SICHERE USB-SPEICHERMEDIEN

Hacking von sicheren USB-Sticks und USB-Festplatten

AGENDA

- Verwendete Technologien
- Angriffsfläche und Angriffsszenarien
- Überblick unserer Forschung
- Gefundene Sicherheitsschwachstellen
- Live-Demo
- Fazit
- Fragen und Antworten

VORSTELLUNG

Matthias Deeg

- Diplom-Informatiker
- Senior Expert IT Security Consultant
- Head of Research & Development
- Seit 2007 bei SySS GmbH
- Seit frühen Tagen an Informationstechnologie interessiert – insbesondere an IT-Sicherheit

VORSTELLUNG

Gerhard Klostermeier

- Pentester / Expert IT Security Consultant
- Seit 2014 bei SySS GmbH
- Teammanager „Embedded Security"
- Interessen: Hardware-Hacking, IoT, Automotive, Funktechnologien, NFC/RFID, Android usw.
- E-Mail-Adresse: gerhard.klostermeier@syss.de

VERWENDETE TECHNOLOGIEN

VERWENDETE TECHNOLOGIEN

Typische Hauptkomponenten eines sicheren Krypto-USB-Sticks:

- NAND-Flash-Memory
- Memory Controller
- USB-Bridge-Controller
- Eingabegerät (z. B. Keypad oder Fingerabdrucksensor)
  - Keypad-Controller
  - Fingerabdrucksensor-Controller
- SPI-Flash-Memory-Chip

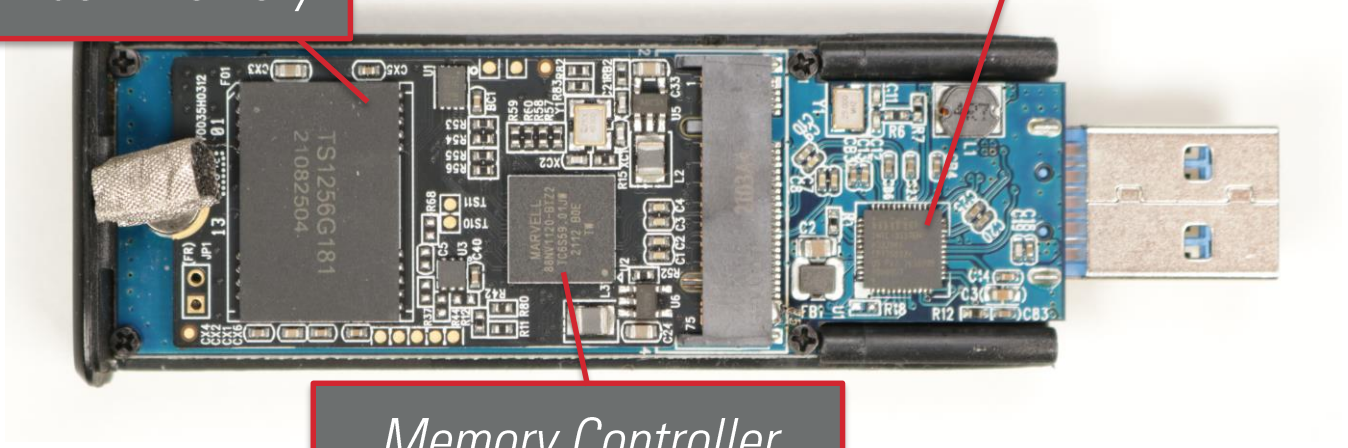
VERWENDETE TECHNOLOGIEN

THE PENTEST EXPERTS.

Beispiel: Verbatim Keypad Secure

NAND-Flash-Memory

USB-to-SATA-Bridge-Controller

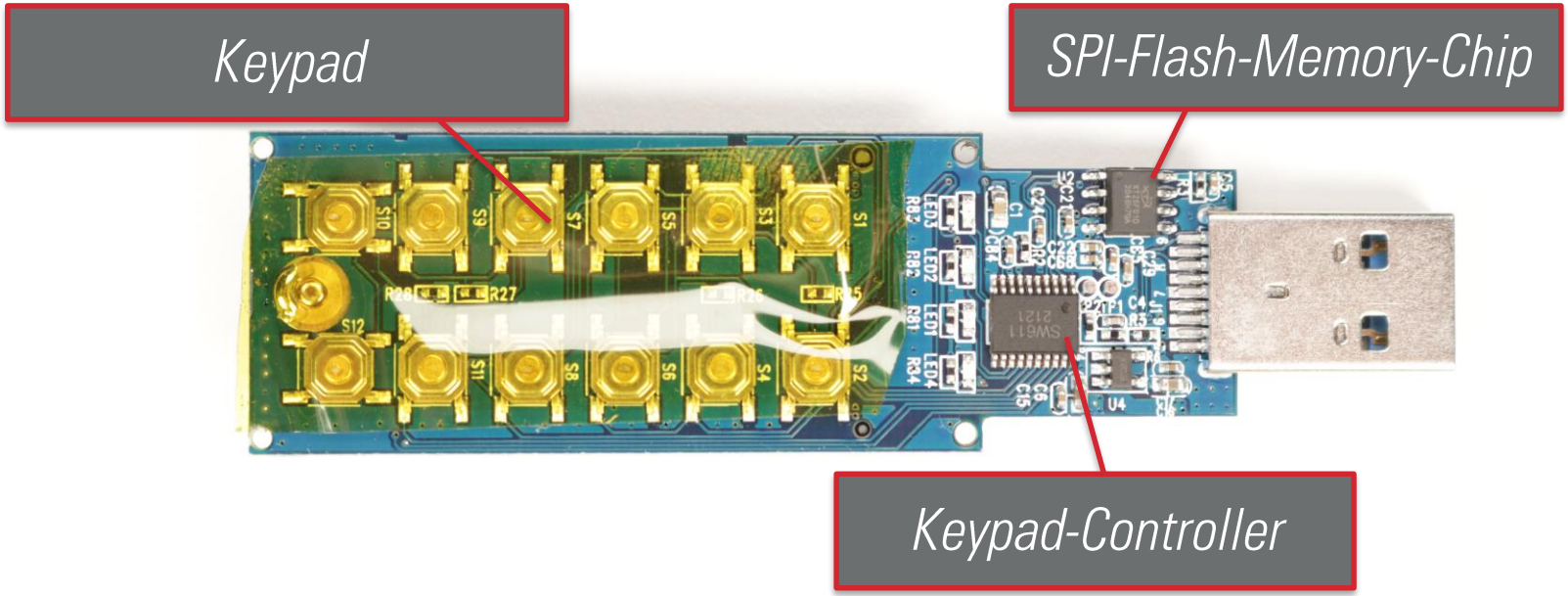


Memory Controller

VERWENDETE TECHNOLOGIEN

THE PENTEST EXPERTS.

Beispiel: Verbatim Keypad Secure



VERWENDETE TECHNOLOGIEN

- 256-bit-AES-Hardwareverschlüsselung
- Benutzerdaten sind mit einem Disk Encryption Key (DEK) verschlüsselt
- DEK ist mit Key Encryption Key (KEK) verschlüsselt
- KEK wird von Benutzereingabe für die Authentifizierung abgeleitet, z. B. durch:
  - Passcode (z. B. via Keypad)
  - Passwort (z. B. via USB-Kommunikation von Clientsoftware)
  - Fingerabdruck (via Fingerabdrucksensor)

ÜBERBLICK UNSERER FORSCHUNG

- Kundenanfrage im Dezember 2021 zur Sicherheit zweier Krypto-USB-Sticks
- Sicherheitsanalyse eines Geräts im Januar 2022
- Mehrere Sicherheitsschwachstellen identifiziert
- Kauf weiterer sicherer portabler USB-Speichergeräte mit ähnlichen Eigenschaften
- Dieselben und andere Sicherheitsschwachstellen in weiteren Geräten gefunden
- Sicherheitsschwachstellen an betroffene Hersteller im Rahmen unseres Responsible Disclosure-Programms gemeldet

ANGRIFFSFLÄCHE UND ANGRIFFSSZENARIEN

- Angriffe gegen die getesteten sicheren portablen USB-Speichergeräte erfordern physischen Zugriff auf die Hardware
- Angriffe sind zu verschiedenen Zeitpunkten des Lebenszyklus eines USB-Speichergeräts möglich:
  - Vor der Verwendung des Geräts durch einen legitimen Benutzer (Supply-Chain-Angriff)
  - Nach der Verwendung des Geräts durch einen legitimen Benutzer (z. B. verlorenes, gestohlenes oder unbeaufsichtigtes Gerät)

BEISPIEL 1: VERBATIM KEYPAD SECURE

Wichtige Eigenschaften:

- 256-bit-AES-Hardwareverschlüsselung
- Eingebautes Keypad für Passcode-Eingabe (bis zu zwölf Ziffern)
- Speichert das Passwort nicht auf dem Computer und nicht im flüchtigen Speicher → sicherer als Softwareverschlüsselung
- USB 3.2 Gen 1-Verbindung
- PC- und Mac-kompatibel

(Quelle: User Manual – Verbatim Keypad Secure USB Drive, Keypad Secure USB_User Manual_EN_1906.pdf)

Note

For the security of your data we highly recommend you change the default passcode. Passcode must be between 5 and 12 digits long.

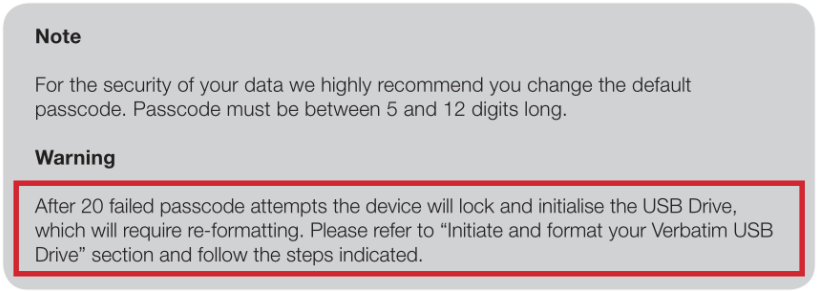
Warning

After 20 failed passcode attempts the device will lock and initialise the USB Drive, which will require re-formatting. Please refer to “Initiate and format your Verbatim USB Drive” section and follow the steps indicated.

DEVICE LOCK AND RESET

Problem #1

- Keine Sperrung des Geräts nach 20 aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen (manueller Passcode-Brute-Force-Angriff)



Note

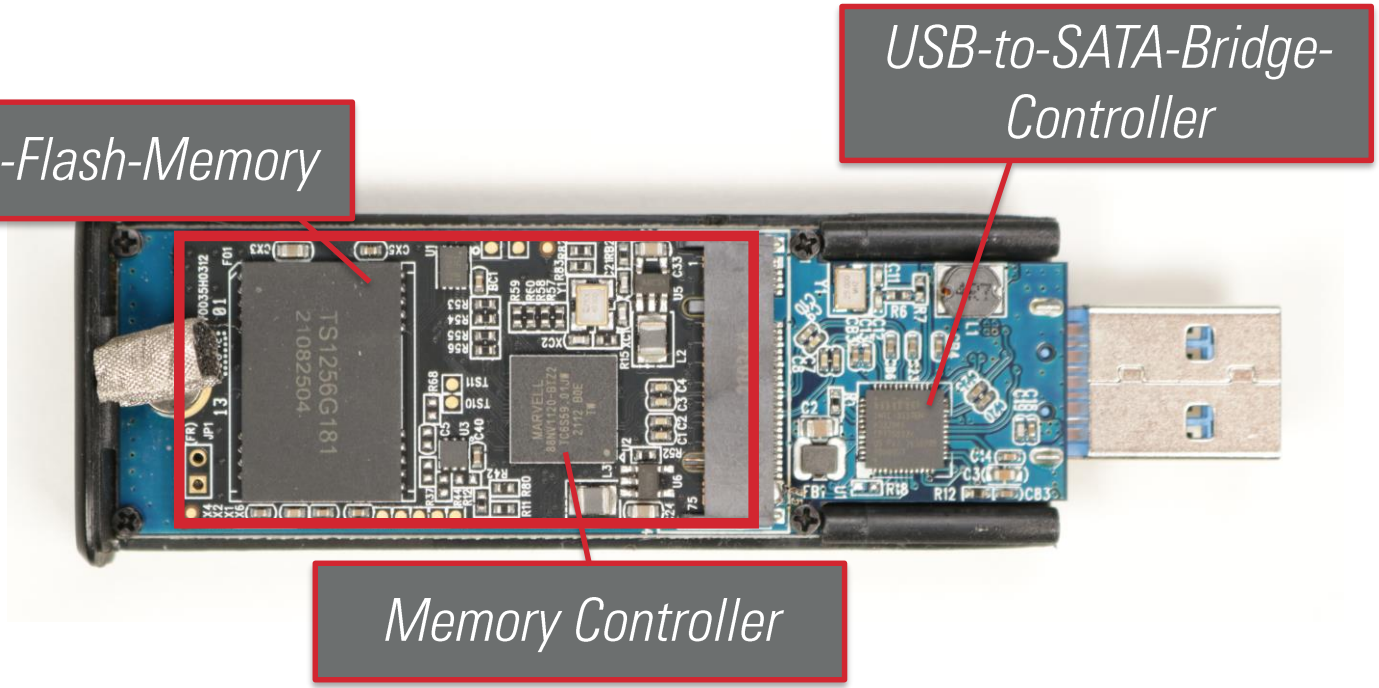
For the security of your data we highly recommend you change the default passcode. Passcode must be between 5 and 12 digits long.

Warning

After 20 failed passcode attempts the device will lock and initialise the USB Drive, which will require re-formatting. Please refer to “Initiate and format your Verbatim USB Drive” section and follow the steps indicated.

- Gerätesperre und erzwungene Rücksetzung funktionieren nicht wie beschrieben
- Ein Angreifer mit physischem Zugriff auf ein solches USB-Gerät kann zur Entsperrung daher mehr Passcodes ausprobieren, als eigentlich vorgesehen ist

SATA-SSD


NAND-Flash-Memory
USB-to-SATA-Bridge-Controller
Memory Controller

SATA-SSD: DATEN UND MUSTER

- Verbatim Keypad Secure enthält eine SATA-SSD mit M.2-Formfaktor
- Die SSD kann mit einem anderen SSD-Gehäuse gelesen und geschrieben werden
- Durch Analyse der verschlüsselten Daten konnte ein offensichtliches Muster erkannt werden

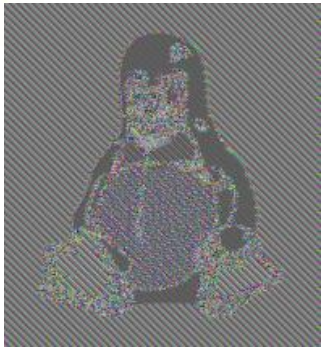
```
# hexdump -C /dev/sda
00000000  c4 1d 46 58 05 68 1d 9a  32 2d 29 04 f4 20 e8 4d  |..FX.h..2-).. .M|
*
000001b0  9f 73 b0 a1 81 34 ef bd  a4 b3 15 2c 86 17 cb 69  |.s...4.....,...i|
000001c0  eb d0 9d 9a 4e d8 04 a6  92 ba 3f f4 0c 88 a5 1d  |....N.....?.....|
000001d0  c4 1d 46 58 05 68 1d 9a  32 2d 29 04 f4 20 e8 4d  |..FX.h..2-).. .M|
*
000001f0  e0 01 66 72 af f2 be 65  5f 69 12 88 b8 a1 0b 9d  |..fr...e_i......|
00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00100000  73 b2 f8 fb af cf ed 57  47 db b8 c7 ad 9c 91 07  |s......WG.......|
00100010  7a 93 c9 d9 60 7e 2c e4  97 6c 7b f8 ee 4f 87 2c  |z...`~,..l{..O.,|
00100020  19 72 83 d1 6d 0b ca bb  68 f8 ec e3 fc c0 12 b7  |.r..m...h.......|
(…)
```

Solche sich wiederholenden Bytefolgen in verschlüsselten Daten sind kein gutes Zeichen

SATA-SSD: VERSCHLÜSSELUNG

Problem #2

- Durch Schreiben bekannter Bytemuster auf ein entsperrtes Gerät konnte bestätigt werden, dass dieselben 16 Byte an Klartext immer in denselben 16 Byte an Ciphertext resultieren
- Blockverschlüsselung mit 16-Byte-langen Blöcken unter Verwendung des Modus Electronic Codebook (ECB), z. B. AES-256-ECB
- Bei manchen Daten kann der Mangel der kryptografischen Eigenschaft „Diffusion“ sensible Informationen selbst in verschlüsselter Form ersichtlich machen



Quelle: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

FIRMWARE-ANALYSE

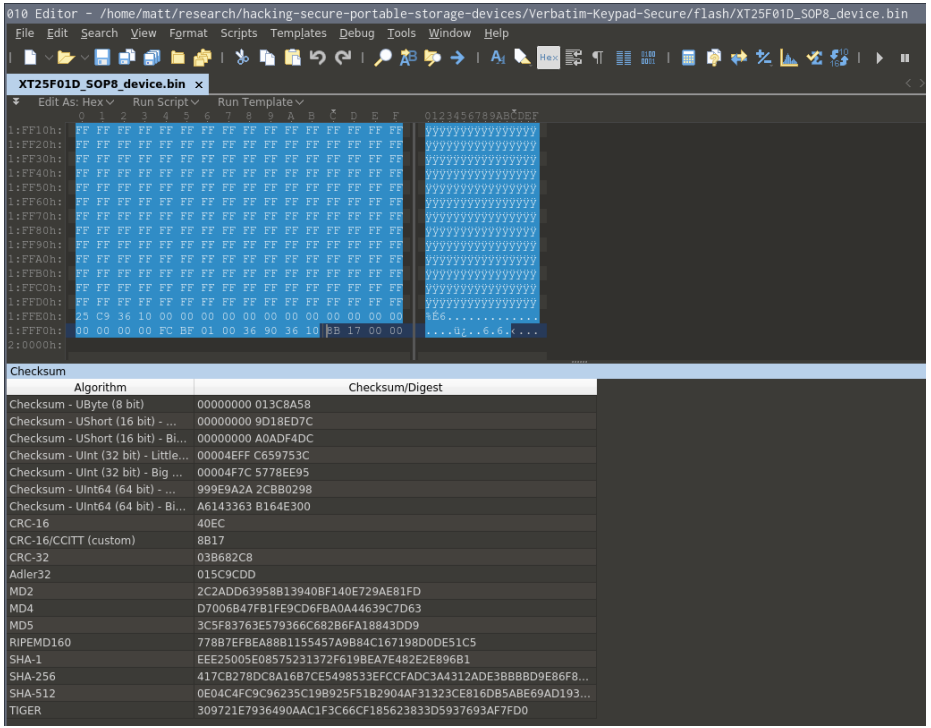
- Der Inhalt des SPI-Flash-Memory-Chips „XT25F01D“ konnte ausgelesen werden (128 KB)
- Enthält die Firmware des USB-to-SATA-Bridge-Controller „Initio INIC-3637EN“
- Für INIC-3637EN konnte kein öffentlich verfügbares Datenblatt gefunden werden
  - Es existieren jedoch öffentlich zugängliche Forschungsarbeiten mit nützlichen Informationen zu ähnlichen Chips wie INIC-3607
  - Besonders die Veröffentlichung „Lost your 'secure' HDD PIN? We can help!“ (Julien Lenoir und Raphaël Rigo) war von großer Hilfe
- INIC-3637EN nutzt das ARCompact Instruction Set
  - Die Veröffentlichung „Analyzing ARCompact Firmware with Ghidra“ von Nicolas Iooss und dessen implementierte Ghidra-Unterstützung waren von großem Nutzen

FIRMWARE-ANALYSE: INTEGRITÄT

Problem #3

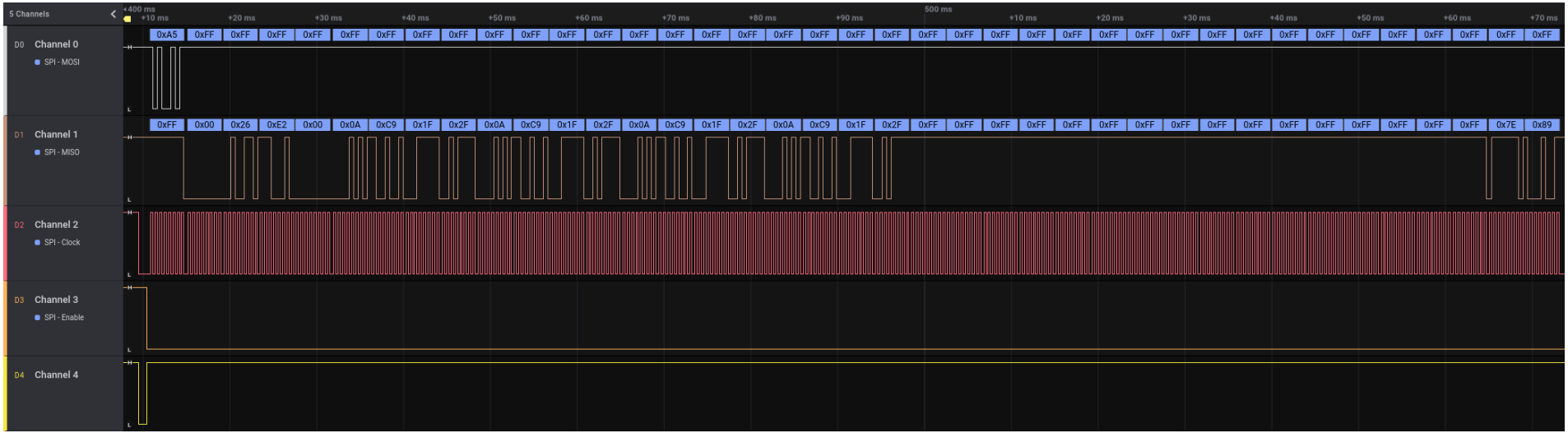
THE PENTEST EXPERTS.

- Bei der Analyse der Firmware konnte festgestellt werden, dass deren Validierung nur mit einer einfachen CRC-16-Prüfsumme erfolgt (XMODEM CRC-16)
- Ein Angreifer kann daher schädlichen Firmware-Code mit einer gültigen Prüfsumme für den INIC-3637EN auf dem SPI-Flash-Memory-Chip speichern



PROTOKOLLANALYSE

- Das Hardwaredesign erlaubt das Mitlesen der SPI-Kommunikation zwischen dem Keypad-Controller und dem USB-to-SATA-Bridge-Controller (INIC-36367EN) (Sniffing)
- Hierbei konnten interessante Muster erkannt werden



PROTOKOLLANALYSE

- Das Nachrichtenformat lautet wie folgt:

0x00	length	command ID	0x00	payload	checksum

- Lock-Message

  `0006E300F741`

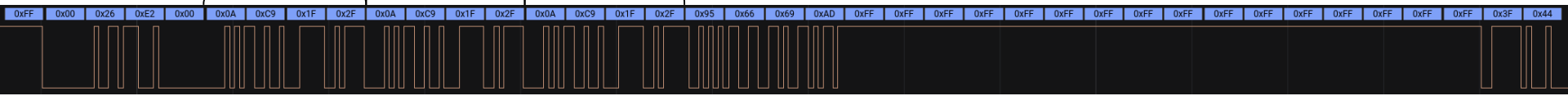
- Unlock-Message mit Passcode „111111111111“ (zwölfmalige Wiederholung von „1“)

  `0026E2000AC91F2F0AC91F2F0AC91F2956669ADFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF3F44`

PROTOKOLLANALYSE

- Die Prüfsumme ist CRC-16 (XMODEM-Konfiguration)
- Alle eingegebenen Passcodes resultieren in einer 32-byte-Payload
- Die letzten 16 Bytes der Payload sind immer „0xFF“
- Offensichtliche Muster können in den ersten 16 Bytes der Payload gefunden werden

„1111“ ergibt immer „0AC91F2F“



- Eine Art Mapping oder Hashing wird für die Benutzereingabe (Passcode) verwendet
- Unglücklicherweise ist der Keypad-Controller mit diesem Algorithmus eine Block Box

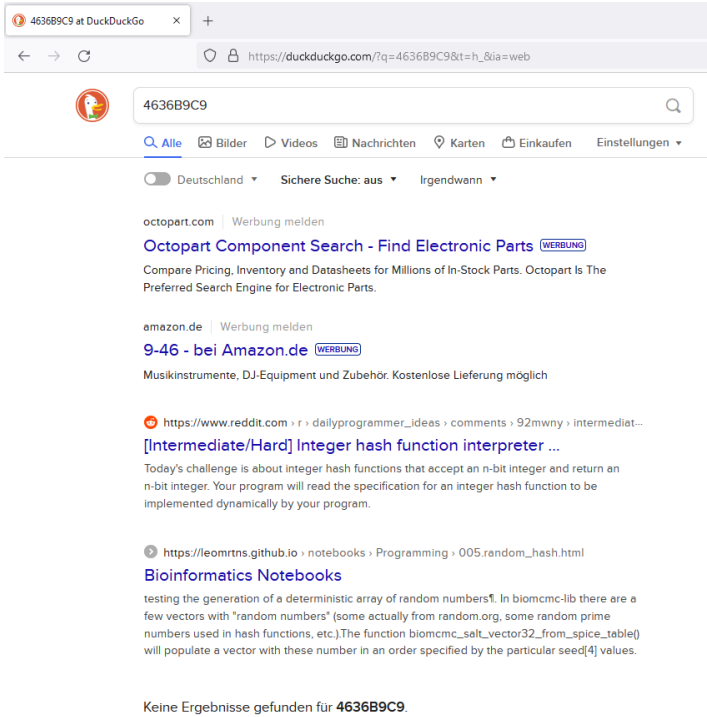
ANALYSE DER HASH-FUNKTION

4-stellige Eingabe	32-bit-Hash
0000	4636B9C9
1111	0AC91F2F
2222	5EC8BD1E
3333	624E6000
4444	B991063F
5555	0A05D514
6666	7E657A68
7777	B1C9C3BA
8888	7323CC76
9999	523DA5F5
1234	E097BCF8
5678	F540AEF4
No input	956669AD

- Es gibt zwei Möglichkeiten mit der Hash-Funktion umzugehen:
  1. Durch Sammeln aller möglichen Eingaben und Erstellung einer Tabelle mit deren Zuordnung
  2. Verständnis der Funktionsweise der Hash-Funktion
- Zu Beginn wurde Lösung 1 verfolgt
- Nach einer Vielzahl an technischen Problemen wurde dieser Ansatz jedoch schließlich abgebrochen

ANALYSE DER HASH-FUNKTION

- Aus Verzweiflung wurde daher nochmals im Internet nach Informationen über den unbekannten Hashing- oder Mapping-Algorithmus gesucht
- Dieses Mal konnte etwas zu dem Hash „4636B9C9“ für die 4-stellige Eingabe „0000“ gefunden werden
- Der Reddit-Eintrag namens „[Intermediate/Hard] Integer hash function interpreter“ in r/dailyprogrammer_ideas hatte die Lösung



ANALYSE DER HASH-FUNKTION

- Der unbekannte Hash-Algorithmus ist die Integer-Hash-Funktion namens „hash32shift2002“ aus diesem Artikel
- Diese Integer-Hash-Funktion wurde offenbar von Thomas Wang entwickelt und eine C-Implementierung lautet wie folgt:

```
uint32_t hash32shift2002(uint32_t hash)
{
    hash += ~(hash << 15);
    hash ^=  (hash >> 10);
    hash +=  (hash <<  3);
    hash ^=  (hash >>  6);
    hash += ~(hash << 11);
    hash ^=  (hash >> 16);
    return hash;
}
```

Sample Output

hash32shift2002():

```
00000000 4636b9c9
00000001 62baf5a0
1703640c d4ed55d9
80000000 a31bdce4
ffffffff dc8b039a
```

BENUTZERAUTHENTIFIZIERUNG

- Durch das Setzen verschiedener Passcodes und eine Analyse der entsprechenden Veränderungen des SSD-Inhalts konnte ein spezieller Sektor (Nr. 125042696) gefunden werden, in dem Authentifizierungsinformationen gespeichert werden
- Die Firmware-Analyse ergab, dass die ersten 112 Bytes (0x70) für das Entsperren des Geräts verwendet werden
- Falls die AES-Engine des INIC-3637EN korrekt konfiguriert ist (Modus und Schlüsselmaterial), müssen die ersten 4 Bytes des entschlüsselten speziellen Sektors die Signatur „INI “ (0x494e4920) ergeben

BENUTZERAUTHENTIFIZIERUNG

- Der AES-Schlüssel ist die 32-byte-Payload, die vom Keypad-Controller an den USB-to-SATA-Bridge-Controller (INIC-3637EN) gesandt wird
- AES-Engine des INIC-3637EN nutzt eine spezielle Byte-Reihenfolge für den AES-Schlüssel:

```
AES_key = reversed(passcode_key[0:16]) + reversed(passcode_key[16:32])
```

- Offline-Brute-Force-Angriff aus folgenden Gründen möglich:
  - Information für die Benutzerauthentifizierung wird in einem speziellen Sektor der SSD gespeichert
  - Die AES-Schlüssel-Ableitung ist aus der Benutzereingabe (Passcode) bekannt
- Weil nur 5- bis 12-stellige Passcodes unterstützt werden, ist der mögliche Suchraum relativ klein

Demo:
Passcode-Brute-Force-Angriff

BEISPIEL 2: VERBATIM EXECUTIVE FINGERPRINT SECURE

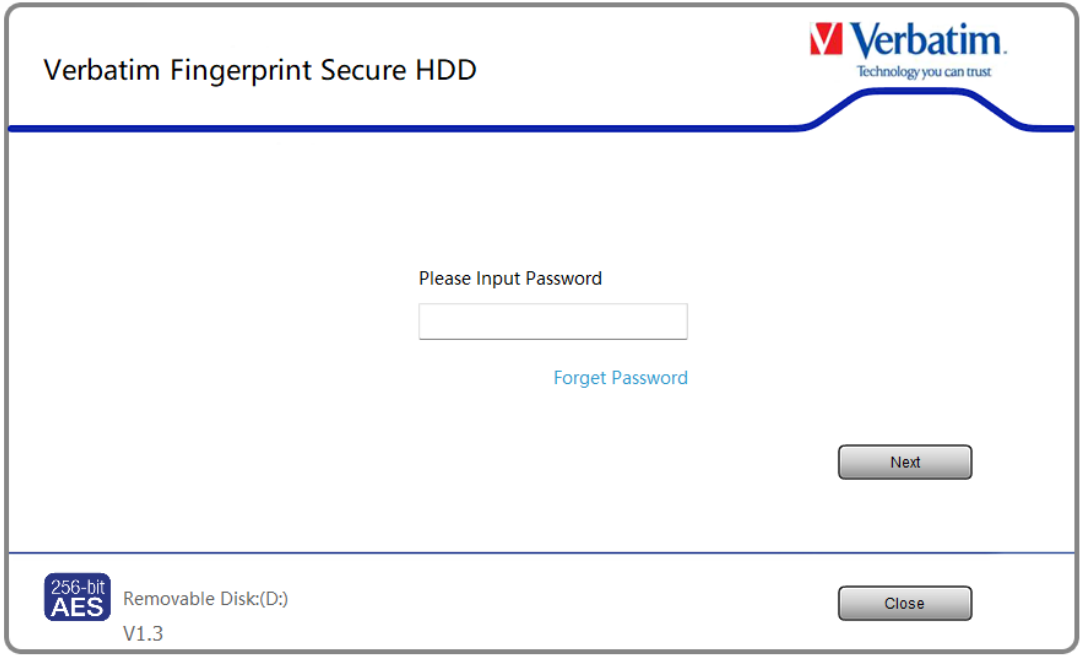
Wichtige Eigenschaften:

- Speichert Daten sicher geschützt auf einer SSD
- Zugriff durch autorisierten Benutzer via Fingerabdruck
- Premium-256-bit-AES-Hardwaresicherheitsverschlüsselung
- Bis zu acht autorisierte Benutzer und zusätzlich ein Administrator (mittels Passwort)

BENUTZERAUTHENTIFIZIERUNG

- Zwei Authentifizierungsverfahren werden unterstützt:
  - Biometrische Authentifizierung via Fingerabdruck
  - Passwortbasierte Authentifizierung
- Für die biometrische Authentifizierung wird ein Fingerabdrucksensor und ein spezifischer Mikrocontroller (INIC-3782N) verwendet
- Zum INIC-3782N konnten keine öffentlich verfügbaren Informationen gefunden werden
- Für die Registrierung von Fingerabdrücken wird eine Clientsoftware (für Windows oder macOS) genutzt
- Die Clientsoftware unterstützt auch eine passwortbasierte Authentifizierung, um administrative Funktionen zu nutzen und die sichere Partition zu entsperren

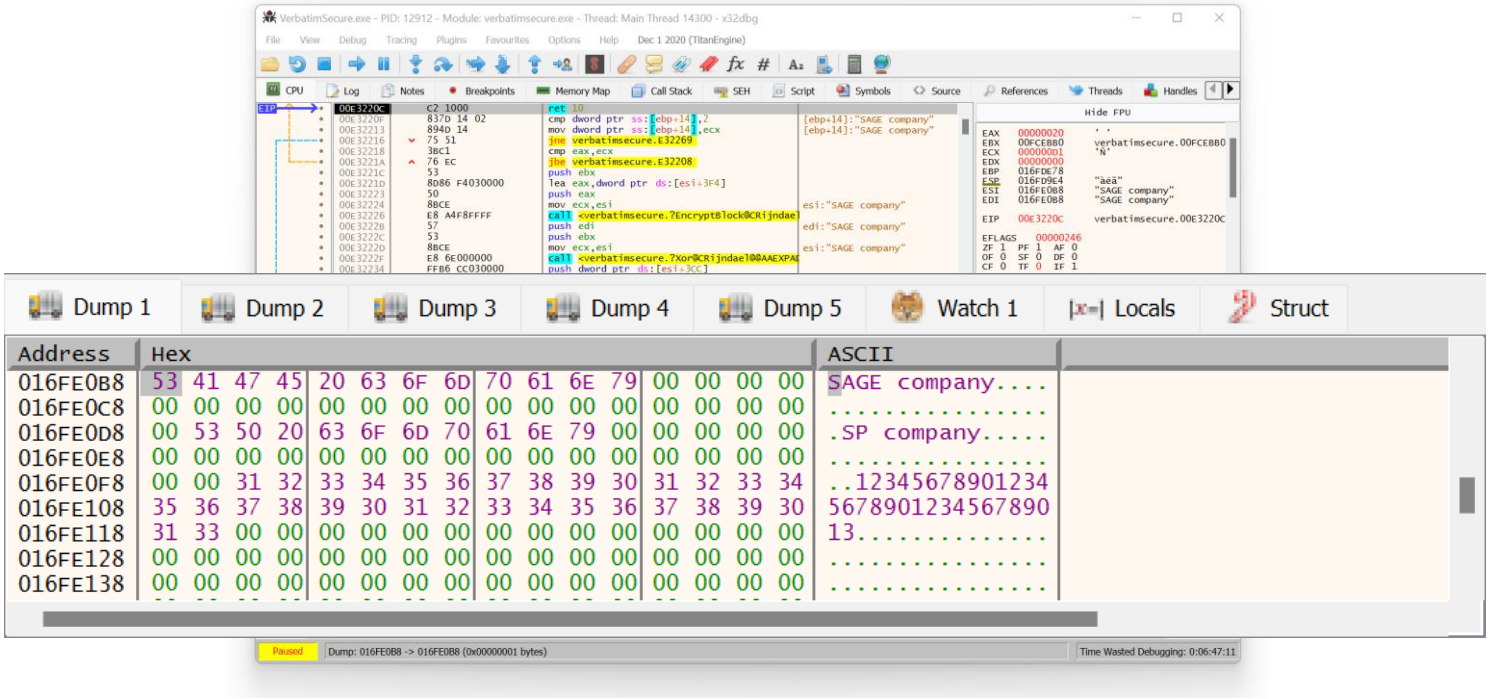
BENUTZERAUTHENTIFIZIERUNG



SOFTWAREANALYSE

- Die Clientsoftware wird auf einem emulierten CD-ROM-Laufwerk bereitgestellt
- Während dieses Forschungsprojekts wurde nur die Windows-Software (VerbatimSecure.exe) analysiert
- Die Windows-Clientsoftware kommuniziert via „IOCTL_SCSI_PASS_THROUGH“ (0x4D004)-Kommando unter Verwendung der Windows-API-Funktion „DeviceIoControl“ mit dem USB-Gerät
- Die USB-Kommunikation ist AES-verschlüsselt

SOFTWAREANALYSE: VERSCHLÜSSELTE USB-KOMMUNIKATION

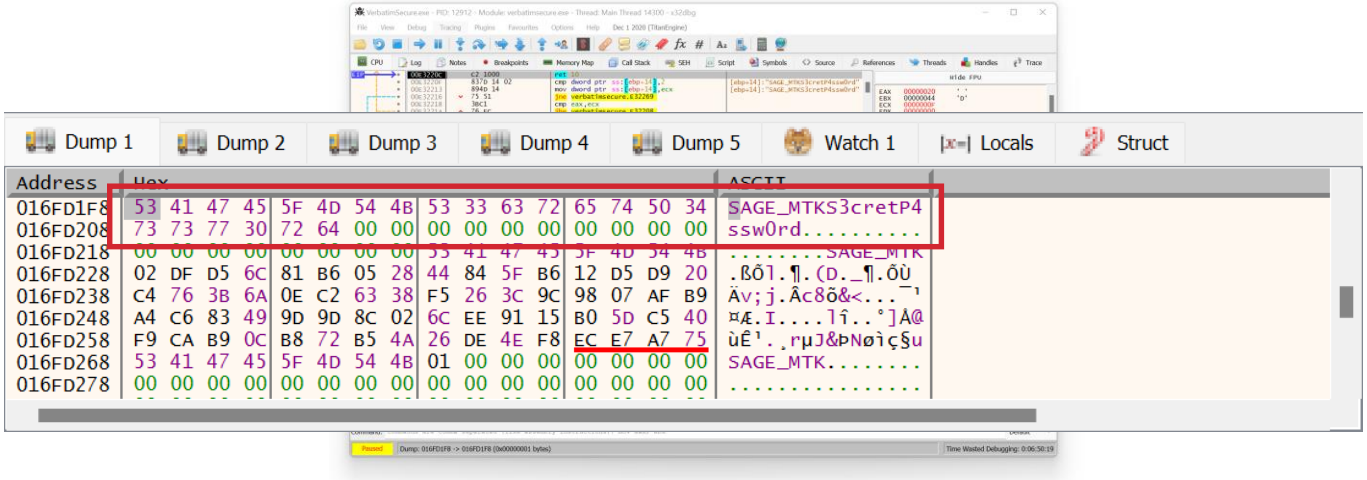


SOFTWAREANALYSE: ADMIN-PASSWORT

Problem #5

SySS THE PENTEST EXPERTS.

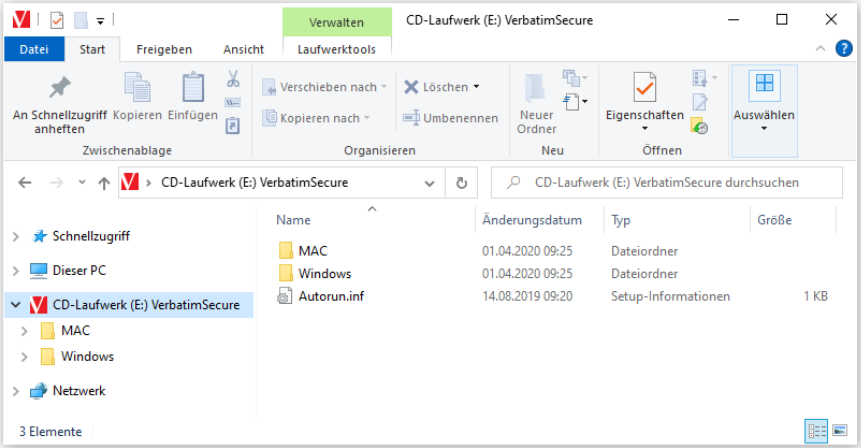
- Bei der Analyse der USB-Kommunikation zwischen der Clientsoftware und dem USB-Gerät konnte eine sehr interessante Beobachtung gemacht werden
- Bevor das Anmeldefenster mit der passwortbasierten Authentifizierung angezeigt wird, fand bereits eine Gerätekommunikation mit sensiblen Daten statt



Demo:
Pfusch oder Hintertür?

AUTHENTIZITÄT VON DATEN

- Die Clientsoftware für administrative Zwecke ist auf einer emulierten CD-ROM-Partition gespeichert
- Deren Inhalt wird als ISO-9660-Image in "versteckten" Sektoren des USB-Laufwerks gespeichert, auf die nur mit speziellen IOCTL-Kommandos oder durch Verwendung eines externen SSD-Gehäuses zugegriffen werden kann



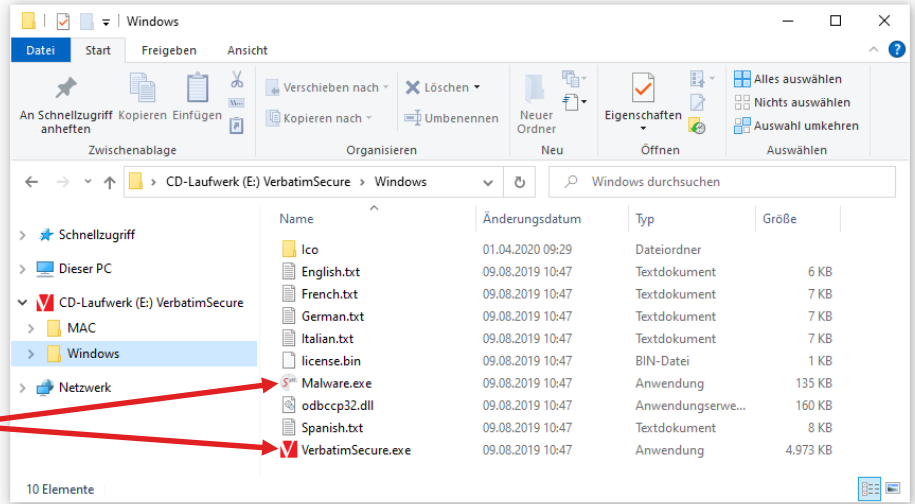
AUTHENTIZITÄT VON DATEN

Problem #6

THE PENTEST EXPERTS.

- Durch Manipulation oder Ersetzen dieses ISO-9660-Image kann ein Angreifer Schadsoftware auf dem emulierten CD-ROM-Laufwerk speichern

Dies könnte Schadsoftware sein



BEISPIEL #3: LEPIN EP-KP001

Wichtig Eigenschaften:

- „Strongest military technology digital encryption U-Disk“
- Schützt Daten und Privatsphäre mit Real-Time-256-bit-AES-XTS-Hardwareverschlüsselung
- 6- bis 14-stellige Passcodes
- Interessante „Passcode Recovery“-Funktion

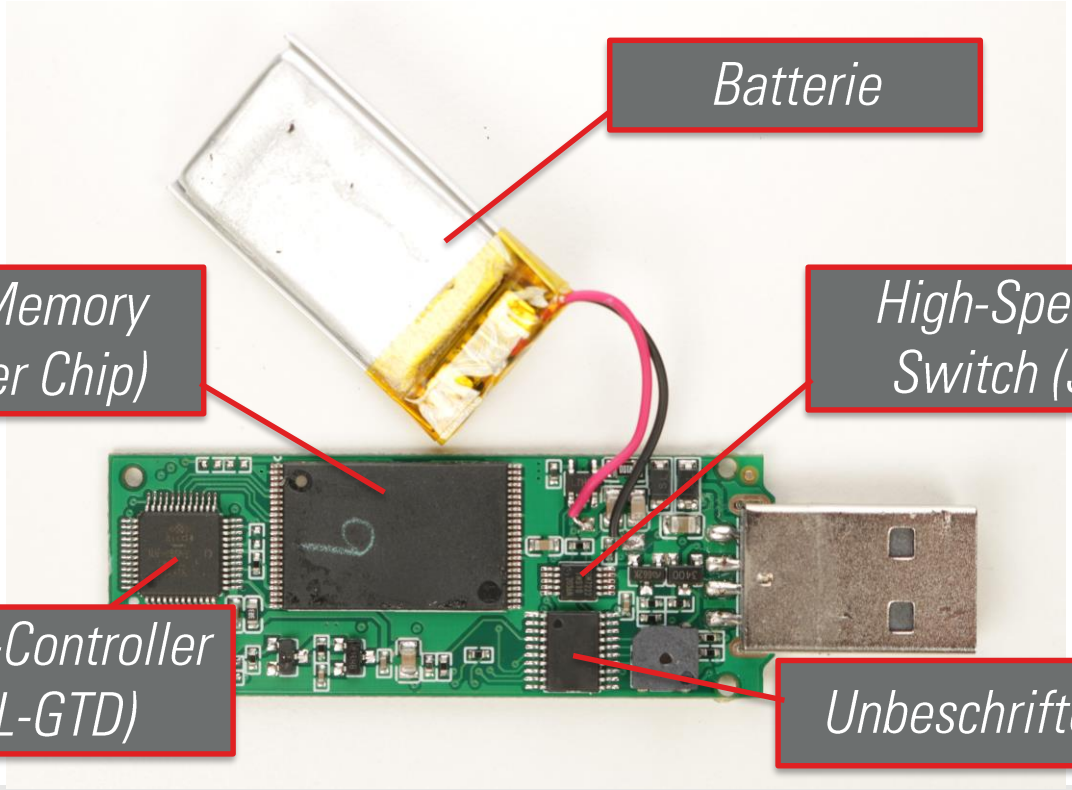
PASSWORTWIEDERHERSTELLUNG

(Quelle: Videodatei "Lepin Encrypted Flash Drive.mp4 " des Lepin-USB-Flash-Drive)

PASSWORTWIEDERHERSTELLUNG

- Bisher keine Antwort auf E-Mails an Lepin_support@163.com erhalten (seit 8. April 2022)
- Wie das erwähnte dynamische Passwort funktioniert, ist immer noch nicht bekannt und eine offene Frage für weitere Forschung

HARDWAREDESIGN

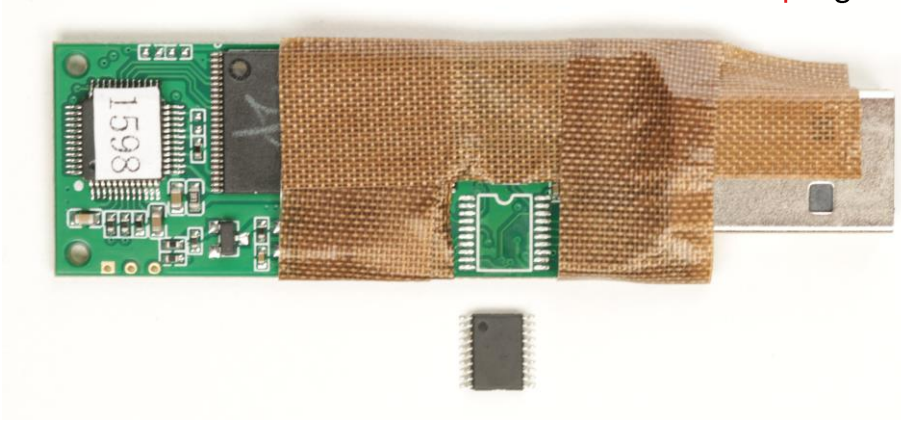


AUTHENTICATION BYPASS

Problem #7

SySS THE PENTEST EXPERTS.

- Einen High-Speed-Analogschalter zu finden, der mit den USB-Datenleitungen verbunden ist, war merkwürdig
- Mit einem Büroklammer-Hack (Paper-Clip-Hack) wurde versucht, diesen Schalter umzulegen oder zu umgehen, um zu sehen, ob sich das Verhalten des Geräts ändert → Kein Erfolg
- Anschließend wurde ein Austausch des nicht beschrifteten Chips getestet → Erfolg



GEFUNDENE SICHERHEITSSCHWACHSTELLEN

#	CVE ID	Vulnerability Type	Affected Products
1	CVE-2022-28382	Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240) (AES-ECB for data encryption)	• Verbatim Keypad Secure USB 3.2 Gen 1 Drive • Verbatim Store 'n' Go Secure Portable HDD • Verbatim Executive Fingerprint Secure SSD • Verbatim Fingerprint Secure Portable Hard Drive • Verbatim Store 'n' Go Secure Portable SSD
2	CVE-2022-28383	Missing Immutable Root of Trust in Hardware (CWE-1326) (Firmware manipulation)	• Verbatim Keypad Secure USB 3.2 Gen 1 Drive • Verbatim Store 'n' Go Secure Portable HDD • Verbatim Executive Fingerprint Secure SSD • Verbatim Fingerprint Secure Portable Hard Drive • Verbatim Store 'n' Go Secure Portable SSD
3	CVE-2022-28384	Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240) (Offline brute-force attack)	• Verbatim Keypad Secure USB 3.2 Gen 1 Drive • Verbatim Store 'n' Go Secure Portable HDD • Verbatim Store 'n' Go Secure Portable SSD
4	CVE-2022-28385	Insufficient Verification of Data Authenticity (CWE-345) (Data integrity check)	• Verbatim Executive Fingerprint Secure SSD • Verbatim Fingerprint Secure Portable Hard Drive
5	CVE-2022-28386	Expected Behavior Violation (CWE-440) (Lockout)	• Verbatim Keypad Secure USB 3.2 Gen 1 Drive • Verbatim Store 'n' Go Secure Portable HDD • Verbatim Store 'n' Go Secure Portable SSD
6	CVE-2022-28387	Use of a Cryptographic Primitive with a Risky Implementation (CWE-1240) (Password retrieval)	• Verbatim Executive Fingerprint Secure SSD • Verbatim Fingerprint Secure Portable Hard Drive
7	CVE-2022-29948	Violation of Secure Design Principles (CWE-657) (Authentication bypass attack)	• Lepin EP-KP001

RÜCKMELDUNG VON HERSTELLERN

- Bis heute keine direkte Rückmeldung an uns
- Verbatim hat im Juli 2022 Updates für verschiedene Produkte veröffentlicht
- Das Sicherheitsupdate enthält ein Windows-Updater-Tool mit neuer Firmware

**** SECURITY UPDATE ****

A software update to improve the security of this product is available now and should be implemented as soon as possible.
Please download the update from the support link at the bottom of the page and follow the instructions from the manual.

Viewing Documents For: Verbatim Keypad Secure USB 3.2 Gen 1 Drive 32GB

Firmware | Manuals | FAQs

File	Description	Format	File Size	Action
Verbatim Keypad Security Update 1.0.0.6 + Manual	July 2022 Verbatim Keypad Security Update + Manual - Download and update according to the attached manual to strengthen security functions	ZIP	8.42 MB	Download

FAZIT

- Neue portable Speichergeräte mit alten Sicherheitsschwachstellen werden trotz besseren Wissens immer noch hergestellt und verkauft
- Manche Sicherheitsschwachstellen in bereits verwendeten Hardwareprodukten sind schwierig oder gar unmöglich zu beheben:
  - Keine oder begrenzte Updatefunktionalität
  - Unsicheres Hardwaredesign
  - etc.
- Forever-Day-Bugs können die Sicherheit eines Produkts bis an dessen Lebensende betreffen

FRAGEN UND DISKUSSION

E-Mail: gerhard.klostermeier@syss.de
Twitter: @iiiikarus

E-Mail: matthias.deeg@syss.de
Twitter: @matthiasdeeg

YouTube: https://www.youtube.com/c/SySSPentestTV
Blog: https://blog.syss.com

THE PENTEST EXPERTS

WWW.SYSS.DE