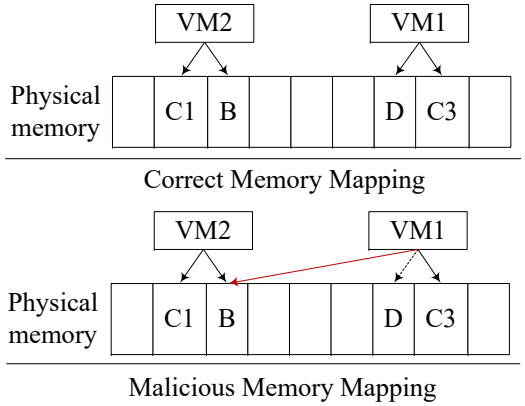
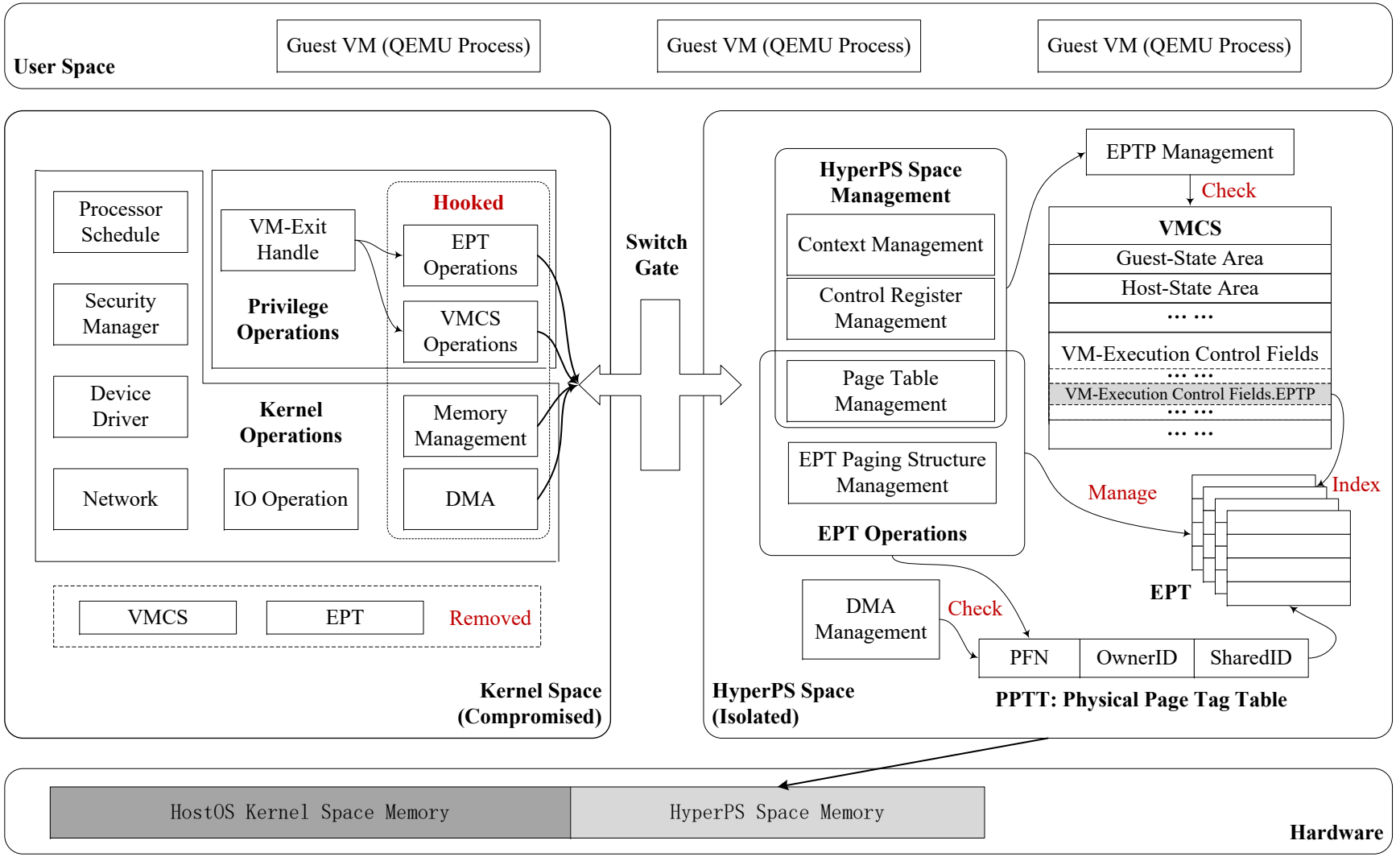
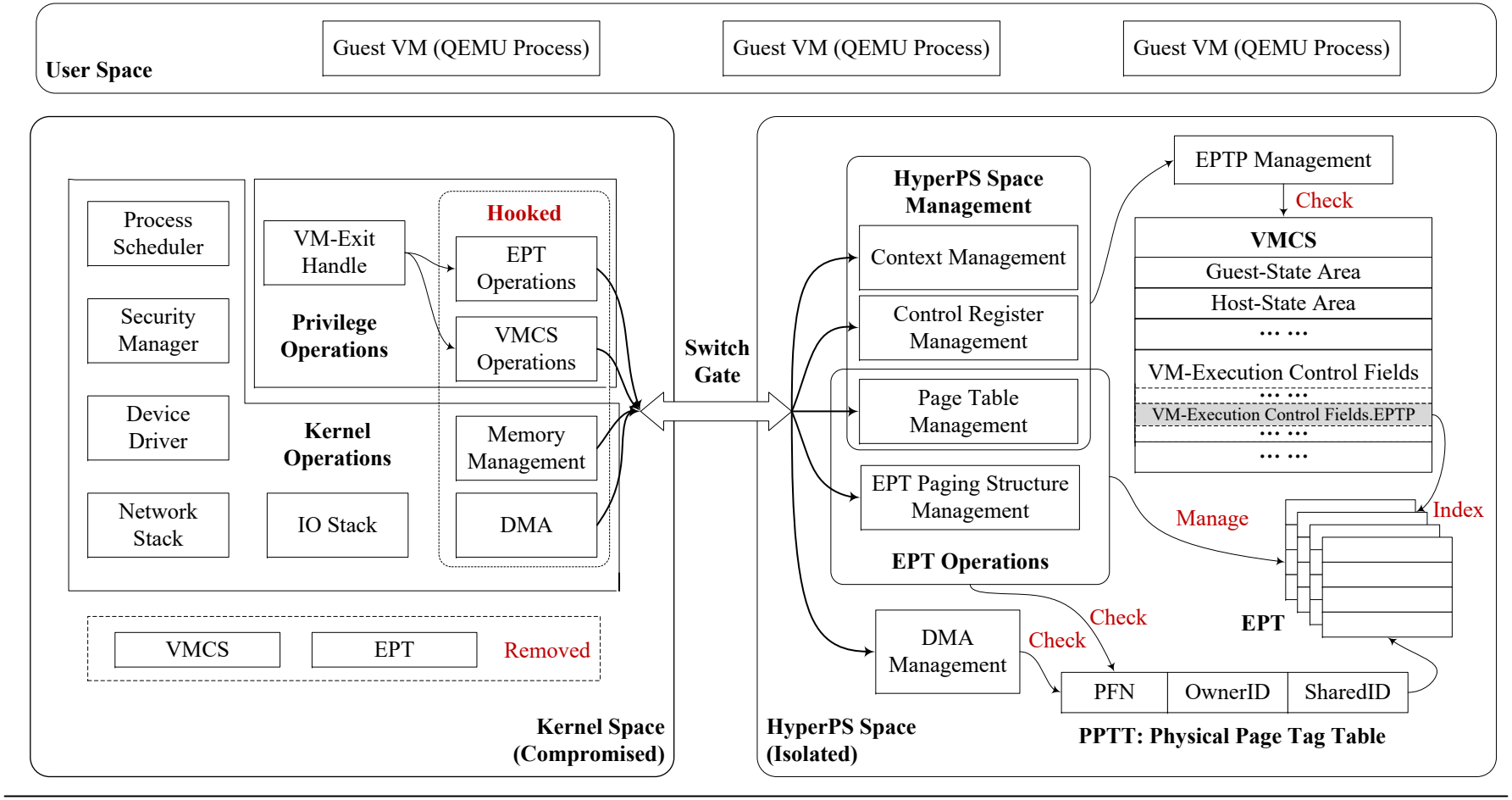
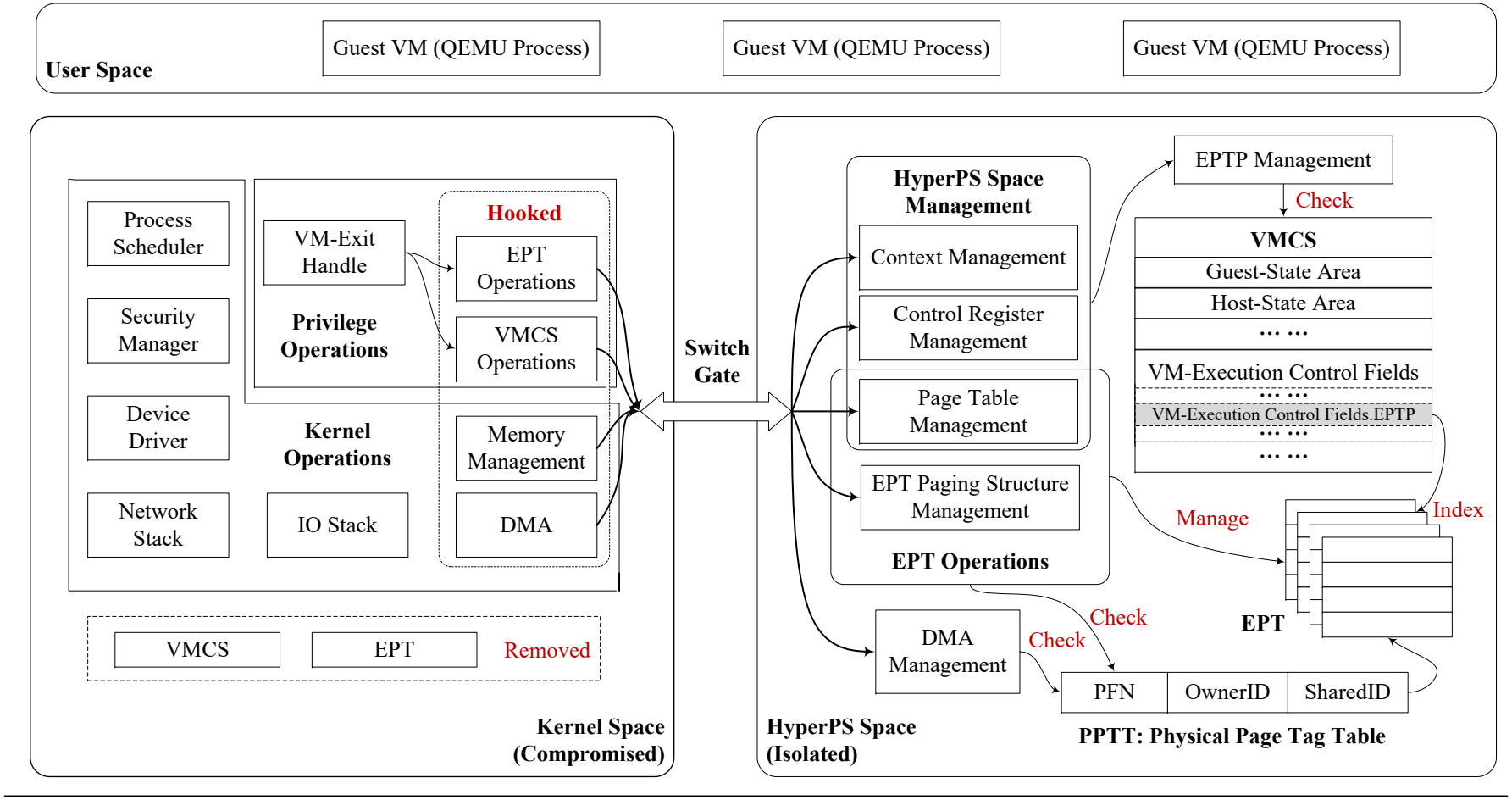

VM2
VM1
Physical memory
C1
B
D
C3
Correct Memory Mapping
VM2
VM1
Physical memory
C1
B
D
C3
Malicious Memory Mapping


User Space
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Processor Schedule
Security Manager
Device Driver
Network
VM-Exit Handle
Privilege Operations
Hooked
EPT Operations
VMCS Operations
Kernel Operations
Memory Management
IO Operation
DMA
VMCS
EPT
Removed
Kernel Space (Compromised)
Switch Gate
HyperPS Space Management
Context Management
Control Register Management
Page Table Management
EPT Paging Structure Management
EPT Operations
EPTP Management
Check
VMCS
Guest-State Area
Host-State Area
VM-Execution Control Fields
VM-Execution Control Fields.EPTP
Manage
Index
EPT
DMA Management
Check
PFN
OwnerID
SharedID
PPTT: Physical Page Tag Table
HyperPS Space (Isolated)
HostOS Kernel Space Memory
HyperPS Space Memory
Hardware


User Space
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Process Scheduler
Security Manager
Device Driver
Network Stack
VM-Exit Handle
Privilege Operations
Hooked
EPT Operations
VMCS Operations
Kernel Operations
Memory Management
IO Stack
DMA
VMCS
EPT
Removed
Kernel Space (Compromised)
Switch Gate
HyperPS Space Management
Context Management
Control Register Management
Page Table Management
EPT Paging Structure Management
EPT Operations
DMA Management
EPTP Management
Check
VMCS
Guest-State Area
Host-State Area
VM-Execution Control Fields
VM-Execution Control Fields.EPTP
Manage
Index
EPT
Check
Check
PFN
OwnerID
SharedID
PPTT: Physical Page Tag Table
HyperPS Space (Isolated)


User Space
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Guest VM (QEMU Process)
Process Scheduler
Security Manager
Device Driver
Network Stack
VM-Exit Handle
Privilege Operations
Hooked
EPT Operations
VMCS Operations
Kernel Operations
Memory Management
IO Stack
DMA
VMCS
EPT
Removed
Kernel Space (Compromised)
Switch Gate
HyperPS Space Management
Context Management
Control Register Management
Page Table Management
EPT Paging Structure Management
EPT Operations
DMA Management
EPTP Management
Check
VMCS
Guest-State Area
Host-State Area
VM-Execution Control Fields
VM-Execution Control Fields.EPTP
Manage
Index
EPT
Check
Check
PFN
OwnerID
SharedID
PPTT: Physical Page Tag Table
HyperPS Space (Isolated)