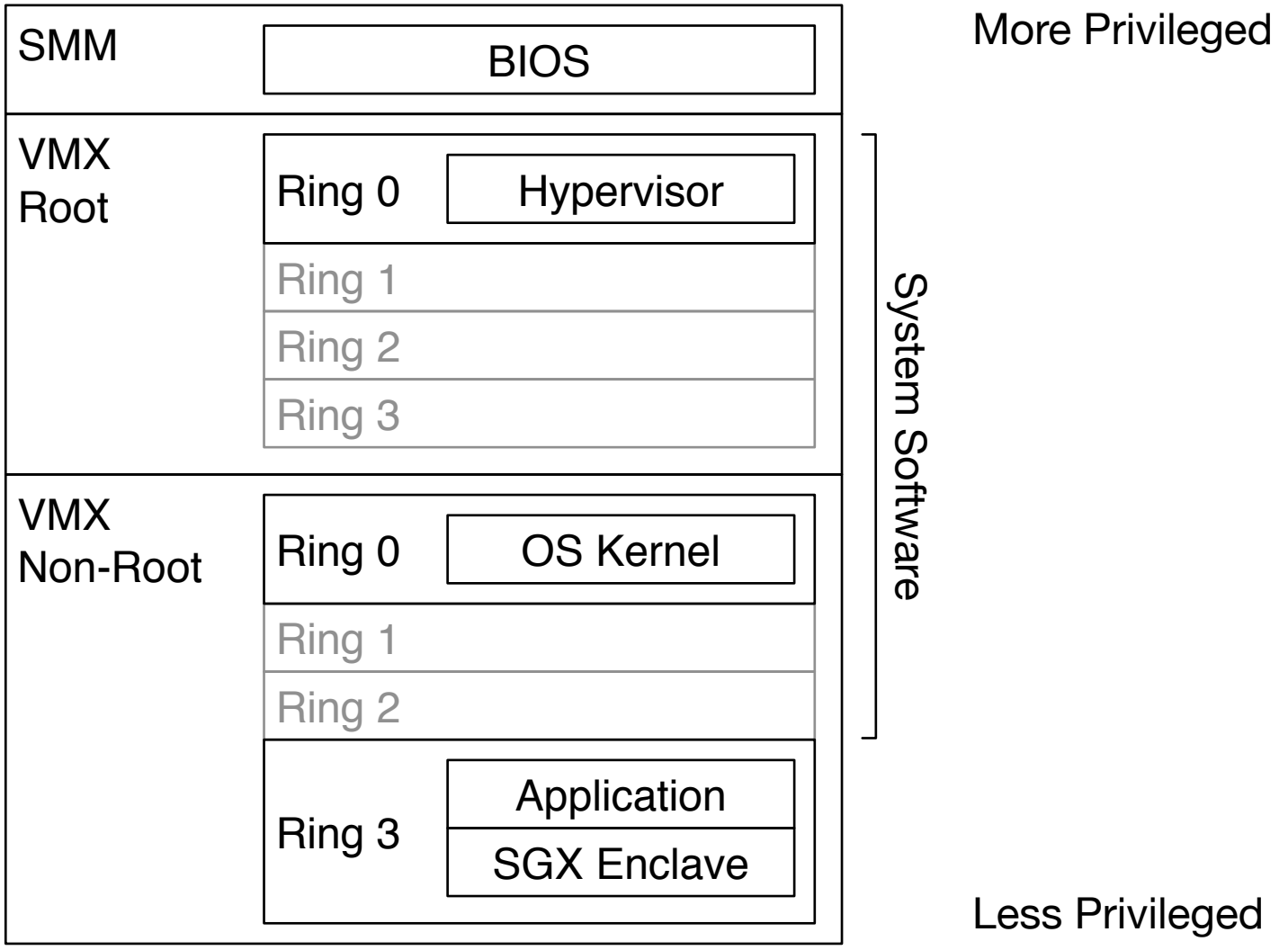
SMM
BIOS
More Privileged
VMX
Root
Ring 0
Hypervisor
Ring 1
Ring 2
Ring 3
System Software
VMX
Non-Root
Ring 0
OS Kernel
Ring 1
Ring 2
Ring 3
Application
SGX Enclave
Less Privileged