CMPS223 Final Project: Virtual Machines & Security

Michael Sevilla

December 5, 2012
Virtual Machines (VMs) and Security

Type 1 VM Environment

Benefits of using a VM

- Resilience: isolation
- Visibility: hw access

Introspection: extract guest OS state from outside VM

Benefits of using a VM

- Intrusion Detection Systems
- Malware Analysis Systems
The problem with introspection...

Getting OS state is easy!

✓ inside OS (programs & APIs)
✓ outside OS (VMM utilities)
The problem with introspection...

Getting OS state is easy!

✗ inside OS
✓ outside OS

Problem: can’t trust guest OS to expose its state

- (programs & APIs)
- (VMM utilities)
Digital Forensics and Introspection

Forensic Memory Analysis (FMA)

- \{locate, reconstruct, “walk”\} OS structs

For security: (1) snapshot, (2) FMA, (3) make decision
Leveraging introspection & FMA tools

Components:
- KBeast: root kit that hides files, processes, & modules
- LibVMI: “live” introspection tool
- Volatility: extract structs from RAM

```bash
0:00 /bin/login --
0:00 [flush-202:32]
0:00 -bash
```

**Components:**
- KBeast: root kit that hides files, processes, & modules
- LibVMI: "live" introspection tool
- Volatility: extract structs from RAM

**Extra Slides**
- Automizing Introsp.
- Leveraging introspection & FMA tools
Leveraging introspection & FMA tools

Components:

- **KBeast**: root kit that hides files, processes, & modules
- **LibVMI**: “live” introspection tool
- **Volatility**: extract structs from RAM

![Diagram showing the components and processes of introspection and FMA tools.](image-url)
Questions?
Automizing Introspection

- (1) train, (2) analyze traces, (3) create host programs
- simple, general, reliable; poor performance

VM Space Traveler (VMST) [Fu et al. IEEE Security & Privacy 2012]
- (1) ID syscall context, (2) ID data, (3) redirect
- fully automated, general, reliable; poor performance

Problem: these are complex and difficult to operate