JAVA RING

Presented by:
Ajay Gupta
Contents

- Introduction
- Components in Java Ring
- Working
- Alternative Identification Technologies
- Advantages
- Security
- Applications
- Disadvantages of Java Ring
- Conclusion
- References
INTRODUCTION

- A Java Ring is a finger ring that contains a small microprocessor with built-in capabilities for the user.

- It contains an inexpensive microprocessor in a stainless steel ibutton running a JVM and it is preloaded with applet.

- The Java Ring is an extremely secure Java-powered electronic token.
COMPONENTS OF JAVA RING

➤ Java Virtual Machine (JVM)

➤ Operating System

➤ RAM

➤ ROM

➤ iButton

➤ Blue dot receptor
**Java Virtual Machine**

- The java virtual machine is the piece of software that recognizes the java language and translates the byte code, which is used by the system which is connected to the java ring via ring reader.

- Automatic garbage collection for efficient reuse of memory space.
RAM

- Java ring contains 134kb of non-volatile random access memory. Program and data is stored in this NVRAM.

- The NVRAM iButton memory can be erased or written as often as necessary without wearing out.
ROM

- The java ring contains 32kb of ROM.

- A special kind of operating system called Ecommerce 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 jewel of the java ring is the java iButton.

It contains the one million transistor single chip trusted microprocessor with powerful java virtual machine (JVM) housed in rugged and secure stainless steel case.

Each iButton has a 8 byte unique and unalterable address laser etched onto its chip inside the can carries a guaranty that no two IButtons have same number.
**BLUE DOT RECEPTOR**

- iButton 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.

- The read/write operation will be done by this blue dot receptor.

- Receptor cable connects to the USB port of PC or any embedded system.

- The information is transferred between the ibutton and pc with momentary touching java ring.
TYPES OF iBUTTON

• Mainly three types of iButton are in use:

➢ Thermochrone iButton
➢ Crypto iButton
➢ Memory iButton
The Crypto iButton addresses both components of secure communication, authentication and safe transmission, making it ideal for Internet commerce and/or banking transactions.

The Crypto ibutton provides hardware cryptographic services such as long-term safe storage of private keys, secure message digest (hashing).
The iButton is a slave device and requires a master to initiate communication to it.

A master can be a PC or a microprocessor.

Communication to iButton can be started by a simple touch to a 1-Wire interface called a Blue Dot Receptor. Every iButton has a unique 64-bit serial number, which gives it a unique 1-Wire network address.

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 do.
Protocol

- 1-Wire protocol is used.
- Half-duplex data transfer.
- Command word sent to iButton slave from the master.
• **Three-Phase Transaction**
  - Device(s) Reset/Synchronization
  - Device Selection—ROM-Level Command
  - Device Function—Device-Level Command

• **Speed**
  - Standard (15.4kbps)
  - Overdrive (125kbps)
1-Wire Signaling—ROM Level

• ROM-Level Commands
  – Skip ROM: Skip Device Selection for Single Device on Bus
  – Read ROM: Read 64-Bit ROM ID of Single Device on Bus
  – Match ROM: Identify Device on Bus with Known ROM ID
  – Resume: Restart Communication with Selected Device
  – Overdrive-Skip ROM: Skip Device Selection and Put Device in Overdrive Mode
  – Search ROM: Find Devices on the 1-Wire Bus
1-Wire Transaction—DS2431 1kb EEPROM

MASTER Tx
FUNCTION COMMAND

0Fh
WRITE
SCRATCHPAD

AAh
READ
SCRATCHPAD

55h
COPY
SCRATCHPAD

F0h
READ
MEMORY

WAIT FOR
RESET

COMMANDS AND DATA SENT LSB FIRST

*A master-initiated communication sequence follows each “Y” flow decision.
ALTERNATIVE IDENTIFICATION TECHNOLOGIES

Barcodes

- Necessity of electromechanical printers and electro-optical printers.

- Sunlight or other ambient light affects the read rate.

- Decoding is necessary as light must be converted to electrical energy.
Alternative Identification Technologies

*Magnetic Strips*

- The stripes can be damaged by a brief contact to other magnets.
- Strong fields can erase or damage data.
- Any dirt will damage the coil and the reader if present during the swipe.
- They have to be removed from the object for writing.
ALTERATIVE IDENTIFICATION TECHNOLOGIES

*Chip Cards*

- Uns suited for labeling, since they have to be removed from object for both reading and writing.

- Limited life time.

- Exposed copper forms a oxide layer which decreases the contact quality and leads to malfunction.

- The chip can crack or the thin gold wires connected to chip can rip off.
ADVANTAGES

- Clam-shell steel container, the Micro can is suitable for harsh environments.

- Contents of NVRAM can be updated dynamically without wearing it out.

- Provides authentication to users which is crucial for many applications.

- Provides real memory and more power.
SECURITY

- The java ring provides very high degree of security for the confidential data and private keys that are stored in the NVRAM memory.

- Data travels on the network in the encrypted form makes hacking virtually impossible.

- Java rings are authorized through Personal Identification Numbers (PINs) so that no one can steal a person’s ring and use that ring.
What is SHA-1?

- Public Hash Function that Uses an Input Message and Secret to Compute a Message Authentication Code (MAC)
- Characteristics: Nonreversible, Collision Resistant, Avalanche Effect
CONTINUE...

- It provides temper resistance through instantaneous clearing of all memory when tempering is detected. This process is called rapid zeroization.

- If an excessive voltage is applied to the sole I/O pin, an electronic fuse renders the chip inoperable to protect the chip.

- The iButton constantly monitors the switch's contacts, and any separation of the cryptographic chip from the switch perform a complete zeroization.
Applications

- The java ring can be used to hold secret codes, credit cards numbers, driver license, other wallet contents, and even some electronic cash.

- It’s greatest promise appears to lie in its capacity to interact with Internet applications to support strong remote authentication and remotely authorized financial transactions.
Applications

- For opening the door
- E-bank application
- Logging in your PC
- Providing security in your car.
Disadvantages of Java Ring

- The cost of implementing the Java ring could be very high.

- The problem with the Java Ring is that many of the organization don't even know the existence of Java Ring.

- Only limited amount of information can be stored so, an individual might need to carry more than one Java Ring.

- Carrying the Java Ring everywhere could lead to theft issues.
CONCLUSION

- A very easy and convenient way for users.

- It is more secure than using passwords, since passwords are short or can be guessed.

- A ring is a personal thing that the user and only the user carries along anytime and anywhere, so that he can authenticate himself in every situation.

- It is also possible to use a tag on the key ring or a watch instead of a ring.
REFERENCES

- www.maxim-ic.com
- www.javaworld.com
- javaring.blogspot.com
- www.useit.com/papers/javaring.html
- electronics.howstuffworks.com

THANK YOU...