Programmierte Unsicherheit – SySS knackt einen weiteren USB-Stick

Der SySS GmbH ist es gelungen, den Hardware-verschlüsselten USB-Stick* ThumbDrive CRYPTO *des Herstellers* Trek Technology *zu knacken.

Dipl.-Inform. Matthias Deeg
Christian Eichelmann
Dipl.-Inform. Sebastian Schreiber

11. Februar 2011

1 Einleitung

Ende 2009 fand die SySS GmbH eine kritische Sicherheitsschwäche in verschiedenen USB-Flash-Laufwerken mit Hardware-basierter AES-Verschlüsselung. Durch das Ausnutzen dieser Schwachstelle war es möglich, mit nur wenigen Mausklicks nicht autorisierten Zugriff auf sämtliche geschützten Daten zu erlangen (siehe [1], [2] und [3]).

Eine kürzlich durchgeführte Sicherheitsanalyse eines weiteren USB-Flash-Laufwerks mit implementierter Hardwareverschlüsselung zeigte, dass solche kritischen Schwachstellen keinesfalls der Vergangenheit angehören.

2 Sicherheitsanalyse

Im Folgenden wird am Beispiel eines USB-Flash-Laufwerkes des namhaften Herstellers Trek Technology gezeigt, dass ein IT-Produkt, welches durch sein Marketing Sicherheit verspricht, durch eine fehlerhafte Programmierung in Wahrheit sehr unsicher sein kann.

Konkret wurde das Produkt

- ThumbDrive CRYPTO [4]

auf Sicherheitsschwächen hin analysiert.

Nach Informationen von Trek Technology handelt es sich bei der von der SySS GmbH getesteten Produktversion um eine speziell für einen Kunden angepasste Version des USB-Flash-Laufwerks ThumbDrive CRYPTO (Zitat: *"customized version of ThumbDrive CRYPTO USB flash drive"*). Dieser Sachverhalt konnte jedoch nicht durch die SySS GmbH überprüft werden, da zum Zeitpunkt dieser Aussage bereits eine Produktversion des USB-Flash-Laufwerks existierte, in der die hier aufgezeigte Schwachstelle nicht mehr vorhanden war.

In den Produktinformationen zu diesem USB-Flash-Laufwerk finden sich unter anderem die folgenden Angaben:

> *ThumbDrive® CRYPTO ensures that 100% of the storage area is encrypted. With this 256-bit hardware AES engine, the ThumbDrive® CRYPTO offers one of the most advanced security solutions available today.*

Um den Massenspeicher des USB-Sticks zu entsperren und um Zugriff auf die geschützten Daten zu erlangen, muss das korrekte Passwort für das Benutzerkonto `Administrator` im Anmeldefenster eingegeben werden, das in Abbildung 1 dargestellt wird.

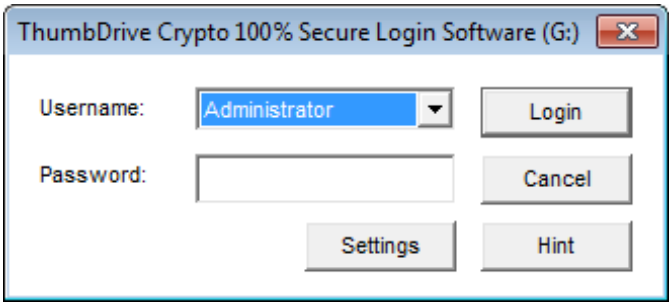

Abbildung 1: Passwort-basierte Authentifizierung

Das Passwort kann mit Hilfe der *Administrative Tools* des Programms `SecureLogin.exe` gesetzt werden, das sich auf einer emulierten CDROM-Partition des USB-Flash-Laufwerks befindet. Abbildung 2 zeigt das Dialogfenster der *Administrative Tools* zum Setzen eines neuen Passworts und eines entsprechenden Passworthinweises.

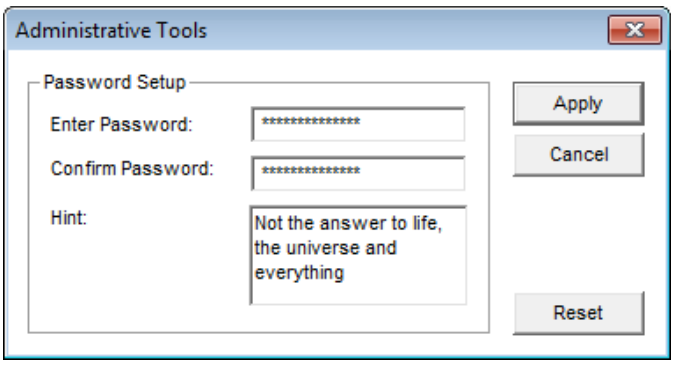

Abbildung 2: Setzen eines Passworts

Das verwendete Passwort muss dabei die Kriterien einer fest einprogrammierten Passwortrichtlinie erfüllen, wobei die maximale Länge des Passworts auf 14 Zeichen beschränkt ist. Abbildung 3 zeigt eine Fehlermeldung bezüglich der Verwendung eines schwachen Passworts.

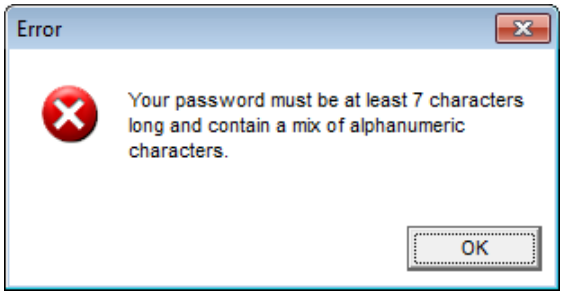

Abbildung 3: Fehlermeldung zur Passwortrichtlinie

Im Rahmen der durchgeführten Sicherheitsanalyse konnte die SySS GmbH eine kritische Schwachstelle innerhalb der Passwort-basierten Benutzerauthentifizierung des USB-Flash-Laufwerks TREK ThumbDrive CRYPTO finden.

Die SySS GmbH stellte fest, dass das Programm `SecureLogin.exe` das vom Benutzer eingegebene Passwort mit Hilfe des in Abbildung 4 dargestellten Algorithmus verschlüsselt.

```
.text:0042123A                jle     short copy_password
.text:0042123C                mov     al, [ebp+897Dh]             ; load encryption key (1 byte)
.text:00421242
.text:00421242 encrypt_password:                                  ; CODE XREF: sub_421170+E1↓j
.text:00421242                mov     cl, [esp+esi+120h+var_104]  ; load cleartext char
.text:00421246                add     cl, al                      ; add key value to char
.text:00421248                inc     esi                         ; point to next char
.text:00421249                not     cl                          ; generate bitwise complement (binary not)
.text:0042124B                mov     [esp+esi+120h+var_105], cl  ; store encrypted char
.text:0042124F                cmp     esi, ebx                    ; check if encryption is comleted
.text:00421251                jl      short encrypt_password      ; if not, encrypt next char
.text:00421253                jmp     short copy_password         ; else jump to copy routine
```

Abbildung 4: Kommentierter Programmcode zur Passwortverschlüsselung dargestellt im Disassembler IDA Pro

Das Ergebnis dieser Verschlüsselungsroutine wird im Anschluss daran mit einem bestimmten Wert verglichen, nämlich dem korrekten Passwort in verschlüsselter Form, wie sich später herausstellte. Abbildung 5 zeigt diesen Passwortvergleich von 15 Bytes Länge (0Fh) an der Speicheradresse `0x40AAB8` zur Laufzeit des Programms `SecureLogin.exe` im Debugger OllyDbg[1].

[1] `http://www.ollydbg.de/`

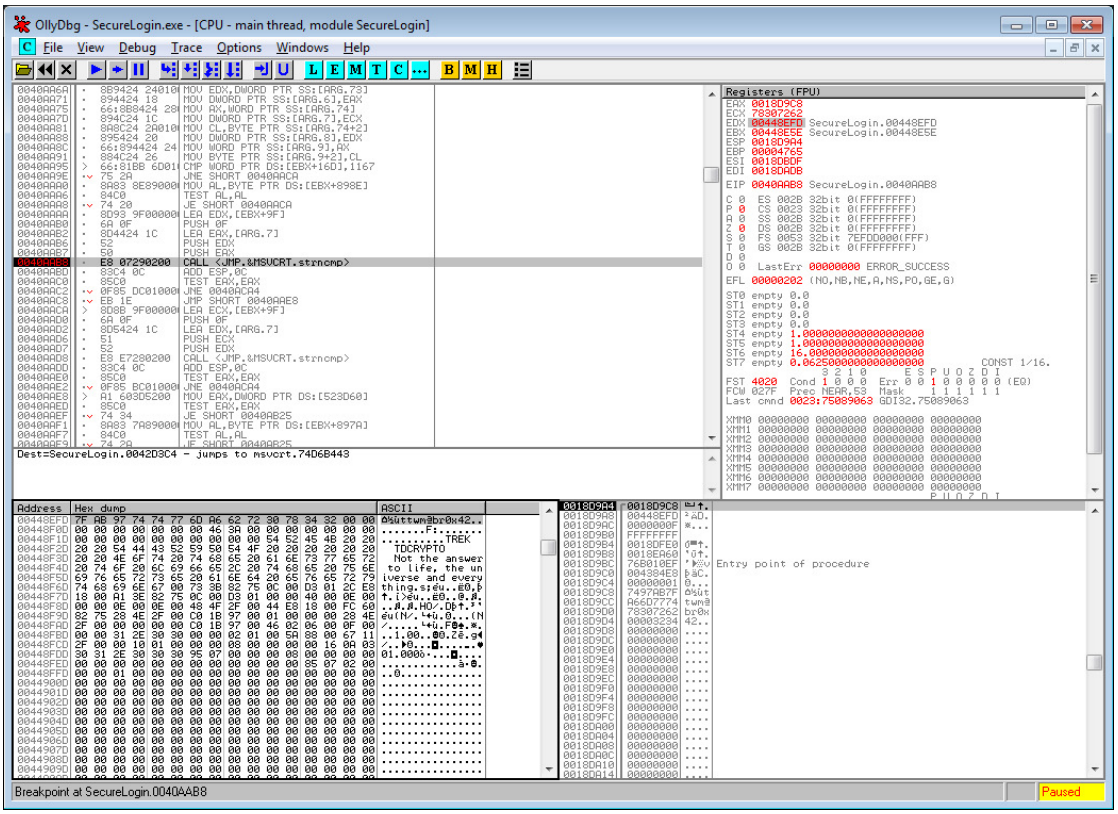

Abbildung 5: Passwortvergleich dargestellt in OllyDbg

Der mit Kommentaren versehene Programmcode des Passwortvergleichs wird in Abbildung 6 illustriert.

```
.text:0040AAAA    lea     edx, [ebx+9Fh]              ; load address of correct encrypted password
.text:0040AAB0    push    0Fh                         ; MaxCount
.text:0040AAB2    lea     eax, [esp+62Ch+user_input]  ; load address of user input
.text:0040AAB6    push    edx                         ; correct encrypted password
.text:0040AAB7    push    eax                         ; encrypted user input
.text:0040AAB8    call    strncmp                     ; compare strings
.text:0040AABD    add     esp, 0Ch
.text:0040AAC0    test    eax, eax
.text:0040AAC2    jnz     loc_40ACA4                  ; bad guy jump
.text:0040AAC8    jmp     short loc_40AAE8            ; good guy jump
```

Abbildung 6: Kommentierte Routine für den Passwortvergleich dargestellt im Disassembler IDA Pro

Weitere Analysen zeigten, dass die Konfiguration des USB-Sticks inklusive des administrativen Passworts in einem speziellen Speicherbereich des USB-Flash-Laufwerks gespeichert wird. Beim Start des Programms `SecureLogin.exe` wird diese Konfiguration mit Hilfe eines USB-Controller-spezifischen Kommandos aus diesem Speicher gelesen. Bei jeder Leseoperation werden dabei 8K große Datenblöcke (8192 Bytes) vom USB-Flash-Laufwerk auf den Host-PC kopiert.

Die beiden Abbildungen 7 und 8 zeigen die ersten Bytes der zwei identifizierten Konfigurationsblöcke, in denen sich das administrative Passwort befindet.

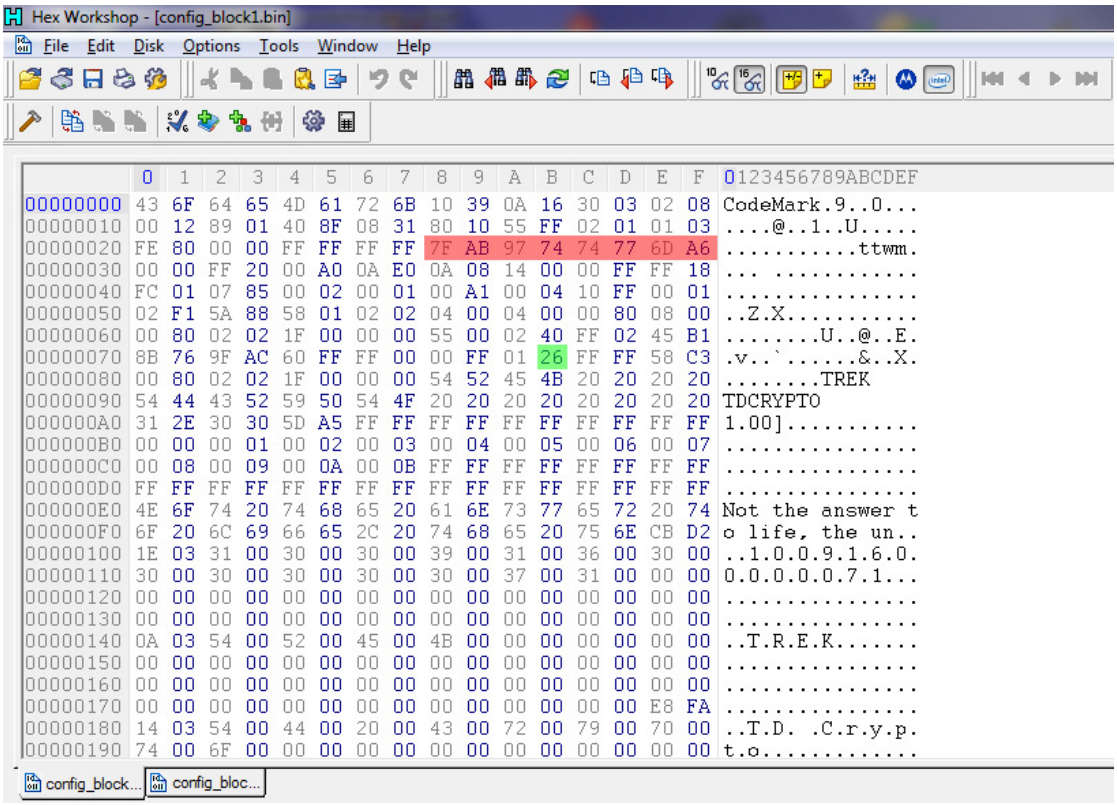

Abbildung 7: Beginn des ersten Konfigurationsblocks (8192 Bytes)

Das administrative Passwort wird dabei in verschlüsselter Form (rot markiert) zusammen mit dem verwendeten Schlüssel (grün markiert) gespeichert. Um genau zu sein, werden lediglich die ersten acht Zeichen des Passworts verschlüsselt (Byte-Folge `7FAB977474776DA6`), die übrigen sechs Zeichen liegen im Klartext vor (Byte-Folge `627230783432`, die der ASCII-Zeichenkette "`br0x42`" entspricht).

Wie Abbildung 4 zeigt, ist der verwendete Verschlüsselungsalgorithmus sehr einfach und im Gegensatz zu kryptografisch sicheren Hash-Algorithmen vollständig umkehrbar – also eine klassische symmetrische Verschlüsselung. Die ersten acht Zeichen werden verschlüsselt, indem der Wert des 1 Byte langen Schlüssels (`26h`) addiert und anschließend eine Bit-weise `not`-Operation durchgeführt wird.

Man erkennt sehr leicht, dass der verschlüsselte Teil des Passworts Zeichen für Zeichen durch eine Bit-weise `not`-Operation gefolgt von einer Subtraktion des Wertes des Schlüssels wieder in Klartext umgewandelt werden kann, wie der Programmauszug 1 zeigt.

Listing 1: Algorithmus zur Passwortentschlüsselung

```
// Passwort entschlüsseln
for (i = 0; i < 8; i++) {
    plaintext[i] = ~ciphertext[i] - key;
}
```

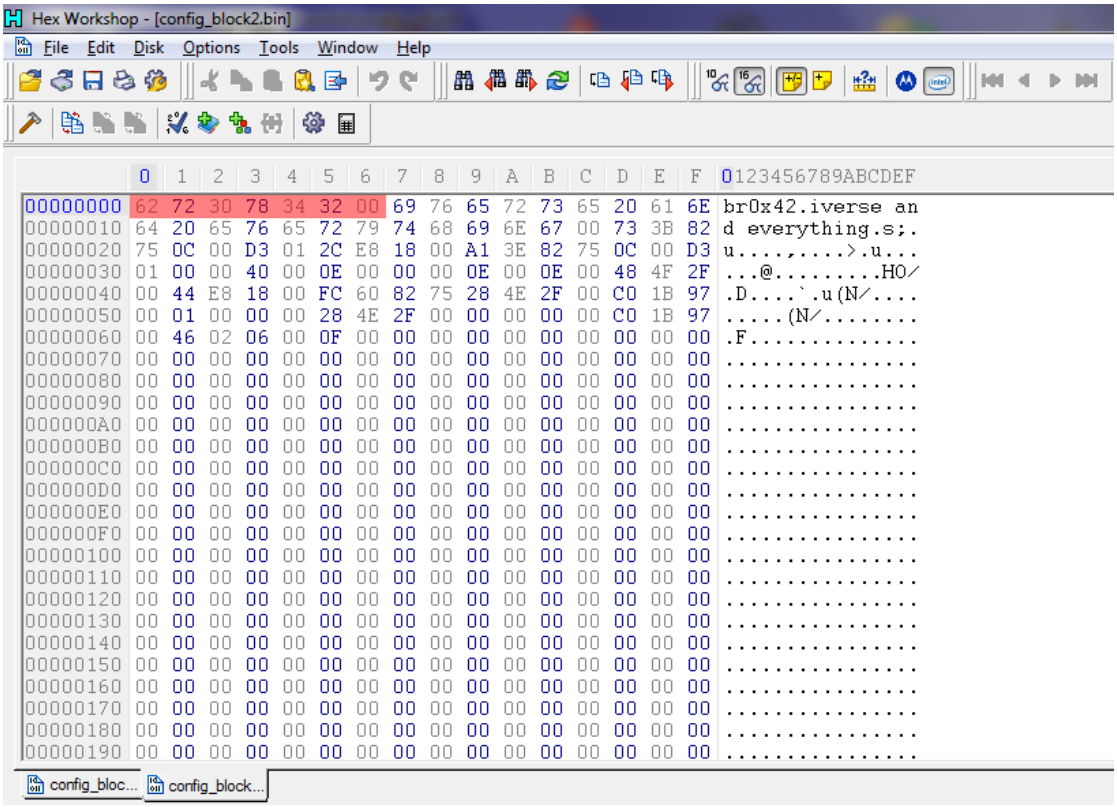

Abbildung 8: Beginn des zweiten Konfigurationsblocks (8192 Bytes)

Der Schlüssel zur Verschlüsselung des Passworts ist eine Zufallszahl zwischen 1 und 254. Ein neuer Schlüssel wird erzeugt, wenn ein neues Passwort für das USB-Flash-Laufwerk TREK ThumbDrive CRYPTO gesetzt wird. Der vollständige Algorithmus für die Erzeugung des Schlüssels wird in Abbildung 9 dargestellt.

```
.text:00421201                push    0                       ; Time
.text:00421203                call    time                    ; get the current time
.text:00421208                push    eax                     ; Seed
.text:00421209                call    srand                   ; initialize PRNG
.text:0042120E                lea     eax, [esp+128h+var_110] ; load address of _ftime structure
.text:00421212                push    eax
.text:00421213                call    _ftime                  ; get the current time
.text:00421218                add     esp, 0Ch
.text:0042121B                xor     al, al                  ; set al to 0
.text:0042121D
.text:0042121D loc_42121D:                                    ; CODE XREF: sub_421170+BE↓j
.text:0042121D                test    al, al                  ; check if al is 0
.text:0042121F                jz      short loc_421225        ; jump, if it is
.text:00421221                cmp     al, 0FFh                ; check if al is 255 (0xff)
.text:00421223                jnz     short loc_421230        ; jump, if it's not
.text:00421225
.text:00421225 loc_421225:                                    ; CODE XREF: sub_421170+AF↑j
.text:00421225                call    rand                    ; call PRNG
.text:0042122A                add     al, [esp+120h+var_10C]  ; add value of _ftime structure to random number
.text:0042122E                jmp     short loc_42121D
.text:00421230 ; ---------------------------------------------------------------------------
.text:00421230
.text:00421230 loc_421230:                                    ; CODE XREF: sub_421170+B3↑j
.text:00421230                mov     [ebp+897Dh], al         ; store random number (= encryption key)
```

Abbildung 9: Kommentierte Routine zur Erzeugung des Schlüssels in IDA Pro

Mit den gewonnenen Erkenntnissen entwickelte die SySS GmbH zu Demonstrationszwecken ein *Proof-of-Concept*-Software-Tool namens ThumbDrive CRYPTO Unlocker, das sowohl das verwendete administrative Passwort ausgibt als auch automatisch den geschützten Massenspeicher eines TREK ThumbDrive CRYPTO USB-Flash-Laufwerks mit einem einzigen Mausklick entsperrt. Dieses *Proof-of-Concept*-Software-Tool zeigt Abbildung 10.

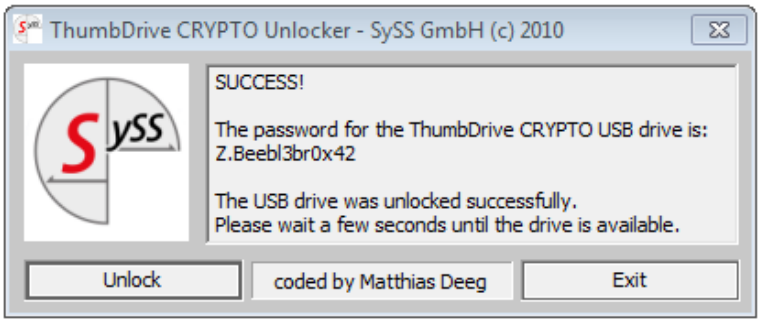

Abbildung 10: *Proof-of-Concept*-Software-Tool ThumbDrive CRYPTO Unlocker

3 Fazit

Die SySS GmbH konnte anhand des getesteten USB-Flash-Laufwerks ThumbDrive CRYPTO erneut demonstrieren, dass ein Softwarefehler in der Passwort-basierten Authentifizierung den Zugriff auf sämtliche gespeicherten Daten mit nur wenigen Mausklicks problemlos ermöglicht. Falls ein entsprechendes Werkzeug im Internet verfügbar wäre, so würden selbst technisch nicht versierte Angreifer ein Sicherheitsrisiko darstellen, sofern sie in Besitz eines solchen Werkzeugs gelangen könnten.

Beim Ausnutzen der gezeigten Softwareschwachstelle erweisen sich implementierte Sicherheitsmechanismen wie die Hardware-basierte 256-Bit AES-Verschlüsselung und die einprogrammierte Passwortrichtlinie als ineffektiv, da sie den gezeigten Angriff nicht verhindern.

Dieses Testergebnis zeigt, dass Hersteller vor allem bei der Entwicklung komplexer IT-Sicherheitsprodukte allergrößte Sorgfalt auf einen hohen Sicherheitsstandard verwenden müssen, um zu vermeiden, dass diese kritische Schwachstellen aufweisen, die ihre hohen Sicherheitsanforderungen ad absurdum führen.

Der Hersteller Trek Technology des USB-Flash-Laufwerks ThumbDrive CRYPTO wurde von der SySS GmbH über die gefundene Schwachstelle in Kenntnis gesetzt. Trek Technology hat schnell reagiert und die aufgezeigte Sicherheitsschwäche in einer aktualisierten Version des ThumbDrive CRYPTO behoben.

Wie bereits zuvor erwähnt, handelt es sich nach Informationen von Trek Technology bei der von der SySS GmbH getesteten Produktversion um eine speziell für einen Kunden angepasste Version des USB-Flash-Laufwerks ThumbDrive CRYPTO (Zitat: *"customized version of ThumbDrive CRYPTO USB flash drive"*). Dieser Sachverhalt konnte jedoch nicht durch die SySS GmbH überprüft werden, da zum Zeitpunkt dieser Aussage bereits eine Produktversion des USB-Flash-Laufwerks existierte, in der die hier aufgezeigte Schwachstelle nicht mehr vorhanden war.

Literatur

[1] Jürgen Schmidt, *NIST-zertifizierte USB-Sticks mit Hardware-Verschlüsselung geknackt*, `http://www.heise.de/security/meldung/NIST-zertifizierte-USB-Sticks-mit-Hardware-Verschluesselung-geknackt-894962.html` 2

[2] Matthias Deeg, Sebastian Schreiber, *SySS knackt* SanDisk *USB-Stick* `http://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_knackt_SanDisk_USB-Stick.pdf` 2

[3] Matthias Deeg, Sebastian Schreiber, *SySS knackt* Kingston *USB-Stick* `http://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_knackt_Kingston_USB-Stick.pdf` 2

[4] Herstellerinformationen zum TREK ThumbDrive CRYPTO, `http://thumbdrive.com/cart/product.php?id_product=29` 2