Cryptographically Secure? SySS Cracks a USB Flash Drive

***The SySS GmbH cracked a hardware-encrypted FIPS 140-2 certified USB flash drive from* SanDisk.**

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

December 18th, 2009

1 Introduction

Portable USB mass storage devices have gained great popularity in recent years. In the course of time not only the storage capacity of these extremely useful USB flash drives has increased but also the demand for data protection. In case of theft or loss it is desirable for the owner of such a device that all stored data stay confidential. Especially military and government authorities but also the free economy, e.g. health and finance companies, require a high level of data protection and confidentiality as sensitive data is often stored on USB flash drives which should not be accessed by unauthorized persons.

Besides a number of commercial as well as free software solutions for encrypting sensitive data on portable mass storage devices, manufacturers also offer USB flash drives with integrated hardware encryption and further security features which are often promoted with flamboyant marketing slogans. Some of these products even possess accredited security certificates attesting them a defined security level.

But as the history of IT security teaches us, cryptography is a complicated area where small mistakes often have a big impact.

2 Security Assessment

In the following section the example of a USB flash drive of the well-known manufacturer SanDisk shows that FIPS 140-2 certified products can be *cracked*.

Concretely the USB flash drive

- SanDisk Cruzer Enterprise - FIPS Edition [1]

was analyzed for security issues.

Detailed information about the used firmware version of the tested USB flash drive is shown in figure 1.

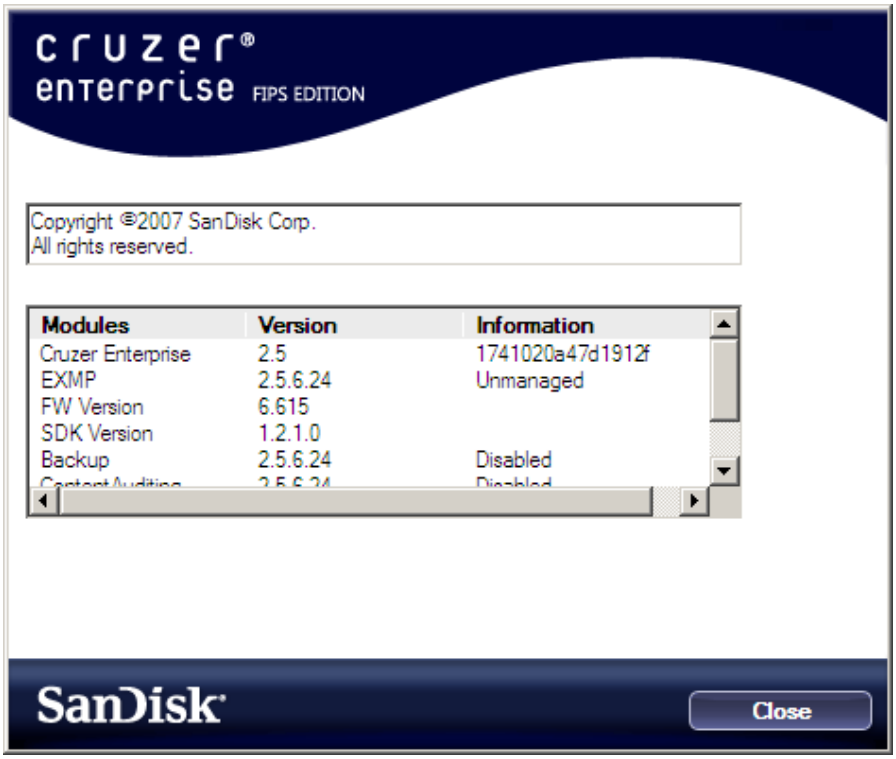

Figure 1: Firmware version of the tested USB flash drive

The following information can be found in the product description of this USB mass storage device:

- FIPS 140-2 level 2 certified
- Hardware based 256-bit AES encryption
- Mandatory access control for all files (100% private partition)
- Strong password enforcement
- "Lockdown" mode when a set number of incorrect password attempts is made

Especially the last point of this listing is of high interest as in general the security of technical systems with password-based authentication can be reduced to the security of the chosen passwords.

In short: If weak passwords are used, further security measures like a 256-bit AES hardware encryption, for instance, are of little importance. The data to be protected are only as secure as the chosen password and not as the cryptographic algorithms used for data encryption.

As figure 2 exemplifies, data on the USB flash drive are protected by a user-supplied password, which has to comply with the password policy of this product.

Figure 2: Password-based authentication

In order to exploit weak passwords, one precondition to be met is the mere possibility of checking a large number of presumably weak passwords. In the case of the tested USB flash drive it means this: If it is possible to obtain full knowledge about the functionality of the implemented password-based authentication including all parameters in use, an arbitrary number of passwords can be verified by performing a so-called *offline attack*.

Launching *password guessing attacks* – no matter whether by the use of a dictionary (*dictionary attack*), with simple sequential attempts (*brute force attack*) or by a combination of both – has proven to be an appropriate means in order to gain access to password protected data. As the article [2] from heise[1] shows, this kind of attack has already been successfully used against a FIPS 140-2 level 2 certified USB flash drive from the manufacturer MXI Security in the past which possessed this particular security weakness.

When examining the USB flash drive from SanDisk, the focus was therefore on the analysis of the password-based authentication. If there are similar security flaws to be

[1] see `www.heise.de`, most published articles are in German though

found as for the USB flash drive from MXI Security, it is possible to recover passwords by means of special password guessing software, so-called *password crackers* or *password recovery tools*. Depending on the cryptographic algorithms in use, be it for generating hash values or for encrypting or decrypting data, many thousands to billions of password candidates can be checked per second with the help of modern hardware, i.e. CPUs and GPUs [3].

Therefore, password guessing attacks are definitely a security issue but are generally not seen as such by most manufacturers and suppliers of USB flash drives with a corresponding functionality. Because if complex passwords are used, attackers will need to have a lot of processing power at their disposal in order to access the encrypted data during their own lifetime and not just in thousands or even millions of years.

Nevertheless it could be found out within the performed security analysis, that even long and complex passwords do not protect the stored data on the tested FIPS 140-2 level 2 certified USB flash drive.

The reason for this is the way how user-supplied passwords are verified. The first security problem here is that the actual password verification is not done in hardware – i.e. on the USB mass storage device itself – but in software on the PC of the user. This fact makes it possible to analyze the password-based authentication process in detail with the help of a software debugger like OllyDbg[2], for instance. The second and bigger problem is, however, that secure[3] cryptographic algorithms, like AES in this case, are used in an insecure way.

These two described security issues are located within the executable file `ExmpSrv.exe` which is part of a software product that is used by the tested SanDisk USB flash drive.

The research of the SySS GmbH showed that the password verification works in the following way:

1. The user-supplied password is converted from `ASCII` to `WideChar`
2. A MD5 hash of the `WideChar` password is calculated
3. A ASCII-HEX representation of the MD5 hash is generated and also converted to `WideChar`; the first half of the result serves as key in the next step
4. With the generated key, 32 bytes of data, which have been read from the USB flash drive before, are decrypted via AES-256-ECB
5. If the result of the decryption corresponds with a specific value, the password is correct and the protected data storage of the USB flash drive can be accessed

In the course of the security analysis it was found out that the result of the decryption in step 5 was always the same when supplying the correct password. This did not even change when a new password was set or when the USB flash drive was formatted.

[2] `http://www.ollydbg.de/`
[3] at the time of writing

The reason for this is that when setting a new password, always the same 32 bytes are encrypted via AES-256-ECB and therefore must consequently be the result of the decryption during the password verification process.

These actual 32 bytes are as follows:

```
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+........
```

The tested software version of the `ExmpSrv.exe` was `2.5.6.24` as figure 3 illustrates.

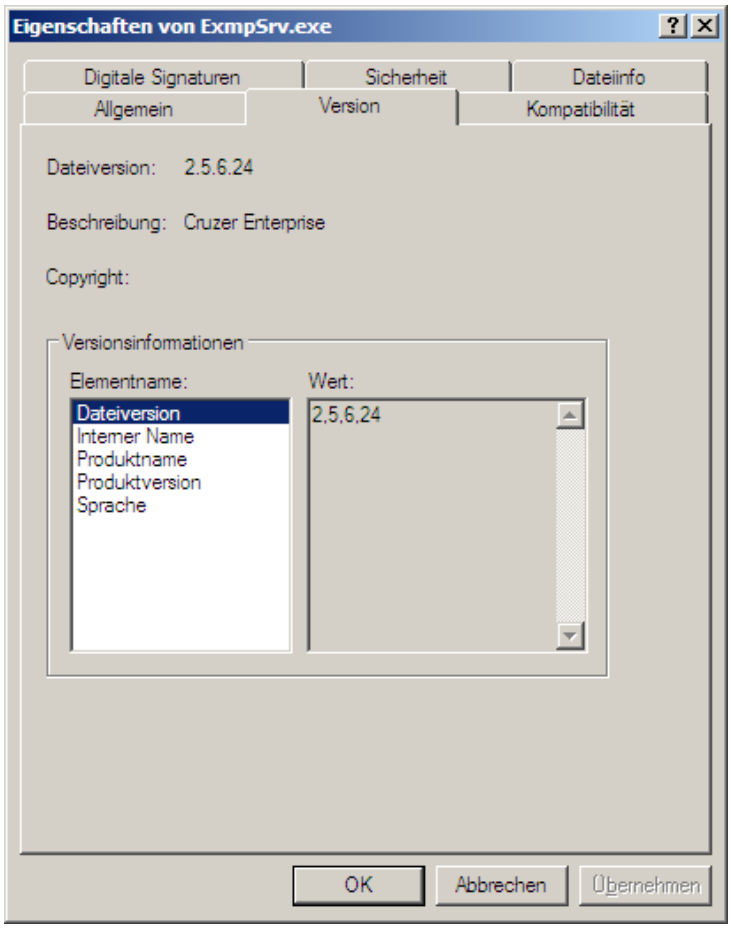

Figure 3: Used software version of the `ExmpSrv.exe`

In order to gain access to the protected mass storage of the USB flash drive, one just has to make sure that the password verification always results in these 32 bytes. In the

further login process those 32 bytes are used for unlocking the protected partition of the USB flash drive.

For demonstration purposes, the SySS GmbH developed a proof-of-concept software tool that exactly accomplishes this task. Figure 4 shows a screenshot of this software tool.

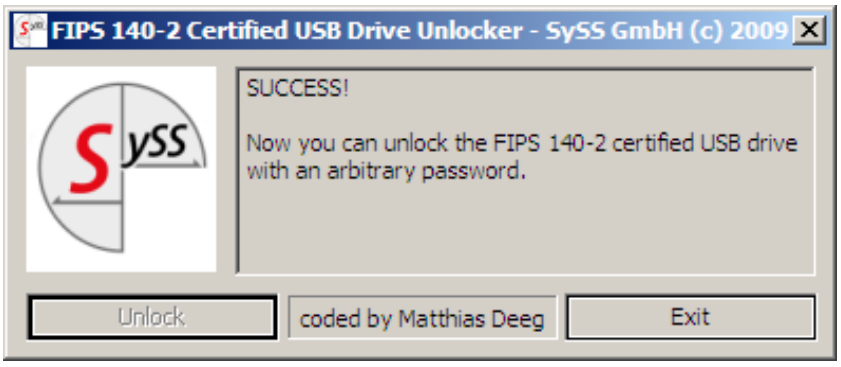

Figure 4: Proof-of-Concept software tool of the SySS GmbH

As the program `ExmpSrv.exe` is unpacked from a read-only partition (emulated CD-ROM drive) to the temporary folder of the current user and started from there whenever the USB flash drive is used, the PoC software tool was realized as a so-called *in-memory patcher*.

The software tool modifies the `ExmpSrv` process during runtime in such a way that the aforementioned 32 bytes are always used in the further login process no matter what the user-supplied password is. Therefore, the protected data storage of the USB flash drive can be accessed with an arbitrary password.

Figure 5 shows a code section of the `ExmpSrv` process serving this purpose within a software debugger. The displayed `memcpy` function call is used to copy the result of the AES decryption, which ideally matches with the shown 32 bytes, to the corresponding memory location. These 32 bytes are inserted into the data segment of the `ExmpSrv` process by the PoC software tool before.

This attack for bypassing the password-based authentication can be successfully launched against the tested USB flash drive SanDisk Cruzer Enterprise - FIPS Edition.

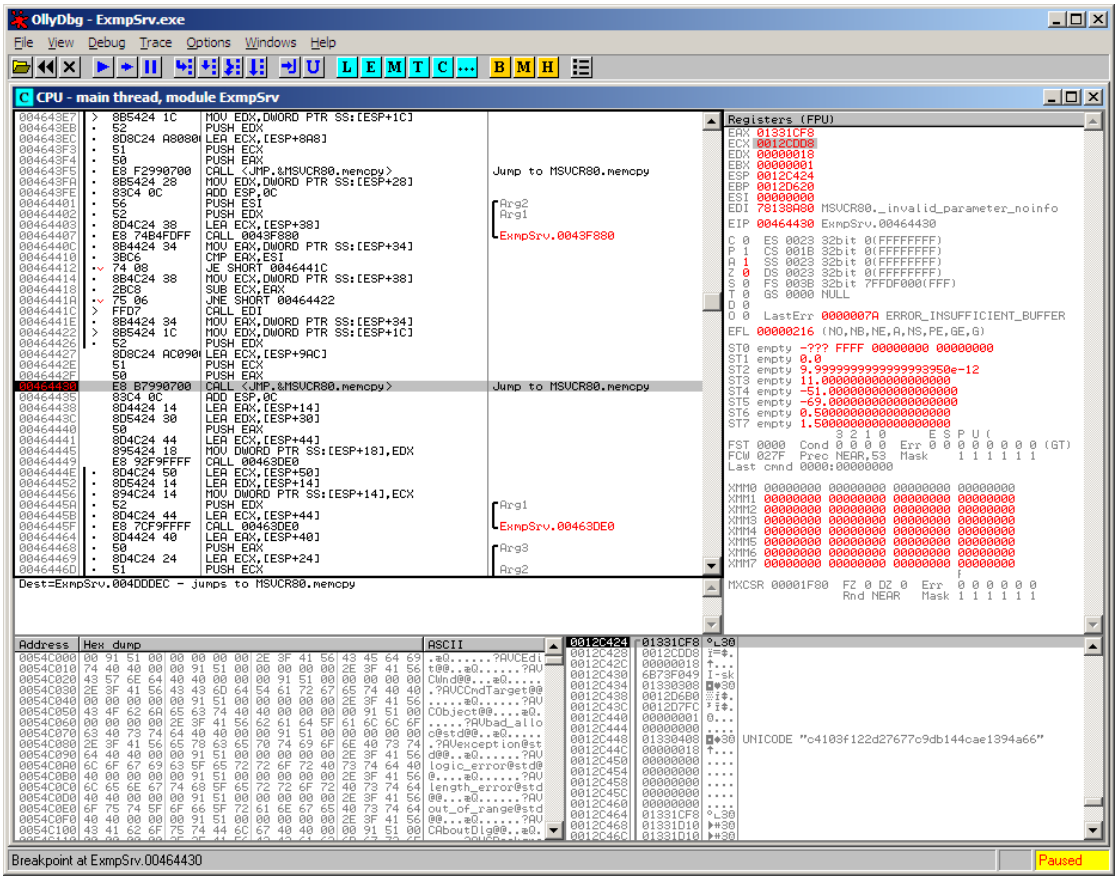

Figure 5: `ExmpSrv` process in OllyDbg

3 Conclusion

The SySS GmbH could demonstrate that a software bug in the password verification mechanism of the tested USB flash drive

- SanDisk Cruzer Enterprise - FIPS Edition

makes it possible to gain access to all stored data by just a few mouse clicks fairly easily. If an appropriate software tool was available on the Internet, even technically inexperienced attackers could pose a security risk when getting hold of such a tool.

By exploiting the shown software vulnerability, implemented security features like the hardware based 256-bit AES encryption, the mandatory access control or the *lockdown mode* are effectively rendered useless as they do not prevent the attack.

This test result shows that small mistakes often have a big impact – especially when it comes to complex IT security products.

In case of the tested USB flash drive, the product is made up of several soft-, firm- and hardware modules using different technologies making it rather complex. One of these modules, the S2 FIPS DiskOnKey Controller, even has been certified by the American *National Institute of Standards and Technology* (NIST) as the documents [4] and [5] prove. However, as could be demonstrated, a single software bug in one of these modules was sufficient to compromise the security of the entire product.

We contacted the manufacturer SanDisk and informed him about our finding. SanDisk responded quickly and has in the meantime provided a software update that fixes the security flaw. We can confirm that the described problem has now been remedied in the new software version. The security bulletin with further information and the software update can be found at [6].

References

[1] Product information about SanDisk Cruzer Enterprise - FIPS Edition, `http://www.sandisk.com/business-solutions/enterprise/cruzer-enterprise-fips-edition` 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` 9

[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` 9

[6] SanDisk, Security Bulletin December 2009, `http://www.sandisk.com/business-solutions/enterprise/technical-support/security-bulletin-december-2009` 9