
하이퍼바이저 루트킷,
어디까지 가봤니?
- 초보 분석가의 눈물겨운 가상화 입문기
www.CodeEngn.com
2014 CodeEngn Conference 10
CodeEngn

Index

About Hypervisor

- ü Origin of the Hypervisor
- ü Hardware Assisted Virtualization

Attack Hypervisor

- ü HVM Rootkit
- ü SMM Rootkit
- ü Hypervisor in Cloud

Protect Hypervisor

- ü Trust Execution Technology
- ü Secure Virtual Machine

Virtualization : 가상화

Virtualization - Hypervisor?!

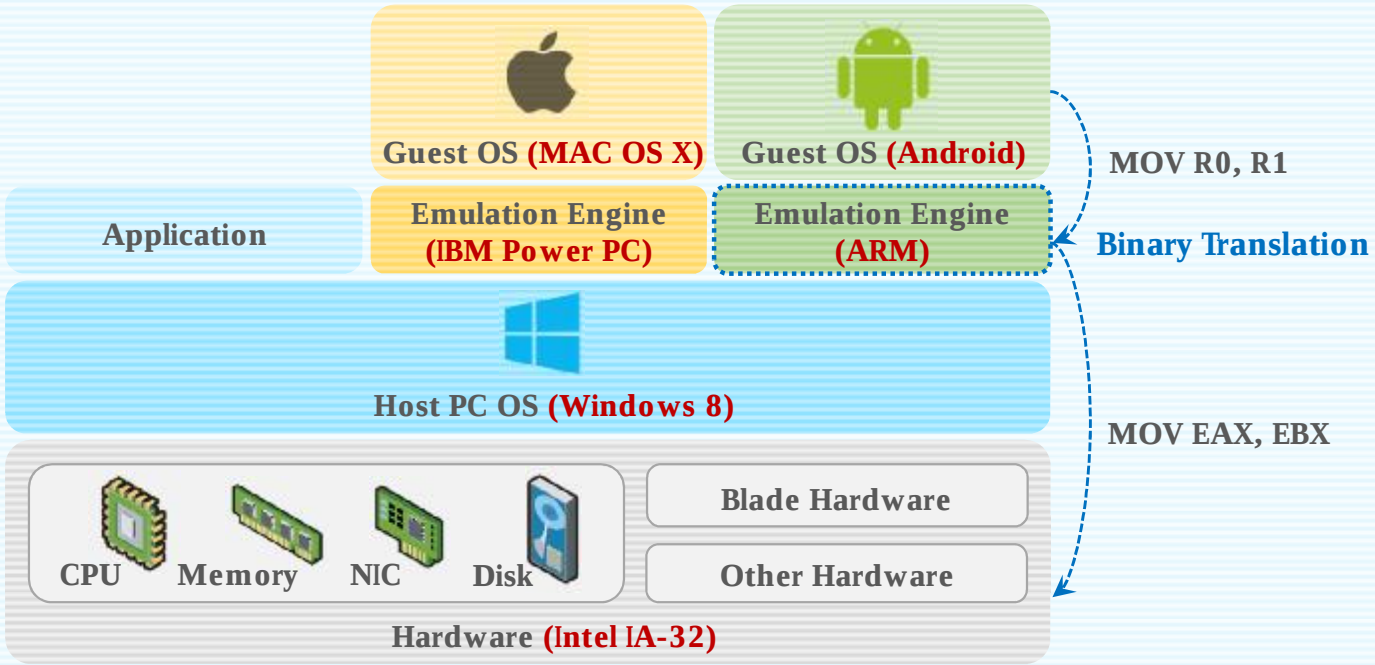
하나의 하드웨어에서
여러 운영체제를
실행할 수 있는 기술

가상화를 구현하기 위해 필요한
논리적인 플랫폼 : **Hypervisor**

Origin of the Hypervisor - Emulator

운영체제와 하드웨어를 **1** 대 **1**로 매칭하여 명령어를 수정해주는 방식

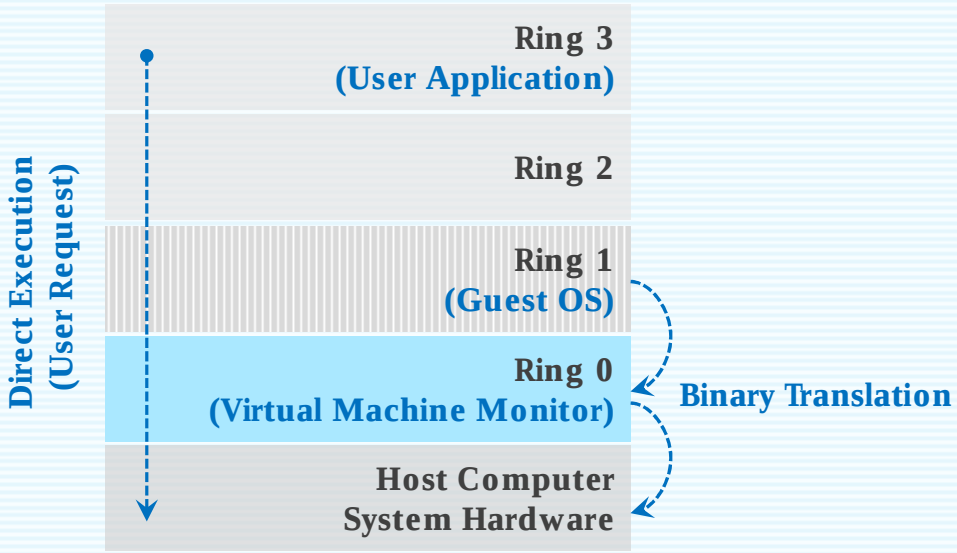
(Binary Translation)



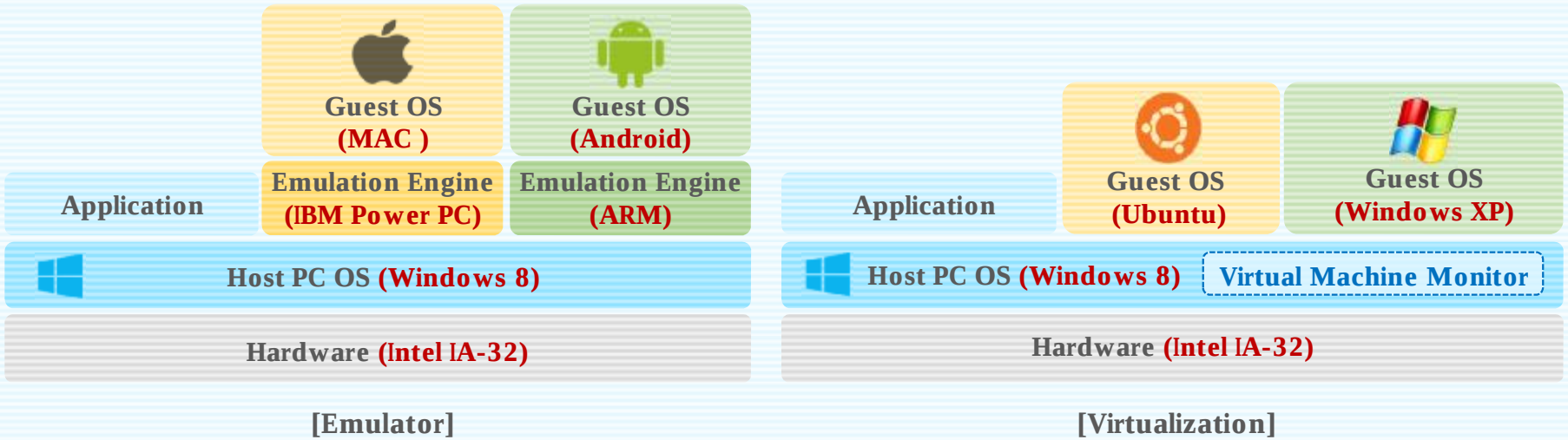
Origin of the Hypervisor - Full & Para

ü Full Virtualization

시스템 전체를 가상화하여 시스템의 **BIOS, CPU,** 메모리 등을 완전히 에뮬레이션 하는 방식



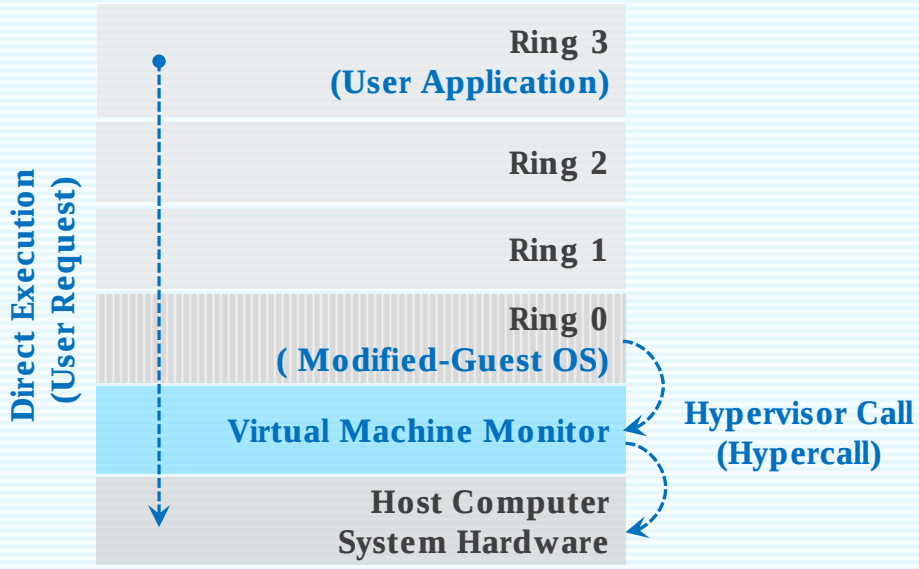
Emulation vs Virtualization? : What's different?



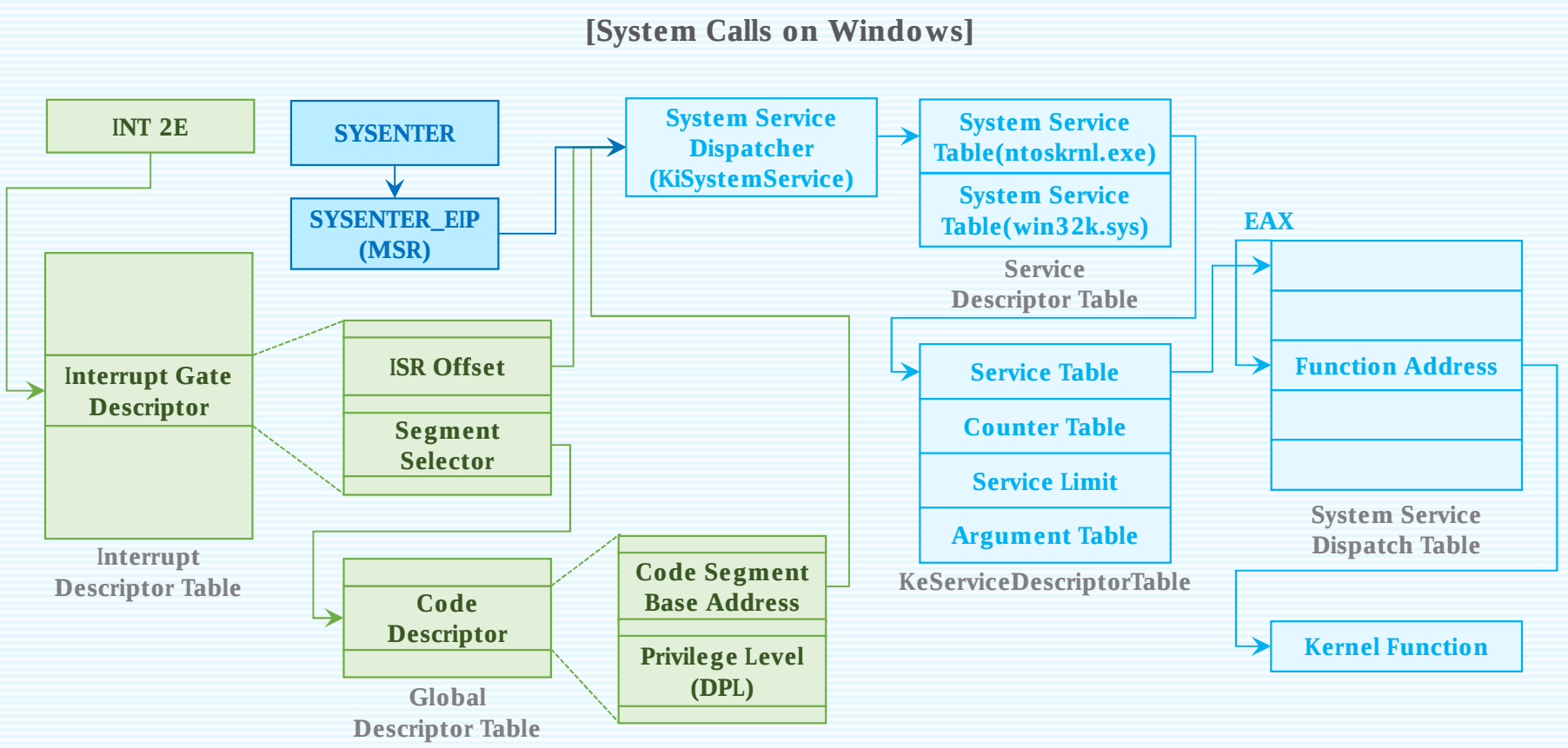
Origin of the Hypervisor - Full & Para

ü **Para Virtualization**

Guest OS의 커널을 일부 수정하여 사용하며**, OS** 레벨 요청을 **Hypercall**이 처리



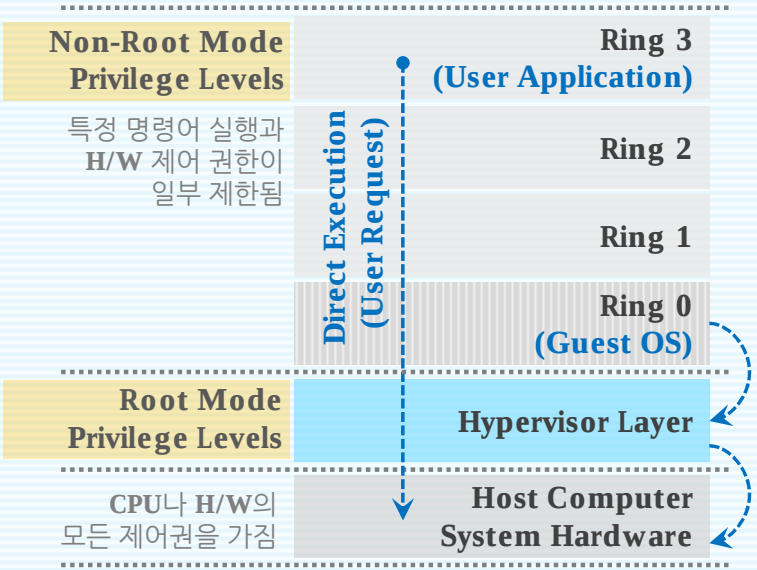
Para Virtualization - Hypercall?

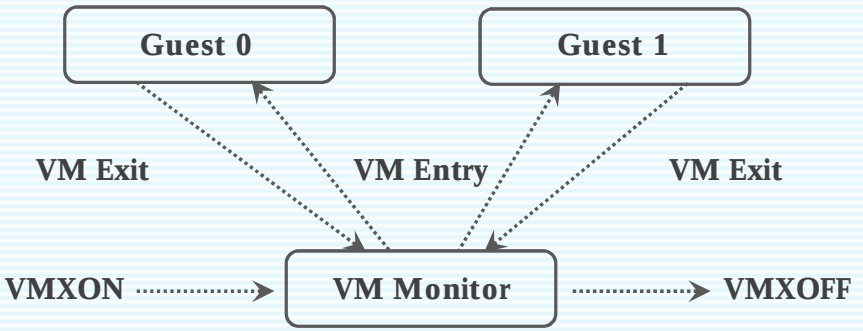


Hypervisor : Hardware-Assist Virtualization

ü Hardware-Assist Virtualization

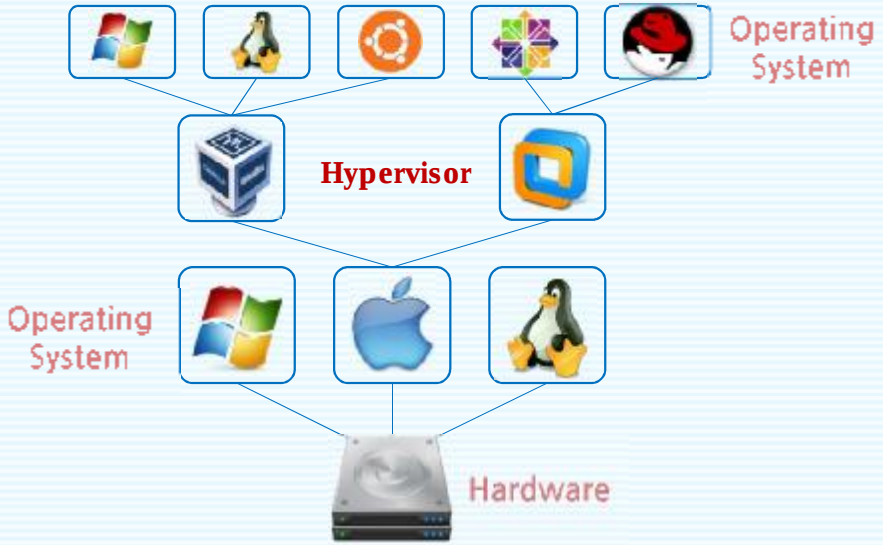
가상화 방식의 가장 큰 과부화 원인인 **Binary Translation**이 없어지고 **CPU**의 지원을 받기 시작함





[INTEL Virtual Machine Monitor & Guests]

Hypervisor - Type of Hypervisor



Native (Bare Metal)

호스트의 하드웨어에 위치하여, 하드웨어 제어와

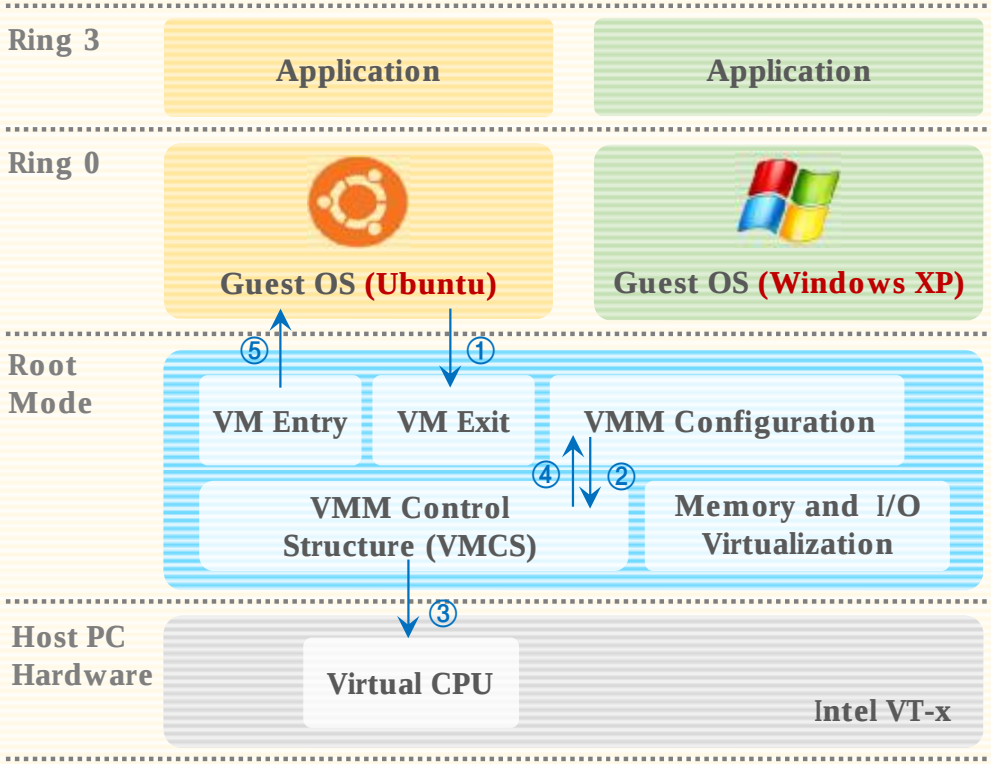
Guest OS 모니터링을 담당함

Hosted

호스트의 운영체제에 위치하며, 단순히

소프트웨어의 역할로써 **Guest OS**에 관리를 담당함

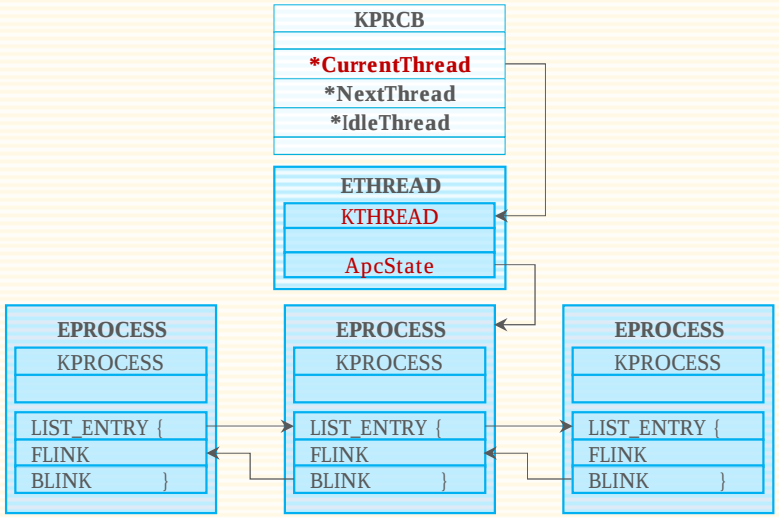
Attack of Hypervisor : Virtual Machine Extensions



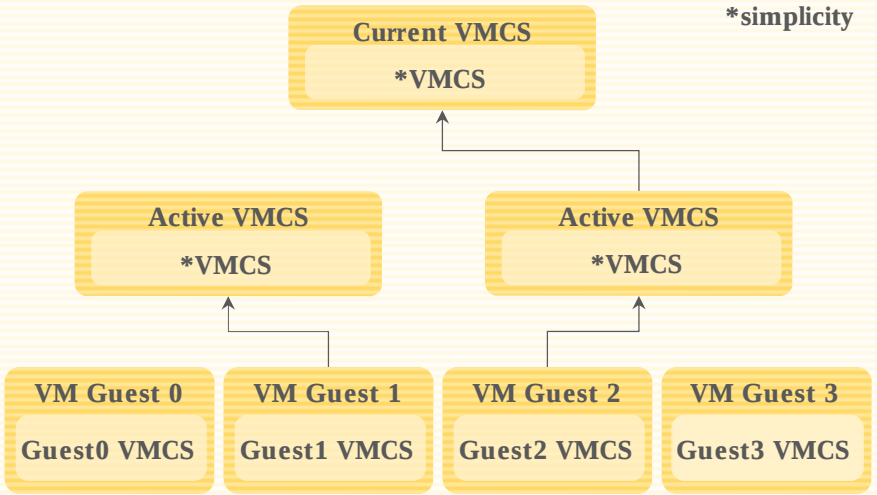
HVM Rootkit : HVM

ü Hardware-assisted Virtualization Machine : HVM

HVM은 일반적으로 **VMCS**를 설정해 **Guest OS**를 구동하고 **Guest OS**의 코드가 실행되다가 설정된 동작을 수행하면 **Exit** 되도록 하여 이를 **VMM**에서 처리



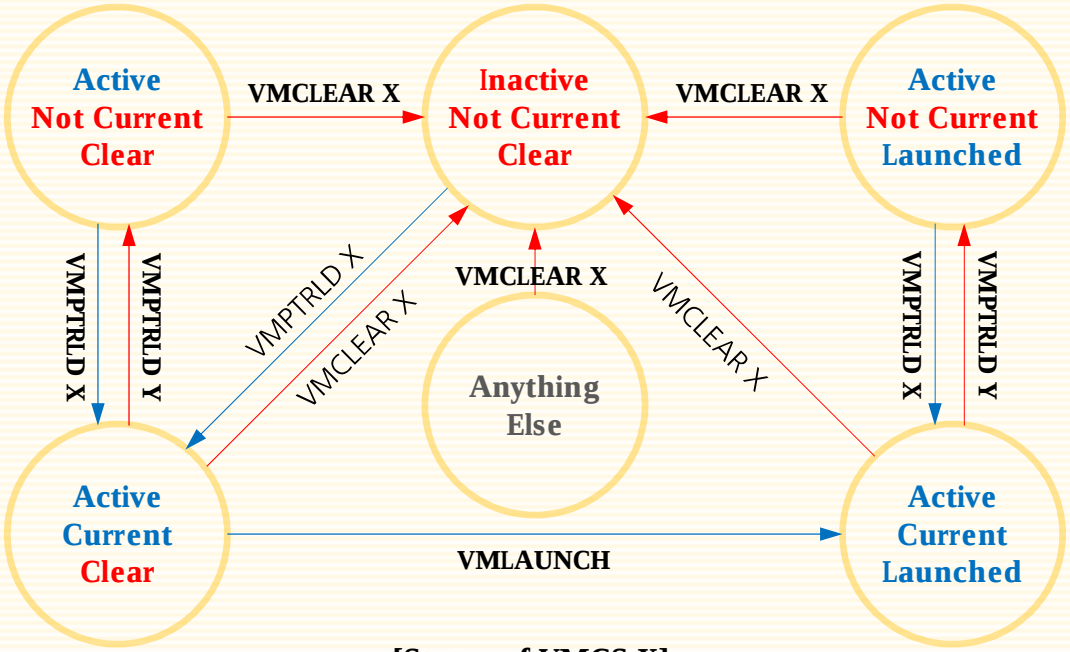
Operating System - Kernel's Processor Control Block (KPCB)



Hypervisor - Virtual Machine Control Data Structures (VMCS)

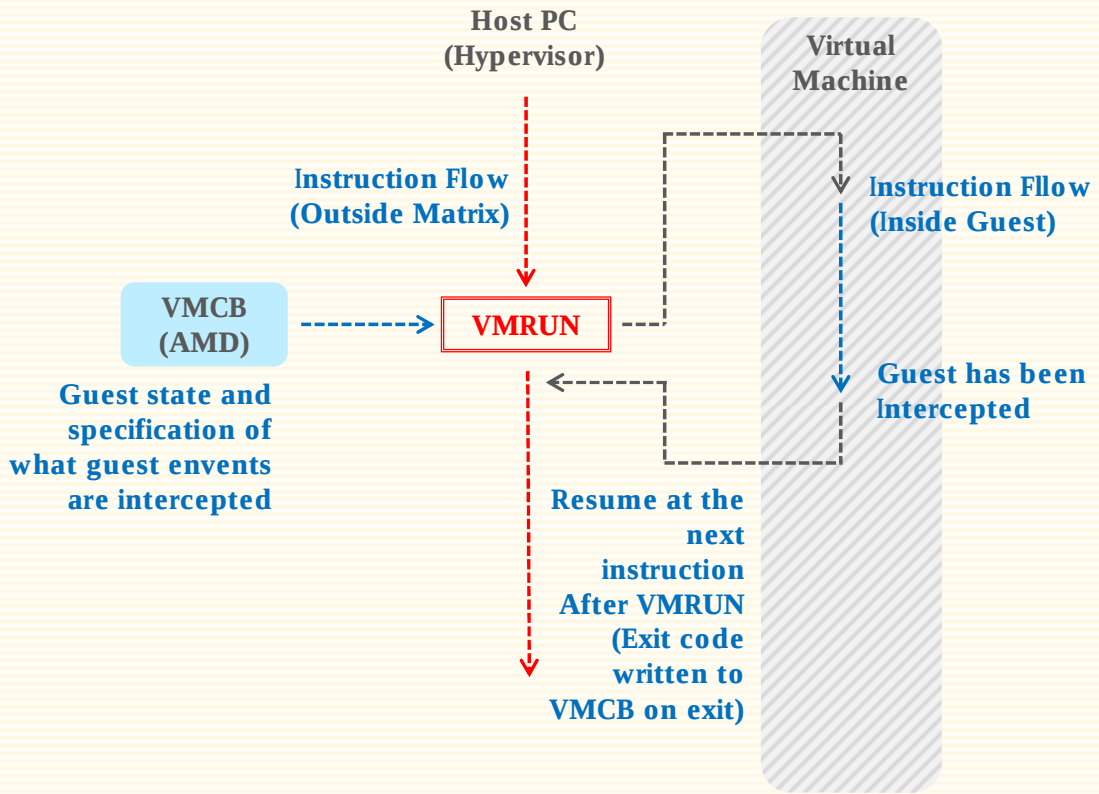
Hypervisor : VMCS (Intel)

VMX Non-Root 오퍼레이션과 **VMX** 전환을 제어하는 구조체

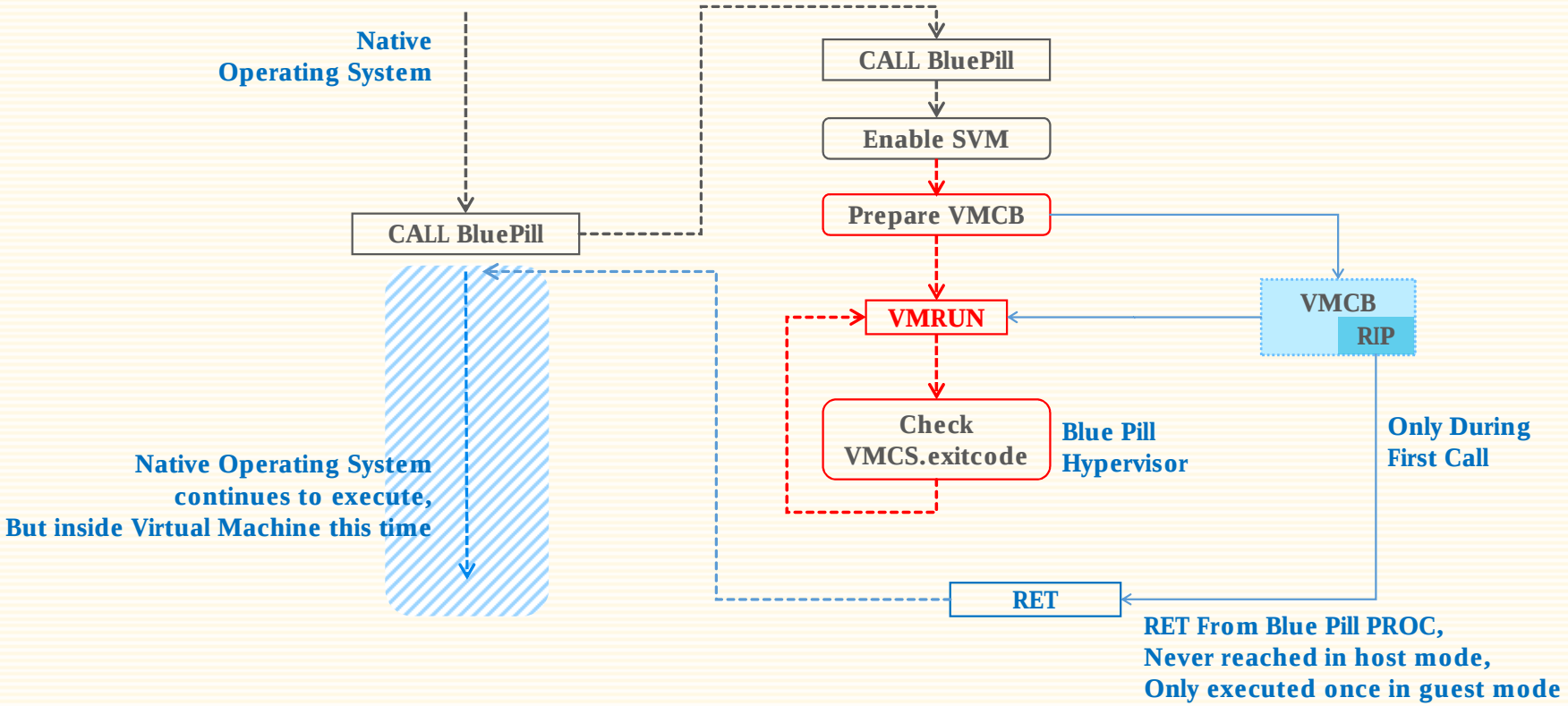


[States of VMCS X]

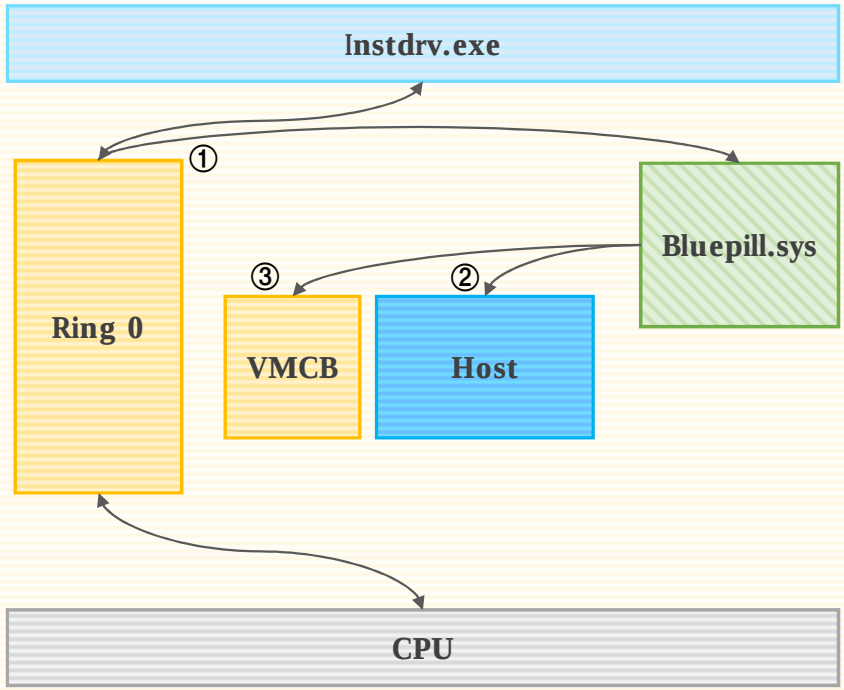
HVM Rootkit : VMRUN Instruction



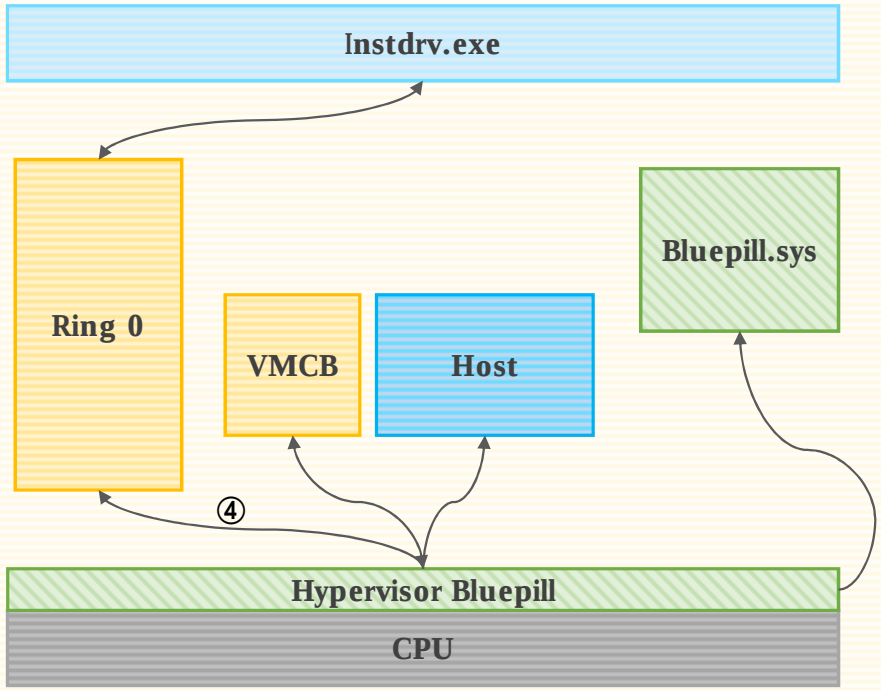
HVM Rootkit : Blue Pill Infection



HVM Rootkit : Blue Pill

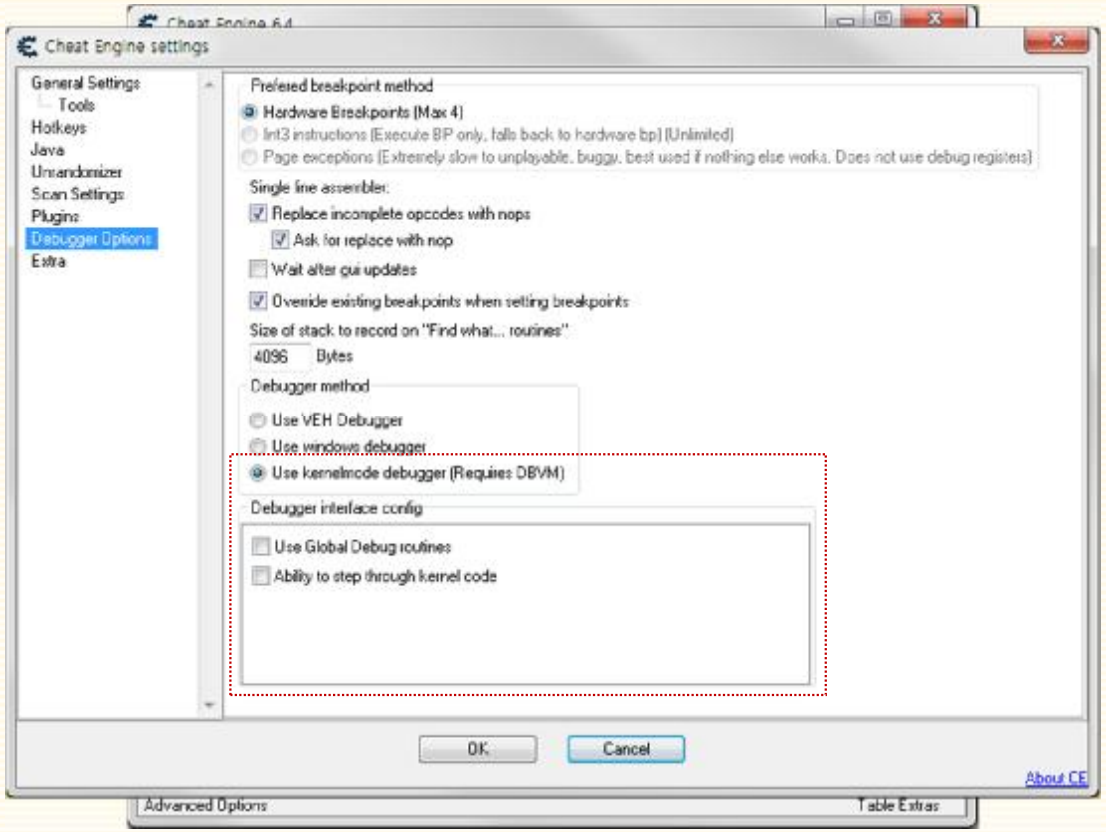


HVM Rootkit : Blue Pill

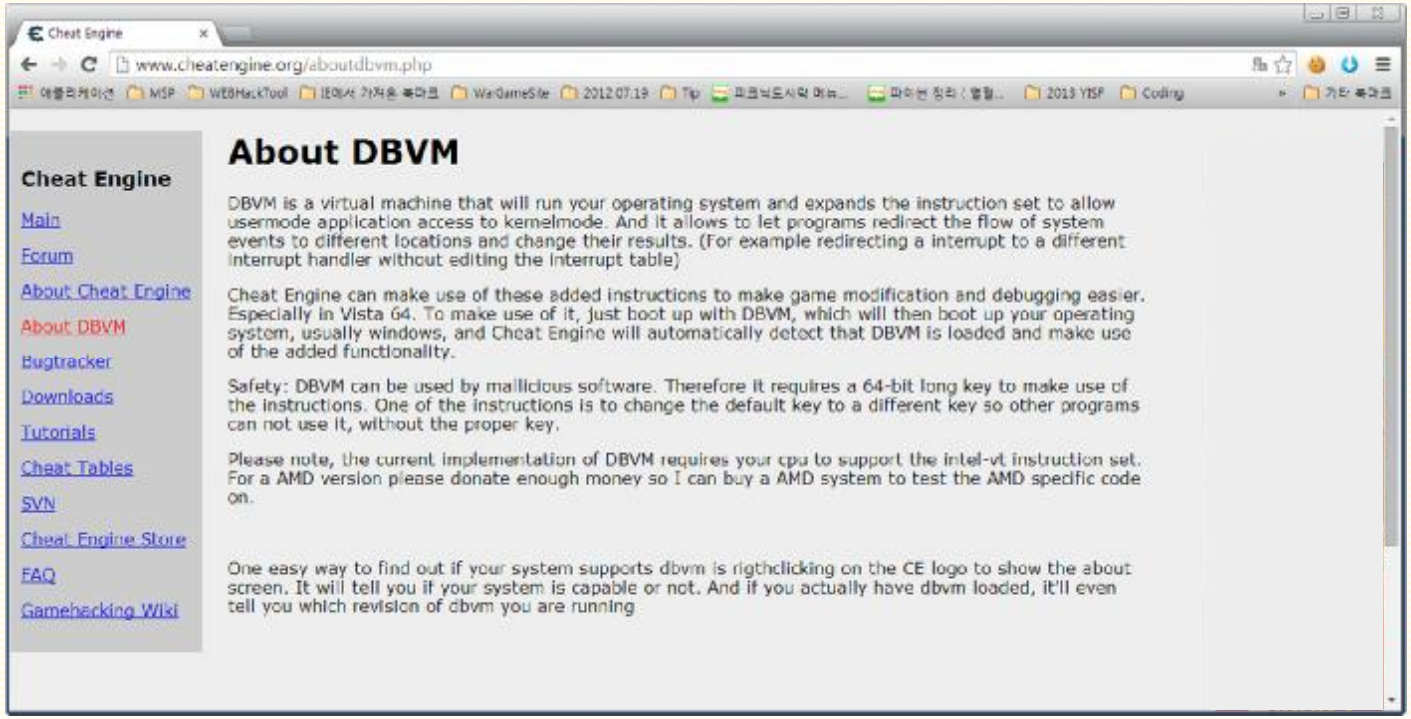


Cheat Engine - DBVM

Cheat Engine - DBVM



Cheat Engine - DBVM



Imagine of Story!

ü Cloud Computing

인터넷 상의 서버를 통하여 데이터 저장, 네트워크, 콘텐츠 사용 등 IT 관련 서비스를 한번에 사용할 수 있는 컴퓨팅

Cloud Computing Services

Software as a Service

End Users

Google apps, salesforce, U+ Box

Platform as a service

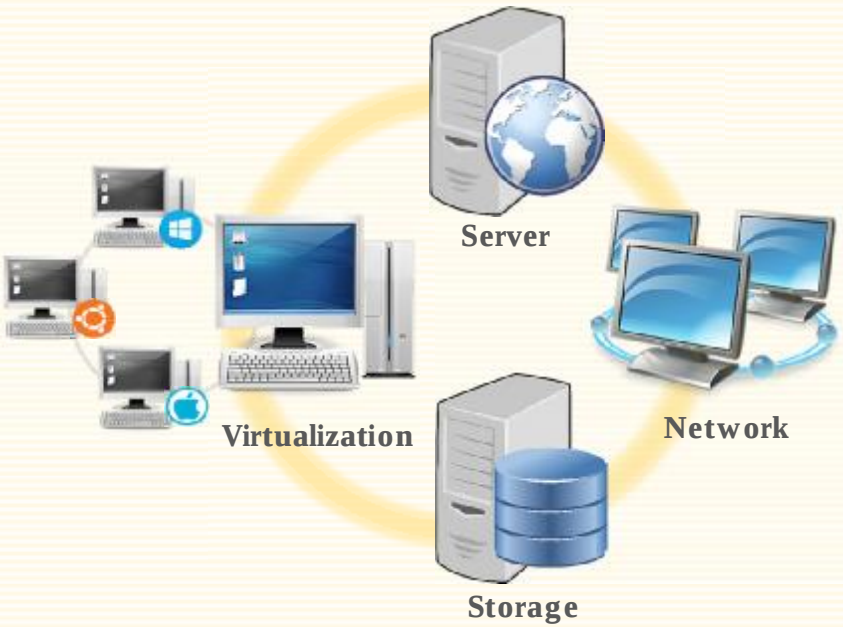
Application Developers

Google app engine

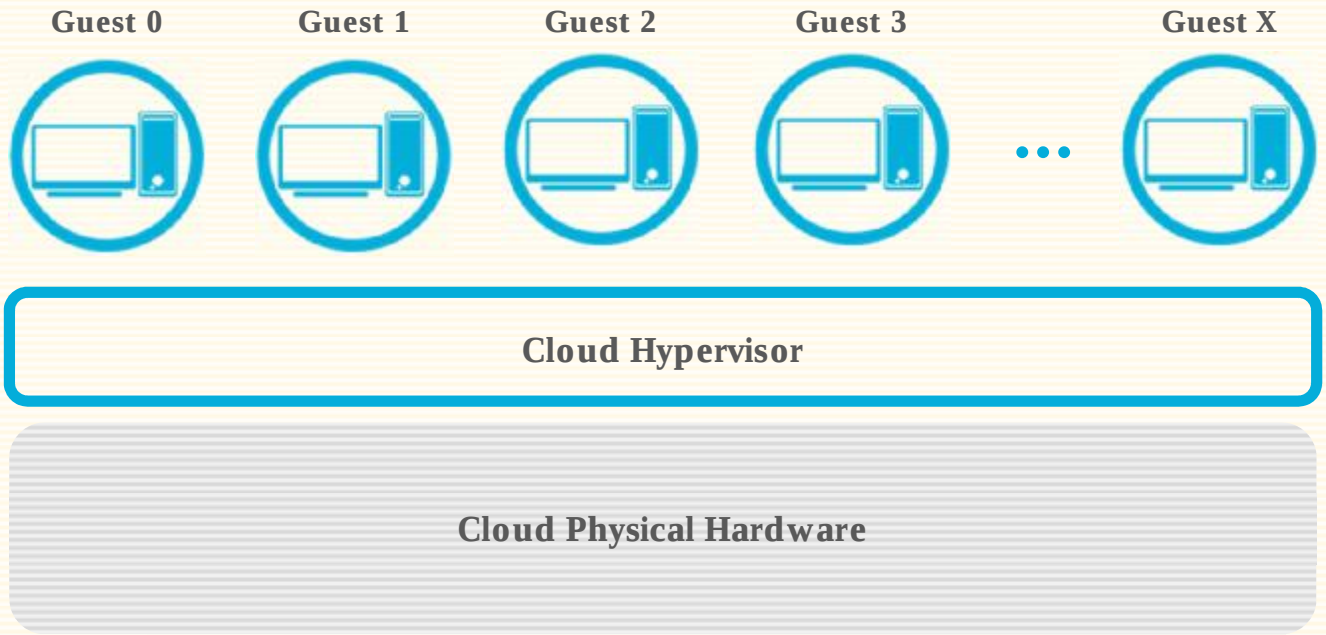
Infra as a service

Network Architects

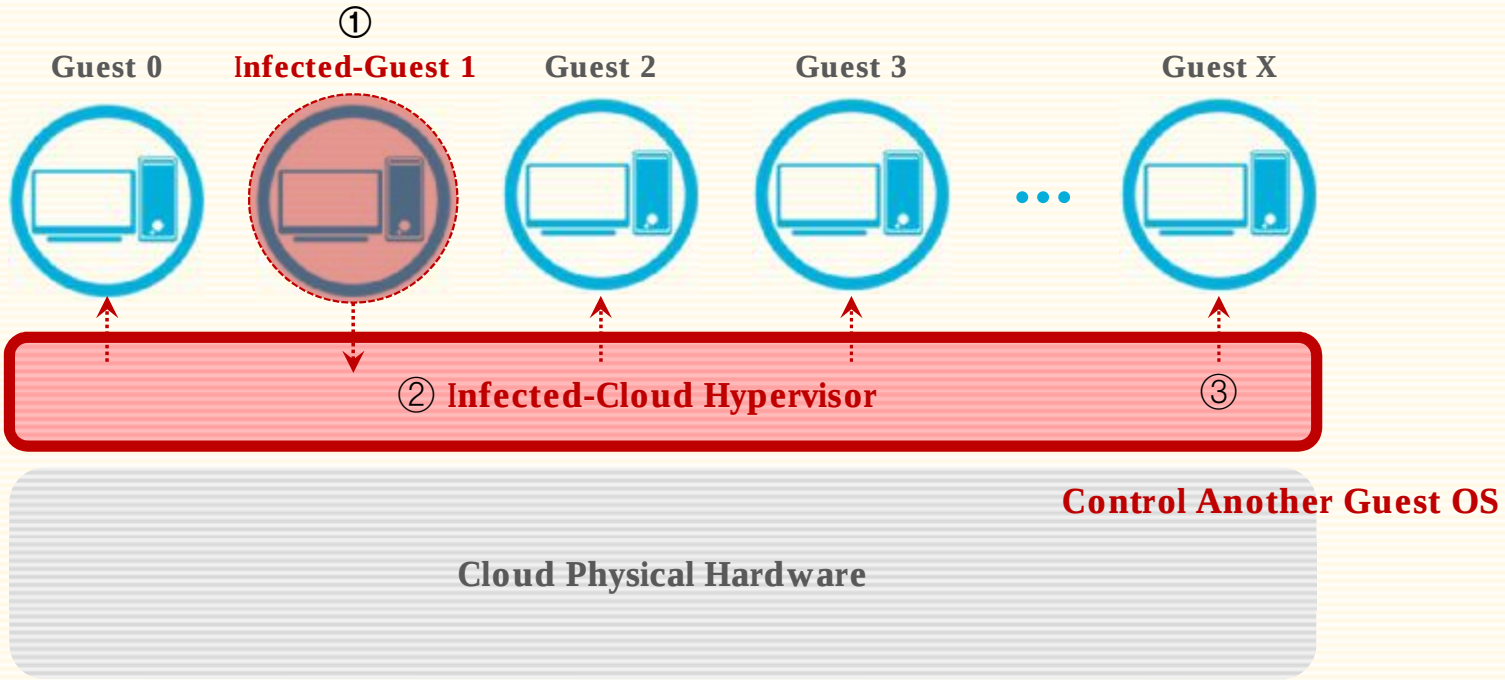
apachecloudstack, HP Helion, amazon web services, openstack



Attack of Cloud System!



Attack of Cloud System!



So, How Detected?

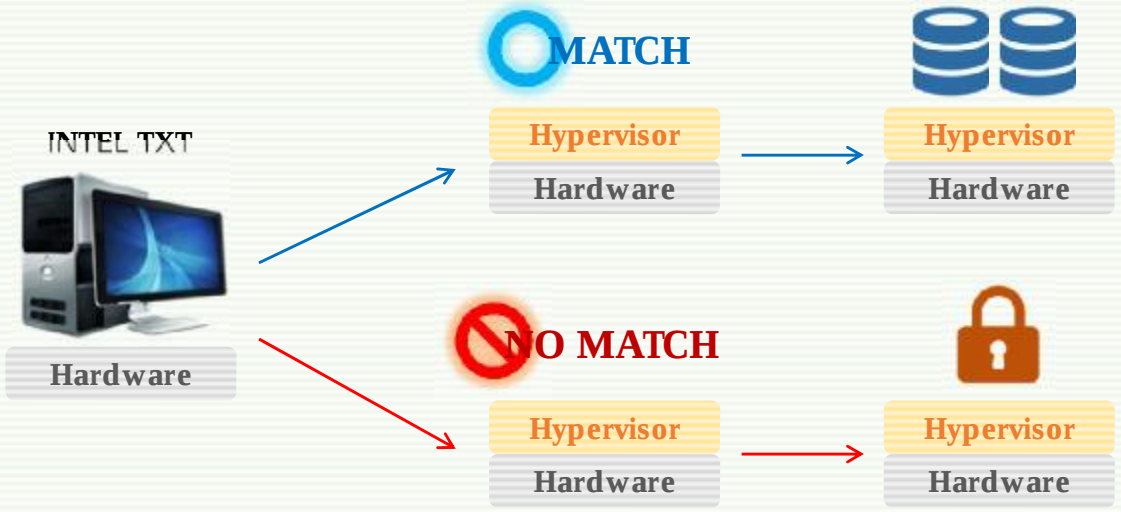
Trust Execution Technology

(TXT)

Secure Virtual Machine

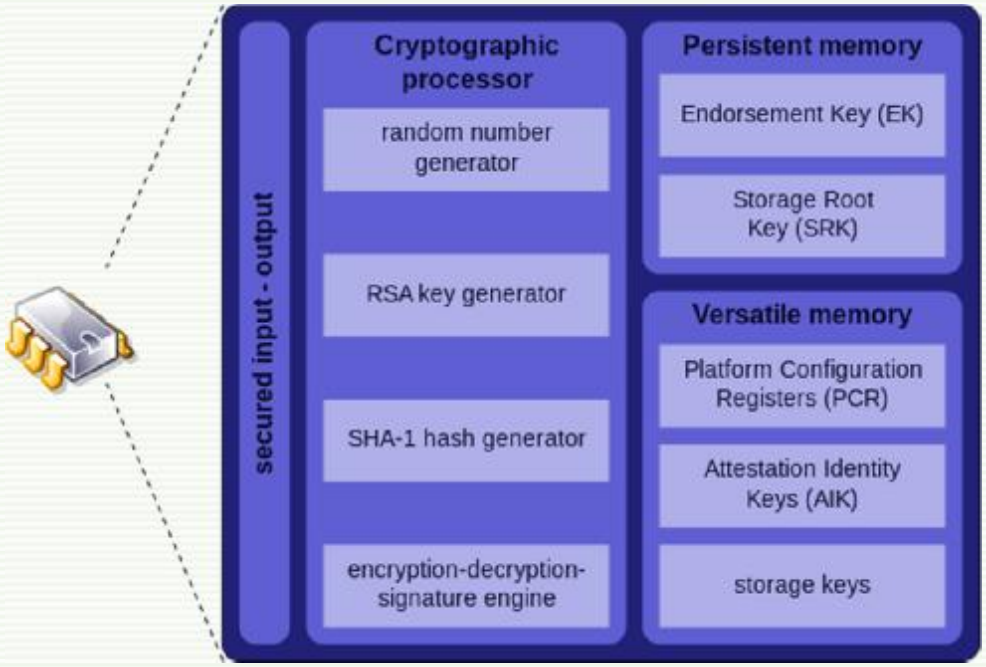
(SVM)

INTEL - Trust Execution Technology



Trusted Platform Module : TPM

장비에 암호화 키를 통합하여 하드웨어를 보호하기 위해 설계된 전용 마이크로 프로세서



Conclusion

Reference

- **Intel, "Intel 64 and IA-32 Architectures Software Developer's Manual"**
- **David Chisnall, "Xen 하이퍼바이저 완벽 가이드"**
- **Joanna Rutkowska, "Introducing Blue Pill"**
- **Rafal Wojtczuk, Joanna Rutkowska, "Attacking Intel Trusted Execution Technology"**
- **Hanbum Bak, "Virtualization Technology for Security"**
- **MJ0011, "Analyzing VMware Operating System & Detecting Rootkit from Outside"**
- **Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology"**
- **Rafal Wojtczuk, Joanna Rutkowska, Attacking Intel TXT via SINIT Code Execution Hijacking**

Speaker Info

순천향대학교 정보보호학과 **SecurityFirst**

hakbaby92@gmail.com (fb.com/hakbaby)

김 학 수