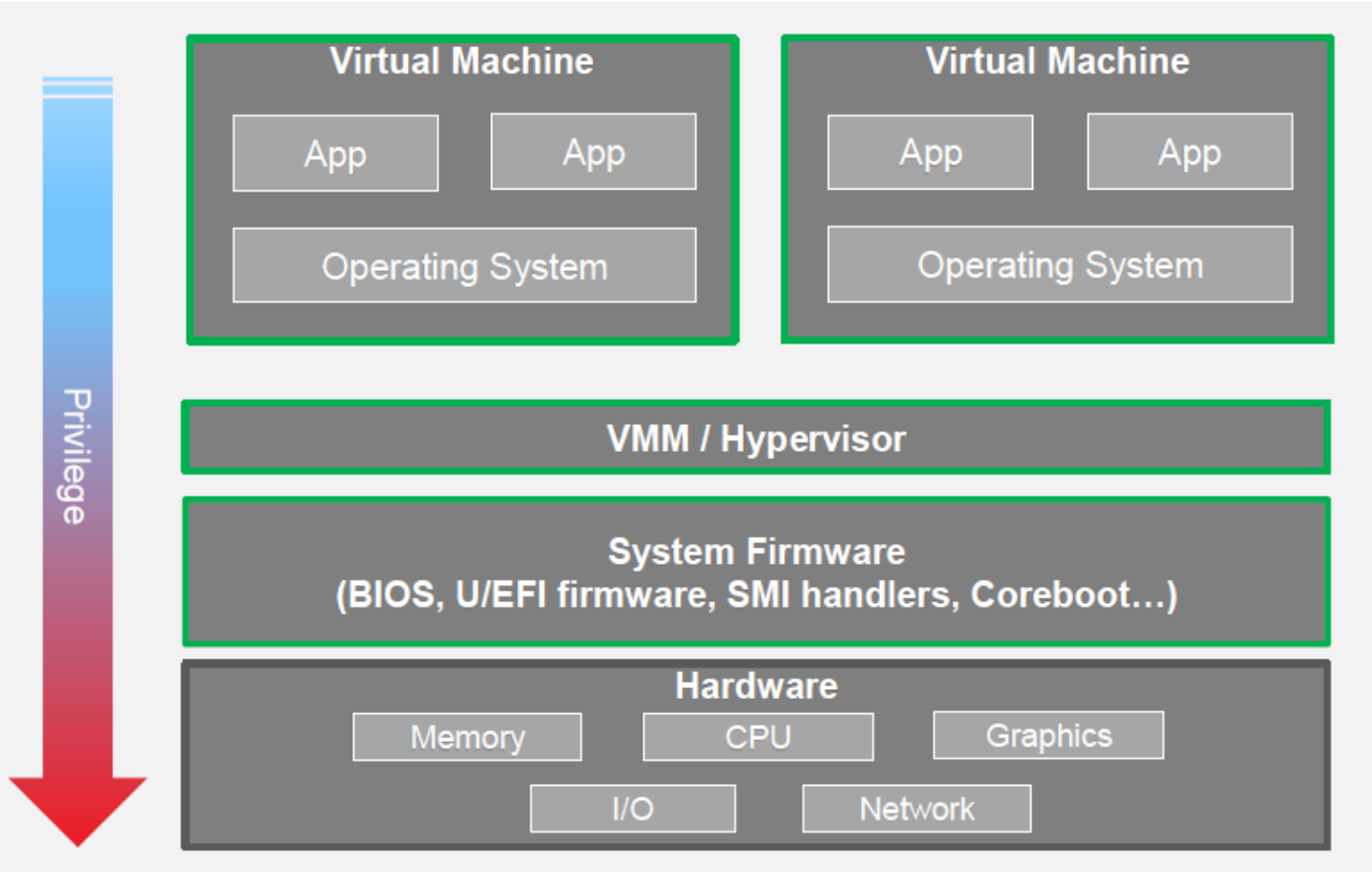
Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

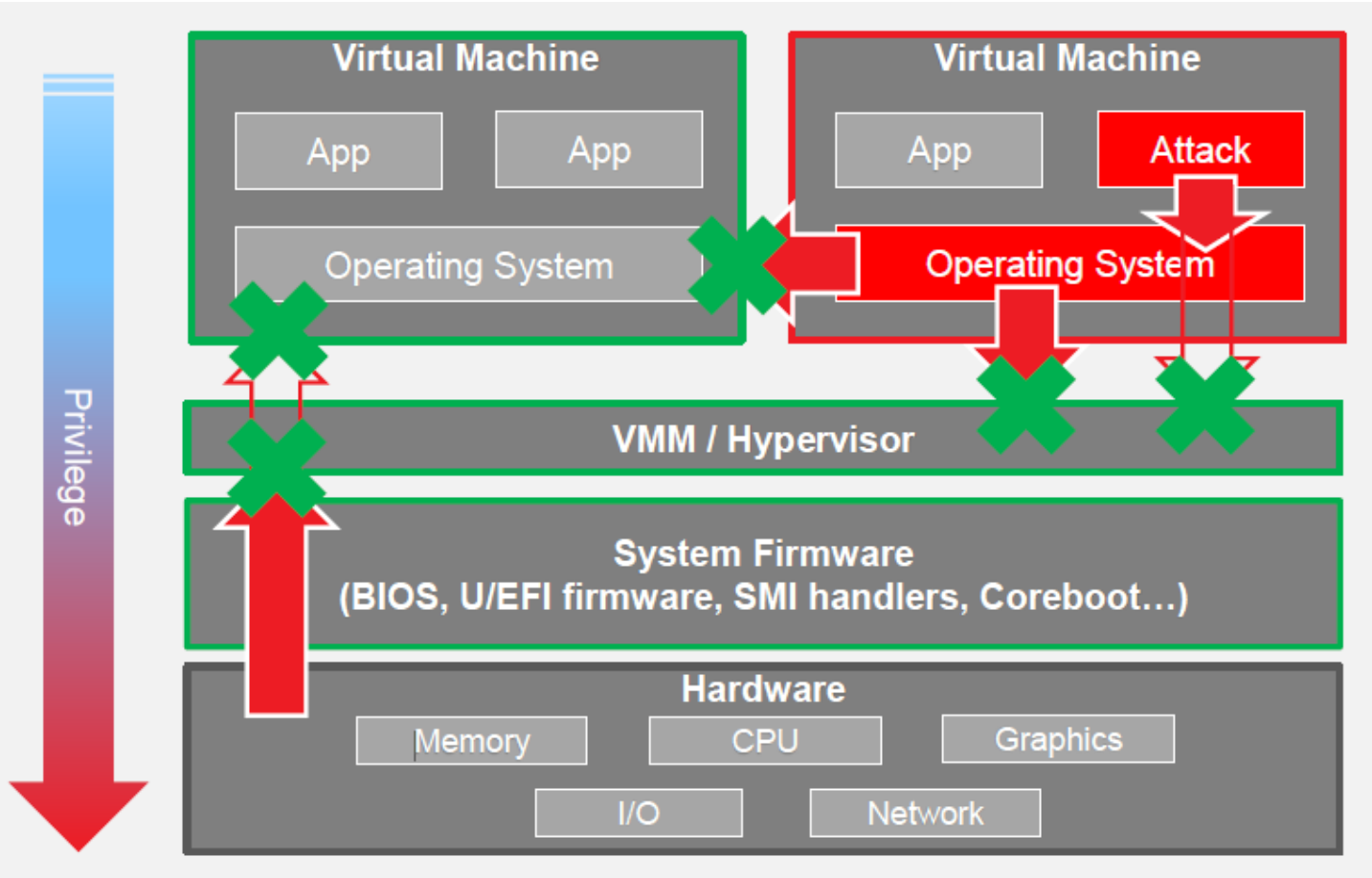
Feb 21, 2017

Outline

Hypervisor Based Isolation

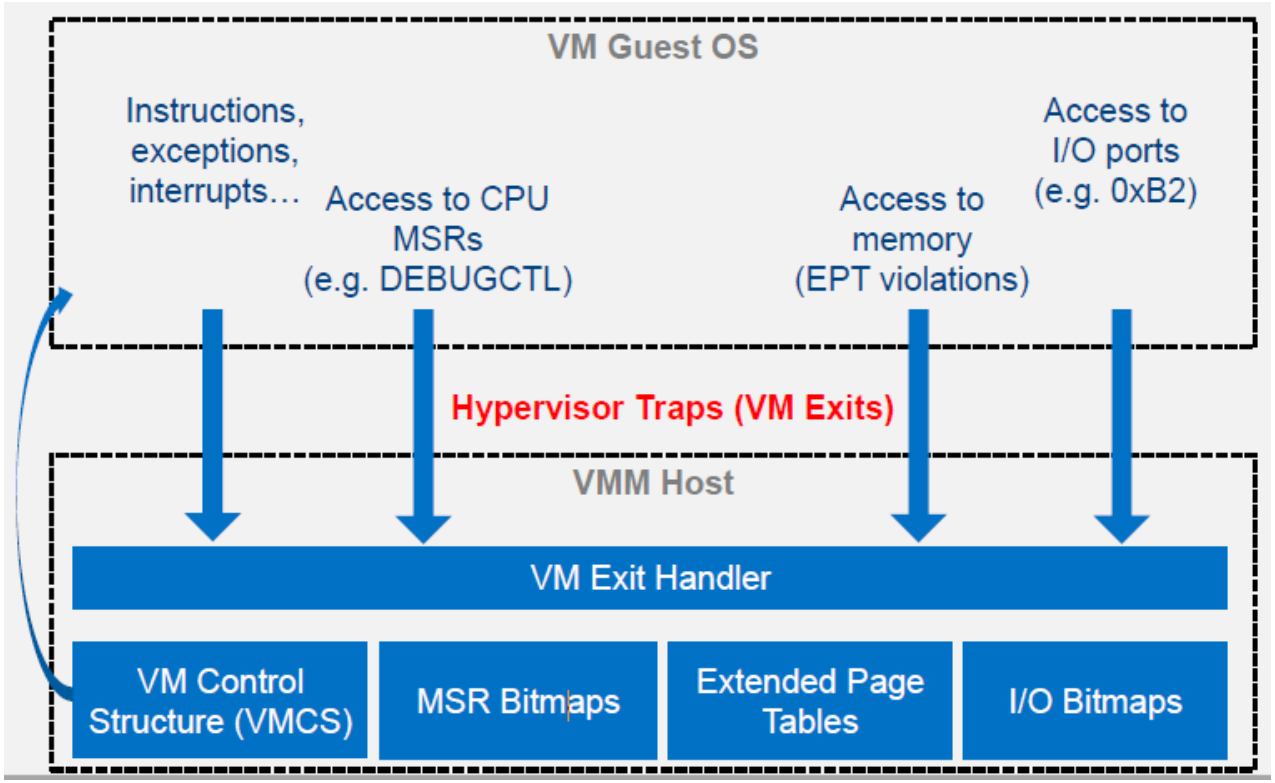


Hypervisor Based Isolation

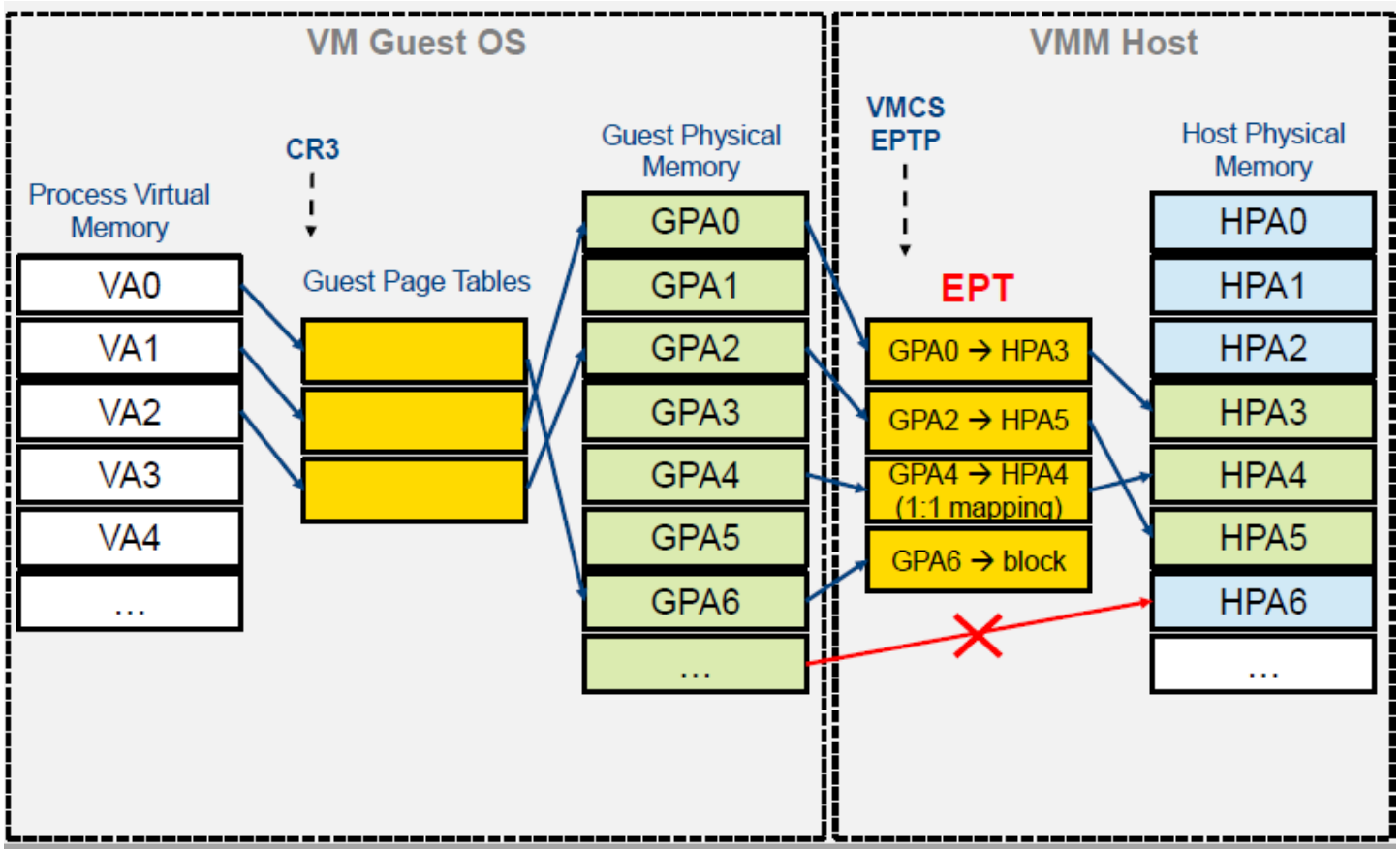


Hypervisor Protections

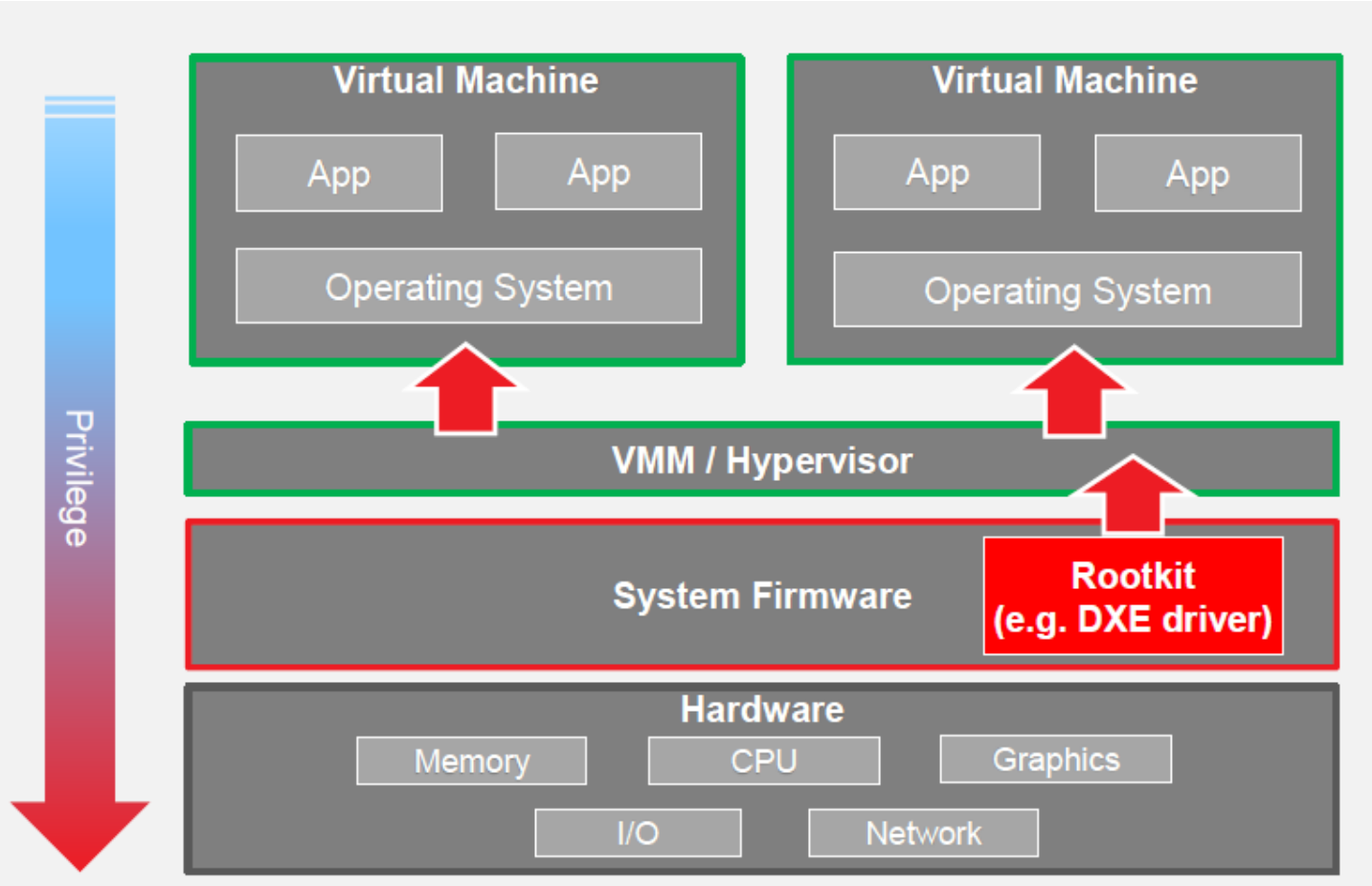
2. Software Isolation:
   - CPU: Traps to hypervisor (VM Exits), MSR & I/O permissions bitmaps.
   - Memory / MMIO: Hardware page tables, software shadow page tables.
3. Devices Isolation:
   - CPU: interrupt remapping
   - Memory: IOMMU, No-DMA ranges



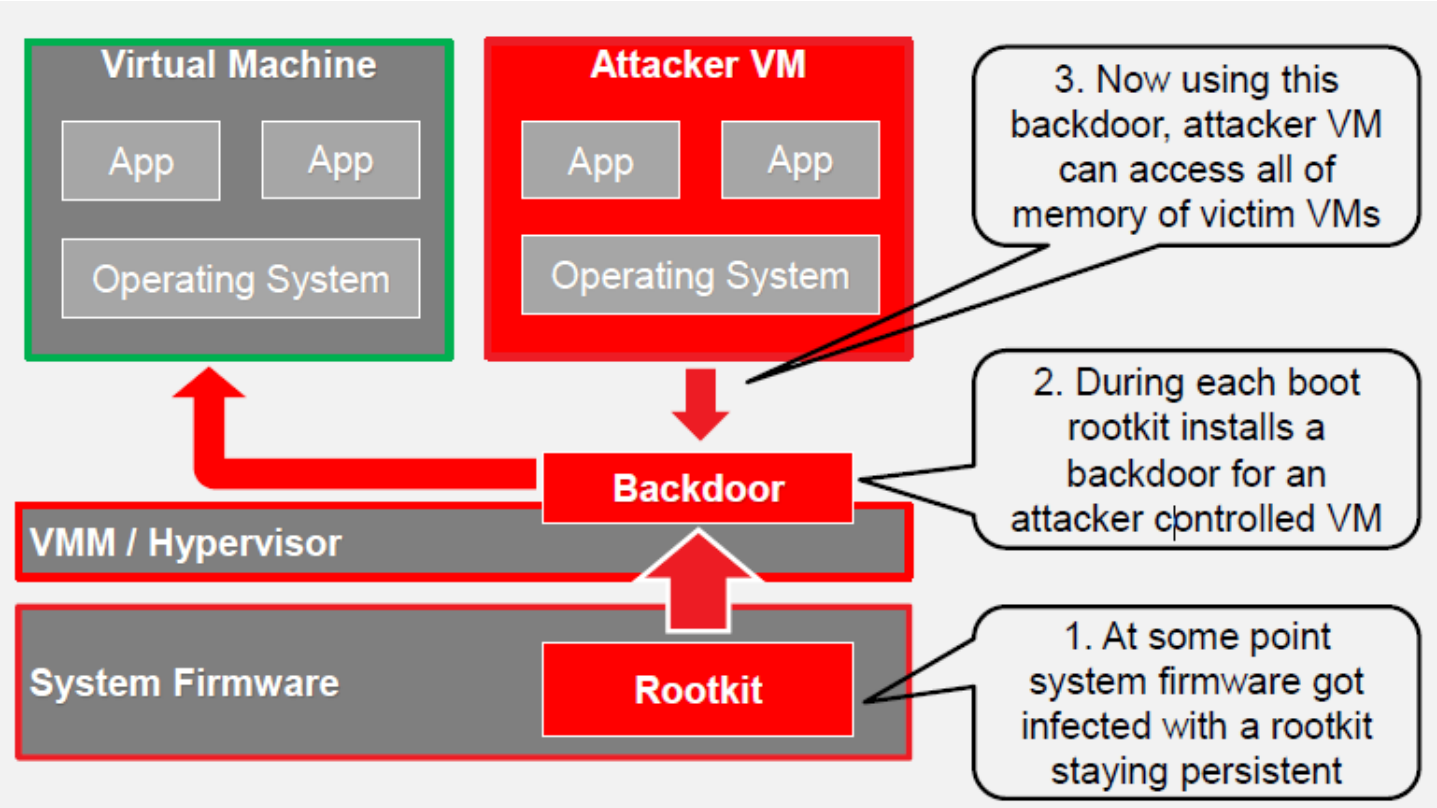
Protecting Memory with HW Assisted Paging



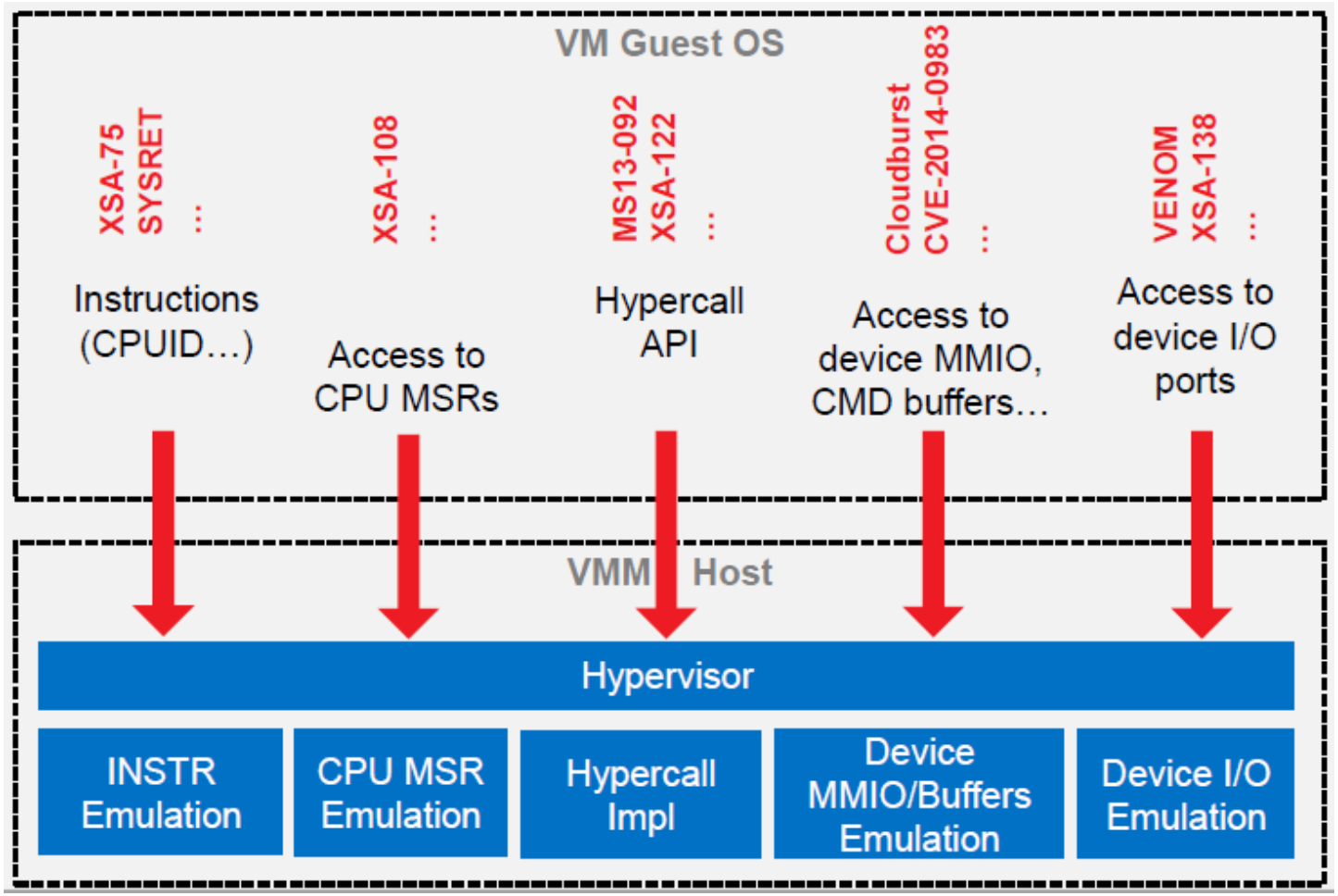
Firmware Rootkit



Firmware rootkit can open a backdoor for an attacker VM to access all other VMs

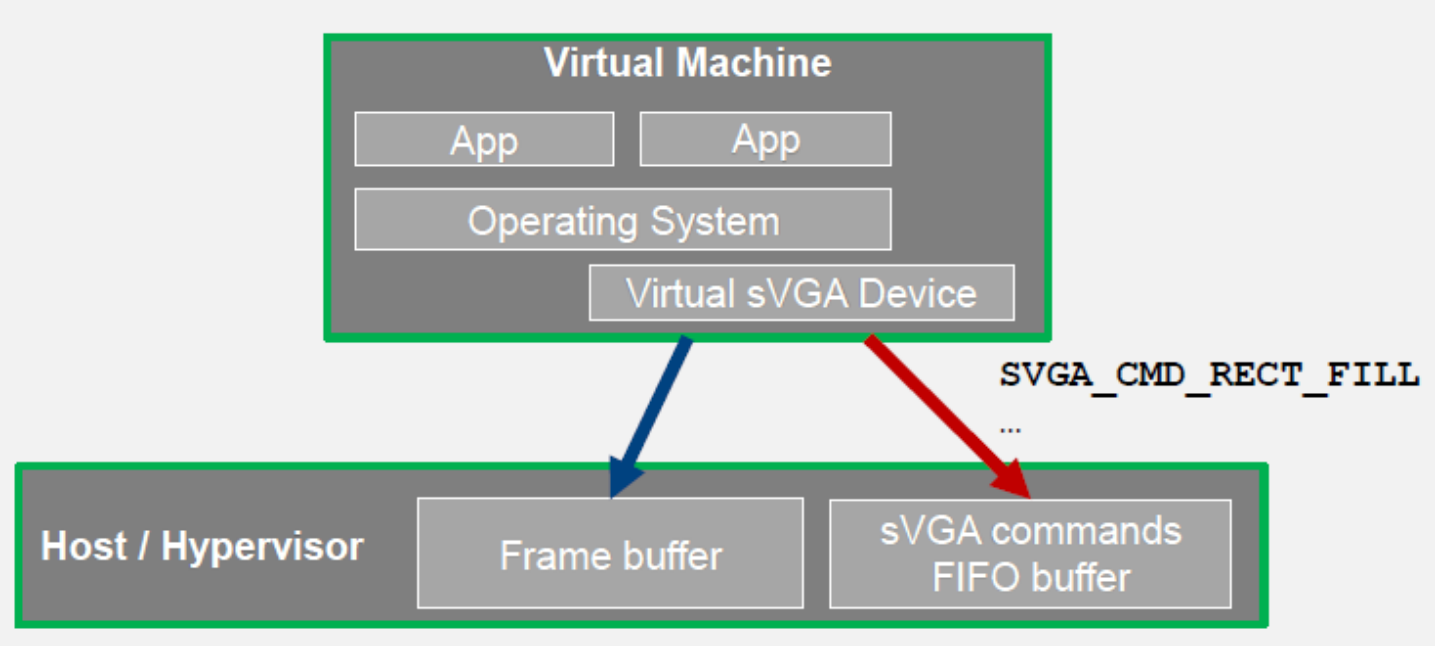


Hardware Emulation Attack Vectors



Did you know that VMMs emulate virtual devices of other VMMs?

1. QEMU and VirtualBox also emulate VMWare virtual SVGA device.



Guest to Host Memory Corruption

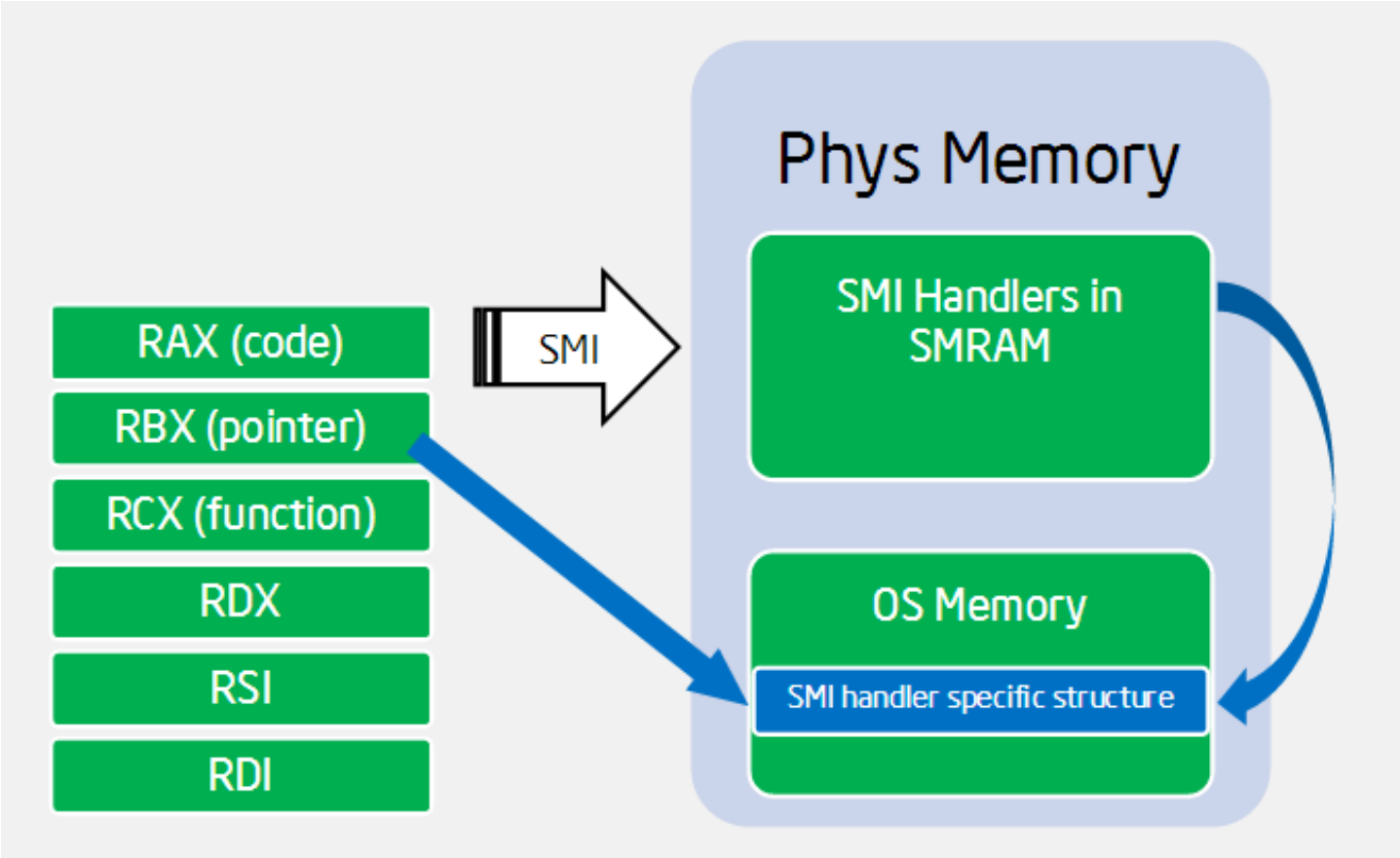
1. **CVE-2014-3689:** 3 vulnerabilities in the vmware-vga driver in QEMU allows local guest to write to QEMU memory and gain host/hypervisor privileges via unspecified parameters related to rectangle handling.
2. **CVE-2014-6588:** Memory corruption in VMSVGAGMRTRANSFER.
3. **CVE-2014-6589, CVE-2014-6590:**Memory corruptions in VMSVGAFIFOLOOP.
4. **CVE-2015-0427:** Integer overflow $\rightarrow$ memory corruption in VMSVGAFIFOGETCMDBUFFER
5. **CVE-2015-0377:** Writing arbitrary data to upper 32 bits of $IA32\_APIC\_BASE$ MSR causes VMM and host OS to crash on Oracle VirtualBox.
6. **CVE-2015-0418, CVE-2014-3646:** VirtualBox and KVM guest crash when executing INVEPT/INVVPID instructions.

Attacking Hypervisors through System Firmware

1. Attacking Hypervisors through System Firmware: with OS kernel access.
2. System Management Mode (SMM):
   - System Management Mode (SMM) is an Intel mode which has the particularity to be transparent to the Operating System (OS).
   - It is initialized by the firmware during the boot to handle the hardware and the security of the computer.
   - Entering in SMM is made by triggering a particular interruption: the System Management Interrupt (SMI).
   - When an SMI is triggered the processor saves the context, disables interruptions and switches to a different address space called System Management RAM (SMRAM).
   - To return from SMM the RSM (Return from System Management) instruction is used, restoring the previous state.
   - This instruction can only be executed from SMM. All of those mechanisms allow the SMM to be transparent to the OS.
   - SMRAM is a range of DRAM reserved by BIOS SMI handlers. Protected from software and device access.

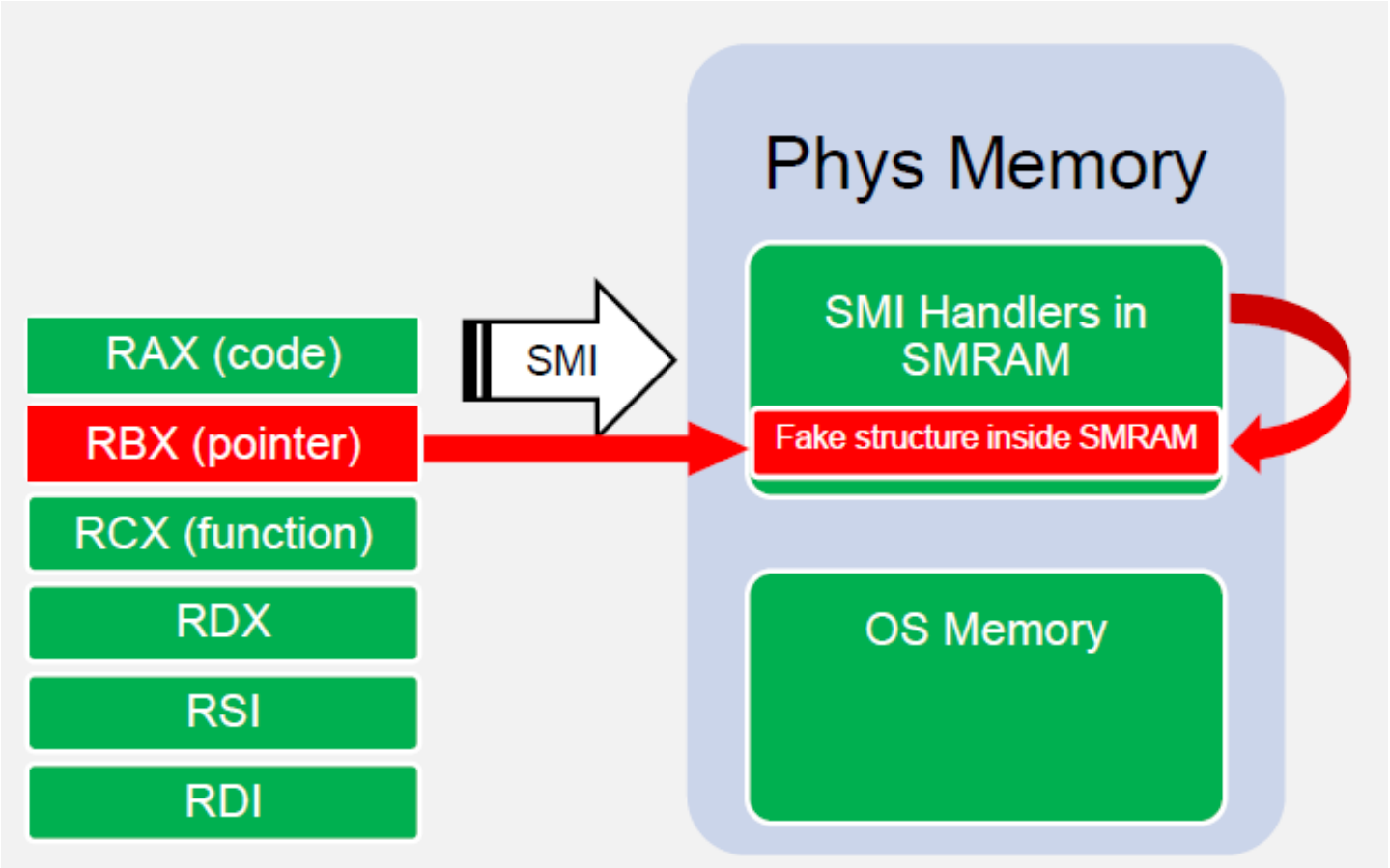
Pointer Arguments to SMI Handlers

1. SMI Handler writes result to a buffer at address passed in RBX.

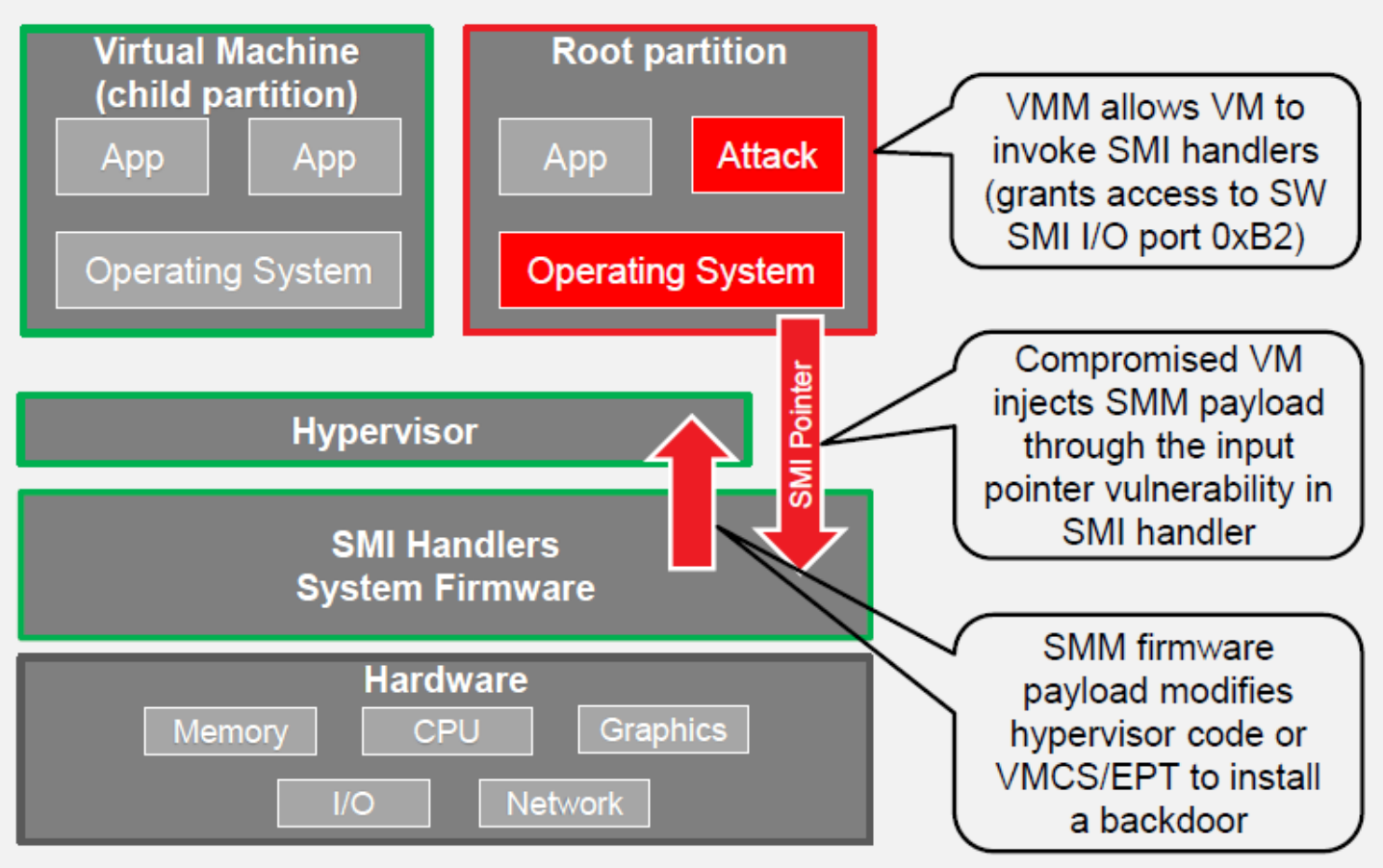


Pointer Vulnerabilities in SMI Handlers

1. Exploit tricks SMI handler to write to an address inside SMRAM.

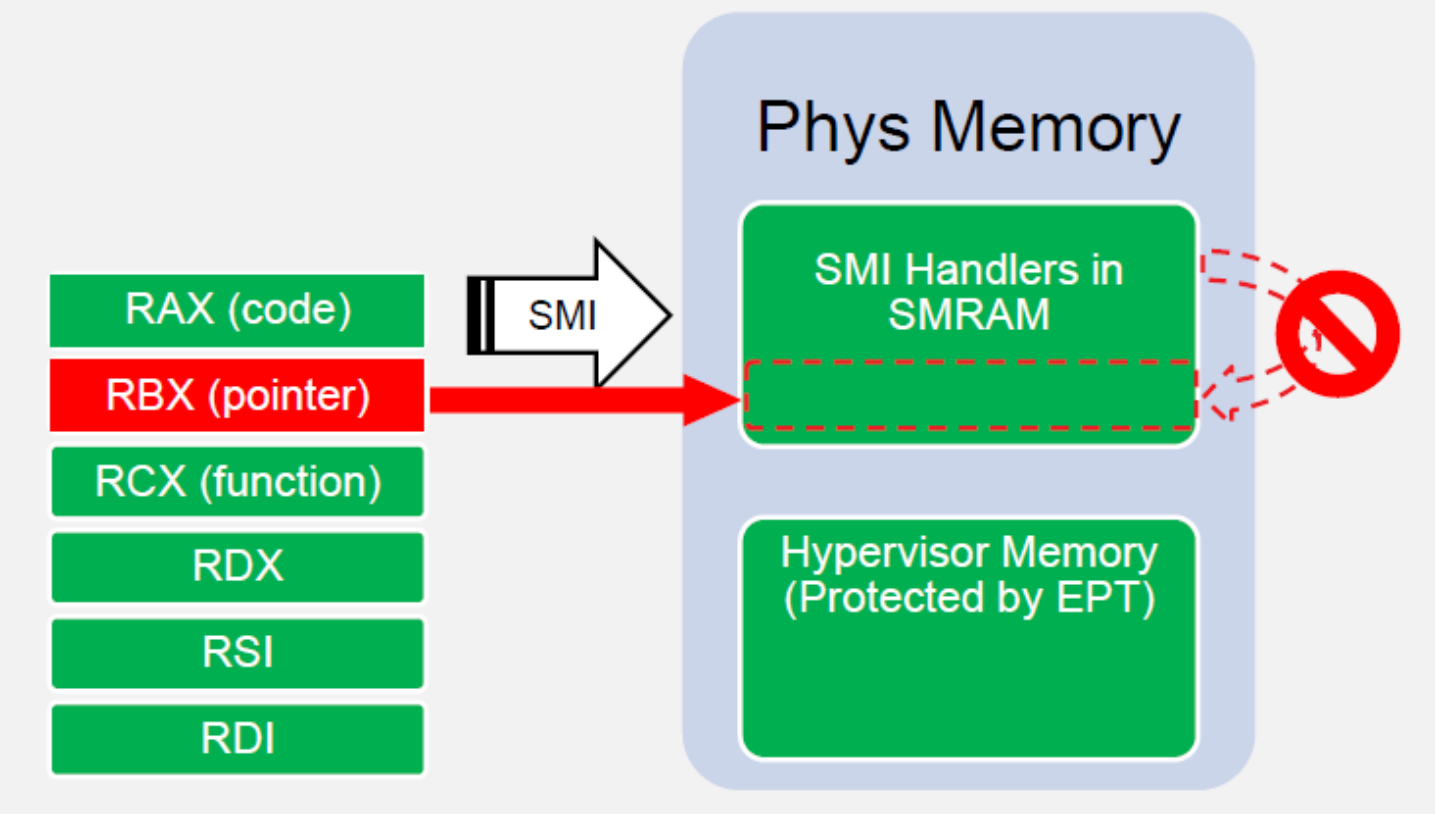


Exploiting firmware SMI handler to attack VMM



Firmware has to validate pointers

1. Firmware SMI handler validates input pointers to ensure they are outside of SMRAM preventing overwrite of SMI code/data



Point SMI handler to overwrite VMM page

1. VT state and EPT protections are OFF in SMM (without STM). SMI handler writes to a protected page via supplied pointer.