Cold Boot Memory Acquisition: An Investigation into Memory Freezing and Data Retention Claims

P. Hannay [1], **A. Woodward**[1]
[1]School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, Australia

Abstract – *A number of claims have been made regarding cold boot memory acquisition techniques. There are numerous potential applications for these techniques should they be shown to be reliable and suitable for use in the field. An investigation into these techniques has been conducted. The results of conducted experiments do not show that cold boot memory acquisition is viable for use in the field in its current state, however future research may change this. In addition to this there are a number of possible countermeasures that should be considered and carefully evaluated before live memory acquisition methods are employed.*

Keywords: digital forensics, memory acquisition, cold boot, forensic acquisition, ram, encryption

1 Introduction

A number of claims have been made recently in regards to various methods of acquiring memory from systems after power to memory modules has been removed. These methods range from the analysis of electro migration which can be detected via the use of an electron microprobe techniques [1] to freezing ram modules to increase data retention time [2]. This paper will serve as an investigation into recent data retention claims as they apply to the cold boot memory acquisition techniques.

2 Potential Applications

There are numerous applications for cold boot memory acquisition should it prove to be feasible for usage when performing acquisitions within the field. The most obvious of these is as a countermeasure to encryption technologies, specifically full disk encryption measures such as TrueCrypt and Microsoft's BitLocker. Full disk encryption is of specific interest as in these cases page file analysis and other analysis methods are not able to be used as a key recovery method.

The idea of live memory acquisition is by no means new, there exist a number of methods to acquire the memory of a running system, these traditionally involve the execution of specially written software that takes a dump of the current memory of the host system on which it is being executed [3]. This particular avenue has its own problems as the execution of any code has the potential to result in the destruction or modification of data existing within memory. Other methods include memory acquisition via firewire, however this method also leads to memory being modified on the host system as firewire drivers and other information is updated on the host system prior to acquisition. Cold boot memory acquisition differs in this way as it allows for a snapshot of memory to be taken without executing any potentially destructive code on the host system.

The destruction of data in memory will still occur in lower address ranges in one specific implementation of cold boot memory acquisition. The implementation is that of acquiring the data from memory modules by using custom software that is executed at boot time. The way that this is currently addressed is by the use of a minimal operating environment that will allow for the memory acquisition whilst limiting the amount of memory that is overwritten. One method of addressing this limitation would be the design of specific hardware to perform the memory acquisition operation, in this way no operating system would need to be loaded into the memory being acquired; as such this would eliminate the need to potentially compromise the integrity of the retrieved data. It would also allow for the acquisition of memory in low address ranges, which could potentially hold encryption keys and other important data.

Finally this technique could potentially allow for the acquisition of memory from systems without firewire, systems running uncommon operating systems for which memory acquisition tools are not available or are unable to be used due to policy restrictions. Cold boot memory acquisition may also provide an improved method for the acquisition of memory from embedded devices such as satellite navigation units, mobile phones and hardware cryptographic devices.

3 Existing Research

Existing research suggests that data is retained in DRAM modules even when in a non powered state. The times associated with this data retention depend heavily on the make, type and temperature of memory modules at the time power to the memory modules is lost. It is also stated that the method of rebooting (hard power off, OS shutdown feature or hard reset switch) will have minimal impact on the data retention of memory modules [4].

The existing research also outlines that there may be issues acquiring ECC memory if the system is rebooted with the memory in place, this is due to the operation of motherboards that require ECC memory as they often clear the contents of memory during the boot process.[4]

4 Possible Countermeasures

Of course a number of possible countermeasures to this attack exist. These countermeasures could potentially be implemented in software or hardware, hardware implementations of course would be more efficient at mitigating the risks associated with cold boot memory acquisition.

At the hardware level it could be possible to encrypt all data as it is written to memory and decrypt data as it is read. This implementation has already been employed in a number of video game consoles in order to hinder reverse engineering efforts. In this instance there would be an increased cost associated with the technology and overhead as a large amount of hardware would need to be replaced. An alternate hardware based approach would be to not store the encryption/decryption keys in DRAM modules at all, instead storing them in CPU cache or a trusted computing module, thus increasing the level of expertise required to acquire this data. Ultimately it seems that hardware based disk encryption (with the encryption keys only existing within the encryption device itself) with battery backed temperature based failsafe would be the most viable solution, such measures are employed within the High Grade Silicon Data Vault (manufactured by Secure Systems) [5], in this specific implementation the memory containing encryption keys is erased when the temperature falls outside of a specified range or a number of other intrusion detection features are tripped.

From a software standpoint it may be possible to increase the difficulty associated in acquiring encryption keys by ensuring that said keys are stored within the first few megabytes of memory, thus increasing the probability that these keys will be overwritten during the acquisition process itself, however this approach could be countered by the use of a purpose built hardware device to acquire the memory modules.

5 Experimental Design

The experimental design was broken down into a number of elements:

- Acquisition software
- Test computer system
- Additional Items

5.1 Acquisition Software

The software used in order to acquire memory is a modified version of the McGrew Security Ram Dumper (msramdump). Msramdump is designed to provide a bootable environment in which physical memory can be dumped to USB storage attached to the system. The software makes use of the SysLinux distribution of linux and is designed to have a minimal memory footprint in order to preserve the greatest amount of data residing in physical memory at the time of use [6].

Msramdump is installed on a USB flash drive and operates by locating an unused partition (indicated by a partition type of ‘40’, this partition is then used as the destination for any memory that is acquired. Following acquisition the partition type is set to 41 indicating that the partition has been used and is no longer available as a destination[6].

Modifications were made to msramdump in order to address a number of issues that prevented the software from operating as intended. In this case the issue was that the software was incorrectly reporting partitions of type ‘40’ as in use, a modification was made to bypass this check for the purposes of the experiment. An additional issue was identified as the software was incorrectly reporting memory reads as unsuccessful when examination of the acquired data showed that the memory reads had completed without issue.

5.2 Test Computer System

The test system used in this instance was a standard IBM S50 desktop PC (3.0Ghz) with 512MB of non-ECC ram.

5.3 Additional Items

A 1GB USB flash drive was used to hold the msramdump software. This device was partitioned with two partitions. The first contained msramdump and the second was a 700MB empty partition of type ‘40’ to be used for the storage of acquired data.

Several cans of ‘freeze spray’ were used in order to cool the memory modules to an approximate temperature of -50 degrees Celsius.

5.4 Tests and Methodology

A number of different tests were performed in order to investigate the validity and overall usefulness of the cold boot memory acquisition methodology in a field environment (in this case the field is defined as an actual forensic acquisition at the scene).

The following will be evaluated:

- Data retention without cooling
- Data retention with cooling
- Data retention when power plug removed (with cooling)
- Data retention when reboot functionality under windows is used (with cooling)
- Data retention when power button held down to cause hard power off (with cooling)

In each of these scenarios the system will be powered back on with a USB flash drive as defined in additional items attached as a boot device. Prior to each iteration of testing the destination partition of the boot device was overwritten with binary zeros, this is so that the acquired data can be clearly identified and to prevent contamination of results from previous iterations of testing.

In order to test the methodology and software configuration the acquisition was performed within a VMWare virtual environment, which has been confirmed to leave data present in memory persisting between reboots. In this instance it was confirmed that the acquisition software works as intended within this environment (it should be noted that an alternate boot method, not effecting the operation of the software was used. This is due to limitations of VMWare which does not allow booting from USB devices).

6 Results

In each iteration of the experiment we were unable to reproduce any data retention. In each case the only data present in the dump of physical memory taken was that of the memory footprint of Syslinux and msramdump. In this case this is seen in the first 7 MB of memory. After this position in memory the data recovered in each case was empty, consisting of all binary zeros.

It should be noted however, that the code used within a VMWare environment (with a non-usb boot method) resulted in the complete memory being acquired when the VMWare machine was rebooted. This result confirms that the experimental design is valid.

7 Discussion of Results

The results of this experiment were inconclusive as a negative result was achieved in all instances of the test. It is not possible to confirm or deny the validity of the cold boot memory acquisition methodology due to the limited range of hardware used. However this does demonstrate that this methodology is limited in its use as it is not viable on a standard corporate desktop system. However the approach of removing the ram modules from one system and inserting them into another where the cold boot memory acquisition methodology is known to work may result in greater degrees of success and thus prove to be a more reliable method to acquire any residual data.

As the experiment gave a negative result it was not possible to evaluate the specific data retention times of different shutdown and temperature combinations.

8 Ongoing Research

Research is currently ongoing with different hardware platforms that will hopefully yield a more conclusive result. In addition to that research is being conducted on satellite navigation and other embedded devices in an effort to evaluate the use of this method on other devices.

9 Conclusion

Cold boot memory acquisition has many significant uses if the methodology and principles can be advanced to the point where the process is reliable and the length of data retention established under varying circumstances. A number of countermeasures exist that could be employed to counter the threat posed by cold boot memory acquisition; however significant cost is associated with these. The experimentation conducted did not yield significant results in terms of data retention times, however the results did demonstrate that there may be issues that prevent this methodology being used for forensic purposes at this point in time, it should be noted however that future research may result in a reliable process that can safely be applied.

10 References

[1] Gutmann, P. (2001). Data Remanence in Semiconductor Devices. Retrieved 12th May, 2008, from http://www.cypherpunks.to/~peter/usenix01.pdf

[2] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., et al. (2008). Center for Information Technology Policy » Lest We Remember: Cold Boot Attacks on Encryption Keys. Retrieved 9 April 2008, from http://citp.princeton.edu/memory/

[3] datagam (2007). Live Memory Forensics. *Journal*. Retrieved from http://toorcon.org/2007/talks/4/Live%20Memory.ppt

[4] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., et al. (2008). Lest We Remember: Cold Boot Attacks on Encryption Keys. *submitted for publication, February*.

[5] Geddes, M. (2007). Silicon Data Vault - Models: LU100, LS100 - Technical Overview. Unpublished Technical Overview. Secure Systems.

[6] McGrew, R. W. (2008). McGrew Security - msramdmp : McGrew Security RAM Dumper. Retrieved 9 April 2008, from http://mcgrewsecurity.com/projects/msramdmp/