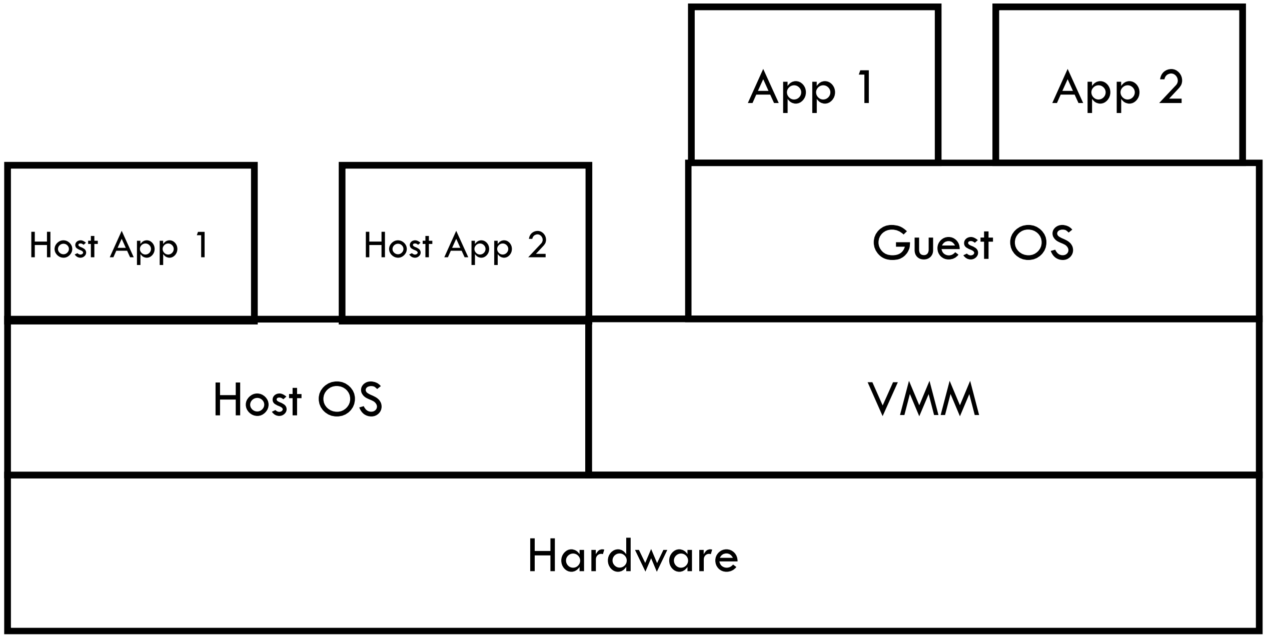
SUBVIRT : IMPLEMENTING MALWARE WITH VIRTUAL MACHINES

Samuel T. King, Peter M. Chen
University of Michigan
Yi-Min Wang, Chad Verbowski, Helen J. Wang, Jacob R. Lorch
Microsoft Research

Presented by : Anuj Sawani

Virtual machines



- The VMM emulates hardware for each virtual machine
- Virtual Machine Monitor (VMM)
  - Manages hardware resources
  - Provides abstractions of virtual machines

Motivation of malware

- Attackers aim to gain maximum control of a system
- Lower layer -> More control
- Advantages of working in a lower layer?
  - Attacker’s perspective?
  - Defender’s perspective?
- Malware is migrating from user-level to kernel-level

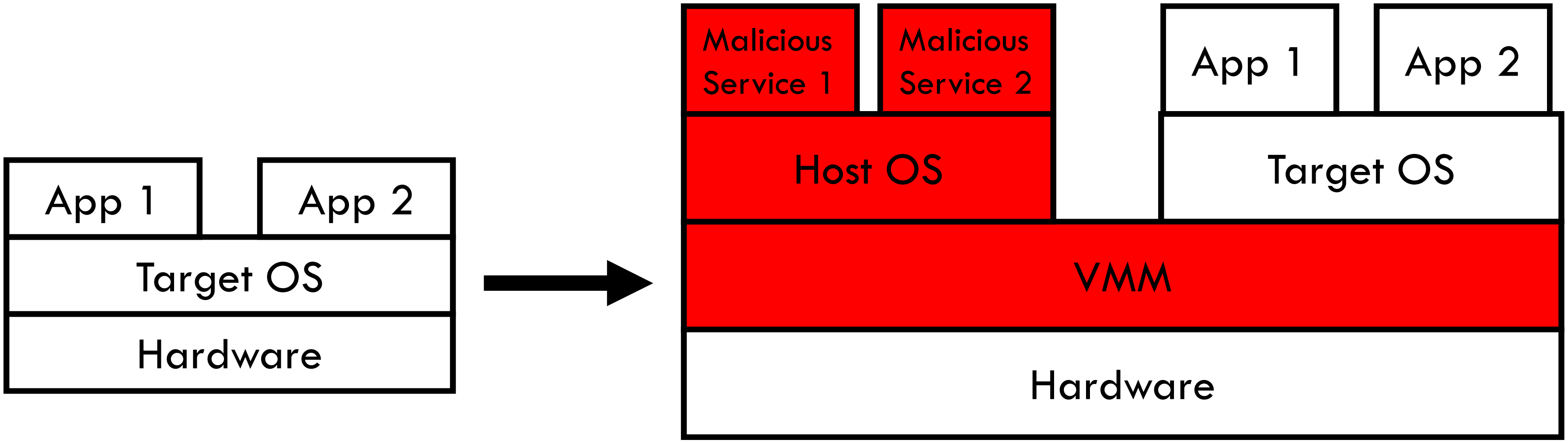
Rootkits

- Kernel-level malware
- Modifies part of an operating system to gain control
- Sony rootkit debacle?
- Non-hostile rootkits?

IF YOU PLAY ONE ON A PC, IT INVISIBLY INSTALLS STUFF INTO YOUR SYSTEM THAT VIRUS WRITERS CAN USE TO HIDE ALL KINDS OF MALICIOUS CODE.
MAKES YOU FEEL SORRY FOR PEOPLE WHO BOUGHT THE NEW CELINE DION ALBUM.

Virtual Machine Based Rootkits (VMBR)

- VMM installed below the OS layer
- Host the attacked OS over the VMM



Before infection

After infection

Installing the VMBR

- Gain root privileges
- Load the VMBR on disk
  - Windows – beginning of primary partition
  - Linux – use swap partition
- Modify boot sequence
  - During final stages of shutdown
    - Avoids detection

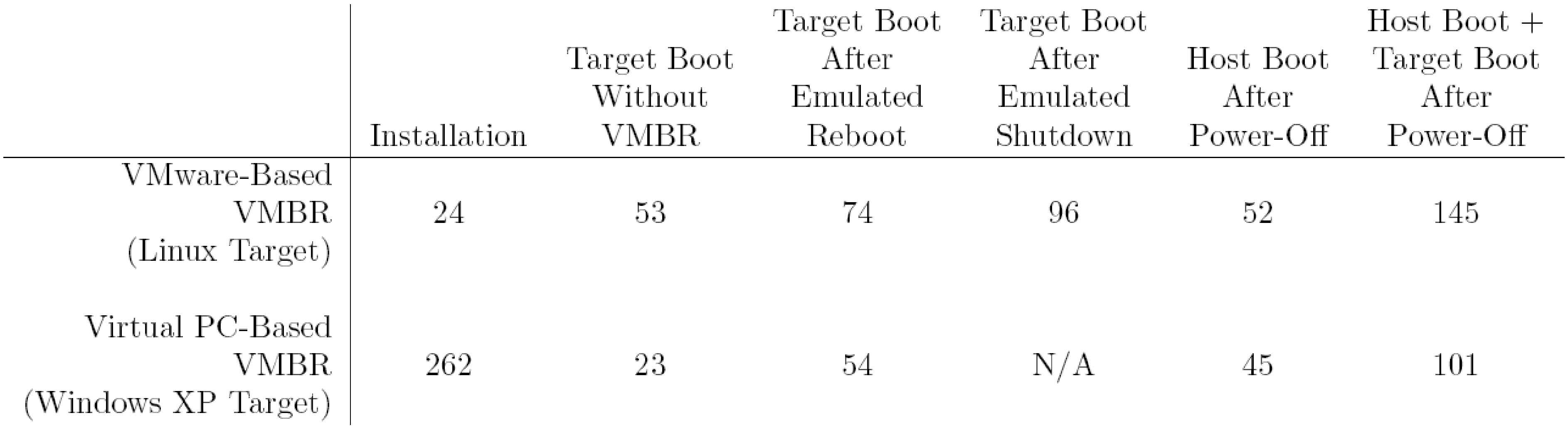
Malicious services

- Three categories
  - Do not interact with target OS
    - Phishing web servers
  - Observe target OS
    - Keyloggers
  - Perturb execution of target OS
    - Prevent detection
      - *redpill*

Maintaining Control

- Control lost during start-up till VMBR loads
- Solution : Virtual power-off
  - Provides only an illusion of shutdown/reboot
  - Uses ACPI sleep states
  - "Astute computer users might notice a difference in power LED after an emulated shutdown, but average computer users probably would not"
    - Really???

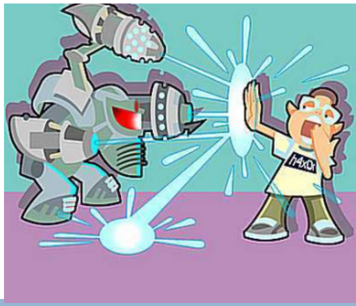
Evaluation



	Installation	Target Boot Without VMBR	Target Boot After Emulated Reboot	Target Boot After Emulated Shutdown	Host Boot After Power-Off	Host Boot + Target Boot After Power-Off
VMware-Based VMBR (Linux Target)	24	53	74	96	52	145
Virtual PC-Based VMBR (Windows XP Target)	262	23	54	N/A	45	101

- Result : Performance affected
  - Users may not notice
  - Weakest link : Can be used to detect a VMM

Defending VMBR



- Software below VMBR layer
  - Trusted computing
  - Boot from a secure medium
  - Run a secure VMM
- Software above
  - CPU overhead
  - Memory overhead
  - Virtualization of I/O devices
    - Indirect DMA access
  - Imperfect virtualization
    - *sidt* instruction

Towards Complete Virtualization

- Good or bad for VMBR?

- Good
  - Future enhancements to x86 architecture
    - Hide VMBR better
- Bad
  - Widespread use of VMM
  - Secure VMM
    - Attestation of state

Conclusion

- VMBR has more control than current malware
- Best way to detect VMBR
  - Work below the VMBR layer
- Disadvantages :
  - Hard to install
  - Require a reboot
  - Impacts performance

Take Away

- VMBR – valid threat

- Virtualization – not necessarily a good thing …