Countering Anti-Forensics with Virtualization Technology

Ralph Palutke

This thesis investigates novel anti-forensic techniques for hiding malicious activity and proposes counter strategies for conducting robust digital analysis through virtualization technology. We begin by surveying the current landscape of memory acquisition, a technique extensively used during forensic investigations. In order to evade analysis, malware nowadays incorporates sophisticated anti-forensics, which hinder the analysis process. We present advances in anti-forensics by introducing new methods for hiding memory from analysis tools to expand existing knowledge. The final part demonstrates analysis techniques that provide resilience against anti-forensics.

First, we define a universal taxonomy of different methods for acquiring a system's memory, many of which have proven to be vital against modern malware threats. Then, based on this taxonomy, we comprehensively survey the field of modern memory acquisition, abstracting from both Operating Systems (OSs) and specific hardware architectures. Finally, we unveil the limitations of today's acquisition techniques and conclude that most approaches are prone to anti-forensics, enabling malware to subvert the analysis process and escape the investigation.

In the second part, we introduce new approaches that hide memory from forensic applications, preventing analysts from accessing the content of specific regions. On the one hand, we manipulate the memory management subsystem of different OSs to alter the memory view of live forensic tools. In addition, we demonstrate different strategies to detect these subversion techniques, providing a possibility to improve respective tools. With Styx, on the other hand, we present a powerful rootkit technique that leverages hardware-based virtualization to counter even robust acquisition methods. Styx subverts the highly privileged hypervisor layer to take complete control over a system without introducing detectable modifications. Furthermore, to prevent acquisition software from noticing the rootkit's memory footprint, Styx locates in particular memory regions reserved for device mappings. As these regions are not always entirely consumed by devices, the resulting offcuts serve our rootkit as a perfect hiding spot. Furthermore, by simulating invalid address ranges which are not accessible to a processor, Styx deceives forensic tools with a tampered view on these leftovers.

Finally, we demonstrate the design of anti-forensic resilient systems which enable a forensically robust analysis through virtualization. We first present SEVGuard which protects (forensic) applications from malicious threats operating at the highest privilege levels. Based on virtualization and encryption features of modern processor architectures, SEVGuard provides a secure execution environment that enforces confidentiality and integrity of existing applications by encrypting their memory and processor state. Instead of protecting an application, StealthProbes hides the analysis component from the examined target, giving analysts the chance to inspect its functionality without risking the sample to notice the investigation. Our system stealthily instruments an application's memory and hides these modifications, leveraging the latest virtualization features and exploiting cache incoherencies that arise from memory address translations. Furthermore, StealthProbes integrates a transparent function-level tracer for enabling deep insight into an application's runtime behavior. As a result, even programs that thwart the analysis by enforcing code integrity are stealthily dissectable. For achieving a forensically sound investigation, the actual deployment or execution of a forensic method must not alter the state of an analyzed system. With HyperLeech, we present a minimally invasive approach which uses Direct Memory Access (DMA) to stealthily deploy a forensic hypervisor through external Peripheral Component Interconnect Express (PCIe) hardware. The hypervisor transparently virtualizes the running target system, serving analysts as a stealthy and privileged execution layer for all kinds of forensic tasks. Without causing a notable impact on the target's state, HyperLeech enables forensic methods to execute without the risk of destroying evidence or alerting malware.