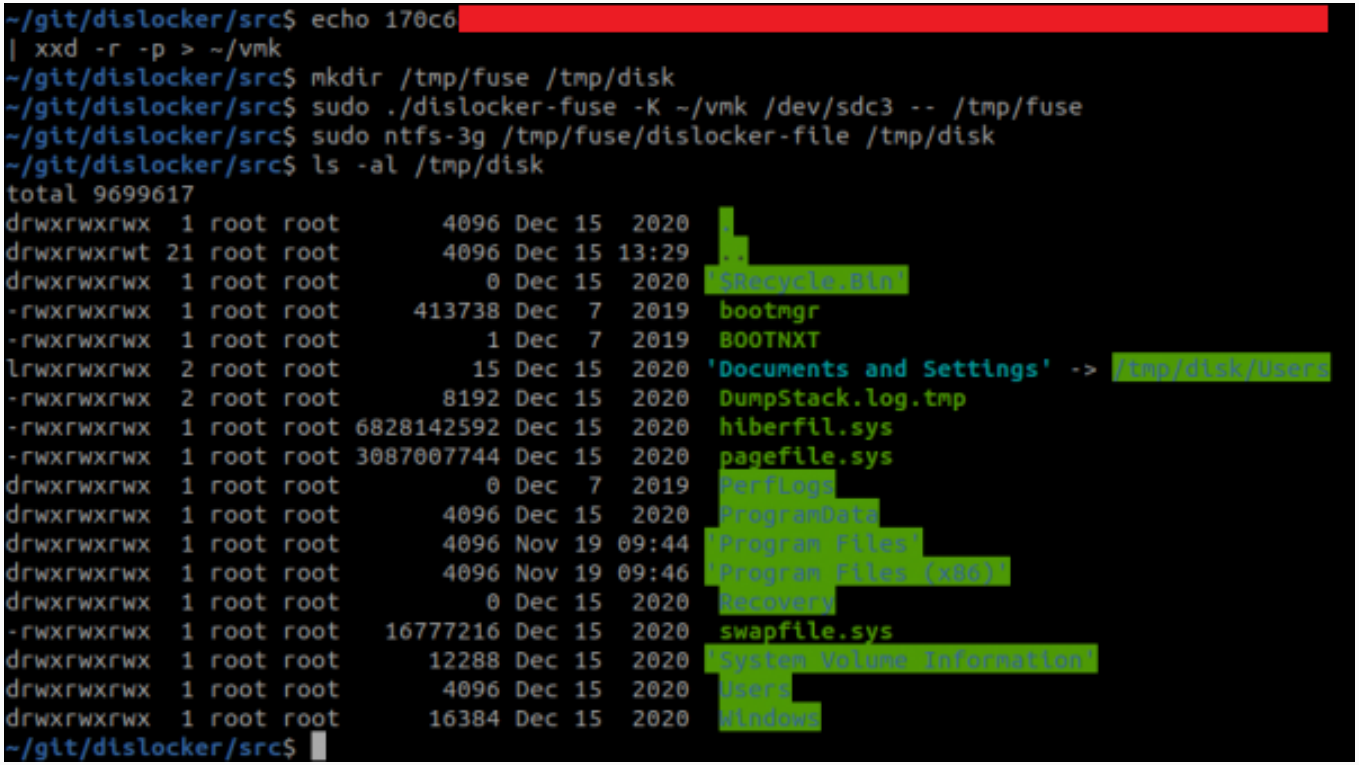

Abbildung 9: Dislocker [4]

Fazit

Evaluation

- Zeit

Evaluation

- Zeit
- Ressourcen

Evaluation

- Zeit
- Ressourcen
- Kosten

Evaluation

- Zeit
- Ressourcen
- Kosten
- Schwierigkeit

Prävention

- Zusätzliche Benutzerverifikation

Prävention

- Zusätzliche Benutzerverifikation
- Einschränkung physikalischer Zugriff

Fragen?

Literatur i

[1] tle62512gxuma1_spl.jpg (webp-grafik, 598 × 510 pixel), 04/10/2021.

[2] Screen+shot+2021-06-16+at+9.38.03+pm.png (png-grafik, 1500 × 705 pixel), 15/12/2021.

[3] flash-and-tpm.png (png-grafik, 600 × 306 pixel), 16/12/2020.

[4] manual-mount.png (png-grafik, 600 × 337 pixel), 16/12/2020.

[5] Dansimp.
Bitlocker countermeasures (windows 10) - windows security, 13/12/2021.

[6] GIGA-BYTE TECHNOLOGY CO., LTD.
B460m ds3h ac b460m ds3h user´s manual.

Literatur ii

[7] Guruprasad Bidare.
BitLocker Full Disk Encryption.
Master, Masaryk University, Bangalore, 2017.

[8] Macronix International Co., LTD.
Mx25l6406e datasheet, 2010.

[9] Sibinger, Christoph AND Müller, Tilo.
Verwendung von festplattenvollverschlüsselung im geschäftlichen und privaten umfeld: Sicherheit 2014 – sicherheit, schutz und zuverlässigkeit.
pages 201–216, 2014.

[10] Trusted Computing Group.
Trusted platform module (tpm) — trusted computing group (tpm), 30/07/2020.

Literatur iii

[11] C. Wootton, editor.
Samsung ARTIK Reference.
Apress, Berkeley, CA, 2016.