Online Companion - Flash Padlock with Password Management

White Paper

April 2007

Prepared by ClevX, LLC

1 INTRODUCTION

The Internet provides access to a vast array of content, services, and users around the globe; it is also a potential threat to you, your data, and your computer.

This article describes some common techniques used by Internet fraudsters to access your personal and confidential information. Also discussed are some precautionary measures that can lower your vulnerability to these threats.

A Flash Padlock™ USB Flash drive equipped with KeePass and Firefox portable applications can help manage passwords and stave off phishing attacks. This integrated solution creates a solution not provided by traditional means.

1. ***Flash Padlock***[1] – is a self-secured, host-independent USB flash drive with a hardware- authentication mechanism[2]. Flash Padlock drives use a PIN to lock/unlock your personal information.
2. ***KeePass*** portable password manager – for individuals with the highest security standards. This utility has been highly recommended by security experts.
3. ***Mozilla Firefox*** portable browser – with its built-in ability to remember passwords can automate the login process for recognized sites. It contains some added benefits when combined with a Flash Padlock drive.

[1] Flash Padlocks are developed and produced by Corsair Memory (www.corsairmemory.com) based on licensed technology from ClevX, LLC (www.clevx.com)

[2] US and Foreign Patents Pending

2 PHISHING AND IDENTITY THEFT

According to PC World Canada, Phishing and Identity theft are considered two of the biggest Internet threats of 2007. Phishing is the criminal act of attempting to fraudulently acquire confidential information from an Internet user. Here are some commonly used methods.

2.1 URL Obfuscation

This phishing method uses obfuscation to hide the fraudulent site's location. The trick is to get someone to view a website unintentionally by tempting them with something they are familiar with. Tricks are based on how URL addresses get resolved.

One example might be www.mybank.com@mibank.com. You think you are about to view mybank.com, but unintentionally end up at mibank.com.

2.2 Phishing by Email

Phishing by email is very common. An email *looks* like it's from a familiar and trusted source. It may say something like there is a "problem" with your bank account and request that you “validate” or "confirm" your account information.

The link provided within the email appears to be the real thing but, in reality, it's a fake. By attempting to “confirm” the bank's records, a person ends up providing account information to somebody that is more than happy to drain your balance.

2.3 Typo-squatting

Typo-squatting is another phishing trick in which a fake site resides at a web address resembling the real one. The hope is that a fast-typing customer will land there unaware of their typo. For example, 'www.amazom.com' instead of 'www.amazon.com' or 'www.mybqnk.com' instead of 'www.mybank.com'.

2.4 Weak Passwords

People tend to use the same password for multiple accounts which, unfortunately, are also usually short and easy to remember. A scammer can exploit this tendency by providing your login and password to a number of different banks, on-line brokers, etc. A successful hit may result in those accounts being drained as well. Information gained from a successful hit can be used to apply for credit cards in your name.

3 SIMPLE MEASURES TO STAY SAFE

- **Do NOT reply to email or pop-ups that ask for personal or financial information**. Don’t click on any links or attachments. As a matter of policy, banks and legitimate companies will not ask for information via email.
- **Use tools to maintain genuine login information.** Use Mozilla Firefox bookmarks in order to access your sites and automatically fill username / password for you. For enhanced security and extended features, use a specialized password utility such as KeePass.
- **Make your login information portable.** Carry applications together with data on your ***Flash Padlock USB Flash Drive***. This will allow you to access your on-line accounts from any computer securely.
- **Use different password for each account.** Try to make your password difficult to guess. Use appropriate tools to generate, store, and keep track of strong passwords.

4 FLASH PADLOCK

Flash Padlock is a *self-secured, platform independent* USB Flash Drive with a *hardware-authentication mechanism*. When locked, a Flash Padlock is invisible to its host; when unlocked, it acts as a standard USB Flash drive.

Authentication is based on recognition of a PIN entered using the on-board keypad. A correct PIN activates 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. The drive will automatically lock itself when unplugged or the host shuts down.

Flash Padlock drives represent both usability *and* privacy.

- **Ease of Use.** The Flash Padlock usage model is intuitive and resembles that of debit cards and ATM machines. The user remembers a short PIN as opposed to a long and complex password. There is no need for extraneous drive partitioning and configuration. The drive provides a single partition that utilizes the entire media.
- **True Host and Operating System Independence.** Since authentication does not depend on host related functions, it works equally well with all operating systems that support the USB Mass Storage Class. In other words, it works equally well on Windows, Mac OS, Linux, and even office equipment.
- **Authentication is self contained.** No special software installation is required. In fact, the host computer is unaware of the authentication process. Flash Padlock provides complete PIN management.
- **Immune to host-originated attacks.** Since a locked Flash Padlock provides no communication channel, it is immune to host originated hacking attempts.

5 THE PERFECT MEDIA FOR PORTABLE APPLICATIONS

An increasing number of people work with multiple computers at home, at the office, at Internet cafes, and while traveling.

A portable application is a computer program (see examples, at www.portableapps.com) that you can carry with you on a portable drive such as Flash Padlock and use on any computer. When your Flash Padlock is plugged in, you can access your software and personal data as you would on your own PC. And, when you unplug the device, none of your activity is left behind.

Flash Padlock provides a unified authentication mechanism for *all* portable applications contained within. Applications and data are inaccessible when the device is unattended, lost, or stolen. You can securely carry your bookmarks, passwords, and documents along with their associated applications. A single PIN is used to access them all.

KeePass (http://www.keepass.info) is a free, open-source password manager that helps you manage Web addresses, passwords, and other sensitive information securely. The database is encrypted using the best and most secure encryption algorithms.

Packaged as a portable application, you can carry all your passwords with you. Using Flash Padlock authentication and the KeePass Key-File feature, a single PIN grants access to all your passwords.

KeePass Portable Web site: http://portableapps.com/apps/utilities/keepass_portable

Mozilla Firefox (http://www.mozilla.com/en-US/Firefox/) is a fast, full-featured web browser that's easy to use. It has lots of great features including the ability to remember login information and automatically access on-line accounts. Firefox Portable leaves no traces of your browsing activity behind: all the following items are retained on your Corsair Flash Padlock:

- Passwords
- Browsing history
- Bookmarks
- Plugins

You can carry your browsing environment wherever you go.

Mozilla Firefox Portable Web site: http://portableapps.com/apps/internet/Firefox_portable

Appendix A – KeePass

KeePass can be installed as part of the PortableApps launchpad. More information about this can be found on the PortableApps home page (http://portableapps.com). The downloads below are from the PortableApps website, but the following tutorial is focused on KeePass installation and its use without the launchpad.

For general KeePass guidance and password management, please use KeePass Help or the KeePass Help Center at http://keepass.info/help/base/index.html.

At the time this paper was written, KeePass is at release 1.07.

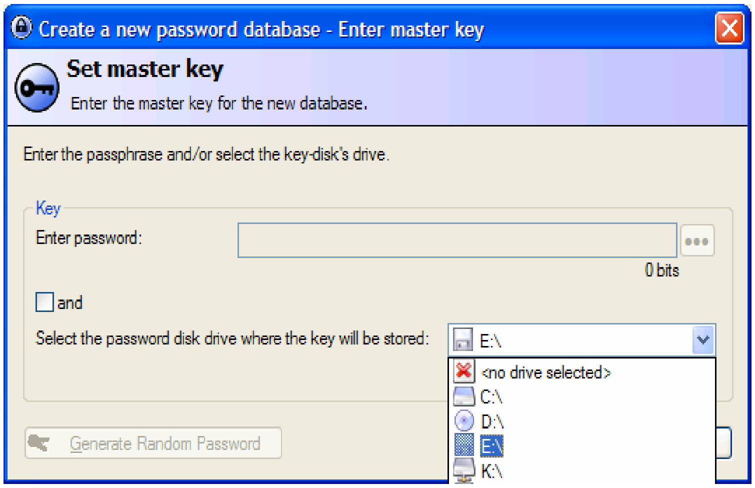
Downloading and Installing

1. Connect an unlocked Flash Padlock to an available USB port.
2. Download "KeePass_Portable_1.07.paf.exe" to Flash Padlock from the following link:

   http://portableapps.com/apps/utilities/keepass_portable
3. Run "KeePass_Portable_1.07.paf.exe" and select the Flash Padlock drive for installation. You should end up with a "KeePassPortable" directory at the root level of your Flash Padlock.
4. You may now delete "KeePass_Portable_1.07.paf.exe."

Creating a new Password Database

1. Activate KeePass by going to the KeePassProtable directory on your Flash Padlock and double-click the KeePassPortable executable (🔒).
2. Click on the "New" 📄 icon or select "File/New" from the menu.
3. KeePass presents the "Set Master Key" form below:



Create a new password database - Enter master key

Set master key

Enter the master key for the new database.

Enter the passphrase and/or select the key-disk's drive.

Key

Enter password:

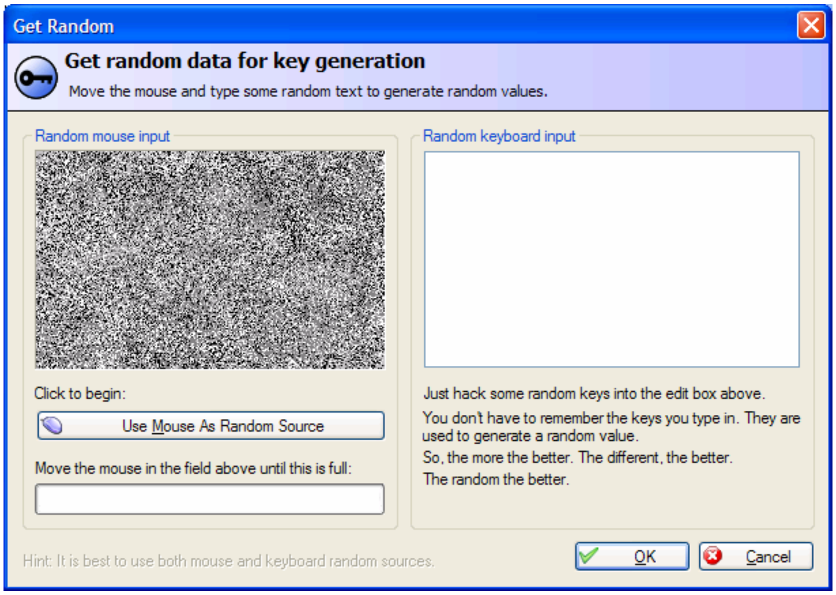
0 bits

□ and

Select the password disk drive where the key will be stored: E:\

Since authentication is provided by your Flash Padlock PIN, a master password is not required. We will use the KeePass key file feature as a source for encryption.

4. Select your Flash Padlock drive from the drop-down menu (drive E: in this case).
5. Click OK.
6. You will now have to generate a random key using the form shown below:



Move the mouse and type some random text to generate random values.

Move the mouse in the field above until this is full:

Just hack some random keys into the edit box above.

You don't have to remember the keys you type in. They are used to generate a random value.

So, the more the better. The different, the better.

The random the better.

Hint: It is best to use both mouse and keyboard random sources.

7. Click "Use Mouse As Random Source."
8. Move your mouse over the dot field until the progress bar registers full.
9. Click OK
10. From the main form, click the save icon 💾 or select "File/Save" from the menu.
11. Save the newly create database file to the KeePassPortable directory (E:\KeePassPortable in this example).
12. Exit KeePass.

Note: creating a new database results in a file called "pwsafe.key" stored in the root folder of your drive. **Do not to remove this file! Without it, your database cannot be accessed.**

Automating KeePass Activation

To open your password database automatically when KeePassPortable is run,

1. Create a batch file that contains the following line:

```
start /B \KeePassPortable\KeePassPortable.exe "\KeePassPortable\database.kdb" -keyfile:pwsafe.key
```

2. Save it as "KeePass.bat" at the root level (E:\).

Double-clicking KeePass.bat will allow you to open and load your passwords from any computer independently of drive assignment.

Note: Always remember to exit KeePass **before** disconnecting your Flash Padlock drive.

Appendix B – Mozilla Firefox Portable

Downloading and Installing Mozilla Firefox Portable

At the time this paper was written, Firefox is at release 2.0.0.3.

1. Connect an unlocked Flash Padlock to an available USB port.
2. Download “Firefox_Portable_2.0.0.3_en-us.paf.exe” to Flash Padlock from the following link:

   http://portableapps.com/apps/internet/firefox_portable
3. Run “Firefox_Portable_2.0.0.3_en-us.paf.exe” and select the Flash Padlock drive for installation.. You should end up with a “FirefoxPortable” directory.
4. If you are not using the launchpad, you can move FirefoxPortable.exe from the FirefoxPortable directory to the root directory to make it more convenient to access.
5. You may now delete “Firefox_Portable_2.0.0.3_en-us.paf.exe.”

Firefox Help contains information about its ability to remember web links and passwords. All Firefox activity is now stored on your Flash Padlock. No traces will be left behind.