Title: Bringing Memory Forensics and Virtual Machine Introspection to Production Environments

Student: Benjamin Taubmann

PhD stage: Third year, finisher

Advisor: Prof. Dr. Hans P. Reiser

Affiliation: Assistant Professorship of Security in Information Systems University of Passau

Research Area: System Security, Memory Forensics, Virtual Machine Introspection

Projects: DINGfest (BMBF), ARADIA (DFG)
Motivation

“Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer’s iPhone”
- CNBC, 2017

What is the problem?

- **Missing interface** for memory access on production systems (cloud, mobile devices)
- **Performance** of current memory forensics and virtual machine introspection tools is too slow for use cases in production environments

Why is it a problem?

- Forensic investigators and common users cannot do memory based forensics on (their) VMs and mobiles devices
- Cloud customers cannot benefit from the **advantages of memory forensics and VMI-based security approaches**: a higher level of isolation, stealthiness and forensic soundness than traditional in-guest security solutions.
Research Questions

1. **Data Acquisition**: How to get access to the memory of production systems such as cloud environments or mobile devices?

2. **Information Extraction**: How to locate and extract high level information efficiently from main memory?

3. **Applications**: How to deploy and adapt VMI methods to the requirements of real world use cases and modern computing systems?
Overall Architecture

1. Data Acquisition
   - Read
   - Trace
   - Write
   - Intercept Network

2. Information Extraction
   - Semantic Knowledge: Data Structure Layout, Function Address
   - Trace Functions
   - Modify Values
   - Trace Syscalls
   - TCP/IP Packet
   - Network Packet Payload

3. Application
   - Digital Forensics
   - Malware Analysis
   - Intrusion Detection

Forensic Framework

Analyzed System
- System State
  - CPU
  - Memory
  - Network

Library
- Application
- ...
Contributions (bold red)

Static Analysis

Libvmi
Coldboot
Snapshot
CloudPhylactor

Dynamic Analysis

Ssh
Honeypot
Intrusion Detection System
Malware Analysis

Digital Forensics
Volatility/
Rekall

Libvmtrace
TlsKex

DroidKex

Drakvuf

Taubmann Digital Forensics on production environments
The main contributions of the thesis are:

1. A generic architecture for digital forensics on production systems
2. Data acquisition architecture for digital forensics in cloud environments and on mobile devices
3. Efficient TLS session key extraction from main memory of applications
4. Adapting resource intensive VMI-based tracing to the requirements of different use-cases that require minimal overhead such as intrusion detection systems

Extended slide set:
Thanks!
Publications


