JAVA RING

A SEMINAR REPORT

Submitted by

RAVI PRAKASH

in partial fulfillment of requirement of the Degree of

Bachelor of Technology (B.Tech)

in

COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF ENGINEERING

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

KOCHI- 682022

AUGUST 2008

DIVISION OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF ENGINEERING

COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

KOCHI-682022

Certificate

Certified that this is a bonafide record of the seminar entitled

JAVA RING

Presented by the following student

RAVI PRAKASH

of the VII semester, Computer Science and Engineering in the year 2008 in partial fulfillment of the requirements in the award of Degree of Bachelor of Technology in Computer Science and Engineering of Cochin University of Science and Technology.

Mr. Sudeep Elayidom
Seminar Guide

Dr. David Peter S.
Head of the Division

Date:

Acknowledgement

Many people have contributed to the success of this. Although a single sentence hardly suffices, I would like to thank Almighty God for blessing us with His grace. I extend my sincere and heart felt thanks to **Dr. David Peter, Head of Department,** Computer Science and Engineering, for providing us the right ambience for carrying out this work. I am profoundly indebted to my seminar guide, **Mr. Sudeep Elayidom** for innumerable acts of timely advice, encouragement and I sincerely express my gratitude to her.

I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Science and Engineering, CUSAT for their cooperation and support.

Last but not the least, I thank all others, and especially my classmates who in one way or another helped me in the successful completion of this work.

RAVI PRAKSH

ABSTRACT

A Java Ring is a finger ring that contains a small microprocessor with built-in capabilities for the user, a sort of smart card that is wearable on a finger. Sun Microsystems's Java Ring was introduced at their Java One Conference in 1998 and, instead of a gemstone, contained an inexpensive microprocessor in a stainless-steel iButton running a Java virtual machine and preloaded with applets (little application programs). The rings were built by Dallas Semiconductor. Workstations at the conference had "ring readers" installed on them that downloaded information about the user from the conference registration system. This information was then used to enable a number of personalized services. For example, a robotic machine made coffee according to user preferences, which it downloaded when they snapped the ring into another "ring reader."

The Java Ring is an extremely secure Java-powered electronic token with a continuously running, unalterable real-time 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.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

The Java Ring is a stainless-steel ring, 16-millimeters (0.6 inches) in diameter that houses a 1-million-transistor processor, called an iButton. The ring has 134 KB of RAM, 32 KB of ROM, a real-time clock and a Java virtual machine, which is a piece of software that recognizes the Java language and translates it for the user's computer system.

At Celebration School, the rings have been programmed to store electronic cash to pay for lunches, automatically unlock doors, take attendance, store a student's medical information and allow students to check out books. All of this information is stored on the ring's iButton. Students simply press the signet of their Java Ring against the Blue Dot receptor, and the system connected to the receptor performs the function that the applet instructs it to. In the future, the Java Ring may start your car.
Mobile computing is beginning to break the chains that tie us to our desks, but many of today's mobile devices can still be a bit awkward to carry around. In the next age of computing, we will see an explosion of computer parts across our bodies, rather than across our desktops. Digital jewelry, designed to supplement the personal computer, will be the evolution in digital technology that makes computer elements entirely compatible with the human form.

The Java Ring, first introduced at Java One Conference, has been tested at Celebration School, an innovative K-12 school just outside Orlando; FL.The rings given to students are programmed with Java applets that communicate with host applications on networked systems. Applets are small applications that are designed to be run within another application. The Java Ring is snapped into a reader, called a Blue Dot receptor, to allow communication between a host system and the Java Ring.

Figure 1: prototype of stainless steel java ring.

2. HISTORY

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 java ring was first introduced in the year 1998, in the java one conference .the ring was built by the Dalas semiconductor corporation.

2.1 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 speedis 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.

3. COMPONENTS

The main components of the java ring are following:-

- JAVA VIRTUAL MACHINE(JVM)
- 134KB OF RAM
- 32KB OF RAM
- REAL TIME CLOCK
- IBUTTOON
- BLUE DOT RECEPTOR

3.1. JAVA VIRUAL MACHINE

Java ring is programmed with java application program and applets ,that communicate with the host application on the networked system. applets are the small application that is designed to run on the another application system. The java virtual machine is the piece of software that recognizes the java language and translate the byte code ,which is used by the system which is connected to the java ring via ring reader.

At Celebration School, the rings have been programmed to store electronic cash to pay for lunches, automatically unlock doors, take attendance, store a student's medical information and allow students to check out books. All of this information is stored on the ring's iButton. Students simply press the signet of their Java Ring against the Blue Dot receptor, and the system connected to the receptor performs the function that the applet instructs it to. In the future, the Java Ring may start your car.

Mobile computing is beginning to break the chains that tie us to our desks, but many of today's mobile devices can still be a bit awkward to carry around. In the next age of computing, we will see an explosion of computer parts across our bodies, rather than across our desktops. Digital jewelry, designed to supplement the personal computer, will be the evolution in digital technology that makes computer elements entirely compatible with the human form.

3.2. RAM

Java ring contains 134kb of non-volatile random access memory. Program and data is stored in this non-volatile random access memory .This non-volatile random access memory offers high read/write speed and also provides temper resistance through instantaneous clearing of all memory when tempering is detected. this process is called rapid zeroization.The NVRAM iButton memory can be erased or rewritten as often as necessary without wearing out. High security is offered by the ability to erase the content of NVRAM extremely quickly.

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.

3.3. ROM

The java ring contains 32kb of ROM .A special kind of operating system called E-Commerce operating system which is based on java and JVM is stored in the ROM.This operating system handles all the operation which is happening in the iButton. It is stored in ROM because it is not supposed to be altered by the user. 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.

3.4. REAL TIME CLOCK

In the java ring real time clock gives the exact time of the day. The real time clock continuously running up to more than 10 years by the energy provided the lithium backup.

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. 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.

3.5. IButton

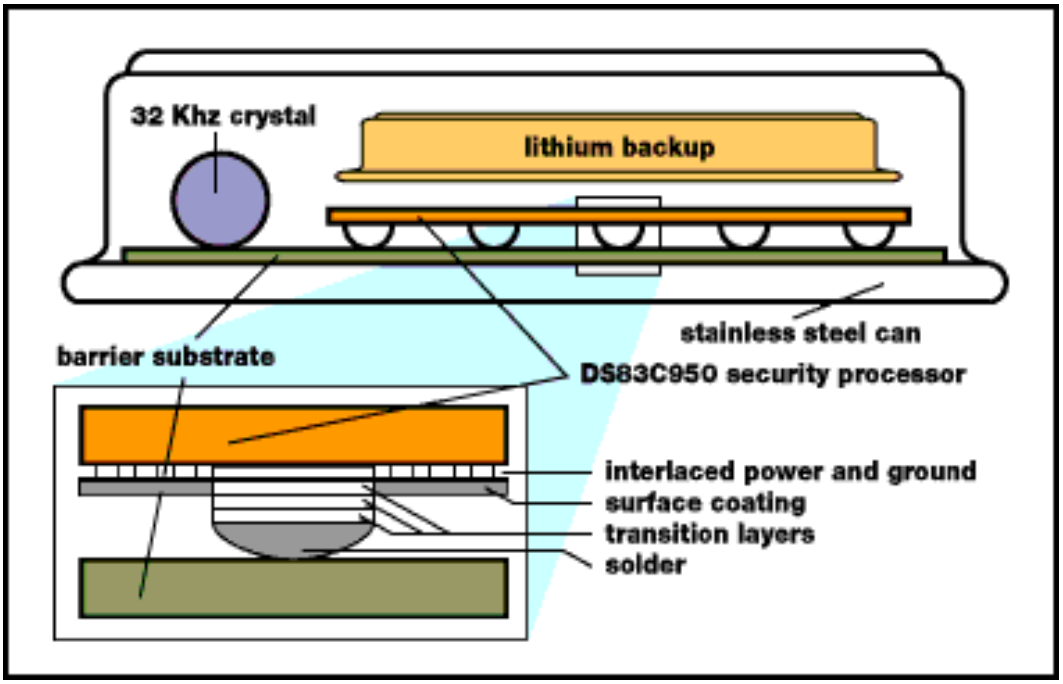

Figure 3.5.1: structure of the iButton

The jewel of the java ring is the java iButton .It contains the one million transistor processor single chip trusted microprocessor with powerful java virtual machine(JVM) housed in rugged and secure stainless steel case. 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.

It is originally called touch memory devices they were later renamed as “iButtons packaged” like batteries. IButton have only a single active electrical contact on the top surface and with the stainless steel shell serving as ground. Every iButton product is manufactured with unique 8 byte serial number and carries a guaranty that no two IButtons have same number. Among the simplest iButton are memory devices which can hold files and directories that can be read and written like small floppy disks. An iButton is a microchip similar to those used in smart card but housed in a round stainless steel button of 17.35mm x 3.1mm - 5.89mm in size (depending on the function). The iButton was invented and is still manufactured

exclusively by Dallas Semiconductor mainly for applications in harsh and demanding environments.

Like a smart card, an iButton does not have an internal power source. It requires connection to a reader (known as a Blue Dot Receptor) in order to be supplied with power and to receive input and send output. Unlike some smart cards, there are currently no contactless iButtons: they require physical contact with a reader to function.

There are iButtons that measure temperature (for food storage and transport); have an electronic ID (for physical access to buildings); and store e-cash (for purchases both in stores and via the web). For e-commerce applications, the iButton can support Java Card 2.0/OpenCard standards in addition to proprietary software.

iButtons have an advantage over conventional smart cards in term of durability and longevity. The stainless steel casing gives iButton a far greater ability to survive in a range of temperatures -- all versions are functional from -40 C to +70 C -- and in a much harsher range of environments (such as exposure to salt water and long term exposure to physical impacts) than the plastic smart card. For e-commerce and personal ID usage, iButtons can be mounted on a range of personal accessories: watch, ring, key chain, or dog tag.

Among the major successes for the iButton have been its use in Turkey as an e-purse for the mass transit system; in Argentina and Brazil for parking meters; and in the United States as Blue Mailbox attachments that improve postal efficiency.

Figures 3.5.2: different types of iButtons available in the market

3.6. BLUE DOT RECEPTOR

The read/write operation in the java ring is done by the blue dot receptor provided by the RS232 serial port adapter. The **DS1402D-DR8** is a part of the DS1402 series. It is a 1-Wire network cable designed to connect any serial or USB **1-Wire** port adapter that has a **RJ11 jack** with up to **two iButtons** simultaneously. The DS1402D-DR8 Blue Dot receptor cable can touch any iButton for reading, but can only retain the F5 version iButtons.

Key Features:-

- Coiled cable for connecting iButtons to 1-Wire networks (8 ft when fully extended).
- Convenient, off-the-shelf connectivity.
- For momentary (F3/F5 MicroCan) or dwelled contact (F5 MicroCan only).
- Adhesive pad for mounting on objects.
- Supports for up to two iButtons at once.
- Can be used with any EDS host adapter equipped with a RJ11 jack (HA7Net, HA7E, HA5-xxx-R, and HA4B)
- Can be used with any Dallas Semiconductor port adapter. (DS9097E, DS9097U, DS9490R)

The DS1402 series incorporates four basic types of connectors, 1-Wire RJ-11, iButton, Touch-and-Hold Probe, and Blue Dot™ Receptor. The DS1402 series of 1-Wire network cables provides connectivity for iButtons. The cables are designed to connect any USB, serial, or parallel port 1-Wire adapter to any iButton. Both, the iButton probe cables and the Blue Dot receptor cables can touch any iButton, but can only hold the F5 version iButtons. The DS1402BR8 is the only cable that connects to the DS1401 iButton Holder. Applications of the DS1402-series 1-Wire network cables range from software protection and access control to asset management and thermal monitoring through handheld computers.IButton and 1-Wire are registered trademarks of Dallas Semiconductor Corporation. The DS1402D Blue Dot Receptors are iButton reader/probes that provide a convenient pipeline into the PC for iButton-to-PC communication. The receptor's cable connects to a USB, serial or parallel-port 1-

Wire adapter, whichever type of port you wish to use. The receptor itself easily affixes to any accessible spot on the front of the PC. The user can elect a quick information transfer with a momentary touch of the iButton to the Blue Dot. For hands-free operation the iButton can be snapped into the Blue Dot and remain there.

Each receptor contains two Blue Dots to accommodate instances where multiple iButtons are required for a transaction. A company's policy may, for example, require both an employee and a supervisor to authenticate access to sensitive information stored on a network server.

Figures3.6: different types of blue dot receptor in the market

4. WORKING

Since java ring is programmed with the applets and the programming is done according to our application and this will specific for the specific user. All information of the user is stored in the java ring.

Figure 4: how java ring is used to open the door

User simply has to press the signet of the java ring against the blue dot receptor and the system connected to the receptor performs the function that the applets instruct it to.java ring has the user profile and the same profile is present in the door embedded system also, when the user press the signet of the java ring against the java ring reader which is embedded at the handle of the door the data is transferred from the ring to door system. if the profile is authentic means user is authentic to open the door the applets president in the ring instruct the door to open. Information is transferred between iButton and a PC with a momentary contact, at up to 142K bits per second. To do that one presses iButton to the Blue Dot receptor, a $15 pipeline into PC. The Blue Dot sticks to any convenient spot on the front of a PC and is cabled to the serial or parallel port in the back. According to the Dallas Superconductor's information, over 41 million iButtons are currently in circulation. List of the major users include the U.S. Post Office, entire truck fleet fitted with iButtons that track vehicle maintenance; Citizens of Istanbul, Turkey, who store digital cash in the iButton, using the device as a small change purse on their mass transit system. it was also said that the U.S. Postal service has approved

the cryptographic iButton as a Postal Security Device to be used in its PC Postage program that allows individuals to download postage off the Internet and print it from their own printers

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.

Information is transferred between iButton and a PC with a momentary contact, at up to 142K bits per second. To do that one presses iButton to the Blue Dot receptor, a $15 pipeline into PC. The Blue Dot sticks to any convenient spot on the front of a PC and is cabled to the serial or parallel port in the back. According to the Dallas Superconductor's information, over 41 million iButtons are currently in circulation. List of the major users include the U.S. Post Office, entire truck fleet fitted with iButtons that track vehicle maintenance; Citizens of Istanbul, Turkey, who store digital cash in the iButton, using the device as a small change purse on their mass transit system. it was also said that the U.S. Postal service has

approved the cryptographic iButton as a Postal Security Device to be used in its PC Postage program that allows individuals to download postage off the Internet and print it from

5. SECURITY

The java ring provides very high degree of security for the confidential data that is stored in the NVRAM memory. The barrier substrate and the triple layer technique effectively deny access the unauthorized access to the NVRAM confidential data. In the worst case if any unauthorized access penetrates the barrier the security processor detects it and immediately the data which is written in the NVRAM. 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.

5.1. SECURITY THROUGH JAVA RING IN CAR

Figure 5.1: how java ring is used in security of car

The Sun concept car's security is based on a Java ring that contains a profile of the user. You connect the Java ring to a ring receptor in the car, and the car knows, based on your profile, what you are allowed to do. For example, a ring given to a mechanic or valet allows that person to see the dashboard and drive 40 miles per hour within a one block radius, but no faster or farther. In a family where both the husband and wife drive the car, each has individualized settings, so that when they enter the car, their environments are configured to the profiles on their rings. Java rings are authorized through Personal Identification Numbers (PINs) so that no one can steal a person's ring and run off with the car.

Sun representatives are also talking to automakers who are developing automated rental cars. In this potential market, a driver can use his or her ring to access a vehicle and simply leave it when done. Billing, reservations, vehicle monitoring, vehicle location, and all other functions are done via wireless communication. The net result is a very inexpensive rental car for local use by residents and tourists. This will create a new business for rental car companies competing for business travelers in the saturated airport rental car market.

6. APPLICATION

The java ring is used initially as rugged portable data carriers. often in harsh environmental condition. it is used for many real world application e.g for opening the door ,in the e-banking application for getting the balance in your account. Logging in your personal computer. Providing security in your car. 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.

Figure 6: application of java ring for getting account balance of an user through internet

This demonstration shows how an e-banking application (Jini client) tries to connect to a bank server (Jini service) to retrieve the current account balance of that user. Since all bank data must be treated confidential, the bank server interacts with the security infrastructure that is installed at the bank, before it responds to the application. The bank's security infrastructure demands that the user must authenticate herself to get the permission. Therefore an authentication scheme is started at user side that asks the user to push her Java Ring on the Java Ring reader. Inside the Java Ring resides a Java interpreter that executes cryptographic routines to perform that task. After the authentication process on the Java Ring, the bank knows the identity of the user and that she is really the one, she pretends to be. Then the bank service can send the confidential and personalized data to the e-banking application that displays the current account balance. This demonstration shows how an e-banking application (Jini client) tries to connect to a bank server (Jini service) to retrieve the current account balance of that user. Since all bank data must be treated confidential, the bank server interacts with the security infrastructure that is installed at the bank, before it responds to the application. The bank's security infrastructure demands that the user must authenticate herself to get the permission. Therefore an authentication scheme is started at user side that asks the user to push her Java Ring on the Java Ring reader. Inside the Java Ring resides a Java interpreter that executes cryptographic routines to perform that task. After the authentication process on the Java Ring, the bank knows the identity of the user and that she is really the one, she pretends to be. Then the bank service can send the confidential and personalized data to the e-banking application that displays the current account balance.

Figure 6.2: application of java ring for configuring your car component according to preferences.

The Sun concept car's security is based on a Java ring that contains a profile of the user. You connect the Java ring to a ring receptor in the car, and the car knows, based on your profile, what you are allowed to do. For example, a ring given to a mechanic or valet allows that person to see the dashboard and drive 40 miles per hour within a one block radius, but no faster or farther. In a family where both the husband and wife drive the car, each has individualized settings, so that when they enter the car, their environments are configured to the profiles on their rings. Java rings are authorized through Personal Identification Numbers (PINs) so that no one can steal a person's ring and run off with the car. Sun representatives are also talking to automakers who are developing automated rental cars. In this potential market, a driver can use his or her ring to access a vehicle and simply leave it when done. Billing, reservations, vehicle monitoring, vehicle location, and all other functions are done via wireless communication. The net result is a very inexpensive rental car for local use by residents and tourists. This will

create a new business for rental car companies competing for business travelers in the saturated airport rental car market.

Figure 6.3: application of java ring in opening the door

User simply has to press the signet of the java ring against the blue dot receptor and the system connected to the receptor performs the function that the applets instruct it to.java ring has the user profile and the same profile is present in the door embedded system also, when the user press the signet of the java ring against the java ring reader which is embedded at the handle of the door the data is transferred from the ring to door system. If the profile is authentic means user is authentic to open the door the applets present in the ring instruct the door to open. Information is transferred between iButton and a PC with a momentary contact, at up to 142K bits per second. To do that one presses iButton to the Blue Dot receptor, a $15 pipeline into PC. The Blue Dot sticks to any convenient spot on the front of a PC and is cabled to the serial or parallel port in the back. According to the Dallas Superconductor's information, over 41 million iButtons are currently in circulation. List of the major users include the U.S. Post Office, entire truck fleet fitted with iButtons that track vehicle maintenance; Citizens of Istanbul,

Turkey, who store digital cash in the iButton, using the device as a small change purse on their mass transit system. it was also said that the U.S. Postal service has approved the cryptographic iButton as a Postal Security Device to be used in its PC Postage program that allows individuals to download postage off the Internet and print it from their own printers.

A few important facts can be stated about the use of the Java Ring:

- Authentication is crucial to most applications, since billing and privacy is based on it.
- A very easy and convenient way for users.
- It is more secure than using passwords, since passwords are short or can be guessed.
- It is easier for administrators to maintain the security infrastructure, since only password can be forgotten.
- A ring is a personal thing that the user and only the user carries along anytime and anywhere, so that she can authenticate herself in every situation.
- It is also possible to use a tag on the key ring or a watch instead of a ring.

7. CONCLUSION

Java ring is highly durable because of its rugged and secure stainless packing. It is used in personal computing. 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 they 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, key fobs, wallets, bracelets, and necklaces, so the user can select a variation that suits his or her lifestyle.

REFERENCES

[1] http://www.javaworld.com

[2] http://www.electronics.howstuffworks.com

[3] http://www.people.uchicago.edu