



## Hydra PC by SPYRUS, Inc. Immune to USB Authentication Vulnerability



**January 21, 2010**

**Document no. 412-070004-01**

**© SPYRUS, Inc. 2010. All rights reserved.**

## Hydra PC by SPYRUS, Inc. Immune to USB Authentication Vulnerability

In their study titled “Cryptographically Secure? SySS Cracks a USB Flash Drive,”<sup>1</sup> authors Matthias Deeg and Sebastian Schreiber of SySS GmbH document a serious password-based authentication vulnerability in the SanDisk Cruzer Enterprise FIPS Edition USB encryption device and similar products from other vendors. All devices containing the authentication vulnerability received FIPS 140-2 Level 2 security validations from the National Institute for Science and Technology (NIST).

The vulnerability resulted from a weak password-authentication service that operates in software on the host computer, outside of the security boundary of the USB encryption drive. A simple application can completely bypass the software-based password authentication and unlock the drive to decrypt the data stored on the drive, regardless of the strength of the password or encryption method.

The study also points out that the vulnerability in this case was not the AES 256-bit encryption algorithm itself, but how a strong algorithm used incorrectly can result in a weak solution. Beyond the vulnerability described in the SySS study, further analysis of the study and the FIPS 140-2 security policy accentuate the inexperience on the part of the product designers. The use of a weak hash such as MD5, the peculiar method used to derive a key from the password, and the very basic encryption mode, provide weak protection, even without the authentication vulnerability.

### Hydra PC USB Encryption Drives Feature Hardware-Based Authentication

Hydra PC USB encryption drives, including the Hydra PC Personal Encryption Device, the Hydra PC Enterprise Edition, the Hydra PC Digital Attaché, and the Hydra PC Locksmith, are immune to the vulnerabilities documented in the SySS study. All Hydra PC USB encryption drives perform all authentication and encryption operations in hardware, within the security boundary of the device. No password or cryptographic key is ever stored on the host computer.

To prevent other types of authentication attacks, Hydra PC drives use no fixed or variable unlock codes. Interfaces between Hydra PC USB encryption drives and the host computer use encrypted secure channels to safeguard against interception attacks.

### Authentication Vulnerability in Detail

The USB encryption drives shown to be compromised in the study all used strong and well-established encryption algorithms, but they were compromised by insecure key management and user authentication.

Attacks that exploit the reported vulnerability depend on a software interface from the host computer to the USB encryption drive that allows users to change passwords or PINS. The password verification process in the software is a simple challenge-response protocol, operating similar to the following example:

---

<sup>1</sup> [http://www.syss.de/fileadmin/ressources/040\\_veroeffentlichungen/dokumente/SySS\\_Cracks\\_SanDisk\\_USB\\_Flash\\_Drive.pdf](http://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_Cracks_SanDisk_USB_Flash_Drive.pdf)

- The user-supplied password is converted from ASCII to WideChar.
- An MD5 hash of the WideChar password is calculated. (MD5 is not a FIPS-approved algorithm, and it has been deprecated by NIST because of its vulnerability to modern cryptographic attacks.)
- An ASCII-HEX representation of the MD5 hash is generated and then converted to WideChar.
- A specific set of 32 bytes of data read from the USB flash drive is decrypted using a key generated from the first half of the result from the previous step via AES-256-ECB.
- The decrypted data is then passed into the cryptographic module.

If the result of the decryption corresponds with a response code that is maintained within the USB's cryptographic module, the password is accepted and the user is authenticated to the USB's cryptographic module. The AES flash media storage encryption key is not exposed in this process, but it can easily be accessed and used to decrypt data stored on the USB device.

A significant flaw in this scheme is that the response code *never* changes, even if the password is changed or the device is reinitialized. Yet the response code has the power to access encrypted data on the USB encryption drive. Once the response code is known, changing or cycling AES-256 keys or the password cannot prevent access to encrypted data on the drive. In the SySS study, attackers used a simple application to gain access to encrypted data without knowing the user's password, completely bypassing the password complexity and lockdown mode designed to prevent password-guessing attacks.

The SySS study verifies that the *same* response code is *always* produced if the correct input is provided.<sup>2</sup> Our analysis indicates that the software-based password verification process explained previously occurs outside the product's FIPS 140-2 Level 2 security boundary, does not use FIPS-approved algorithms, and would be unlikely to pass FIPS 140-2 validation even if the authentication process had been implemented within the FIPS security boundary.

Because the same response code was used for all USB encryption drives analyzed in the study, even though they were sold by different vendors, the same risk applies to every device.

For any solution to the risk imposed by this authentication vulnerability, the boundary of protection must include the FIPS 140-2 cryptographic module, the host computer, communications between the two, and partitioning of cryptographic implementations. Several vendors of affected devices now offer a software fix, but only a firmware update to the USB encryption drive can produce an effective solution that cannot be circumvented by an attacker with knowledge of the response code. Any change to the firmware most likely would invalidate the existing FIPS 140-2 validation of these USB encryption drives.

## Hardware-Based Hydra PC USB Encryption Drives

SPYRUS introduced the first hardware-based encrypting flash drive in 1996. Our second-generation Hydra PC USB encryption drives provide the strongest encryption commercially available today. The term "hardware-based" means that Hydra PC devices perform all encryption and user authentication operations exclusively within the hardware cryptographic

---

<sup>2</sup> See SySS study, page 6.

boundary to completely avoid the password-based authentication vulnerability cited by the SySS study.

Hydra PC USB encryption drives include models with hardware-based, AES 256-bit file-based encryption and XTS-AES 256-bit sector-based encryption. The attack described in the SySS Study is impossible to use against any Hydra PC model, and their proof-of-concept software agent will consistently fail to unlock the USB encryption drives. Here is why:

- All Hydra PC products satisfy the FIPS 140-2 Level 3 requirement for Identity-Based authentication that *every* user possess a unique password or PIN. Absolutely no common authentication check value such as the response code is ever used, not even internally.
- The Hydra PC products perform authentication in hardware but never store the password or a hash of the password on the device. Authentication recovers a high-entropy encryption key generated through the use of a FIPS-approved, third-party validated pseudo-random-number generator. The benefit of this approach is that encryption keys are not limited by the protection provided by the low entropy of most passwords, and the keys are therefore protected from data-at-rest attacks.
- Authentication always occurs by FIPS-approved key generation within the hardware cryptographic module, never on the host computer.
- Cryptographic hardware limits the number of incorrect logon attempts allowed. If the policy-enforced maximum number of attempts is exceeded, the device is blocked, and the keys become permanently inaccessible.
- A secure channel handles authentication traffic between the computer and the Hydra PC with the same Suite B elliptic

### What is FIPS 140-2?

The National Institute of Standards and Technology (NIST) develops security standards to evaluate encryption products that protect unclassified data. The current Federal Information Processing Standard (FIPS) 140-2 validates products at four increasing levels of security to allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments:

- FIPS 140-2 Level 1 (the lowest level) requires at least one approved algorithm or security function.
- FIPS 140-2 Level 2 adds requirements to provide evidence of physical tampering that might indicate an attempt to access plaintext keys and critical security parameters.
- FIPS 140-2 Level 3 requires additional physical security mechanisms to prevent intruder access to the cryptographic module. These security mechanisms must have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. In particular, roles, services, and authentication (how the device limits access to only the designated user), self-test and design assurance, and cryptographic key management (how keys are generated and maintained securely), are closely evaluated.
- FIPS 140-2 Level 4 (the highest level) requires detection of and resistance to all types of attack. In the event of any attack, all keys and other critical parameters must be zeroized. Resistance to physical attack is intensely analyzed using national laboratory resources, including scanning electron microscopes and other esoteric attack methods. Level 4 devices must also detect environmental changes that might compromise security, such as freezing the module to prevent it from zeroizing.

Security requirements for FIPS 140-2 are organized into 11 categories that are each validated to one of the security levels 1-4 described above. Categories include: Cryptographic Module Specification, Ports and Interfaces, Roles, Services and Authentication, Finite State Model, Physical Security, Operational Environment, Key Management, Electromagnetic Interference/Compatibility, Self-Tests and Design Assurance, and Mitigation of Other Attacks. The overall level of security assigned to the entire product is the lowest level assigned to each of the 11 categories.

Of the 11 categories, Roles, Services, and Authentication is the most relevant to authentication vulnerability. A fundamental discriminator is implementation of role-based authentication (for level 2) and identity-based authentication (for levels 3 and 4).

The USB encryption drives analyzed in the SySS study all achieved FIPS 140-2 Level 2 in all 11 categories.

curve cryptography (ECC) recommended by the U.S. Government to protect national security systems and national security information.

- All Hydra PC models include multiple hardware security processors, all within the epoxy-protected cryptographic boundary, that concurrently implement and test cryptographic functions.

Confining secure encryption operations within the cryptographic boundary so that keys and other critical data are never distributed between a trusted, validated FIPS module and a less secure host environment is a critical differentiator for Hydra PC devices. No encrypted response codes travel between the device and the host computer, no keys are ever hashed on the host computer, and the response code is never decrypted and passed over an unprotected channel for comparison. Passwords are exchanged only over a protected secure channel, and authentication uses FIPS-approved processes.

## Summary

The password authentication vulnerability discovered in the USB encryption drives analyzed in the SySS study poses a potentially devastating security risk to all users of those drives. Publication of the response code in the SySS study essentially invalidates the security mechanisms of all USB encrypting drives using it for authentication and leaves user data stored on those USB encryption drives susceptible to attack, decryption, and exposure. The exposure could be minimized if there were firmware upgrades available, but those upgrades most likely would invalidate the FIPS validation of the drives.

Hydra PC USB encryption drives are designed to perform all encryption and authentication operations within the hardware cryptographic boundary, making them invulnerable to the risk described in the SySS study.

Compare some key features of Hydra PC models with other USB encryption drives:

- All Hydra PC models satisfy FIPS 140-2 Level 3 requirements for Identity-Based Roles, Services, and Authentication. FIPS 140-2 Level 2 requires only much weaker Role-Based authentication.
- Hydra PC USB encryption drives never use challenge response protocols such as those cited in the SySS study for authentication or password changes.
- Hydra PC devices never use response codes as the logon response criteria.
- Whenever the Hydra PC logon password changes, authentication data also changes.
- Hydra PC hardware-based encryption protects logon passwords in transit over the USB connection.
- Passwords are never stored on the Hydra PC, not even in hashed or encrypted form.
- No password, AES key(s), or ECC private key can ever be extracted or exported from the Hydra PC cryptographic module.
- The Hydra PC never uses a response code in any form or any similar value, so it is never at risk of the authentication vulnerability exposed in the SySS study.
- At initialization, each Hydra PC device generates a unique encryption key using a FIPS-approved, third-party-validated pseudo-random-number generator.

Unlike the USB encryption drives analyzed in the SySS study, hardware-based Hydra PC drives protect against many types of password authentication vulnerabilities and other attacks. Simply changing the password blocks any attacker with knowledge of a logon password, and most Hydra PC models can be configured to require one or two authentication factors in addition to the password. An attacker cannot learn the password by eavesdropping on the secure channel.

SPYRUS has specialized in portable, Government-approved commercial hardware-based encryption devices for more than 15 years. SPYRUS was the first company to merge hardware encryption with flash, the first to implement the full set of Suite B cryptographic algorithms, and the first and only company to support both hardware-based file encryption and sector-based encryption. We also offer the only commercial USB encryption device approved by U.S. Government to protect classified data

You can rest assured when your data is Secured by SPYRUS™.



## About SPYRUS

SPYRUS, Inc. provides high-assurance security technology for the U.S. Government, industries required to comply with security regulations, and everyday users who want the best protection for sensitive information. Secured by SPYRUS™ security technology is designed, developed, and manufactured in the USA. SPYRUS products support the strongest commercially available cryptographic algorithms, including elliptic curve cryptography (ECC), AES, and SHA-2, collectively known as Suite B. In December 2007, the Hydra PC Personal Encryption Device became the first, and as yet the only, commercially available USB encryption device to be approved for protecting tactical classified data at the Secret level and below, when used in accordance with the approved operational security doctrine. SPYRUS, Inc. is headquartered in San Jose, California. See [www.spyrus.com](http://www.spyrus.com) for more information.

SPYRUS, the SPYRUS logos, Hydra Privacy Card, Hydra PC, Hydra PC Digital Attaché, Hydra PC Locksmith, Secured by SPYRUS, and Security to the Edge are either registered trademarks or trademarks of SPYRUS, Inc., in the U.S. and/or other jurisdictions. All other company, organization and product names are trademarks of their respective organizations.

SPYRUS products embody technology protected by one or more of the following SPYRUS patents or patent applications: U.S. Pat. Nos. 7,380,140; 6,088,802; 6,003,135; 6,981,149; U.S. Pat. Appl. Ser. Nos. 12/018,094; 12/126,759.