Implicit Hardware Binding for Enhanced Security over Web Applications

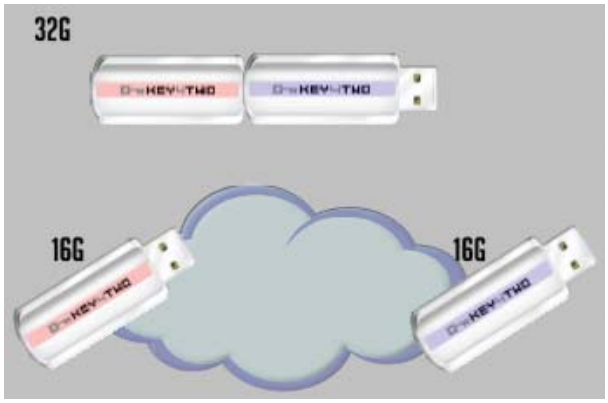
Zhibin Lei, Hong Kong Applied Science & Technology Research Institute

Authentication and hardware-based security build the fundamental infrastructure for Open Web Platform. Several forms of secure tokens (from smartcards to secure micro-SD) have been rapidly maturing and different services can be provided by those trusted elements (storage, cryptographic operations, secure operations, authentication etc.). Nevertheless, combined issue of security and usability have not been adequately addressed in many web based applications (for example, social network, content sharing, and work group activities) where sharing, exchange, or cross-verification is a prerequisite.

We introduce an implicit hardware binding technology which can both enforce the security and enhance the usability for sharing based web applications. Security technology shall not be a hindering factor in Open Web Platform, but rather an enabling technology to help promote the usage, ease the concern, and reduce the complexity in using the cryptography based security in web applications.

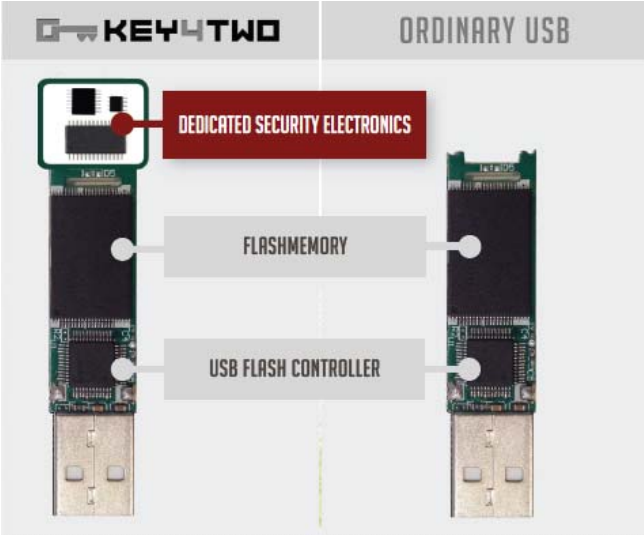
1. What is “implicit hardware binding”?

Implicit binding is a way to establish relationship (for example, “.doc” postfix would invoke Microsoft word program). Two or more hardware devices can also be bound equally (e.g. peer-to-peer) or unequally (e.g. client and server). When an implicit binding is established among devices such as secure USB disks, it can render great benefits such as security protection and connectivity establishment – and all these functions can be performed in the background. It is one form of machine-to-machine (M2M) mechanism. Devices themselves make the connection and find remote data/content and securely communicate between the ones that meet the pre-set requirements. For end users, instead of going to the network or Internet to get the content, it actually comes to them automatically and safely.



One way to support implicit hardware binding is to add a secure module into the existing hardware devices and establish prior binding or matching of the hardware keys between these devices at the manufacturing floor. It is also possible to match devices on the fly by invoking the hardware binding API. Such an API can be part of the Open Web Platform.

2. Implementation of implicit hardware binding



KU-Disk (Keyed-USB flash storage) is one implementation of implicit hardware binding in USB devices. It is the normal USB storage plus a hard identity key and additional electronics for encryption, security and networking control – so the identity key and security management are “hardened” to the hardware that has little exposure to external environments. While almost all existing computer security protection enforced by software or PC environment are fallible to vicious attackers, keyed USB disks provide unprecedented level of data protection, user privacy and anti-virus assurance.

Through a series of keyed USB-like smart devices, user can manage any data with security mechanism enforced by the hardware in the devices. The user can work on, share, and restore his data in local USB, PC, private clouds, public clouds, and social networks all with hardware level of security protection.

There are many considerations from security point of view. But from an end user’s point of view, he cares mostly about two things: the content/data/file and the computer programs which operate on them. With implicit hardware binding, the multi-dimensional security technology requirements and convenience in usage are built into one unit: a minute device with storage, networking, security, and personal identity key for computer programs (locally or remotely) to securely operate the files on it.

3. Typical usage scenario: Key-4-Two Persons | Places | Devices | Objects

KU-Disk can be built for password protected USB with encrypted cloud backup over private or public cloud storage. Key4Two are prior bound KU-disks for file sharing between home and office, or two persons (data recover or deletion can be achieved after loss of device or forgotten password).

Security risks arise when people exchange information or move data around. Key4Two embodies a trust relationship in a pair of portable smart USB flashes with on-board security electronics. Users can now rest assured about the security of files on his and the paired devices. Even the loss of the device itself is not a concern because a secured backup copy is always there on the cloud, and the KU-Disk will not be functional to unauthorized parties.

Key4Two is plug-n-play with application GUI supporting drag and drop. All files dropped in the app are automatically protected with hardware encryption module. All the encrypted files are synchronized with the cloud storage and backup copies made. All files on the cloud are accessible anywhere by either one of the paired devices (or more pre-set peers). User can share files among “paired” persons on the cloud. The underlying process is automatically managed by the smart app on board and is transparent to the users. The app can recognize the computer that Key4Two is commonly used with. Password or other credentials will be asked if an unknown computer is detected.

Multiple devices can be bound to provide secured file sharing between a group of people, e.g. school (teacher--students), business (manager--staff, or peer-to-peers), content

delivery (artist--listeners). Users will find hardware binding attractive because it enables a new paradigm of data storage, content transfer and information sharing over secured and trusted platform. For example, it can be used for teacher-to-student learning platform, many-to-many community sharing, secure email, voice, or video communication, etc. It can extend enterprise security to home or public environment, or creates secure mobile environment to share. Real friends can securely share private photos or tweets while still maintain a public account open to all on the same social network (e.g. Facebook or Twitter). It helps to build valuable secure layers within current open social networks – should social networks be layered to start with?

4. Hardware binding for virtual machine and virtual program

Users can save a lot of software license expenses by moving to VM, and the operating cost is far lower as well. Centralized management of VM simplifies IT maintenance, audit, and security process, thus improves the availability, confidentiality and system integrity. For most end users, they cannot tell the difference between real machines and VMs. The great advantage with VMs is that users can use their machines anywhere with Internet connection. VMs can be shared or even co-operated by several parties, making collaboration between users much easier too.

While many current virtual desktop applications rely on password and software key management infrastructure, a virtual desktop solution enforced by secure hardware binding makes it easy for users to work securely over cloud environment without comprising the usability provided by dedicated hardware key and key network.

It provides unprecedented security for VMs for business and yet is convenient to end-users and easy to set up and maintain. The access control to the virtual machine is encrypted in the dedicated hardware on binding devices. The authentication is conducted automatically when user inserts the devices into any computer connected to the Internet. In case sensitive data is on the storage of the VM, the hardware key can be configured to enable AES-256 full-disk encryption.