# Kryptografisch sicher?
# SySS knackt USB-Stick

***Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von* SanDisk *zu knacken, welcher über eine FIPS-Zertifizierung verfügt.***


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

18. Dezember 2009

# 1 Einleitung

Portable Massenspeicher in Form von USB-Sticks erfreuen sich seit vielen Jahren großer Beliebtheit. Mit der Zeit vergrößerte sich bei diesen im Alltag äußerst praktischen Datenträgern nicht nur deren Speicherkapazität, sondern es gab auch eine wachsende Nachfrage nach dem Schutz der gespeicherten Daten. Denn im Falle eines Diebstahls oder allgemein des Verlustes eines portablen USB-Flash-Laufwerks ist es für den Besitzer wünschenswert, dass seine vertraulichen Daten auch dann noch vertraulich bleiben. Vor allem für Militär- und Regierungsstellen, aber auch in der freien Wirtschaft, etwa im Gesundheits- und Finanzwesen, besteht erhöhter Schutzbedarf, weil oft sehr sensible Daten auf USB-Flash-Laufwerken gespeichert werden, auf die Unbefugte keinen Zugriff haben sollten.

Neben zahlreichen kommerziellen wie auch freien Softwarelösungen zur Verschlüsselung sensibler Daten für portable Massenspeicher bieten verschiedene Hersteller mittlerweile auch USB-Sticks mit integrierter Hardwareverschlüsselung und weiteren Schutzmechanismen an, die im Marketing-Jargon vollmundig angepriesen werden. Darüber hinaus verfügen einige dieser Produkte über anerkannte Sicherheitszertifikate, die ihnen ein definiertes Schutzniveau bescheinigen.

Doch wie uns die Geschichte der IT-Sicherheit lehrt, ist Kryptografie ein kompliziertes Feld, bei dem kleine Fehler oft große Auswirkungen haben.

# 2 Sicherheitsanalyse

Im Folgenden wird am Beispiel eines USB-Flash-Laufwerks des namhaften Herstellers SanDisk gezeigt, dass FIPS 140-2 zertifizierte Produkte *knackbar* sind.

Konkret wurde das Produkt

- SanDisk Cruzer Enterprise - FIPS Edition [1]

auf Sicherheitsschwächen hin analysiert.

Detaillierte Informationen bezüglich der verwendeten Firmware werden in Abbildung 1 dargestellt.

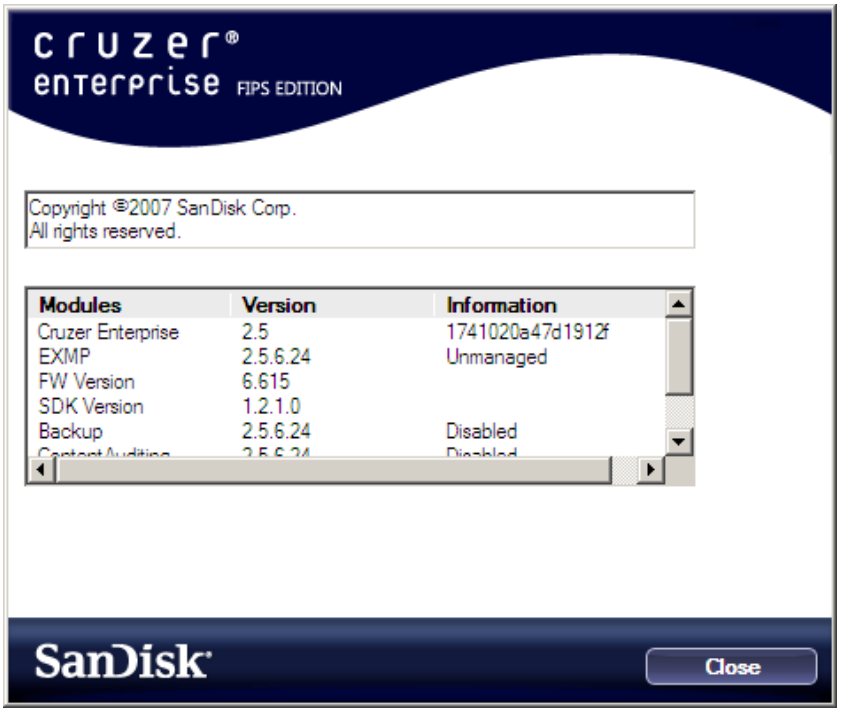


Abbildung 1: Firmwareversion des getesteten USB-Flash-Laufwerks

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

- FIPS 140-2 Level 2 zertifiziert
- Hardwarebasierte 256-Bit AES-Verschlüsselung
- Obligatorische Sicherheitsmaßnahmen für alle Dateien (100 % private Partition)
- Erzwingung von starken Kennwörtern
- Sperrmodus bei Eingabe einer festgelegten Anzahl falscher Kennwörter

Vor allem der letzte Punkt dieser Aufzählung ist von Interesse, da sich bekanntlich die Sicherheit von technischen Systemen mit passwortbasierten Authentifizierungsverfahren generell auf die Sicherheit der gewählten Passwörter reduzieren lässt.

Kurz gesagt: Werden schwache Passwörter verwendet, sind weitere Sicherheitsmechanismen, wie beispielsweise eine 256-Bit-AES-Hardware-Verschlüsselung, von geringer Bedeutung. Die geschützten Daten sind nur so sicher wie das gewählte Passwort, nicht wie das gewählte kryptografische Verfahren zur Verschlüsselung der Daten.

Wie Abbildung 2 beispielhaft zeigt, werden die Daten auf dem USB-Flash-Laufwerk durch ein vom Benutzer gewähltes Passwort geschützt, das auf dem untersuchten Produkt gewissen Passwortrichtlinien entsprechen muss.


Abbildung 2: Passwortbasierte Authentifizierung

Um die Verwendung schwacher Passwörter ausnutzen zu können, muss natürlich die Voraussetzung erfüllt sein, dass sich überhaupt eine größere Anzahl an vermeintlich schwachen Passwörtern überprüfen lässt. Im Falle der getesteten USB-Sticks bedeutet dies Folgendes: Falls die Möglichkeit besteht, den implementierten Passwortabgleich vollständig mit allen verwendeten Parametern in Erfahrung zu bringen, so können beliebig viele Passwörter mit Hilfe einer sogenannten *Offline*-Attacke überprüft werden.

Die Durchführung von Passwort-Rate-Attacken, sei es mit Wörterbüchern (*Dictionary Attack*), mit einfachem sequentiellen Durchprobieren (*Brute Force Attack*) oder mit einer Kombination aus beidem, erweist sich in der Praxis als probates Mittel, um an passwortgeschützte Daten zu gelangen. Wie in einem heise-Artikel vom vergangenen Jahr nachzulesen ist, wurde diese Methode bereits erfolgreich gegen ein FIPS 140-2 Level 2 zertifiziertes USB-Flash-Laufwerk des Herstellers MXI Security eingesetzt, der über entsprechende Schwachstellen verfügte [2].

Bei der Untersuchung des USB-Sticks von SanDisk lag der Fokus daher ebenfalls auf der Analyse des passwortbasierten Authentifizierungsverfahrens. Denn sollten sich darin

ähnliche Schwachstellen finden wie bei bei dem zuvor erwähnten USB-Stick von MXI Security, so können mit Hilfe entsprechender Passwort-Rate-Programme, welche auch *Password Cracker* genannt werden, gültige Zugangsdaten für die Entschlüsselung der geschützten Daten wiederhergestellt werden. Abhängig von den verwendeten kryptografischen Algorithmen, sei es für die Erzeugung von Hash-Werten oder für die Ver- beziehungsweise Entschlüsselung von Daten, können dabei auf moderner Hardware in Form von CPUs und GPUs viele Tausende bis Milliarden von Passwortkandidaten pro Sekunde überprüft werden [3].

Passwort-Rate-Attacken sind somit definitiv ein Sicherheitsproblem, werden jedoch von den meisten Anbietern von USB-Sticks mit entsprechender Funktionalität nicht als solches angesehen. Denn bei der Wahl komplexer Passwörter müssen Angreifer aktuell in der Regel über sehr viel Rechenleistung verfügen, um noch zu deren Lebzeiten und nicht erst in Tausenden oder gar Millionen von Jahren an die verschlüsselten Daten zu gelangen.

Wie sich im Rahmen der durchgeführten Sicherheitsanalyse herausstellte, schützen selbst lange und komplexe Passwörter im Fall des getesteten FIPS 140-2 Level 2 zertifizierten USB-Flash-Laufwerks die Daten nicht.

Die Ursache hierfür liegt in der Art und Weise, wie bei diesem USB-Stick die vom Benutzer eingegebenen Passwörter auf Korrektheit überprüft werden. Das erste Sicherheitsproblem dabei ist, dass die Überprüfung nicht in Hardware, also durch den USB-Stick selbst, sondern in Software auf dem PC des Benutzers durchgeführt wird. Dieser Umstand ermöglicht eine detaillierte Analyse des Authentifizierungsverfahrens mit Hilfe eines Debuggers, wie beispielsweise OllyDbg[1]. Die Funktionsweise des Prozesses, welcher für die Verifizierung des eingegebenen Passworts zuständig ist, kann damit vollständig analysiert werden. Das zweite und größte Sicherheitsproblem ist jedoch, dass sichere kryptografische Verfahren, wie in diesem Fall AES, unsicher verwendet werden.

Diese beiden beschriebenen Sicherheitsschwächen befinden sich innerhalb der ausführbaren Datei `ExmpSrv.exe`, die Teil eines Softwareproduktes ist, das auf dem getesteten SanDisk-USB-Flash-Laufwerk eingesetzt wird.

Die Untersuchungen der SySS GmbH zeigten, dass der verwendete Algorithmus zur Überprüfung des Passworts wie folgt arbeitet:

1. Passwort wird von `ASCII` nach `WideChar` konvertiert
2. MD5-Hashwert des `WideChar`-Passworts wird berechnet
3. `ASCII-HEX`-Repräsentation des MD5-Hashwerts wird erzeugt und ebenfalls nach `WideChar` konvertiert; die erste Hälfte des Ergebnisses dient im nächsten Schritt als Schlüssel
4. Mit dem erzeugten Schlüssel wird ein 32 Byte großer Datenblock via AES-256-ECB entschlüsselt, der zuvor vom USB-Stick gelesen wurde

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

5. Entspricht das Ergebnis der Entschlüsselung einem bestimmten Wert, so war das eingegebene Passwort korrekt und es kann auf die geschützten Daten des USB-Massenspeichers zugegriffen werden

Im Verlauf der Sicherheitsanalyse stellte sich heraus, dass das Resultat der Entschlüsselung in Schritt 5 bei der Eingabe des korrekten Passworts immer dasselbe war. Dies änderte sich auch dann nicht, wenn ein neues Passwort gesetzt oder das USB-Flash-Laufwerk formatiert wurde. Der Grund hierfür ist, dass beim Setzen eines neuen Passworts immer derselbe 32 Byte große Datenblock via AES-256-ECB verschlüsselt wird, der dann wiederum bei der Überprüfung des Passworts das Ergebnis der Entschlüsselung sein muss.

Konkret handelt es sich bei dieser Konstanten um den folgenden Wert:

```
Hex dump                                          ASCII
00 00 00 00|B5 D3 68 DC|8A 4D A5 B1|FD 2E 68 84| ....h?M.h
4D F2 0D 52|1E 2B F9 CD|00 00 00 00|00 00 00 00| M.R+........
```

Die getestete Softwareversion der `ExmpSrv.exe` ist `2.5.6.24`, wie Abbildung 3 zeigt.

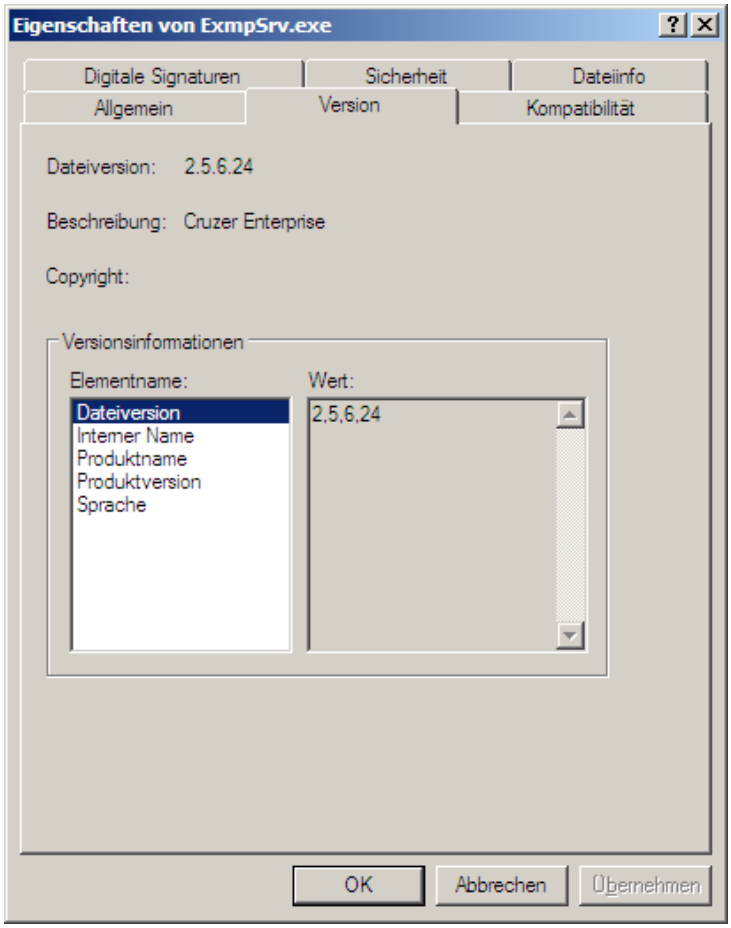


Abbildung 3: Eingesetzte Softwareversion der `ExmpSrv.exe`

Um Zugriff auf den geschützten Massenspeicher der USB-Sticks zu erhalten, muss man lediglich dafür sorgen, dass die Überprüfung des Passworts immer diese 32 Bytes zum Ergebnis hat. Denn diese 32 Bytes werden im weiteren Verlauf des Anmeldeprozesses für die Aktivierung der geschützten Partition des USB-Massenspeichers verwendet.

Die SySS GmbH entwickelte zu Demonstrationszwecken ein *Proof-of-Concept*-Softwaretool, das genau dies bewerkstelligt und in Abbildung 4 dargestellt wird.

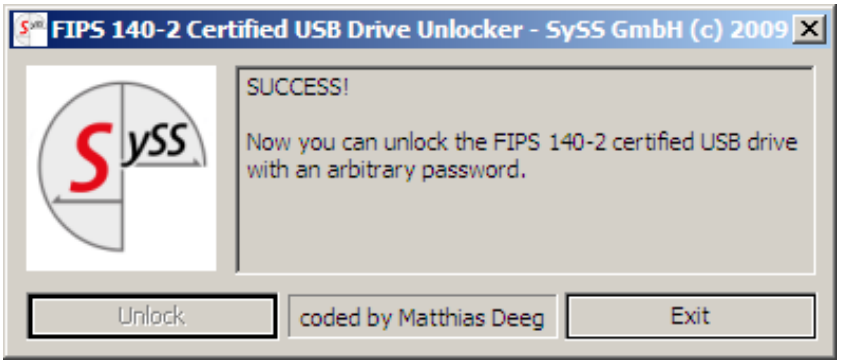


Abbildung 4: *Proof-of-Concept*-Softwaretool der SySS GmbH

Da das Programm `ExmpSrv.exe` bei jeder Nutzung des USB-Sticks von der nur lesbaren Partition (emuliertes CD-ROM-Laufwerk) in das temporäre Verzeichnis des Benutzers entpackt und von dort aus aufgerufen wird, wurde das PoC-Softwaretool als sogenannter *In-Memory Patcher* realisiert.

Das Softwaretool modifiziert den `ExmpSrv`-Prozess zur Laufzeit so, dass bei der Passwortüberprüfung ungeachtet des tatsächlich eingegebenen Passworts immer die besagten 32 Bytes im weiteren Anmeldeprozess verarbeitet werden. Dadurch kann mit einem beliebigen Passwort auf die geschützten Daten des USB-Flash-Laufwerks zugegriffen werden.

Abbildung 5 zeigt einen Codeabschnitt des `ExmpSrv`-Prozesses im Debugger OllyDbg, der sich zu diesem Zweck eignet. Der dargestellte `memcpy`-Aufruf wird dazu verwendet, um an die entsprechende Stelle im Hauptspeicher das Resultat der AES-Entschlüsselung zu kopieren, was idealerweise den erwähnten 32 Bytes entspricht. Diese 32 Bytes werden dabei zuvor durch das Softwaretool in das Datensegment des `ExmpSrv`-Prozesses eingebracht.

Dieser Angriff zur Umgehung der passwortbasierten Authentifizierung funktioniert gegen das getestete USB-Flash-Laufwerk SanDisk Cruzer Enterprise - FIPS Edition.

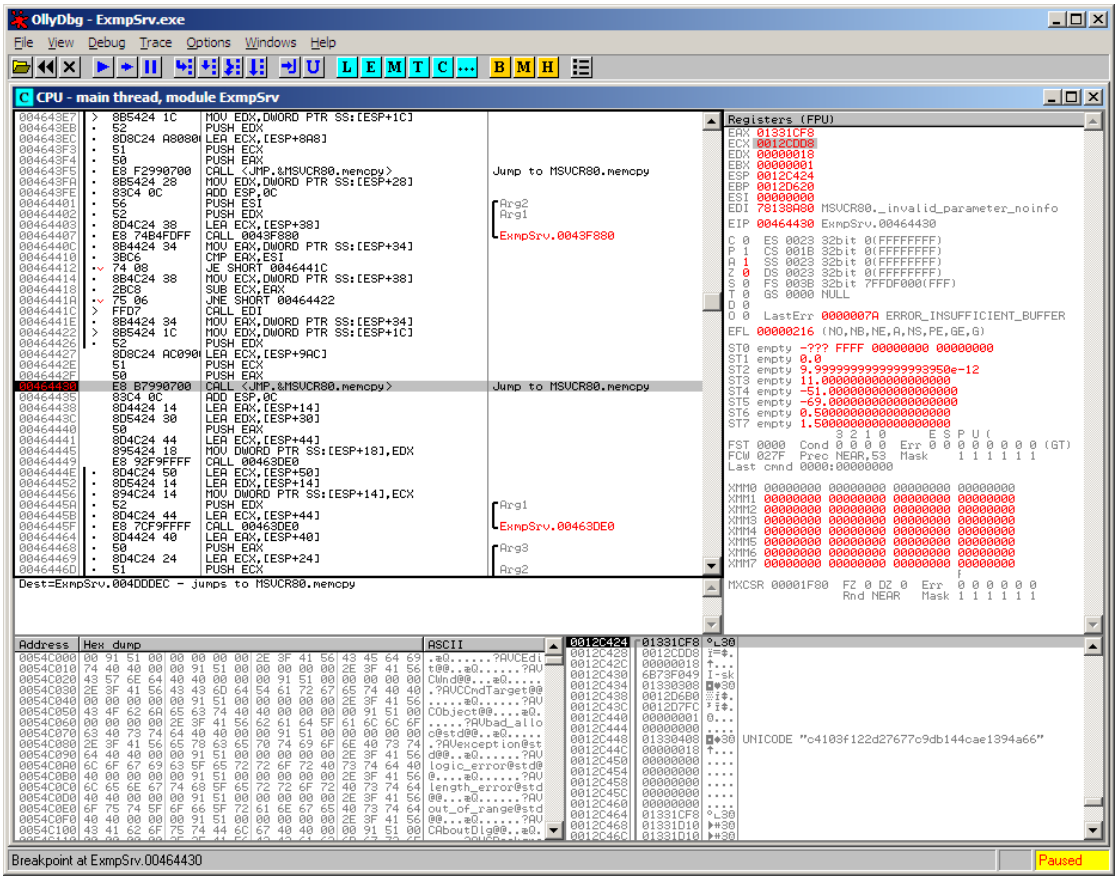


Abbildung 5: `ExmpSrv`-Prozess in OllyDbg

# 3 Fazit

Die SySS GmbH konnte demonstrieren, dass ein Softwarefehler bei der Verifizierung von Passwörtern des getesteten USB-Flash-Laufwerks

- SanDisk Cruzer Enterprise - FIPS Edition

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 hardwarebasierte 256-Bit AES-Verschlüsselung, die obligatorischen Sicherheitsmaßnahmen für alle Dateien und der Sperrmodus bei Eingabe

einer festgelegten Anzahl falscher Kennwörter als ineffektiv, da sie den Angriff nicht verhindern.

Dieses Testergebnis zeigt, dass kleine Fehler oft große Auswirkungen haben – besonders wenn es um komplexe IT-Sicherheitsprodukte geht.

Im Fall des getesteten USB-Flash-Laufwerks besteht das Produkt als solches aus mehreren Soft-, Firm- und Hardwaremodulen, die unterschiedliche Technologien verwenden, was dieses in seiner Gesamtheit recht komplex macht. Eines dieser Module mit der Bezeichnung S2 FIPS DiskOnKey Controller wurde sogar von dem US-amerikanischen *National Institute of Standards and Technology* (NIST) zertifiziert, wie die beiden Dokumente [4] und [5] belegen. Aber wie gezeigt werden konnte, genügte ein einziger Softwarefehler in einem dieser Module, um die Sicherheit des gesamten Produktes zu gefährden.

Wir haben den Hersteller SanDisk kontaktiert und ihn über unseren Fund in Kenntnis gesetzt. SanDisk hat schnell reagiert und bereits ein Softwareupdate bereitgestellt, das die Sicherheitsschwachstelle beseitigt. Wir können bestätigen, dass in der neuen Softwareversion das beschriebene Sicherheitsproblem nicht mehr vorliegt. Das *Security Bulletin* mit weiteren Informationen und dem Softwareupdate ist unter [6] zu erreichen.

## Quellen

[1] Herstellerinformationen zum SanDisk Cruzer Enterprise - FIPS Edition, `http://www.sandisk.de/OEM/ProductCatalog%281383%29-Cruzer_Enterprise_FIPS_Edition.aspx` 2

[2] Philippe Oechslin, *Verpfuschte Sicherheit - USB-Stick mit Hardware-AES-Verschlüsselung*, `http://www.heise.de/security/artikel/USB-Stick-mit-Hardware-AES-Verschluesselung-geknackt-270086.html` 4

[3] Stefan Arbeiter, Matthias Deeg, *Bunte Rechenknechte - Grafikkarten beschleunigen Passwort-Cracker*, c't-Archiv, 6/2009, Seite 204 5

[4] NIST Security Policy, *S2 FIPS DiskOnKey Controller*, `http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp932.pdf` 10

[5] NIST FIPS 140-2 Validation Certificate, *S2 FIPS DiskOnKey Controller by SanDisk Corporation*, `http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt932.pdf` 10

[6] SanDisk, Security Bulletin December 2009, `http://www.sandisk.com/business-solutions/enterprise/technical-support/security-bulletin-december-2009` 10