Understanding Hardware-Based Software Security
Technical Overview
KEYLOK 2014

Summary

KEYLOK's® hardware-based security solutions protect your software applications from unauthorized use and duplication, thereby increasing revenues associated with software sales. Using dongles protects licensing revenue by enabling enforcement of product license agreements. Enforceable license models include time-based, features, modules, usage counts and pay-per-use. Security is transparent to your end-user once the hardware device is plugged in to the computer's USB, parallel or serial port.

Since dongle and software use is an 1:1 ratio (network dongles excepted), customers experience the convenience of installing the software on multiple machines without concern over breaching license agreements. Your customers can easily restore or reinstall copies of your software following frustrating events such as hard disk failures. These advantages provide customers with the flexibility they require while simultaneously preserving your revenue, protecting valuable IP and minimizing customer support.

How Do Dongles Actually Work?

KEYLOK dongles use a number of sophisticated techniques for verification of the device's presence. The KEYLOK dongle provides 112 bytes (5,120 bytes for Fortress) of field programmable READ/WRITE memory. No special programming adapters are required to program the hardware key memory.

- ✓ When an application is first attempting to communicate with the dongle, it is necessary to successfully complete an exchange of bytes between the host and the device that differs during each use (i.e.: using an active algorithm).
- ✓ If this sequence is properly executed, the device will return a customer unique 32-bit identification code that confirms that the dongle is installed on the computer.
- ✓ If an improper data exchange occurs, the security system returns to the host a random 32-bit code in place of the proper identification code.
- ✓ Upon successful completion of the authentication sequence, the host computer then sends a 48-bit customer unique password to the device to authorize memory READ operations.
- ✓ Memory WRITE operations require the successful transmission of yet another 48-bit customer unique password to the device. The WRITE password must be sent after transmission of the proper READ authorization sequence.
- ✓ If the dongle is sent the incorrect READ/WRITE password, then subsequent memory operations are ignored and random information is returned to the program.
- ✓ In summary, a total of 176 bits of customer unique codes must be known in order to alter the memory within the hardware key.

Up to fifty-six (56) separate 16-bit counters (values of 0-65535) can be independently maintained within KEYLOK2 and KEYLOK3 devices; 2,560 counters for standard Fortress memory. Counters are particularly useful for controlling demonstration copies of software, as well as pay-per-use software.

At the time of shipping, each device is programmed with both an identifier unique to each customer (and/or product line) and a unique serial number. This provides the capability to identify the specific device (and the specific end-user) for customers requiring this level of control.

Algorithms are used to perform secure remote memory modifications to the device. The Remote Update procedure involves the exchange of encrypted information between the software provider and their end-customer.

KEYLOK Fortress Products

KEYLOK has three product lines: KEYLOK2, KEYLOK3 and Fortress. The driverless Fortress product line provides enhanced security through its smartcard computing platform. The design of its integrated circuit chip provides a secure computing platform, complete with processor, I/O controller, operating system, memory and storage. The security features are built into the chip's operating system which has been designed to provide the highest levels of security currently available and is certified to international standards. The most advanced PHILIPS 16-bit smartcard chip used within Fortress has reached the highest grade in the global hi-tech sector of EAL 5+.

- ✓ The Fortress file system is organized similar to your typical microcomputer operating system. There is a root directory and sub directories. Each directory has its own level of security. The files stored on the device cannot be read directly. All access to the directory structure is provided by the smartcard operating system.
- ✓ Three types of files are supported: executable files, data files and key files. The data files can only be accessed by the executable files loaded onto the device. Key files contain the RSA key for encryption purposes.
- ✓ Fortress has built-in support for RSA, DES and TDES cryptographic algorithms, as well as SHA1, MD5 and MD2 hashing algorithms.

Fortress offers the ability to transfer executable code onto the device itself (CodeVault) and have it run in a completely separate and secure environment. This separation of code and hardware certification is a new and unique solution for software protection. Functions implemented in CodeVault can be implemented to utilize bi-directional data encryption.

CodeVault provides a complete computing platform that runs in parallel to the main application computer. With CodeVault, application algorithms and functions can be stored and run on the hardware device, without ever being loaded into the main computer memory. All data is exchanged through the USB port. This structural flexibility provides an extremely secure environment and unlimited possibilities for the protection of an application or data.

To learn more about KEYLOK's high-value, low-cost solutions to combat software piracy and enforce licensing, try our products for free. Simply request a free Evaluation Kit by visiting www.keylok.com.