Practical Password Harvesting from Volatile Memory

Stavroula Karayianni and Vasilios Katos

Information Security and Incident Response Unit,
Democritus University of Thrace
skarayianni@gmail.com, vkatos@ee.duth.gr

Abstract. In this paper we challenge the widely accepted approach where a first responder does not capture the RAM of a computer system if found to be powered off at a crime scene. We investigate the presence of confidential data in RAM such as user passwords. Our findings show that even if the computer is switched off but not removed from the mains, the data are preserved. In fact, when a process is terminated but the computer is still operating, the respective data are more likely to be lost. Therefore capturing the memory could be as critical on a switched off system as on a running one.

Keywords: memory forensics, order of volatility, data recovery.

1 Introduction

Forensic analysis of volatile memory is a rapidly developing topic in the recent years [1]. The need to capture and analyse the RAM contents of a suspect PC grows constantly as remote and distributed applications have become popular, and RAM is an important source of evidence [2] containing network traces [3] and unencrypted passwords. However the RAM is captured only when the computer is switched on; in the opposite case the first responder would typically seize the hard disk and other non-volatile media which are further examined according to a dead forensic analysis process.

This paper has two aims. The first aim is to investigate the robustness and reliability of a method of examining RAM data of a system even when turning it off. The second aim is to investigate the feasibility of obtaining sensitive data such as unencrypted passwords from a practical perspective. In order to meet the first aim we introduced two definitions that will assist on structuring and studying the underlying problems.

The paper is structured as follows. In Section 2 the dynamics of seizing volatile memory are presented. In Section 3 the approach for capturing and extracting passwords and cryptographic keys is presented. Section 4 presents the concluding remarks.

2 A Measure of Volatility

The observation that the computer's volatile memory can maintain content for certain seconds even minutes after shut down of power supply, was made first by a team of

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 17–22, 2012.

researchers from the University of Princeton [4]. It was demonstrated that with the use of a bottle of compressed air one could freeze the memory and maintain its contents intact for up to hours. This indicates that confidential data such as cryptographic keys can be exposed.

Flushing memory is an expensive operation and not favoured by operating systems developers. Non-surprisingly, there is no correlation between the operating systems and preservation of RAM contents. The latter depends solely on the hardware and whether the computer system is connected to the mains when switched off.

Definition 1. Complete volatile memory loss is the state of memory where it is not possible to distinguish, for any memory address location, whether the stored value is a result from some past system or user activity.

The above definition refers to the complete "erasure" of the activities in a system – from a volatile memory perspective. Here erasure does not necessarily require that all values are zeroed out; in fact we are interested in the ability to distinguish whether a particular bit stored in memory was part of a particular process activity. Depending on the context of the forensic investigation, the different types of data may have a different weight in terms of forensic value. For example, in malware forensics, the data containing the execution commands of the binary will surely be of some interest since these will be used to extract the malware signature and footprint to be incorporated in an antivirus solution. In contrast, when investigating user activities – say downloading illicit material – the focus would be on the data area of the process. Nonetheless the need to secure the integrity of the data remains, and therefore in a complete volatile memory loss state any data recovered would not be admissible.

However as in most digital forensics cases it suffices to recover portions of data that are capable of proving or refuting a hypothesis therefore even if parts of the memory are valid they may contain the "smoking gun" evidence, or other pieces of data that may support an investigation such as passwords and encryption keys.

Definition 2. Partial volatile memory loss is the state of memory where for m>0 memory address positions their stored values can be correlated with past system or user activity.

It can be claimed that when $t=t_{shutdown}$ (the moment of deactivation of the computer) we have partial memory loss, whereas in time $t=t_{shutdown}+t_{off}$ with $t_{off}\rightarrow\infty$ we have total memory loss. The rate of memory loss depends on the technology of the memory and may also depend upon external conditions (such as temperature). In DDR type RAM there is no memory loss if the computer is switched off but connected to mains. This means that a first responder should enrich the widely accepted procedure of removing and making a bit-stream copy of a hard disk as follows:

Forensic acquisition process

System conditions: Computer is switched off and plugged into mains.

1. Remove power from all hard disks.
2. Connect/replace a DVD/CDROM with a liveCD containing msramdmp or equivalent tool.
3. Connect a forensically prepared USB stick to store the image
4. Power on the PC and configure the BIOS to boot from CD
5. Reset the PC and acquire the image

It is recommended that a liveCD is used instead of a liveUSB as the former is more widespread among systems and therefore it is a safer option.

We performed a memory dump in a very common scenario, where a user accesses facebook, gmail, msn and skype. There were dumps performed straight after closing the application, after 5, 15 and 60 minutes. The results are presented in Fig. 1. The charts depict references to application data over time.

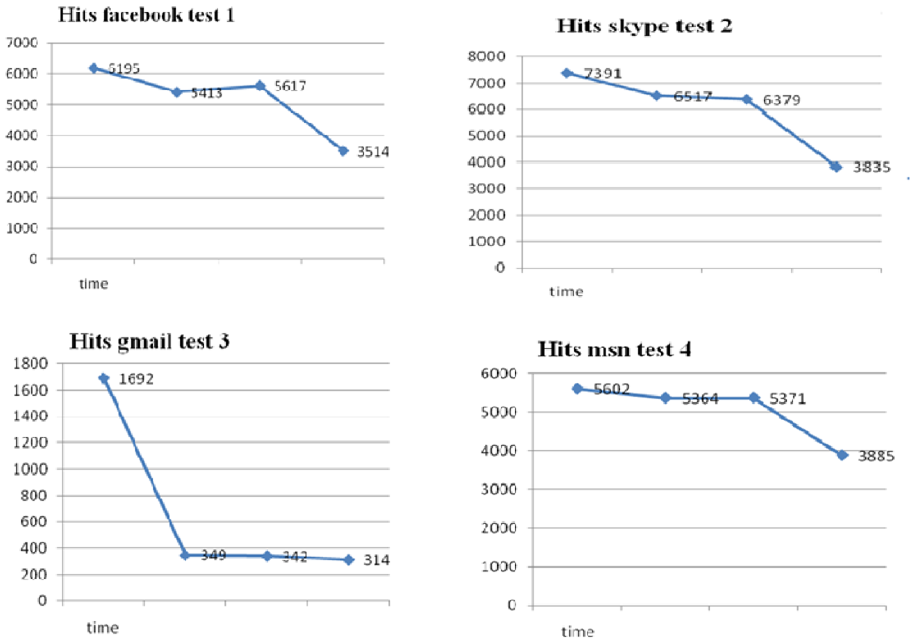
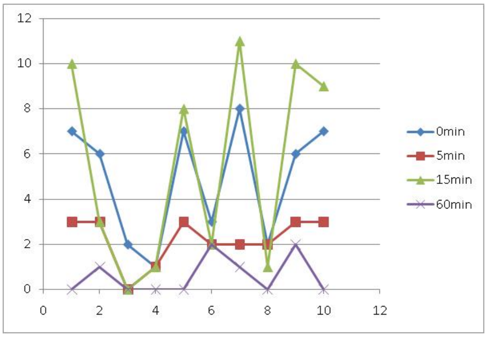


Fig. 1. Application references (hits)

An interesting observation is that the references are not necessarily monotonically decreasing upon the termination of the respective process. This is due to the memory management operations, virtual memory and swapping as implemented by the underlying operating system. Therefore although a user may have terminated a process, the information is not necessarily lost. In fact, in the event that the user shuts down the computer it can be seen that the sooner the computer is shut down (after closing the application in question), the more data are preserved. In addition during a forensic investigation, the population of the hits can be used to offer an estimate as to how long ago a process was terminated. This estimate can be improved by augmenting the proposed approach with other methods establishing the user activity in the system [5].

However, as shown in Fig. 2 the presence of passwords when visiting a web application (in our case Facebook), is less predictable. As expected after 60 minutes of logging out of the application and terminating the browser, the number of password copies drops, but surprisingly there is an increment after 15 minutes of logging out.



	0m	5m	15m	60m
Mean	4.9	2.2	5.5	0.6
Stdev	2.60	1.03	4.45	0.84

Fig. 2. Password hits and descriptive statistics for a Facebook session

3 Password Discovery

The images described in Section 2 were examined for passwords. It is highlighted that the corresponding applications were terminated prior to performing a memory image dump. This was done in order to cover the case of the computer being switched off or the user terminating the process as in the opposite case – that is when the process is active – all userspace data as well as metadata can be unambiguously identified through memory analysis tools such as the Volatility Framework [6].

To assist the analysis we developed a simple tool that combines strings, egrep and bgrep to search for patterns primarily as regular expressions in a memory dump image. The syntax of the tool is

```
totalrecall.sh <image_file> <pattern_file>
```

where image_file is the memory dump image and pattern_file is the file containing the regular expressions or hex patterns for the strings and binary search respectively. Our findings are summarised and categorised in Table 1.

From the above we can conclude that volatile memory loses data under certain conditions and in a forensic investigation such memory can be a valuable source of evidence.

4 Conclusions and Outlook

Against conventional forensic acquisition recommendations we argue that capturing memory should be performed even when a computer is found to be switched off at a

Table 1. Password states

<table>
<tr><th>Application/use case</th><th>Encoding</th><th>Detection method</th></tr>
<tr><td>Firefox 3</td><td>plaintext</td><td>Regular expression patterns.
Gmail signin:
&Email==[0-9]?{15}[a-z]?{15}%40([a-z]{8}\.)?[a-z]{8}\.com&Passwd==
Facebook:
locale=el_GR&email=[0-9]?{15}[a-z]?{15}%40([a-z]{8}\.)?[a-z]{8}\.com&pass=[0-9]?{15}[a-z]?{15}
Hotmail signin:
MSPPre=[0-9]?{15}[a-z]?{15}@[a-z]{8}.com|[a-z]?{18}[0-9]?{18}||MSPCID=[a-z]?{18}[0-9]?{18}</td></tr>
<tr><td>Firefox 4</td><td>Unicode</td><td>Hex patterns of the form:
00.xx.00.yy.00.xx.00...</td></tr>
<tr><td>MSN</td><td>Plaintext in cookie</td><td>Regular expression patterns.
MSPPre=[0-9]?{15}[a-z]?{15}@[a-z]{8}.com|[a-z]?{18}[0-9]?{18}||MSPCID=[a-z]?{18}[0-9]?{18}</td></tr>
<tr><td>Winrar</td><td>Plaintext</td><td>Indexed strings for dictionary attack</td></tr>
</table>

crime scene. This is because memory is not flushed during a system shutdown as this is an expensive and unnecessary operation which is avoided. In addition if the computer is connected to the mains, most of the data are preserved. The position that volatile memory should be considered as an unreliable means of storage when the computing system is switched off is of course valid. However, from a forensic perspective such a coarse consideration is not sufficient. Therefore we have introduced two finer grained definitions of volatile memory loss, offering a more suitable representation of the forensic value of the memory.

Provided that every case is distinct, the primary data gathered in the paper are relatively limited in scope as they were used as a proof of concept to develop the forensic process and submit the recommendation of conducting a memory dump of a switched off computer. Although that it is generally recommended that a memory dump should be performed, it is the first responder's judgment as to whether the memory is examined.

Another well known issue reinstated by this research is the importance of security considerations that need to be adopted by the application developers. Firefox for instance does not protect the sensitive password values. A possible solution could be to erase (zero out) any memory address spaces associated with HTML password type variables. Although these are expected to be protected during transit (through SSL) and they have to be in plaintext in RAM, they can be more ephemeral and be deleted as long as they are not required. Apart from the legitimate needs of a forensic examiner, many organisations have been affected nowadays from advanced persistent threats (APTs) and a malware can trivially perform a RAM dump straight after infecting a computer to speed up the harvesting of passwords.

Lastly, as part of ongoing and applied research a knowledge of different types of RAM chips and motherboard combinations should be developed in order to capture the volatility measurements, as data persistence in memory depends upon the hardware.

References

1. van Baar, R., Alink, W., van Ballegooij, A.: Forensic Memory Analysis: Files. Mapped in Memory. In: Digital Forensic Research Workshop, vol. 5, pp. 52–57 (2008)
2. Gavitt, B.: Forensic analysis of the Windows registry in memory. Digital Investigation 5, 26–32 (2008)
3. Adlestein, F.: Live forensics: diagnosing your system without killing it first. Communications of the ACM 49(2), 63–66 (2006)
4. Halderman, J., Schoen, S., Heninger, N., Clarkson, W., Paul, J., Calandrino, A., Feldman, A., Appelbaum, J., Felte, E.: Lest We Remember: Cold Boot Attacks on Encryption Key. In: 2008 USENIX Security Symposium (2008)
5. Carrier, B., Spafford, E.: Categories of digital investigation analysis techniques based on the computer history model. Digital Investigation 3S, 121–130 (2006)
6. The Volatility Framework: Volatile memory artifact extraction utility framework, `https://www.volatilesystems.com/default/volatility`