Privacy-Aware Malware Detection

Department of Computer Science
University of Maryland
Sanghyun Hong, Mingfei Gao, Parsa Saadatpanah, Andrew James Pachulski
Overview

- **Stealing Credentials**
  - Customers can sell Virtual Machine (VM) images via a market place
  - The VM images include open-source or 3rd-party software in themselves
  - Attacker can create VM images that include infected (malicious) software
Overview

- **Denial of Services (DoS) attacks**
  - Customers can sell Virtual Machine (VM) images via a market place
  - The VM images includes open-source or 3rd-party software in themselves
  - Attacker can create VM images that includes infected (malicious) software
Motivation

- **Malware Detection**
  - Malware detection techniques can help to find out infected VMs
  - Privacy issue: current detection methods need semantic information in VMs
  - Can we do malware detection without accessing to virtual machines?
How to Solve

• Malware Detection Framework

Virtualization Indicators

Precise performance counters
Branch Trace Stores (BTS)
Last branch report
Hardware events
- Retired instructions
- Retired branch instructions
- L1 cache stores
- I/O operations
- Function return addresses
Additional indicators
- Hyper/system calls in Dom0
- Calltrace of binaries in Dom0
Why this is awesome!

- **Limit**: Prior works need introspection of VMs, which potentially leaks users’ credentials
- **Limit**: Other methods require to attach custom, extra hardwares to the infrastructure
- We’re able to address these issues without *jeopardizing* the users’ privacy, or *touching* the infrastructure
Q & A

Department of Computer Science
University of Maryland

Sanghyun Hong, Mingfei Gao, Parsa Saadatpanah, Andrew James Pachulski
{shhong, parsa, mgao, ajp}@cs.umd.edu