



ITIS e-Newsletter

Issue 7

OneLock: Prevent data leakage resulting from USB lost

Author: Prof David Cheung
Center for E-Commerce Infrastructure Development
Department of Computer Science
The University of Hong Kong

Abstract

In this article, Professor David Cheung, Director of the Center for E-Commerce Infrastructure Development (CECID), shares his research team's recent novel technology – OneLock – a separate keys cryptosystem which strengthens data protection on any off-the-shelf portable storage device like USB flash drive. OneLock is designed to offer a proved, practical and powerful solution to combat data leakage. It protects encrypted data in USB storage beyond a single password. It locks encrypted data in USB storage with a password, as well as confines access to designated computers to improve data security. One of the remarkable merits of OneLock is in the scenario when a USB storage is lost or being stolen, together with the password also being cracked. In such case the data in the lost USB storage still could not be accessed and viewed by unauthorized user without the designated computer.

Data Leakage Threat

The occurrence of many personal data leakage incidents has caused alarming concern on data security issue in recent years. A handy USB storage device can conveniently carry hundreds of gigabytes of information. For instance, a 16GB USB memory stick can carry 10,000 files of 100-pages business reports, contact information of a whole yellow page telephone directory, 10,000 patients' full medical records, or a week's non-stop voice recordings. However, data stored in USB device usually is not well-protected.

Data Encryption

Encryption is one of the common effective techniques used to protect data and enforce confidentiality. It is a process of scrambling and transforming information using mathematical / cryptographic algorithm to make it unreadable. To make the encrypted information readable again, one needs to decrypt the content with a key – a chunk of code (e.g. r5w0c1su2a3b42s3) that determines the functional output of the cryptographic algorithm.

Among all of the existing methods, AES (Advanced Encryption Standard) encryption is the highest acclaimed standard and is adopted by many governments to protect top secret level documents. For example, a 128-bit AES encryption gives a total of 3.4×10^{38} possible combinations, with a key length of 128-bit. Assuming you have a super computer, it will still take more than 100 trillion years to crack the key, making it extremely hard, if not impossible. A little downside is that the key is also difficult to be remembered, needless to say for an even higher power 256-bit AES encryption. So a workaround is to store the key somewhere and the data owner could create his/her password to protect the container.

Shortcoming of Password Protection

In general, the more cryptic and longer the password is, the harder it is for hackers to crack. Yet, passwords created by humans are often too short or too easy to be predicted. According to a statistical report¹ on password usage pattern by Acuentix that focuses on web application security, password selection is usually weak. Out of the 10,000 leaked Hotmail passwords, 42% of the users used

passwords containing only characters from 'a' to 'z' (e.g. iloveyou), and 19% used passwords involving numbers '0' to '9' only (e.g. 123456). In such cases, the power of data protection is highly reduced.

Data Protection Beyond Password

In view of the fact that password only provides limited protection, CECID has researched and developed a novel applied technology – OneLock – to enhance data security beyond a single password. Basically, the encrypted data in USB storage is protected with a password as usual. In addition, data access is confined to designated computers to improve data security. That is, both protection factors: (1) password; and (2) the designated computer will be required to recover the key for decryption. In contrast to other common authentication mechanisms, OneLock does not require specialized hardware (e.g. fingerprint USB drive), nor require user to bring an extra gadget (e.g. a security token). It can be applied to all off-the-shelf USB storage device while staying as easy-to-use as possible.

How does OneLock Work to Achieve Data Protection?

First of all, data in the USB storage device is protected with strong 256-bit AES encryption. Unlike common encryption USB storage, in OneLock, the encrypted key will not be stored inside the USB storage. This separation of storage of encrypted content with encryption key is commonly known as "separation of key", which could effectively reduce the risk of losing both the encrypted sensitive information and the encryption key at the same time.

To illustrate the merit, an analogy will be a vault lock. The traditional password-based encrypted storage resembles a vault with a combination lock. The password protecting the encryption key acts like the security code for the lock. When the security code is matched, the confidential information inside the vault will be accessible. The security code can be cracked sooner or later by trying out all the different combinations.

A double lock system is implemented in OneLock to enhance the security of the vault. To retrieve the encrypted content in the USB storage, two protection components will be required at the same time to unlock the vault: (1) the security code (i.e. password), and (2) a physical key (i.e. the designated computer).

Case Scenario

In practice, OneLock allows user to encrypt a USB drive and restricts access with a password as usual.

In normal cases, i.e. scenario 1 in figure 1, when a user connects the encrypted USB drive to the designated computer, the user will be prompted for password, and upon successfully entering it, the encrypted content will be accessible.

In case the USB storage is lost or being stolen, even when someone pick up the USB drive and crack the password, the encrypted content. (i.e. scenario 2 in figure 1) still cannot be read without the designated computer,

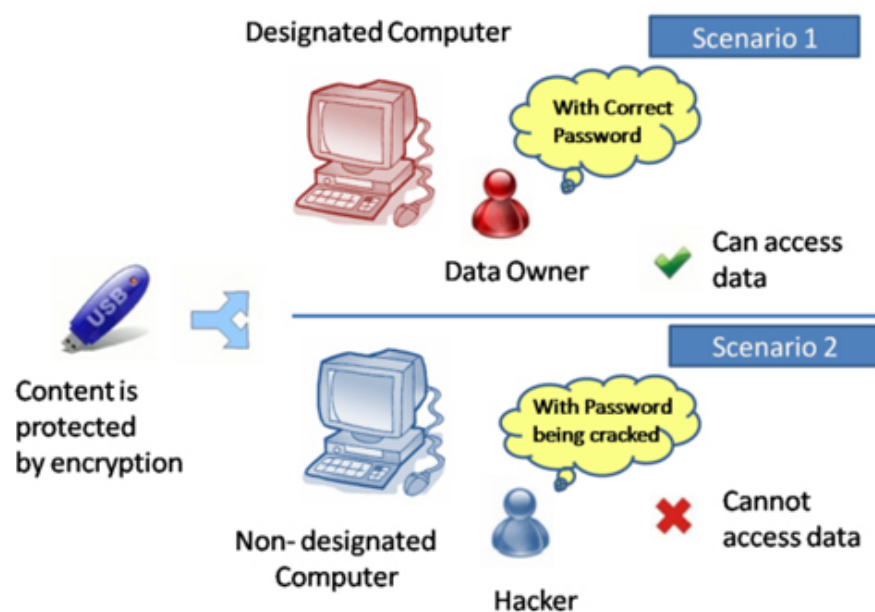


Figure 1: Illustration on Data Protection with OneLock

To get a taste of how it really works and safeguard your USB data, check out OneLock at <http://community.cecid.hku.hk/index.php/product/onelock/>.

¹ <http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/>

[Print this article](#)



[Back](#)