By Stephen M. Curry

HOW-TO

An introduction to the Java Ring

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

JavaWorld | Apr 1, 1998 12:00 AM

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

It's in the details

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

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

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

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

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

provided the first opportunity to combine two areas of expertise when a secure microp
designed into an iButton.

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

An agreement between Dallas Semiconductor and RSA Data Security Inc. provides a pai
for anyone using the Crypto iButton to perform RSA encryption and digital signatures s
further licensing of the RSA encryption technology is required. High security is afforded
ability to erase the contents of NVRAM extremely quickly. This feature, rapid zeroization
requirement for high security devices that may be subjected to attacks by hackers. As a
high security, the Crypto iButton is expected to win the FIPS 140-1 security certification
National Institute of Standards and Technology (NIST).

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

The Java connection

and run on demand to support a wide variety of financial applications. The Java Card 2. specification provided the opportunity to implement a useful version of the JVM and ru environment with the limited resources available to a small processor.

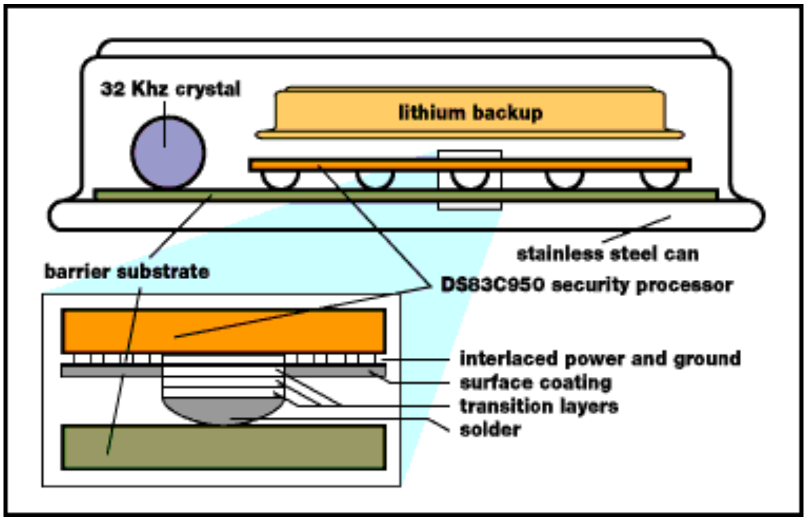
Java Ring

The Crypto iButton also provides an excellent hardware platform for executing Java bec utilizes NVRAM for program and data storage. With 6 kilobytes of existing NVRAM and t to expand the NVRAM capacity to as much as 128 kilobytes in the existing iButton form Crypto iButton can execute Java with a relatively large Java stack situated in NVRAM. Th acts as conventional high-speed RAM when the processor is executing, and the lithium preserves the complete state of the machine while the Java Ring is disconnected from t There is therefore no requirement to deal with persistent objects in a special way -- obj or not depending on their scope so the programmer has complete control over object p As in standard Java, the Java iButton contains a garbage collector that collects any obje out of scope and recycles the memory for future use. Applets can be loaded and unload Java iButton as often as needed. All the applets currently loaded in a Java iButton are ef 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 JavaSo The agreement called for the development of a Java Card 2.0 implementation and also design of "plus portions" that take advantage of the unique capabilities afforded by the iButtons NVRAM, such as the ability to support a true Java stack and garbage collection addition of the continuously running lithium-powered time-of-day clock and the high-s

which all electrical contacts are made. This barrier substrate and the triple-layer metal
techniques employed in the silicon fabrication effectively deny access to the data store
NVRAM. If any attempt is made to penetrate these barriers, the NVRAM data is immedia
This construction technique and the use of NVRAM for the storage of private keys and c
confidential data provides a much higher degree of data security than that afforded by
memory. The fact that the communication path between the Crypto iButton and the out
is limited to a single data line provides additional security against hardware attacks by
range of signals accessible to the hacker.

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



Conclusion

Dallas Semiconductor has produced more than 20 million physically-secure memories a
computers with hard-shell packaging optimized for personal possession. The Java iButt

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.