B29 The Application of Virtual Machine Introspection to Digital Forensics

Brian Hay, PhD, PO Box 84064, Fairbanks, AK 99708*

After attending this presentation, attendees will understand the general concepts associated with Virtual Machine Introspection (VMI) and how VMI can be applied to recover data of interest to a digital forensics investigator. While virtualization is increasingly common in many environments, investigations tend to still be conducted using traditional approaches (e.g., static analysis of media or "traditional" live forensics using tools executed within the Virtual Machine (VM)).

This presentation will impact the forensic science community by describing and demonstrating new capabilities that can be applied to investigations in virtualized environments.

As virtualization becomes increasingly common, it is important to explore the extent to which existing techniques can be applied to virtualized environments, and what new forensic techniques may be applicable. VMI is a process by which the virtualization layer (e.g., a hypervisor) can unobtrusively inspect the complete state of a running virtual machine. VMI is particularly applicable to live digital forensics, as it allows the state of a running VM to be examined without requiring the investigator to install (or even run) software or tools on the VM under investigation, nor does it require that the investigator possess valid user credentials for the VM. Using this technique, forensically valuable data such as process lists, network connections, user activity, and memory contents can all be transparently extracted from the VM.

Recent work for this study (with funding from the DARPA Cyber Fast Track program) in the area of VMI has extended these capabilities to include the ability to gain direct access to cryptographically protected content on the VM. In particular, a digital forensic investigator can use this newly developed VMI tool set to examine a VM and recover cryptographic keys, monitor-encrypted (e.g., SSL and SSH) communication channels, and access encrypted files and storage volumes. Much of this content is either highly volatile or inaccessible without the cryptographic keys and, as such, would be unlikely to be accessible using more traditional digital forensics techniques.

This presentation will describe the applicability of VMI to digital forensics in general, and demonstrate its use to recover system data (e.g., process and network state information) and cryptographically protected content.

Virtualization, VM Introspection, Cryptography

