The State of Modern Forensics: an overview of memory analysis

[redacted]
Indiana University of Pennsylvania

Abstract

Computer forensic science is heavily reliant on the action of memory analysis. Over time, new processes have been discovered which recover deleted data more effectively. Today there are many different techniques and tools to implement those techniques on many types of devices to accomplish memory analysis.

Introduction

The process of memory analysis is used in digital forensics to discover information about running and previously run programs, the operating system, and the overall state of a device. This has been useful in not only recovering data for personal use, but also to be used as evidence to aid in criminal investigations. This way this process is carried out differs among type of devices (desktop, smartphone, etc.), operating systems, and the tools needed. Though it is a complicated process, it is becoming not only easier to perform, but also increasingly vital to society as their use of technology grows.

Tools and Techniques

Regardless of the operating system, the memory analysis always has the same initial steps. First, the evidence must be collected as either physically seized software or copied software. Then, a bit-by-bit copy of the memory is created in a process called memory imaging. From this point, the actual analysis occurs (Memory Imaging). The investigator must "translate the obtained stream of bytes into structured information (Garcia)." One method of analysis is String Searching. This is one of the more traditional approaches to memory analysis. The investigator searches certain strings which could hold information important to the case, such as

passwords and network addresses. Programs such as Strings.exe and Grep.exe return string information from memory. The problem with these programs is that no context is given to how these strings were actually used on the device in question. The investigator also must compile a list of strings to search on their own before running the program (Beebe & Clark).

Another technique is Finding Process objects. These techniques search for the EPROCESS that is associated with all Windows processes. According to Microsoft, "The EPROCESS structure is an opaque structure that serves as the process object for a process". An example of a took which uses this method is Process and Threat Finder, or simply PTFinder. PTFinder searches for the EPROCESS and ETHREAD structures left by all former processes and threads after a memory dump. Another program called Lsproc is very similar but only searches for the EPROCESS structures. This method is extremely effective at finding malware. Another tool which is based off of this method is KnTList which is used to interpret the structure of the target device's memory.

A third technique is to find objects' signatures. Signatures are intended for authentication and to assure the integrity data. Programs implementing this technique scan the collection of bits looking to identify recognizable signatures which reveals hidden objects. A tool which uses this method is GrepEXEC. This tool's main function "is to verify objects such as driver object, device object, EPROCESS and ETHREAD objects. It searches through the acquired image for recognizable objects signatures (Garcia)."

Another popular contemporary tool used for memory analysis worth mentioning is WinDbg. This is a debugger designed by Microsoft and is available commercially. It maps strings to their corresponding objects and exposes memory structures (windbg.org).

Conclusion

Memory analysis has become a vital part of policing now that the cyber world has become such a strong force on everyday life. Many crimes are now committed with a computer or at least evidence of those crimes will be documented in its memory. Digital forensics in general allows many more cases to be solved than ever before. Just as technology is ever increasing in its capabilities, so must the techniques used which police that technology. It is vastly important to develop multiple methods to retrieve and analyze dumped data in order to ensure that evidence can never truly be lost or hidden. Technology will continue to evolve as we continue into the Digital Age; it is impossible to tell what the next new breakthrough will be for our devices and when it will come, but the techniques and tools needed to analyze its data will not be far behind.

References

Beebe, N., & Clark, J. (n.d.). Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results. Science Direct. Retrieved September 29, 2015, from http://www.dfrws.org/2007/proceedings/p49-beebe.pdf

EPROCESS. (n.d.). Retrieved September 28, 2015, from https://msdn.microsoft.com/en-us/library/windows/hardware/ff544273(v=vs.85).aspx

Garcia, G. (2007, October 12). Forensic physical memory analysis: An overview of tools and techniques. University of Texas at San Antonio. Retrieved September 28, 2015.

Memory Imaging. (2014, July 1). Retrieved September 28, 2015, from http://forensicswiki.org/wiki/Memory_Imaging

Schuster, A. (n.d.). KnTTools and KnTList released. Retrieved September 29, 2015, from http://computer.forensikblog.de/en/2007/04/knttools-and-kntlist-released.html

WinDbg. (n.d.). Retrieved September 29, 2015, from http://www.windbg.org/