November 2019

# OS AND HW INDEPENDENT MEMORY SNAPSHOT TOOL FOR ANALYZING SYSTEM STATE AND REVERSE ENGINEERING MALWARE AND BUGS

HP INC

# OS AND HW INDEPENDENT MEMORY SNAPSHOT TOOL FOR ANALYZING SYSTEM STATE AND REVERSE ENGINEERING MALWARE AND BUGS

A method for obtaining a memory snapshot of a computer while in operation is disclosed. This method involves using a System Management Interrupt (SMI) to read memory and write it out to a designated output for further analysis.

The ability to look at system memory when analyzing a PC system for malware or bugs is invaluable. Traditionally, memory snapshots have been obtained using software in the OS or specialized hardware. Software cannot capture a true snapshot because the OS is still running and modifying memory. Specialized hardware can halt the OS, but can be expensive, hard to find, and hard to use. Both capture methods can be detected by malware running on the system. If the snapshot is detected by malware, the malware could manipulate the data being captured to hide itself, modify pieces of itself to make reverse engineering difficult, spread common malware fingerprints throughout memory to increase the difficulty of memory forensics, or several other anti-memory forensics techniques.

With SMM, system management mode, it is possible to halt the OS and obtain a snapshot of all memory and registers while remaining transparent to the OS. First, an SMI handler, which will ultimately take the snapshot, is registered in the firmware. Next a user initiates the snapshot, at any time, by triggering the SMI. This freezes the OS and transitions the processor into SMM. While in SMM, the processor can read all system memory and registers. It will then write those values to a target area (such as a reserved area of system flash or a file) and return control to the OS. The snapshot can be further configured on a timer or other pattern allowing a user to obtain snapshots over time for dynamic analysis.

An example of such a system is comprised of an embedded controller, a keyboard connected to the embedded controller, and firmware that runs in system management mode. The user can trigger a snapshot of system memory at any time by pressing a preconfigured key on the keyboard. The EC will see the keypress and generate a hardware SMI. The SMM code will perform the snapshot and output it to a file on the hard drive. Afterwards, execution will return to the OS, and the user can analyze the memory snapshot.

*Disclosed by Mason Gunyuzlu, Robert Ste Craig and Tevin Richards, HP Inc.*