Secure Computer Systems

Virtualization and Security

Mustaque Ahamad, Ph.D.

Professor & Associate Director: Educational Outreach, Institute for Information Security & Privacy

Georgia Tech - College of Computing

Virtualization: Definitions, Implementations and Security Benefits

Georgia Tech

Before We Begin

- **We keep going back to the trusted computing base (TCB) idea**
- We addressed the isolation requirement of TCB in last module.
- How about complete mediation and correctness?
  - OS already does some resource virtualization, but we will explore if done at the full machine level, can it help even more.
- **Virtualization offers many benefits**
- We will limit our discussion of virtualization to its relevance to security.

Why Virtualization?

Georgia Tech

Complete Mediation & Virtualization

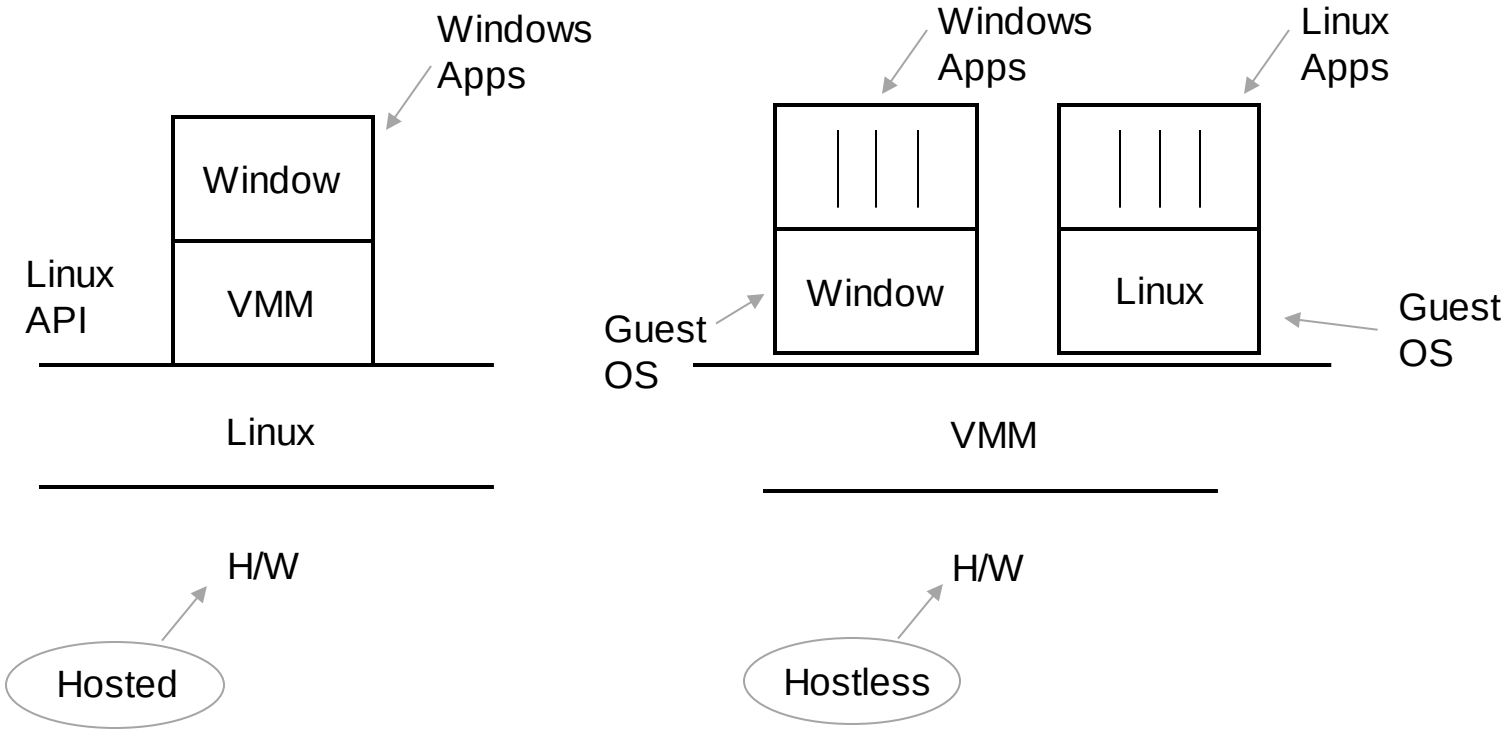
- Virtualization allows user applications to work with virtual rather than physical resources
- This makes it necessary to map virtual resources references to physical resource pointers
- User code can only manipulate virtual resource references
- By having the TCB control virtual-to-physical mapping, we can ensure complete mediation
- Examples
  - Virtual memory – page fault handling
  - Files – disk blocks
  - Sockets – network interfaces
- Assumption: All I/O instructions are privileged

Virtualization Could Lead to Simpler/Smaller TCB

- Operating system both allocates resources among processes and manages them
- Can we separate resource allocation from management?
- Virtualization at full machine level: Virtual machine monitor (VMM) or hypervisor
- VMM should expose the physical machine to the operating system but multiplex its resources among virtual machines (VMs) that have operating systems that do resource management
    - Simpler and smaller VMM more likely to be correct (economy of mechanism design principle)
- VMM Types
    - Type I (Hostless) and Type II (Hosted)

Virtualization Models

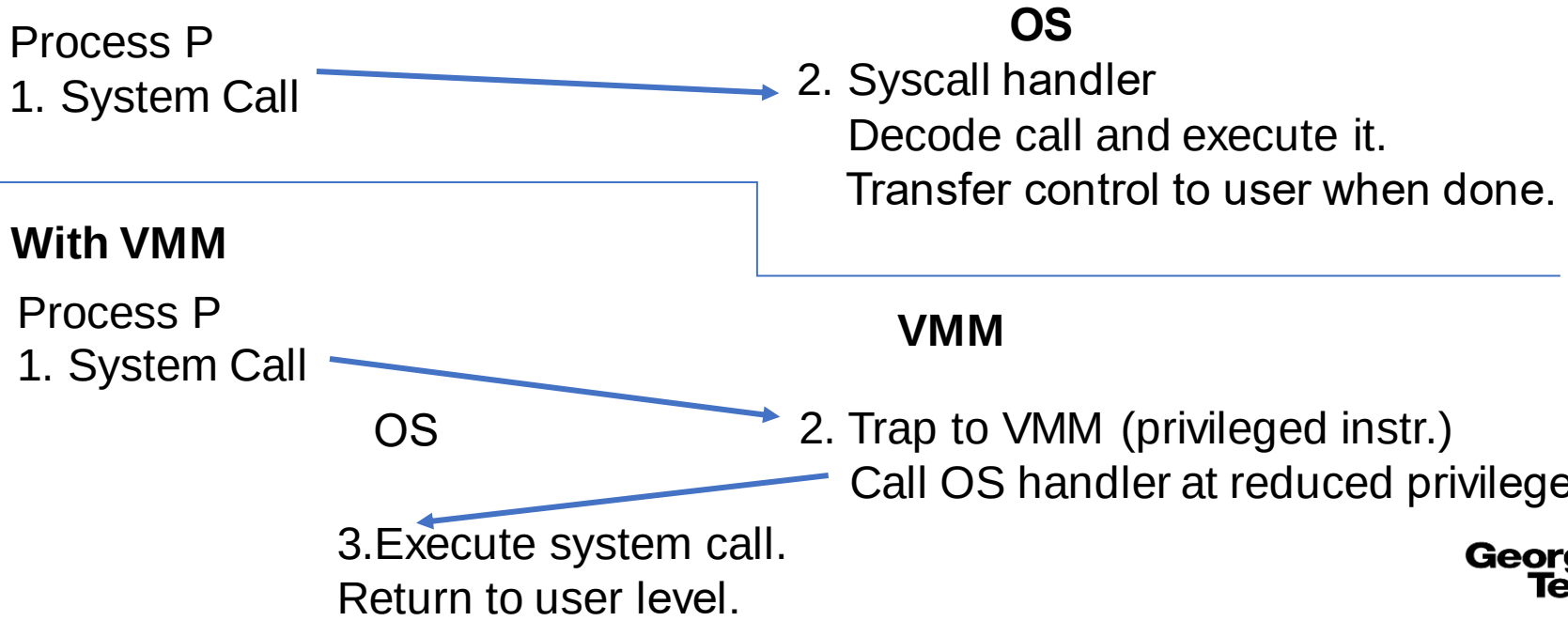
Hosted vs. Hostless VMMs



Georgia Tech

Revisiting System Calls (Control Transfer Across Protection Domains)

- **No VMM**



- **With VMM**

TCB in Hostless Virtualization

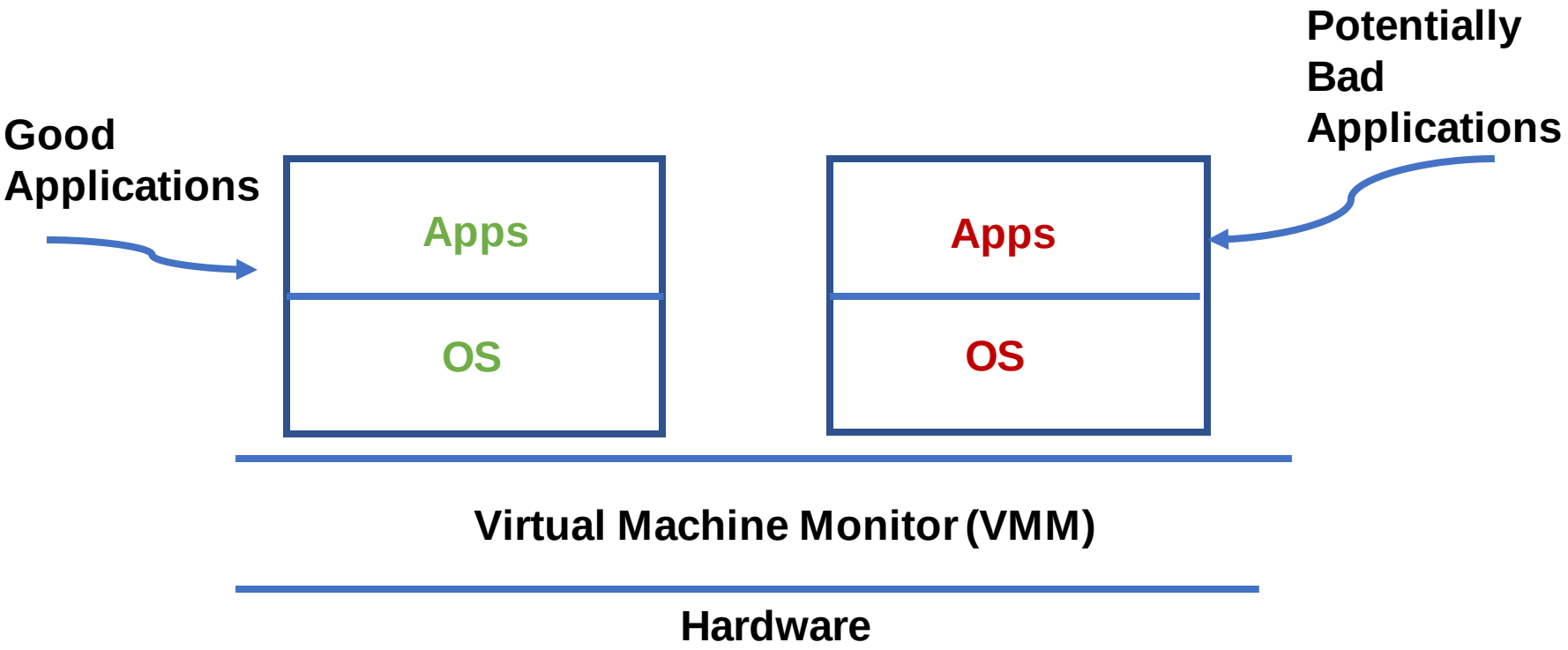
- VMM is the TCB
- Smaller, more likely to be correct
- Partitions hardware resources among virtual machines (VMs)
- Guest OS in VM manages resources
- Popular VMMs or hypervisors
    - Xen
    - VMWare ESX
    - Hyper V
    - KVM

Georgia Tech

Green & Red Virtual Machines

Georgia Tech

Green VM/ Red VM



Georgia Tech

Questions About Green/Red VMs

- Is green VM affected by exploitation of a red VM application?
- Is green VM application affected by red VM guest OS compromise?
- Is green VM affected by the compromise of the VMM?
- Does a green VM application only need to trust the VMM or also the green VM guest OS?
- What benefit do green/red VMs offer?
  - Isolation from potentially vulnerable applications

Georgia Tech

VMM Requirements and Full Virtualization vs. Para-virtualization

Georgia Tech

VMM Requirements

- **Transparency**
- VMM must provide execution environment identical to underlying physical machine (modulo performance degradation)
- **Complete Mediation**
- VMM must control all real (physical) resources
- **Efficiency**
- Most VM instructions should execute natively

VM Requirements for Type I VMM

- Non-privileged instructions should be executed the same way in user, guest VM OS and VMM
- All privileged instructions executed outside of VMM must trap to it.
- What instructions are privileged?
    - Instructions that attempt to reference mode of VM and state of physical machine
    - Instructions that read or write into sensitive registers and memory locations
    - Instructions that impact memory protection system and address translation
- Intel Pentium had sensitive instructions that were not privileged
- Virtualization technology (VT-x)

Georgia Tech

Paravirtualization vs. Full Virtualization

- OS likes to run in ring 0
- VMM must be most privileged
- OS aware it is not in ring 0?
  - Para-virtualization
  - Changes to OS (transparency requirement is not met)
- Other reasons for paravirtualization
  - Certain x86 instructions prior to VT were sensitive but not privileged
- Also related, binary rewriting to handle sensitive instructions

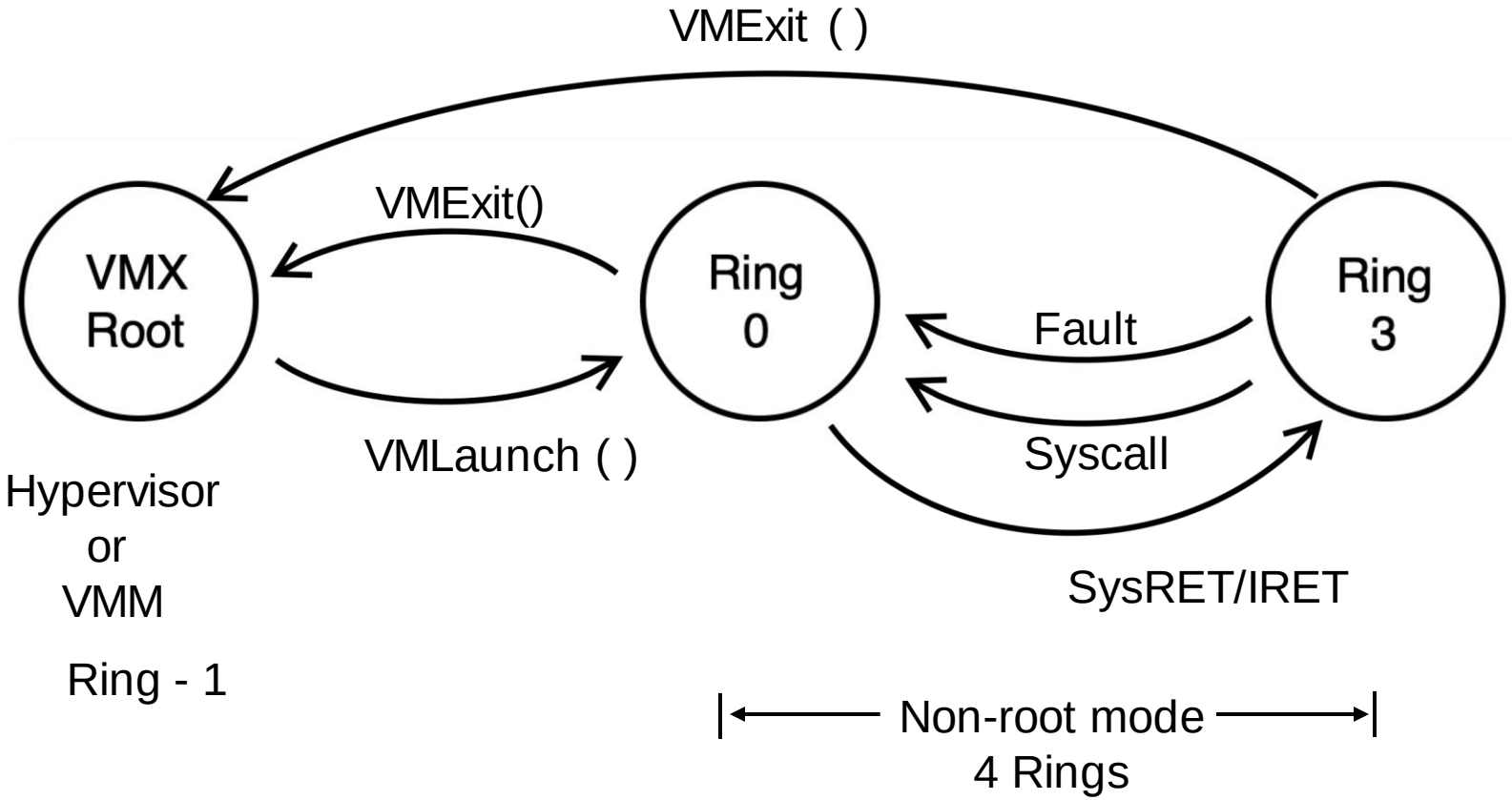
Hardware Support for Virtualization

Georgia Tech

Intel Virtualization Extensions – Hardware Support for Virtualization

- **Processor operation modes**
  - VMX Root (VMM)
  - VMX Non-Root (Guest)
  - VMX Non-root restricts access to certain registers and privileged instructions even when guest OS in ring 0
  - New instructions in root mode
- **Transitions**
  - VMEntry (from VMM to VM)
  - VMExit (from VM to VMM)

VT-x Privilege Rings



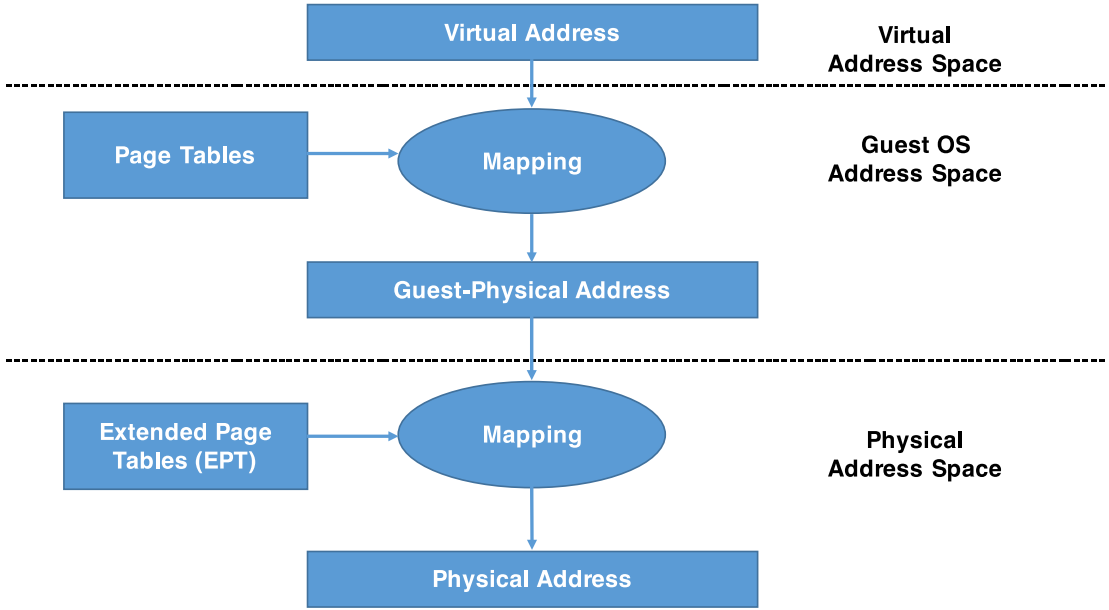
Georgia Tech

Address Translation in VT-x

Address Translation with VT-x

- Operating system likes to manage logical to physical address mapping
  - Problem: does not have direct control of physical memory
- Operating system maps to a ***guest-physical*** address in guest-physical address space
- VMM maps *guest-physical* to actual physical address with another paging structure
- *Extended page tables* (EPT) facilitate this

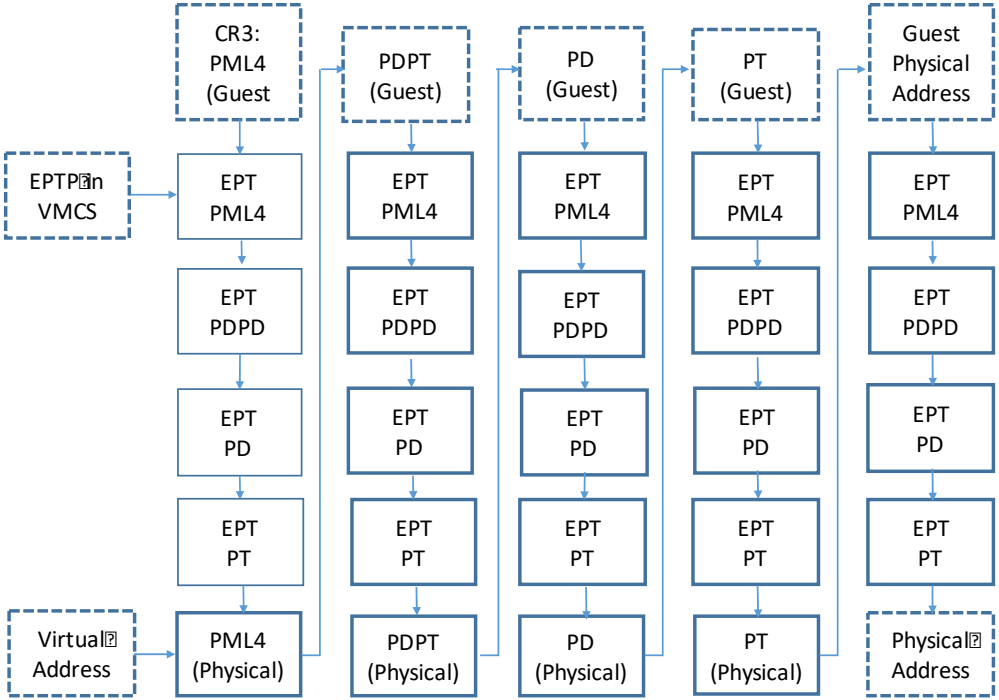
Extended Page Tables



- Source: Intel SGX Explained by Costan and Devadas, Page 10

Georgia Tech

More on VT-x Address Translation



- Intel SGX Explained, Page 11.

Georgia Tech

SGX: Finer-grain Protection without a Trusted VMM

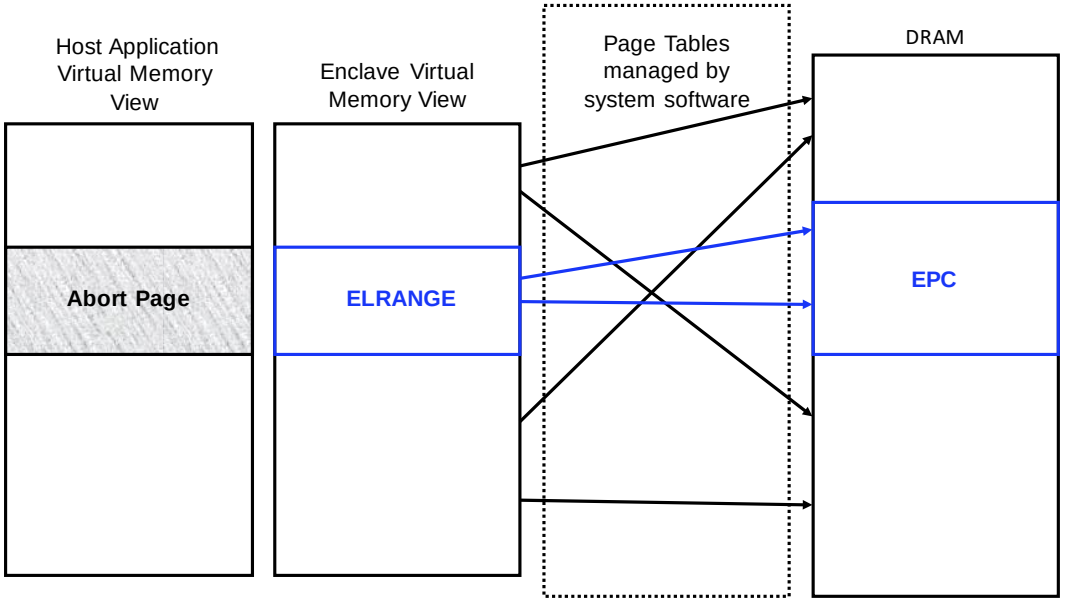
Georgia Tech

SGX – So We Do Not Trust the VMM

Hardware protected enclave in an address space that can store code and data that cannot be accessed by code outside of the enclave including hypervisor

So, on whose behalf this enclave code runs?

- Wait until we get to distributed system security



Georgia Tech

Attacks Against Virtualization Systems

Georgia Tech

VMM Vulnerabilities & Attacks

- **VMM is smaller so should have fewer vulnerabilities but they do exist**
- Many vulnerabilities going back to over a decade - checkout NVD
- Software vulnerabilities (see VMware security advisories)
- Cross VM row hammer attack
- Malware exploiting SGX?

- **What is TCB in a Xen based system?**
- Xen VMM
- Dom 0 and its privilege level
- Why might it still be better than no virtualization?

Virtualization & Threat Intelligence: Sandboxes for Malware Analysis

Georgia Tech

VMs and Malware Analysis

- **Large volume of malicious software**
- GT receives several hundred thousand a day
- **Dynamic analysis (execution of malware) provides valuable insights**
- Execute malicious program and collect artifacts such as accessed files, communication etc.
- **Can we use VMs to run malicious programs?**
- Yes, to scale up analysis but evasion could be a problem
- **Transparent malware analysis**

Georgia Tech

Summary

Summary

- **Virtualization and systems security**
  - Resource virtualization helps with complete mediation and smaller VMM helps with correctness of TCB
- **Type I hypervisor is of interest to us when we are concerned about security**
  - Hardware extensions enable full virtualization
- **Cloud computing relies on virtualization**
  - Cloud security: what is different?
  - How are containers related to virtualization?
- **Readings**
  - What goes in the hypervisor and guest OS (self-study, Xen paper)
  - Virtualization H/W support (Pentium paper)
  - Intel VT-x (Intel doc, VT paper and SGX Explained paper)
  - Ether malware analysis paper