Flash Padlock™

Self-Secured and Host-Independent USB Flash Drive

White Paper

April 2007

Prepared by ClevX, LLC for Corsair Memory

1 INTRODUCTION

Millions of USB Flash Drives (UFDs) are being used for data backup, transfers, as well as intermediate and primary storage. UFDs pose a unique security challenge. Being tiny and highly portable, they are easily lost or stolen along their content. Thus, many people are reluctant to employ UFDs to store financial data, user names, passwords, credit card data, and other sensitive information.

In addition, most mid and large sized organizations restrict the use of UFDs as they pose a potential corporate information leak as referenced by Sarbains-Oxley. Sensitive information, if copied to one of these drives, might end up in the wrong hands. To protect the UFD and its content from malicious and unauthorized access, ***user authentication*** is required.

This white paper describes existing UFD authentication practices and their inherited drawbacks. It then describes Flash Padlock™ - a *self-secured, host-independent (cross platform)* USB Flash Drive with a *hardware authentication mechanism**. Finally, we compare Flash Padlock with existing solutions to demonstrate its optimal balance of usability, security, and price.

* - US and Foreign Patents Pending

www.clevx.com

2 LACK OF STANDARD AUTHENTICATION

Currently, the computer's standard USB Mass Storage Class has no provision for authentication. The UFD connects to the computer and the host's Operating System (OS). The detection of a USB drive prompts loading of a standard driver that results in mounting the device as standard file system disk. This mechanism is provided by a number of operating systems and some embedded equipment such as that used in offices and manufacturing.

Authentication, if required, is the responsibility of the host; it must engage the user in a authentication procedure to grant access. A commonly used method is *software based password authentication* that becomes a proprietary functional extension of the USB Mass Storage class. Another is fingerprint recognition known as *biometric authentication.*

2.1 Password Based Authentication

Password authentication requires host software to extend the functionality of the standard driver. Typically, UFDs are shipped with a single public memory partition. To activate security, the user is required to re-format the drive, dividing it into two, fixed sized, partitions: one public, one private.

A program executed from the public partition controls access to the private partition. Typically, a password grants access to the private partition that results in a switch: the private partition mounts at the expense of the public partition. File operations now pass through an encryption process to the private partition. This configuration remains until the user exits to reconnect with the public partition or unplugs the drive.

Password based authentication has a number of drawbacks:

- **Authentication is Host and OS dependent.** While the public partition is visible to any USB Mass Storage Class compliant OS, access to the private partition is controlled by a proprietary authenticating application. Therefore, authenticating applications must be customized for different operating environments.
- **Complex Usability.** Many users avoid, or give up altogether, because the procedure is perceived as complex and not particularly intuitive.
    - **Non-computer savvy users find it complex.** Formatting the device results in erasing the entire the drive. Previously stored information requires backup prior to formatting.
    - **Partitioning the UFD is static.** Users are unable to anticipate the required size for private partitioning. If more space is needed later, repartitioning requires reformatting.
    - **Cumbersome partition management.** Users perceive the UFD as fragmented media and need to be consciously aware of file location (private or public?). Copying files between partitions is cumbersome as intermediate media is required to hold files during a partition switch. Backup and restoration of an entire drive is non-trivial as partitions need to be accessed separately.
    - **Good security requires complex passwords.** In order to defend against dictionary and similar attacks, it is recommended to use pass phrases that are long, complex, and include special characters. Policy dictates a frequent change of passwords that make them even more difficult to remember. In reality, passwords don't frequently change and tend to be simple and easy to remember. Often times, the same password is used for multiple logins and access.
- **Security breaches.** A keyboard provided password might introduce a security breach.

- **Password Extraction by malicious software.** Keyboard loggers and other spyware might intercept passwords and redirect to a malicious source. This is risky in security hostile environments such as public computers in a place such as a library, Internet café, kiosk, etc.
- **Extract password by dictionary/brute-force attack.** A malicious application can generate a great number of passwords in an attempt to gain access to a protected UFD. This may take some time and is password dependent. As mentioned above, users typically use simple passwords as it is difficult to recall "strong/good" passwords.

2.2 Biometric Authentication

Less common than passwords, Biometrics utilizes a small finger-print scanning sensor. Authentication is quite similar to password based drives with both public and private partitions. The private partition is made available when the authorized fingerprint is recognized.

Biometric authentication is more resistive than password based attacks. However, there are drawbacks to this method as well.

- **Authentication is Host and OS dependent.** While the public partition is visible to any USB Mass Storage Class compliant OS, access to the private partition is restricted to a OS application that is capable of executing authentication.
- **Long-term reliability has not yet been established.** Current methods of finger print recognition, when packaged in a small scale UFD, do not provide the necessary reliability. There are many reports indicating problems with false-positive and false-negative readings.

  A back door password is often used to compensate for inherit unreliability. This undermines the basis for biometric authentication in the first place. Thus, it has all the vulnerabilities of password protection.

  Fingerprint recognition is best performed when the finger is clean without cuts. Changes in skin surface can potentially create problems.
- **Biometrics is expensive.** Biometrics adds a considerable price premium. Biometric drives have seen limited success in the market place.
- **Restricted to office environments.** It is impossible to work with biometric sensors wearing gloves, which may be required for biotech and military applications.

3 FLASH PADLOCK

Flash Padlock is a self-secured, host independent (cross platform) USB Flash drive with a hardware authentication mechanism. When locked, a Flash Padlock is invisible to its host.

Authentication is based on correct entry of a user defined PIN using the on-board keypad. A correct PIN activates a Flash Padlock allowing it to operate as a standard USB mass storage device. A PIN can consume up to 10 digits and is not stored anywhere that is accessible from the computer.

Battery equipped, PIN entry can be performed while detached from a host computer. Status indicators provide visual feedback for authentication. A red status indicator means the drive is locked; green indicates the drive is unlocked and ready for operation.

An auto-locking feature allow Padlocks to lock themselves when removed or the host shuts down. If the drive is unlocked under battery power, it will automatically re-lock if a host is not detected within 15 seconds.

Flash Padlock represents both usability *and* security.

- **True Host Independent and Cross Platform.** Since authentication does not depend on host functions, it works equally well with all operating systems that support the USB Mass Storage Class: for example Windows, Mac OS, Linux, and office equipment.
- **Authentication is self contained.** No special software or driver installation required. In fact, the host computer is not involved and unaware of the authentication process. Flash Padlock provides complete PIN management.
- **Zero File System Configuration.** Since the drive can only mount after authentication, there is no need for extraneous partitioning. The user experiences a single partition that utilizes the entire media.
- **Ease of Use.** The Flash Padlock usage model is intuitive and resembles that used with debit cards and ATM machines. The user remembers a short PIN as opposed to a long and complex password.
- **Immune to host-originated attacks.** Since no Flash Padlock communication channel exists when locked, it is immune to attacks originating from its host.
- **Two Factor Authentication.** Flash Padlock makes a natural Two Factor Authentication device recommended by government and financial institutions. The term “Two Factor Authentication” is used to describe an authentication mechanism that requires (1) something you have (Flash Padlock) and (2) something you know (PIN).

4 SUMMARY

The proliferation of UFDs poses a unique security threat for people and institutions that need to protect sensitive information. A *robust authentication mechanism is required to secure Flash drives and their content.*

Password authentication is host dependent, complex, and susceptible to hacking attacks. Biometrics are expensive and unreliable. Flash Padlock is a s*elf-secured and cross platform* USB Flash drive that takes a new approach to drive security. Flash Padlocks strike the optimal balance between usability, security, and price.

Flash Padlocks are developed and produced by Corsair Memory (www.corsair.com) based on licensed DataLock™ technology from ClevX, LLC (www.clevx.com).

5 APPENDIX: AUTHENTICATION COMPARISON TABLE

Feature	Flash Padlock	Password	Biometric
Locking principle	Electromechanical - the UFD is inaccessible until the correct PIN combination is entered on the device itself	Encrypted private zones accessed by password - authentication from host	Encrypted private zones accessed by finger print authentication with password backup
Requires Media Partitioning	No	Yes	Yes
Host exchanged password	No	Yes	Yes*
Detectable by host	Only when unlocked	At all times	At all times
Device locked by default	Yes	No	No
Requires pre-configuration	No	Yes	Yes
Functions supplied by host	None	Yes	Yes
Offline operation	Yes	No	No
Host/OS independence	Yes	No	No
Vulnerability to hacking from host	None	Possible	Possible
Security profile reconfiguration	Optional	Yes	Yes
Reliability	High	High	Medium
User must remember	Short PIN	Password	Backup Password
Reliability depends on password length and complexity	No	Yes	Yes **
Vulnerability to password grabbing	No	Yes	No
Vulnerability to off-line password guessing	No	Yes	Yes*
Impact on price	Minor	Minor	Substantial

* Vulnerability is present via the password backup mechanism

** User must remember backup password