ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Prevention of Cold Boot Attacks on Linux Systems

Siddhesh Patil[1], Ekta Patel[2], Yogini Bazaz[3]

Bachelors of Engineering, Department of I.T., Atharva College of Engineering, Mumbai, India[1,2]

Professor, Department of I.T., Atharva College of Engineering, Mumbai, India[3]

ABSTRACT: Contrary to the popular belief, DDR type RAM modules retain stored memory even after power is cut off. Provided physical access to the cryptosystem, a hacker or a forensic specialist can retrieve information stored in the RAM by installing it on another system and booting from a USB drive to take a RAM dump. With adequate disassembly and analytic tools, this information stored in the RAM dump can be deciphered. Hackers thrive on such special-case attack techniques to gain access to systems with sensitive information. An unencrypted RAM module will contain the decryption key used to access an encrypted file system. Bits of data are stored in capacitors where a charge or a discharge denotes a 0 or a 1. Even on withdrawal of power from the RAM module, the capacitors still retain their values for a certain time frame. This window of time is highly vulnerable to a cold boot attack, and it can be extended by using proper cooling techniques. Cold boot attacks have been widely demonstrated even on modern Android handsets with the use of a custom recovery. We go through various flaws present in modern RAM technology and take a look at some of the counter-measures that ensure safety. We present an approach to design a preventive technique that will reduce the possibility of a cold boot attack.

KEYWORDS: Cold Boot Attack, Data remanence, Random Access memory

I. INTRODUCTION

Most computer users assume that switching off their machine removes any data held in random access memory (RAM) as it is referred to as volatile memory, and anything contained in RAM is considered lost when a computer is switched off. But as RAMs are made up of semiconductors, the contents are not lost immediately from it when the power supply is disconnected. It exhibits a property called data remanence. Data retention is observed for a period of time ranging from several seconds to several minutes. Random access memory or physical memory is used by the computer to temporarily hold data currently used by a given application. All the data manipulated is written temporarily in RAM for example texts, saved files, passwords and encryption keys. The more recent the activity, the more likely it is for the data to still be in RAM. So it may contain sensitive information, which if exploited, can cause loss for an individual or an organization. An attacker having physical access to a computer could recover some or all the important data from that session. So it is important that the sensitive data should be either wiped off or should be overwritten by scrambled information so that it erases all traces from that session on that computer. Most systems do not have techniques to ensure prevention of side-channel attacks. Unencrypted RAMs are more susceptible to cold boot attack techniques. We implement measures to ensure that data stays secure on system shutdown. Data security is critical for most of the business and even home computer users. RAM is used to store non-persistent information into it. When an application is in use, user-specific or application-specific data may be stored in RAM. The goal of most unethical hackers / attackers is to disrupt the services and to steal information. He/she can take a RAM dump and gain all the contents of the RAM. The aim of this project is to prevent cold boot attack on Linux system so that all the sensitive data retained by RAM for a window of time can be protected by attackers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. RELATED WORK

Information is stored in bits on capacitors. Each capacitor houses one bit of information as a 0 or a 1. A low charge denotes a 0 and a high charge is read as a 1. This positive logic methodology enables a sequential storage of information on capacitors. DRAM cells need to be continually refreshed as they lose their charge after a certain period of time. DRAM specifications assign a specific refresh time interval after which the cells are refreshed. Research [1] showcased an experiment to demonstrate data remanence in different RAM modules. Lower temperatures can significantly increase the retention times, to measure this effect in DRAMs a series of experiments was conducted [1]. A pseudo random test pattern was loaded into the memory. The computer was running a memory module to approximately -50 degrees Celsius. The machine was then Powered off and maintained at that temperature until the power was restored. These temperatures were achieved using canned air products. A significant lower rate of decay was observed at these temperatures. As an extreme test another experiment was conducted using liquid nitrogen where the memory module was submerged in it for 60 minutes. The decay rate was observed to be at merely 0.17%. This indicated that memory modules can retain memory for hours or days provided that they are housed in sufficient cooling environments.

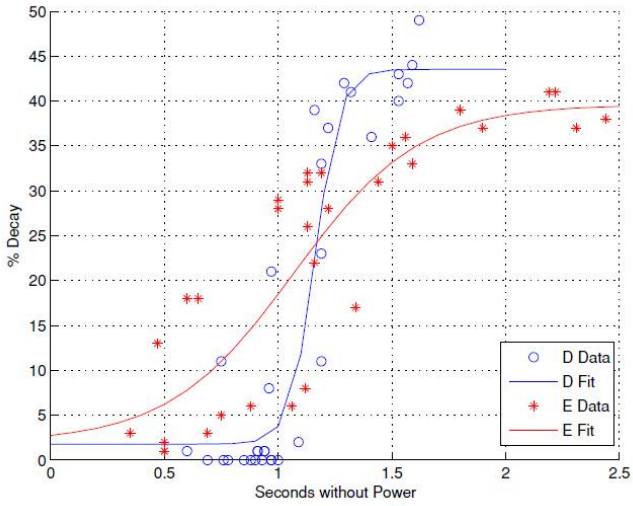

Fig. 1. Decay of information with time and temperature [1]

III. PROPOSED SYSTEM

A. *Tools used:*

- Secure – delete module for wiping RAM. [2]

B. *Proposed Approach:*

The aim of the project is to wipe the RAM before shutdown. This is achieved by the use of secure-delete toolkit [2]. This tool called as sd-mem, is used to wipe residual information in the random access memory. Secure delete makes the use of Peter Gutmann method [3] to wipe the data. When data is deleted it still remains in the RAM and can be retrieved. A safer way to prevent recovery is to rewrite the memory with random or 0x00 bytes.

Step 1: Setup sd-mem toolkit

To install the toolkit on any Linux based system use the command sudo apt-get install secure-delete. Once the toolkit is setup on the system, it can be launched via the terminal.

Step 2: Shutdown script

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A simple script can be made which invokes sdmem and then shuts down the system. Sdmem should be used with 3 flags, first being l, where only one random plus one pass with 0xff are written, the second flag being another l with a pass of 0xff in insecure mode. The third flag being f, which disables sync between writes to the RAM, for faster overwrite. Shutdown command in the script will immediately shutdown the system after sdmem is finished executing. The script should include 2 lines. First being sdmem -llf, second being shutdown -h. The h flag on the shutdown command immediately shuts the system.

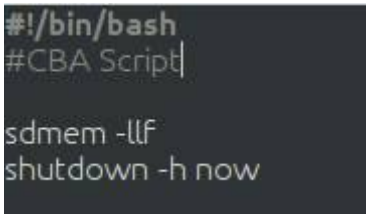

Fig.2. A snapshot of a script using SD-Mem and shutdown after wiping memory

Step 3: Execution

Use chmod to set the right permission for execution on the script. Execute it via terminal. The proposed system makes use of the sdmem tool to prevent the chances that even if a cold boot attack happens the memory retrieved will have been overwritten by sdmem.

IV. COLD BOOT ATTACK

Cold - boot attacks can be initiated with the right tools. We have looked at how memory can remain in the physical module due to data remanence flaw in the nature of semiconductor technology. Further by cooling the RAM module the decay rates can be slowed down which enables this side channel attack. Thus data can be retrieved by using a pre execution boot environment tool.

We revisit the steps to initiate a cold boot attack by using the modified PXE boot image [1].
Step 1: Get the PXE boot image source [4].
Step 2: Use tar command to extract the bios_memimage-1.2.tar.gz

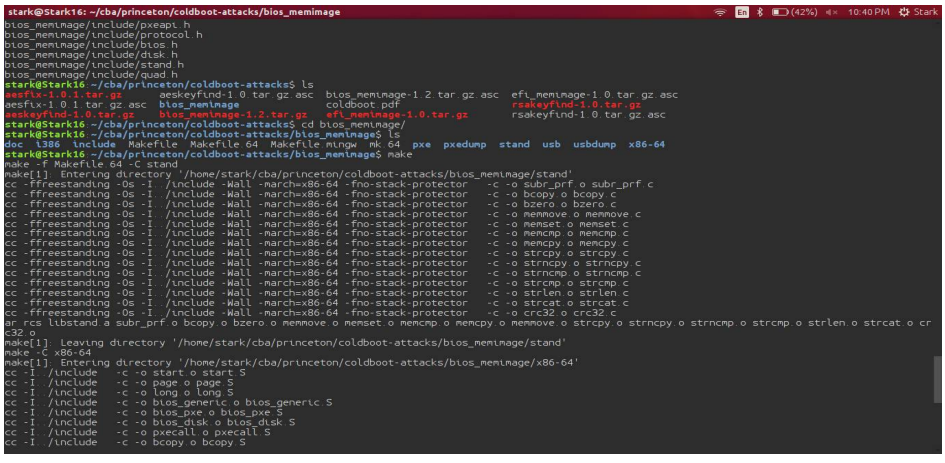

Fig.3. Compiling the bios image source

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Step 3: Compile the source by the use of make command, use the .64 makefile if the system is 64 bit.
Step 4: A scrapper.bin file will be generated which needs to be loaded into a USB drive.
Step 5: Use dd if =scrapper.bin of=/dev/name, here change the name to the name of your USB drive.
Step 6: Now the USB is ready to take a RAM dump. Shutdown the computer.
Step 7: Freeze the RAM module, this can be done via the use of an Aerosol spray.

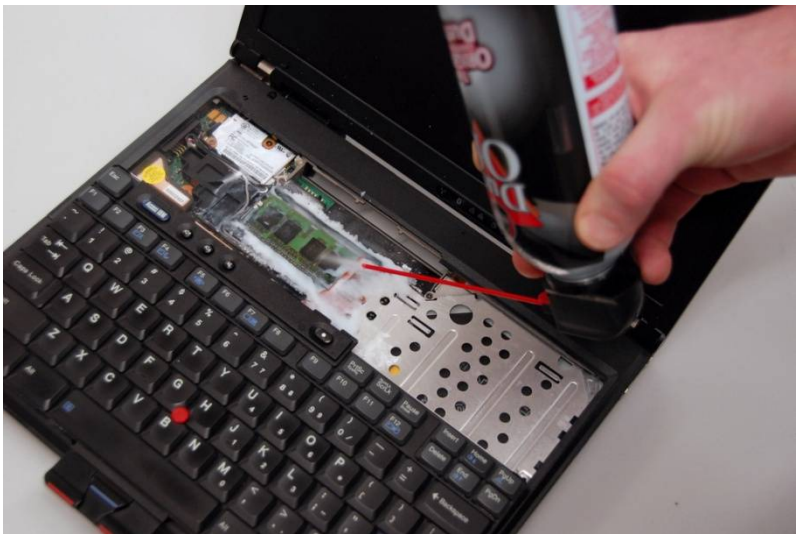

Fig.4. Use of an Aerosol spray to freeze RAM

Step 8: Boot the machine into the bios and set boot sequence priority to USB, this will boot from the USB drive.

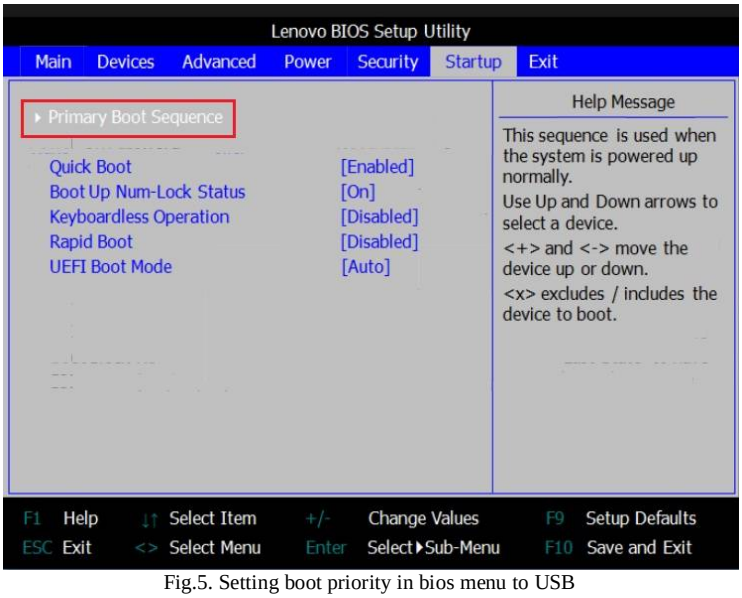

Fig.5. Setting boot priority in bios menu to USB

The boot image on the USB drive will take a dump of the RAM, while it is frozen to a lower temperature. The speed of the RAM dump will depend on the read write speed on the USB in use and the read write speed of the RAM. Once the dump is complete, the information in the dump can be analyzed for sensitive information. Keys can be retrieved

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

with the use of key finder tools [4]. Thus a cold boot attack is very much possible even on modern semiconductor modules. This attack is a special case scenario where an attacker has physical access to the target machine.

V. RESULTS AND STATISTICS

Taking a RAM dump is an essential part of cold boot attack. We mentioned how to take a RAM dump in a pre-boot environment by using the modified boot image. Taking a dump of the whole physical memory while the OS is utilizing the memory post-boot is a different scenario. To take a full memory dump, we use LiME [9], a tool to take full memory dumps. LiME can be loaded as a kernel object to take full dumps of memory.

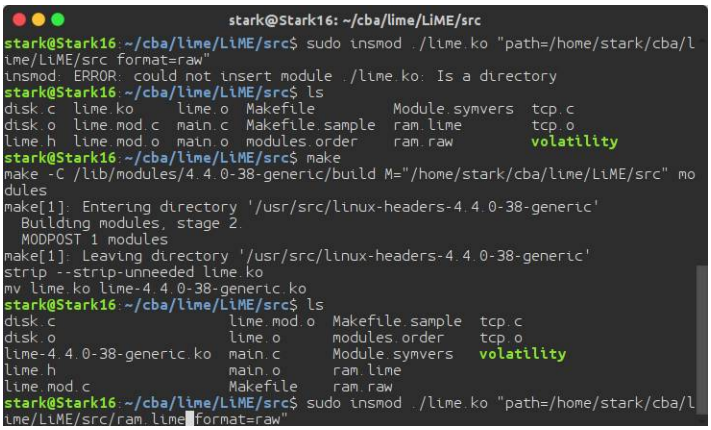

Fig.6. Use of LiME to take ram dump

A full dump of physical memory will take different times on different CPUs and HDDs. The time taken to take a RAM dump will depend on RAM module type. On the system we took a dump on a DDR3 type RAM is used which has speed of 1600 Mhz. Using LiME to take a RAM dump it takes approximately 1 minutes and 19 seconds. Note that, the system is using a 5400 RPM hard drive. Similarly using the BIOS boot image, it should take similar times to take a dump of the physical memory.

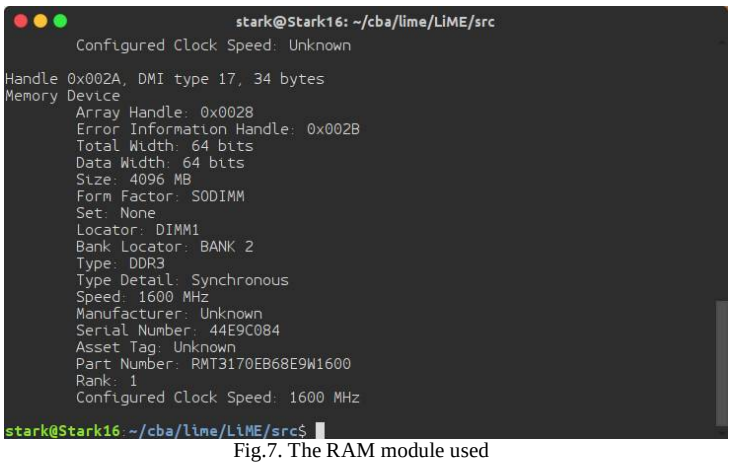

Fig.7. The RAM module used

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Fig.8. Using SD-Mem to wipe RAM on runtime

Here Fig.8. Shows a script that makes use of SD-mem to wipe the physical memory, the system will shut down after the RAM is wiped. SD-Mem can also be invoked manually in the terminal, thus wiping the memory.

VI. CONCLUSION

The secure delete toolkit provides a way using Peter Gutmann overwrite method to securely wipe RAM. We use it to wipe the RAM module and then shutdown the system. However, a sudden power off can still enable an attacker to initiate a successful cold boot attack. Another approach is to detect sudden drop in temperature and wipe the RAM has also been proposed. However, none of these methods are effective and cold boot attacks are still possible. By using RAM dump utilities, a dump of RAM can be taken before overwrite and after overwrite to make comparisons between the overwritten information and the effectiveness of the overwrite.

REFERENCES

1. Halderman, J. Alex; Schoen, Seth; Heninger, Nadia; Clarkson, William; Paul, William; Calandrino, Joseph A; Feldman, Ariel J.; Appelbaum, Jacob; Felten, Edward W. "Lest We Remember: Cold Boot Attacks on Encryption Keys". Princeton University, 2008-02-22.
2. Secure Delete toolkit by Van Hauser https://github.com/gordonrs/thc-secure-delete
3. Peter Gutmann"Secure Deletion of Data from Magnetic and Solid-State Memory" Department of computer science, University of Auckland by, 6th USENIX Security Symposium, July 22-25 1996
4. Tools by Princeton University for Preboot RAM dump https://github.com/Truestark/coldboot-attacks
5. Jos Wetzels "Hidden in snow, revealed in thaw: Cold boot attacks revisited", Cornell Library, 2014
6. Michael Gruhn and Tilo Muller "On the Practicability of Cold Boot Attacks",Friedrich-Alexander-University, Erlangen-Nurnberg, Germany
7. P. McGregor, T. Hollebeek, A. Volynkin, and M. White, "Braving the Cold: New Methods for Preventing Cold Boot Attacks on Encryption Keys," in Black Hat Security Conference. BitArmor Systems, Inc., Aug 2008.
8. T. Muller and M. Spreitzenbarth, "FROST: ¨ Forensic Recovery Of Scrambled Telephones — ITSicherheitsinfrastrukturen (Informatik 1)"
9. LiME Loadable kernel module https://github.com/504ensicsLabs/LiME

BIOGRAPHY

Siddhesh Patilis a Student in the Information Technology Department, Atharva College of Engineering, University of Mumbai. He is an Android systems developer working on various Android sources. His interests are system security, malware analysis and reverse engineering.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Ekta Patel is a Student from Information Technology Department, Atharva College of Engineering, University of Mumbai. Her interests are in web based computing solutions, information security and data analytics.

Yogini Bazaz is a professor at the Information Technology Department, Atharva College of Engineering, University of Mumbai. Her interests are in software development and software deployment solutions.