JAVA DEVELOPER

By Stephen M. Curry

HOW-TO

An introduction to the Java Ring

Learn about the inner workings of this secure, durable, wearable Java-powered electronic token

JavaWorld | Apr 1, 1998 12:00 AM

This month's column is split into two parts. The first part, embodied in this article, offers the history of the *Java Ring* and the technology used to build it, as well as a brief discussion of the suitability of the iButton for security applications and other applications. The second part, demonstrates how to use the Java Card 2.0 API with the Java iButton and provides the reader with a very early look at how to design an application, download it, and then communicate with an application running on a Java Card.

It's in the details

The Java Ring is an extremely secure Java-powered electronic token with a continuously running, unalterable realtime clock and rugged packaging, suitable for many applications. The jewel of the Java Ring is the *Java iButton* -- a one-million transistor, single-chip trusted microcomputer with a powerful Java virtual machine (JVM) housed in a rugged and secure stainless-steel case. Designed to be fully compatible with the Java Card 2.0 standard (for more on Java Card 2.0, see last month's **Java Developer** column, "Understanding Java Card 2.0 ") the processor features a high-speed 1024-bit modular exponentiator for RSA encryption, large RAM and ROM memory capacity, and an unalterable realtime clock. The packaged module has only a single electrical contact and a ground return, conforming to the specifications of the Dallas Semiconductor 1-Wire bus. Lithium-backed non-volatile SRAM offers high read/write speed and unparalleled tamper resistance through near-instantaneous clearing of all memory when tempering is detected, a feature known as *rapid zeroization*. Data integrity and clock function are maintained for more than 10 years. The 16-millimeter diameter stainless steel enclosure accommodates the larger chip sizes needed for up to

128 kilobytes of high-speed nonvolatile static RAM. The small and extremely rugged packaging of the module allows it to attach to the accessory of your choice to match individual lifestyles, such as a key fob, wallet, watch, necklace, bracelet, or finger ring.

Historical background

In the summer of 1989, Dallas Semiconductor Corp. produced the first stainless-steel-encapsulated memory devices utilizing the Dallas Semiconductor 1-Wire communication protocol. By 1990, this protocol had been refined and employed in a variety of self-contained memory devices. Originally called "touch memory" devices, they were later renamed "iButtons." Packaged like batteries, iButtons have only a single active electrical contact on the top surface, with the stainless steel shell serving as ground.

Data can be read from or written to the memory serially through a simple and inexpensive RS232C serial port adapter, which also supplies the power required to perform the I/O. The iButton memory can be read or written with a momentary contact to the "Blue Dot" receptor provided by the adapter. When not connected to the serial port adapter, memory data is maintained in non-volatile random access memory (NVRAM) by a lifetime lithium energy supply that will maintain the memory content for at least 10 years. Unlike electrically erasable programmable read-only memory (EEPROM), the NVRAM iButton memory can be erased and rewritten as often as necessary without wearing out. It can also be erased or rewritten at the high speeds typical of complementary metal oxide semiconductor (CMOS) memory, without requiring the time-consuming programming of EEPROM.

Since their introduction, iButton memory devices have been deployed in vast quantities as rugged portable data carriers, often in harsh environmental conditions. Among the large-scale uses are as transit fare carriers in Istanbul, Turkey; as maintenance record carriers on the sides of Ryder trucks; and as mailbox identifiers inside the mail compartments of the U.S. Postal Service's outdoor mailboxes. They are worn as earrings by cows in Canada to hold vaccination records, and they are used by agricultural workers in many areas as rugged substitutes for timecards.

The iButton product line and its many applications are described at Dallas Semiconductor's iButton Web site, which is listed in the Resources section. Every iButton product is manufactured with a unique 8-byte serial number and carries a guarantee that no two parts will ever have the same number. Among the simplest iButtons are memory devices that can hold files and subdirectories and can be read and written like small floppy disks. In addition to these, there are iButtons with password-protected file areas for security applications, iButtons that count the number of times they have been rewritten for securing financial transactions, iButtons with temperature sensors, iButtons with continuously running date/time clocks, and even iButtons containing powerful microprocessors.

The postal security device

For over 10 years, Dallas Semiconductor also has been designing, making, and selling a line of highly secure microprocessors that are used in satellite TV descramblers, automatic teller machines, point-of-sale terminals, and other similar applications requiring cryptographic security and high resistance to attack by hackers. The U.S. Postal Service's (USPS) Information Based Indicia Program Postal Security Device Specification, intended to permit printing of valid U.S. postage on any PC, provided the first opportunity to combine two areas of expertise when a secure microprocessor was designed into an iButton.

The resulting product, named the *Crypto iButton*, combines high processor performance, high-speed cryptographic primitives, and exceptional protection against physical and cryptographic attack. For example, the large integer modular exponentiation engine can perform 1024-bit modular exponentiations with a 1024-bit exponent in significantly less than a second. The ability to perform large integer modular exponentiations at high speed is central to RSA encryption, Diffie-Hellman key exchange, Digital Signature Standard (FIPS 186), and many other modern cryptographic operations.

An agreement between Dallas Semiconductor and RSA Data Security Inc. provides a paid-up license for anyone using the Crypto iButton to perform RSA encryption and digital signatures so that no further licensing of the RSA encryption technology is required. High security is afforded by the ability to erase the contents of NVRAM extremely quickly. This feature, rapid zeroization, is a requirement for high security devices that may be subjected to attacks by hackers. As a result of its high security, the Crypto iButton is expected to win the FIPS 140-1 security certification by the National Institute of Standards and Technology (NIST).

A special operating system was designed and stored in the ROM of the Crypto iButton to support cryptography and general-purpose financial transactions -- such as those required by the Postal Service program. While not a Java virtual machine, the E-Commerce firmware designed for this application had several points of similarity with Java, including an object-oriented design and a bytecode interpreter to interpret and execute Dallas Semiconductor's custom-designed E-Commerce Script Language. A compiler was also written to compile the high-level language representation of the Script Language to a bytecode form that could be interpreted by the E-Commerce VM. Although the E-Commerce firmware was intended primarily for the USPS application, the firmware supports a variety of general electronic commerce models that are suitable for many different applications. The E-Commerce firmware also supports cryptographic protocols for secure information exchange such as the Simple Key-Management for Internet Protocol (SKIP) developed by Sun Microsystems Inc. The E-Commerce iButton and the SDK for programming it are described in detail on the Crypto iButton home page (see Resources).

The Java connection

With experience designing the E-Commerce operating system and VM for the Crypto iButton hardware platform, the firmware design team at Dallas Semiconductor could readily appreciate the advantages of a new operating system for the Crypto iButton based on Java. With a Java iButton, a vast number of existing Java programmers could easily learn to write applets that could be compiled with the standard tools available from Sun Microsystems, loaded into the Java iButton, and run on demand to support a wide variety of financial applications. The Java Card 2.0 specification provided the opportunity to implement a useful version of the JVM and runtime environment with the limited resources available to a small processor.

Java Ring

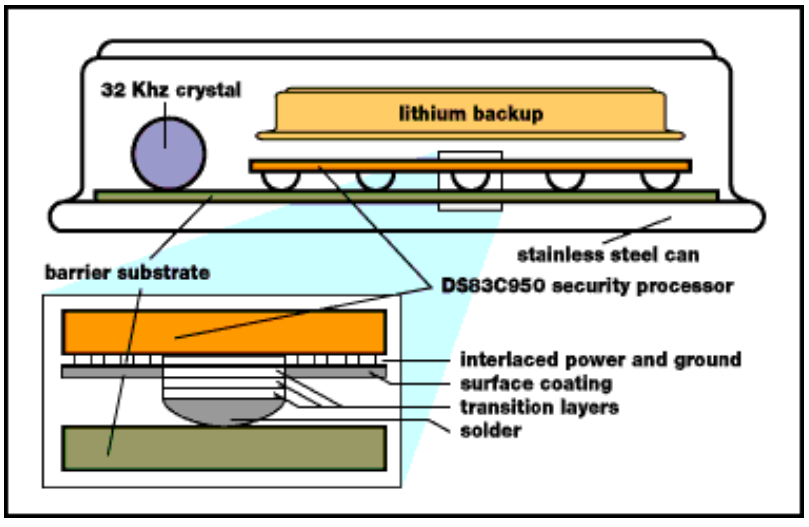
The Crypto iButton also provides an excellent hardware platform for executing Java because it utilizes NVRAM for program and data storage. With 6 kilobytes of existing NVRAM and the potential to expand the NVRAM capacity to as much as 128 kilobytes in the existing iButton form factor, the Crypto iButton can execute Java with a relatively large Java stack situated in NVRAM. This memory acts as conventional high-speed RAM when the processor is executing, and the lithium energy preserves the complete state of the machine while the Java Ring is disconnected from the reader. There is therefore no requirement to deal with persistent objects in a special way -- objects persist or not depending on their scope so the programmer has complete control over object persistence. As in standard Java, the Java iButton contains a garbage collector that collects any objects that are out of scope and recycles the memory for future use. Applets can be loaded and unloaded from the Java iButton as often as needed. All the applets currently loaded in a Java iButton are effectively executing at zero speed any time the iButton is not in contact with a Blue Dot receptor.

As the Java Card 2.0 specification was proposed, Dallas Semiconductor became a JavaSoft licensee. The agreement called for the development of a Java Card 2.0 implementation and also for the design of "plus portions" that take advantage of the unique capabilities afforded by the Crypto iButtons NVRAM, such as the ability to support a true Java stack and garbage collection. With the addition of the continuously running lithium-powered time-of-day clock and the high-speed, large-integer modular exponentiation engine, the Java iButton implementation of Java Card 2.0 with plus portions promises an exciting new feature set for advanced Java Card applications.

Keeping your money safe

The Crypto iButton hardware platform offers a unique set of special features expressly designed to prevent private keys and other confidential information from becoming available to hackers. Figure 1 shows a detail of the internal construction of the Crypto iButton. The silicon die containing the processor, ROM, and NVRAM memory is metallurgically bonded to the barrier substrate through which all electrical contacts are made. This barrier substrate and the triple-layer metal construction techniques employed in the silicon fabrication effectively deny access to the data stored in the NVRAM. If any attempt is made to penetrate these barriers, the NVRAM data is immediately erased. This construction technique and the use of NVRAM for the storage of private keys and other confidential data provides a much higher degree of data security than that afforded by EEPROM memory. The fact that the communication path between the Crypto iButton and the outside world is limited to a single data line provides additional security against hardware attacks by limiting the range of signals accessible to the hacker.

In addition, the processor itself is driven by an unstabilized ring oscillator operating over a range of 10 to 20 megahertz, so that the clock frequency of the processor is not constant and cannot be determined by external means. This differs from the design of alternative devices in which the processor clock signal is injected by the reader and is therefore exactly determined by the host processor. External control of the clock provides a valuable tool to hackers, since they can repetitively cycle such a processor to the same point in its execution simply by applying the same number of clock cycles. Control of the clock also affords a means to induce a calculation error and thereby obtain information that can ultimately reveal secret encryption keys. A 32-kilohertz crystal oscillator is used in the Java iButton to operate the time-of-day clock at a constant and well-controlled frequency that is independent of the processor clock.



Conclusion

Dallas Semiconductor has produced more than 20 million physically-secure memories and computers with hard-shell packaging optimized for personal possession. The Java iButton, therefore, is simply the latest and most complex descendant of a long line of products that have proven themselves to be highly successful in the marketplace. With its stainless steel armor, it

offers the most durable packaging for a class of products that likely will suffer heavy use and abuse as personal possessions. The iButton form factor permits attachment to a wide variety of personal accessories that includes rings, watchbands, keyfobs, wallets, bracelets, and necklaces, so the user can select a variation that suits his or her lifestyle.