Compressed RAM in Linux and Mac OS X: Impacts on Live Forensics

Golden G. Richard III, Ph.D., University of New Orleans, Department of Computer Science, 2000 Lakeshore Drive, New Orleans, LA 70148
Irfan Ahmed, Ph.D., University of New Orleans, Department of Computer Science, 2000 Lakeshore Drive, New Orleans, LA 70148

After attending this presentation, attendees will understand the key characteristics of modern virtual memory systems that impact memory analysis in live forensics investigations, with a focus on emerging "compressed swap" facilities. Despite the decreased costs of RAM upgrades and growing memory capacities of modern computer systems, there is substantial interest among operating systems developers in improving utilization of physical memory. There are various reasons for this, including the popularity of extremely portable and relatively resource poor ultrabooks and pervasive use of virtualization. Compressed RAM facilities will "break" current generation memory analysis tools, and while modification of existing tools will not necessarily be trivial, there are potentially great rewards in doing so. The talk will survey the compressed RAM facilities in both Linux and Mac OS X and discuss the impact on both memory analysis tools and capabilities.

This presentation will impact the forensic community by providing an accessible introduction to virtual memory system internals, the structure of current generation memory acquisition and analysis tools, emerging mechanisms for compressing RAM to increase performance and decrease swapping in Mac OS X and Linux, and the impact these mechanisms will have on memory analysis. This work is important because virtually all memory acquisition tools will require adaptation to return complete and correct results in the presence of compressed RAM.

Historically, efforts to compress RAM to make more memory available for applications has had limited success. Applications like RAM Doubler for Mac OS X were popular decades ago, yet improved system performance only under a restrictive set of circumstances. The advent of modern multicore processors is providing new life for RAM compression mechanisms, which will advent in both Mac OS X Mavericks (Mac OS 10.9) and in newer versions of the Linux kernel. The goal of these mechanisms is to better utilize physical memory resources, reduce swapping to hard drives/SSDs, and improve system performance. Despite increasing memory capacities are increasing and the cost of memory upgrades decreasing, these facilities make sense in a number of circumstances, because even with modern SSD designs in desktop systems, bandwidth is capped at just over 1GB/sec, while physical memory bandwidth may reach 60GB/sec or more, making swapping extremely expensive.

The deployment of these compressed RAM mechanisms will break virtually all current-generation memory acquisition and memory analysis tools. Further complicating this issue is that the facilities in Mac OS X and Linux are different and that Linux will actually offer several alternatives for deploying compressed RAM. Memory analysis tools rely on accurate and complete physical memory acquisition and with the introduction of compressed RAM, the relatively platform-independent methods currently used for acquiring RAM on Intel-based systems will now require OS-specific (and compressed RAM mechanism-specific) techniques for acquisition, substantially increasing complexity. The benefits of compressed RAM for live forensics analysis, however, may far outweigh the effort in fixing tools, since memory pages that were previously swapped out (and therefore not analyzable by most memory analysis frameworks) may actually be present in the compressed areas of a memory capture.

Keywords: Digital forensics, Live Forensics, Memory Analysis, Compressed RAM