STM/PE & XHIM

Eugene D. Myers
Trust Mechanisms
Information Assurance Research
NSA/CSS Research Directorate
May 24, 2018

Overview

- SMM
- STM
- STM/PE
- XHIM, an STM/PE application
- Future Plans

System Management Mode (SMM)

X86 Processor Mode

Entered via an SMI

- Cannot be blocked
- Brings all CPUs into SMM
- Entry is “invisible” to the O/S

Executes in SMRAM

-Area defined by chipset & processor

-Protected from I/O and non-SMM access

Exited via RSM instruction

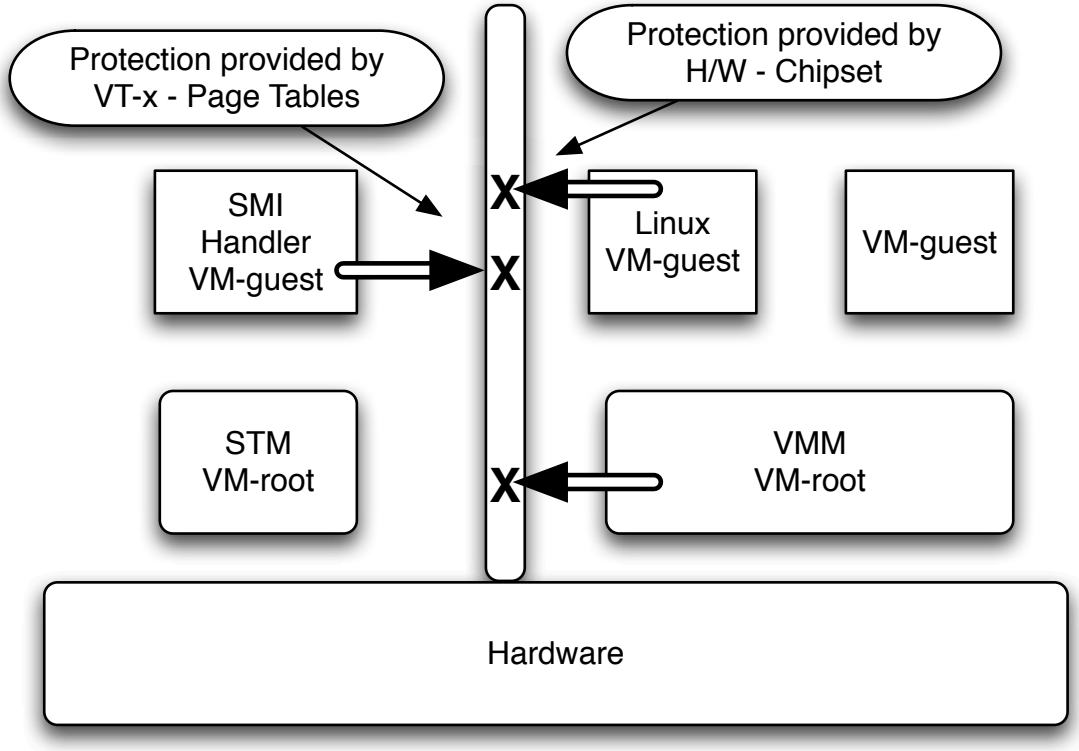
SMM Dual Monitor Treatment

- VTX added Dual Monitor Treatment
- SMM root-VM is a peer to the ring-0 root-VM
- Two possible methods of entry
  - VMCALL (root-VM only)
  - SMI
- Translated to a VMEXIT to the SMM root-VM
- Interrupted/calling VM becomes the guest-VM

SMI Transfer Monitor (STM)

- Simple Hypervisor
  - VMCS Switcher
- SMI-handler now runs in a guest-VM
  - Restricted by the VM protections
- Manages the security policy to restrict the SMI handler's access
  - In coordination with the O/S

STM



SMI Transfer Monitor (STM)

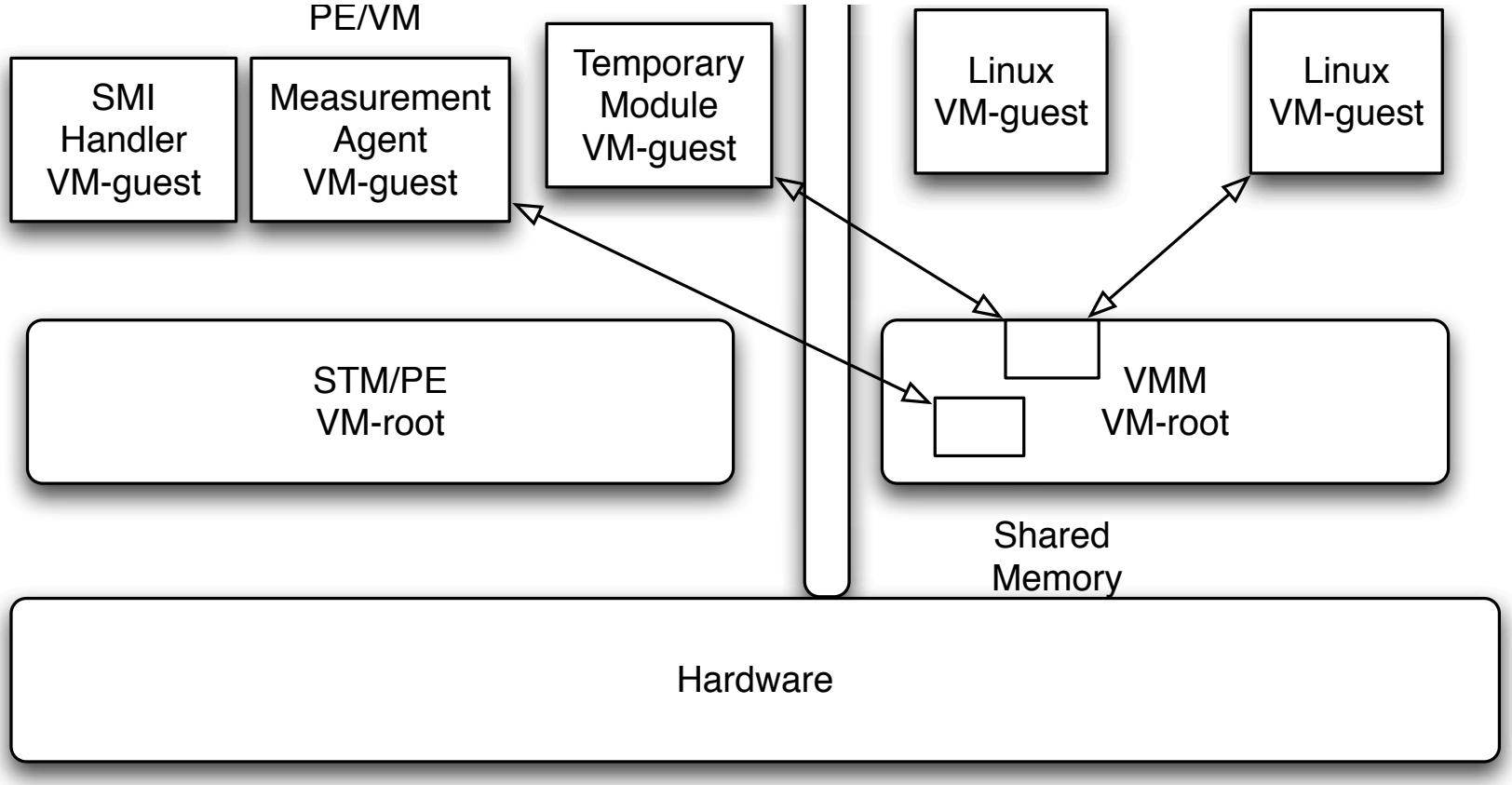
STM/PE Overview

- Protected Execution (PE)
- STM/PE – NSA mods to a “stock” STM
- XHIM – Dynamic integrity measurer
- Current Status and Future Plans

Protected Execution

- Execution that cannot be viewed external to the “container”
  - By OS
  - Other processors
- Executing a VM in SMM where that VM is located in SMRAM can provide this

STM/PE


PE/VM
SMI Handler VM-guest
Measurement Agent VM-guest
Temporary Module VM-guest
Linux VM-guest
Linux VM-guest
STM/PE VM-root
VMM VM-root
Shared Memory
Hardware

STM/PE based on

- Dell STM
  - Developed by Dell for NSA as a POC
- Intel Reference STM
  - Open-source (On github)
  - Includes instructions to add STM support to TianoCore BIOS
  - Info at: firmware.intel.com

Protected Execution Support

- Security-PE module access is restricted by explicit permissions vice BIOS centric model used in STM spec
  - PE/VMs will not have access to I/O, MSRs etc.
  - Allowed access only to specific areas in memory.

STM/PE Gotchas

- O/S support is necessary to deal with the “disappearance” of a processor
- This true of any technology where the CPU goes into a different mode without telling the O/S
- Q: Is it possible to have a feature for the O/S to learn this w/o thinking that there is a failure

XHIM, an STM/PE application

- Based on LKIM
- Linux Kernel Integrity Measurer
- KIM “Engine” is core to
  - LKIM – Linux
  - XHIM – XEN (Protected by STM/PE)
  - WinKIM – Windows 10
- Dynamic Integrity Measurement

Dynamic Integrity Measurement

- Does not rely on signatures
- Characterizes how legitimate software is supposed to behave
- Software behaves in very predictable ways according to its source code
- Malware often changes kernel state in a manner that is inconsistent with the kernel's source code
- Identifies any deviation as malicious / bug

KIM detects two kinds of attacks

- Kernel code injection
- Kernel control flow attacks
- Implants cause inconsistent system state
- KIM detects the inconsistent state
- Can detect the effects resulting from a Zero Day
- Can also detect bugs

XHIM and STM/PE

- XHIM is a permanent PE module
- STM/PE protects XHIM from interference by other elements in the system
- Access to system memory is limited to:
  - r/w region to pass back results and
  - XEN kernel memory (r/o) for scanning

Starting XHIM

XHIM Starts by either a

- vmcall from ring-0 (debug)
- SMI timer interrupt (production)
  - In this case, XHIM is loaded during XEN setup
  - Currently, runs in this mode on development box every 16 seconds

XHIM – Current Status

- Incorporated into LKIM source tree
  - Updated to current LKIM version
- Utilizes the hardware state information provided by the STM
  - CR3 (page table pointer)
  - Active VMCS's (Virtual Machine Control Structure)
- Baselining streamlined

STM/XHIM Support– Current Status

- Both on-demand and timer execution
- Provides processor state info for all processors
- Provides VMCS layout info
  - Calculates this information on initial request
- Clears XHIM heap before each execution
  - “reset hashable” – known state for each run

Future

- STM/PE and XHIM is basis for our internal pilot
  - Will use Open-XT
  - Will be incorporated into a larger measurement appraisal management system
  - WinKIM and LKIM will measure Windows and Linux VMs respectively
- Run a virtual TPM (vTPM) in a temporary PE/VM
- Soon to be open sourced


RESEARCH DIRECTORATE
SECURITY AGENCY
ADVANCING INTELLIGENCE THROUGH SCIENCE
R&E DIRECTORATE

Questions