NetSec-KR 2020
(Tech. Session Talk)

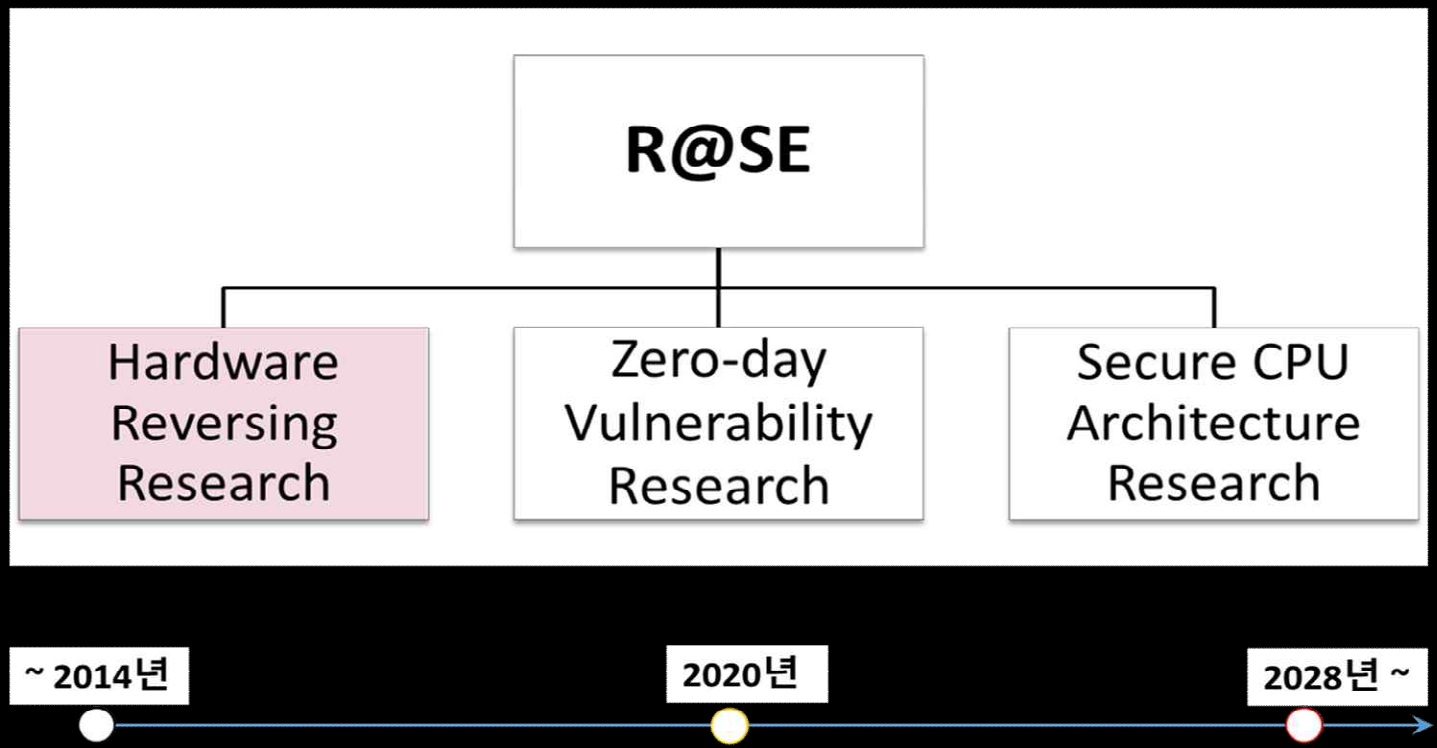
PCB/Firmware-level
Supply Chain Attack Analysis

ByeongCheol Choi
corea@etri.re.kr
ETRI

R@SE

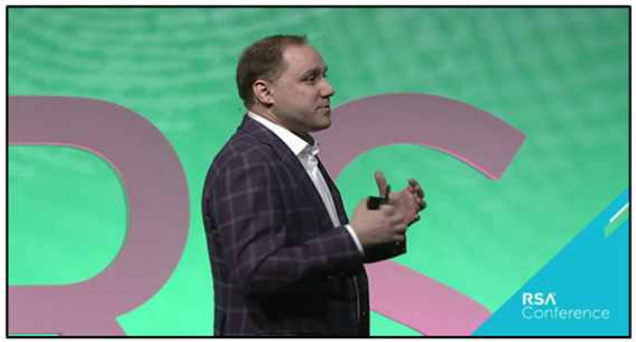
Reverse and Security Engineering

ETRI R@SE Lab (보안취약점분석연구실)



Issues

RSAC 2020 분석보고 : 2019년 보안 위협 (랜섬웨어, APT 공격), 2020년 새로운 공격 대응 기술 필요



Hacking Exposed : Global Threat Brief

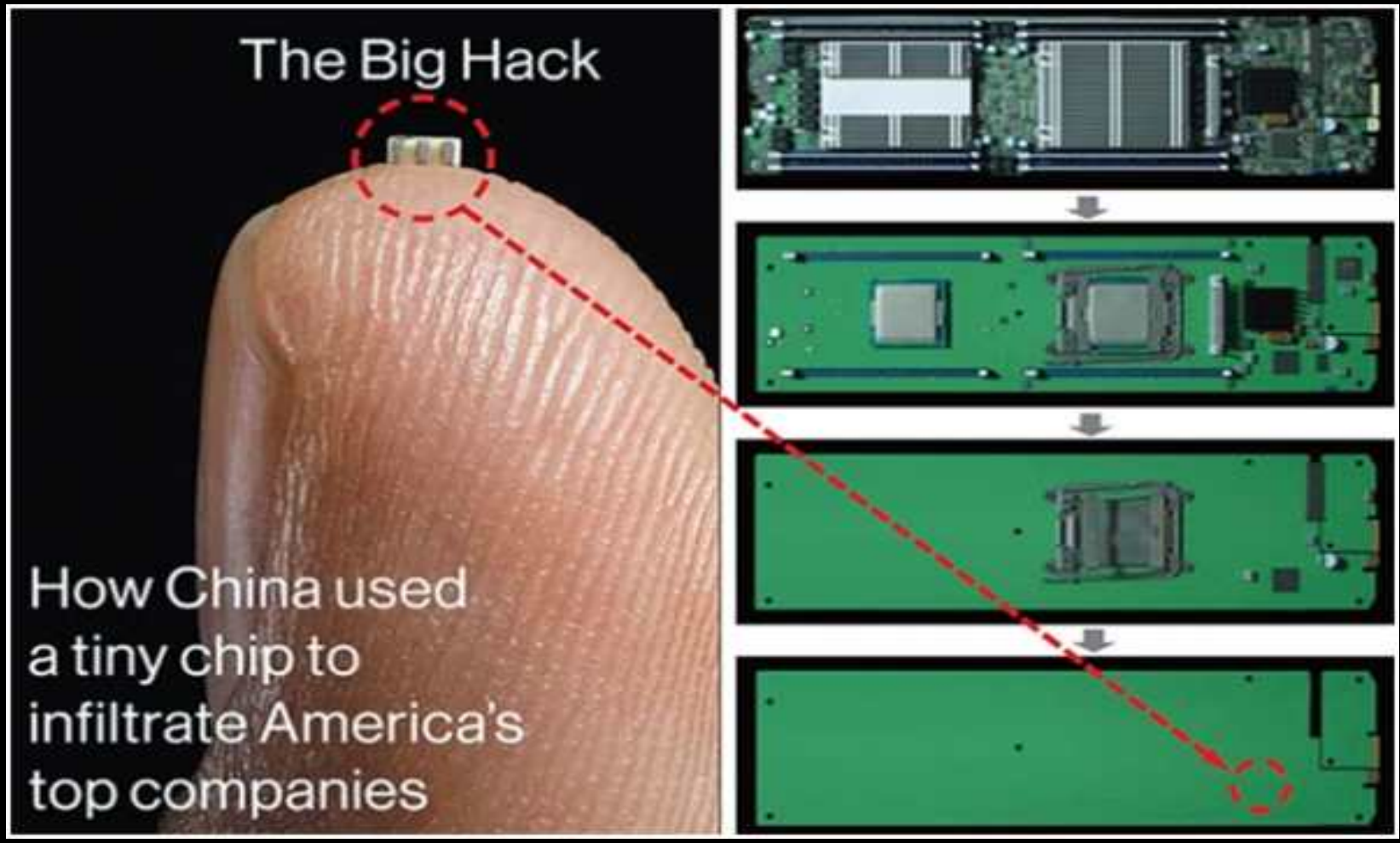
Keynote

- 랜섬웨어 (Ransomware)
  : "Everyone is a target", Ryuk 랜섬웨어(러), $100~$1M 비용
- 국가별 APT 공격 유형
  : 중국 – PLA 소속 해커들의 지속적인 스파이 활동
  : 러시아 – 이란을 포함한 중동이 공격 대상
  : 북한 – SWIFT 등의 전세계 금융 기관을 공격
  : 이란 – 미국과 중동의 전략정보 수집

The Five Most Dangerous New Attacks

Keynote

- Command & Control (C2) Returns
- Deep Persistence
  : 지속적 공격 (예시 – USB 충전 케이블 악성코드 등)
- Mobile Device Integrity
- How 2FA Can Hurt You
  : 2FA – Two Factor Authentication 취약점, ID/PW 연계 필요
- Enterprise Perimeter Vulnerabilities



https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
http://www.businesskorea.co.kr/news/articleView.html?idxno=25730

RSAC 2020 Panel Discussion

How to Reduce Supply Chain Risk (Huawei)

- Huawei 공급망 위협에 대한 논쟁 (패널 토의)
  : US DoD, Huawei CSO, 하버드 대학(Schneier 교수) 등
- Schneier 교수
  : 미국 DoD의 공급망 보안위협에 대한 정책 비판
  : 백도어를 통한 공급망 위협에서 정보의 도청뿐만 아니라 언젠가 이루어질 은밀한 명령에 의한 알 수 없는 작동을 우려
  : 즉, 예측할 수 없는 은밀한 명령을 통한 잠재적 위협 강조

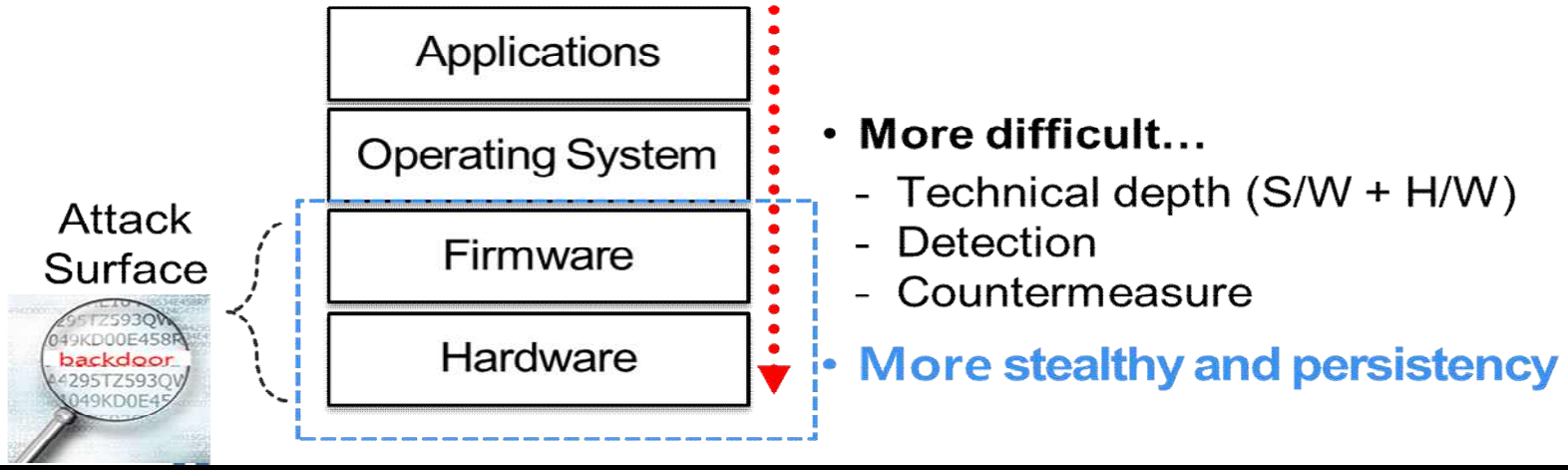
https://www.rsaconference.com/usa/agenda/how-to-reduce-supply-chain-risk-lessons-from-efforts-to-block-huawei

HW-level Supply Chain Attacks

HW Backdoors

HW 공급망 공격 유형 (Attack Surface)

- 중요 ICT 시스템의 하드웨어, 펌웨어 대상으로 의도적인 대체/변경 또는 악성코드, 백도어, 스파이칩 등 삽입
  - 펌웨어 공급망 공격 (Firmware Supply Chain Attack)
  - 하드웨어 공급망 공격 (Hardware Supply Chain Attack)



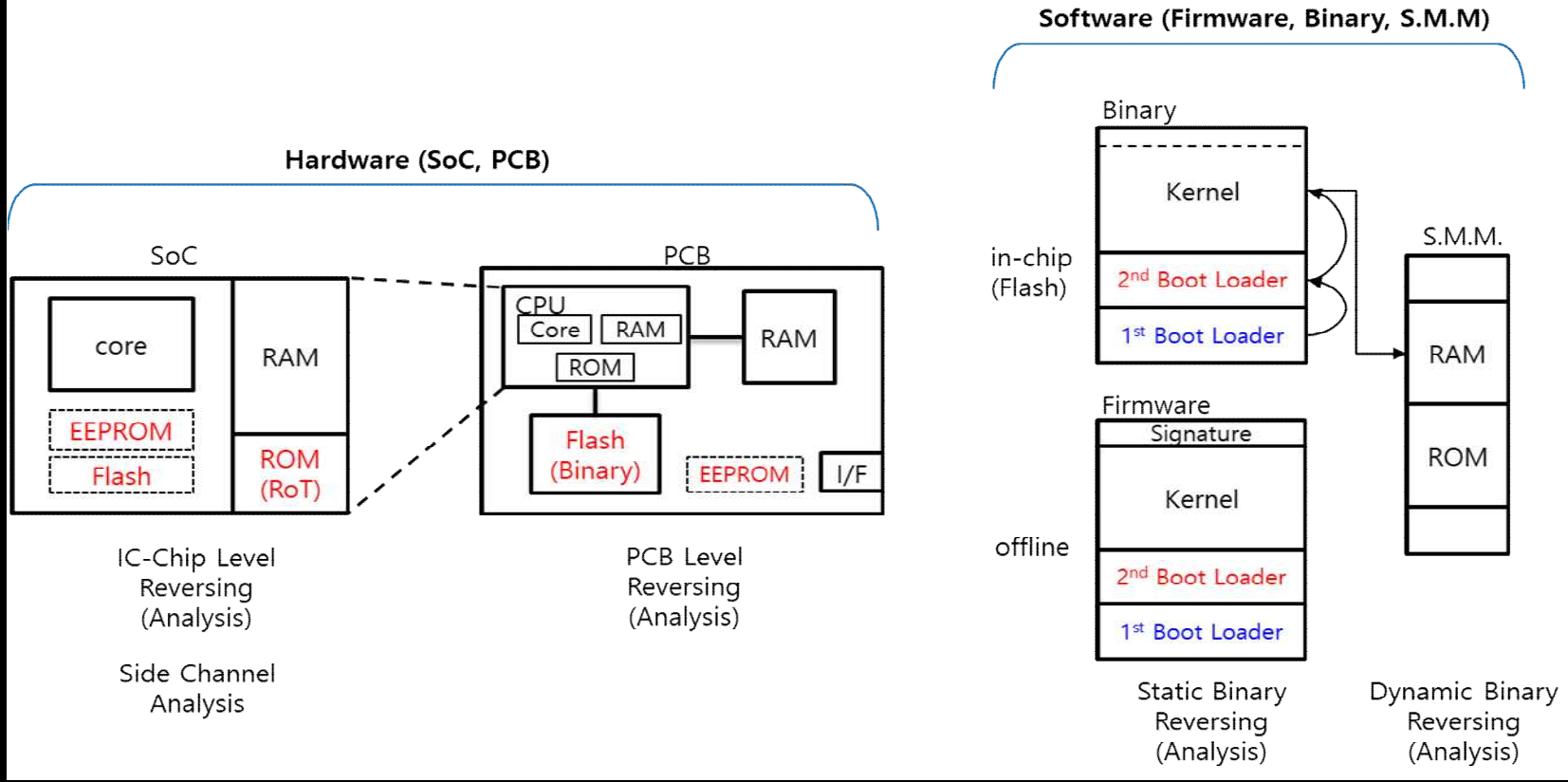
HW Backdoors

HW Backdoors/Trojans
> on-chip backdoor
- spychip
> in-memory backdoor
- spyware

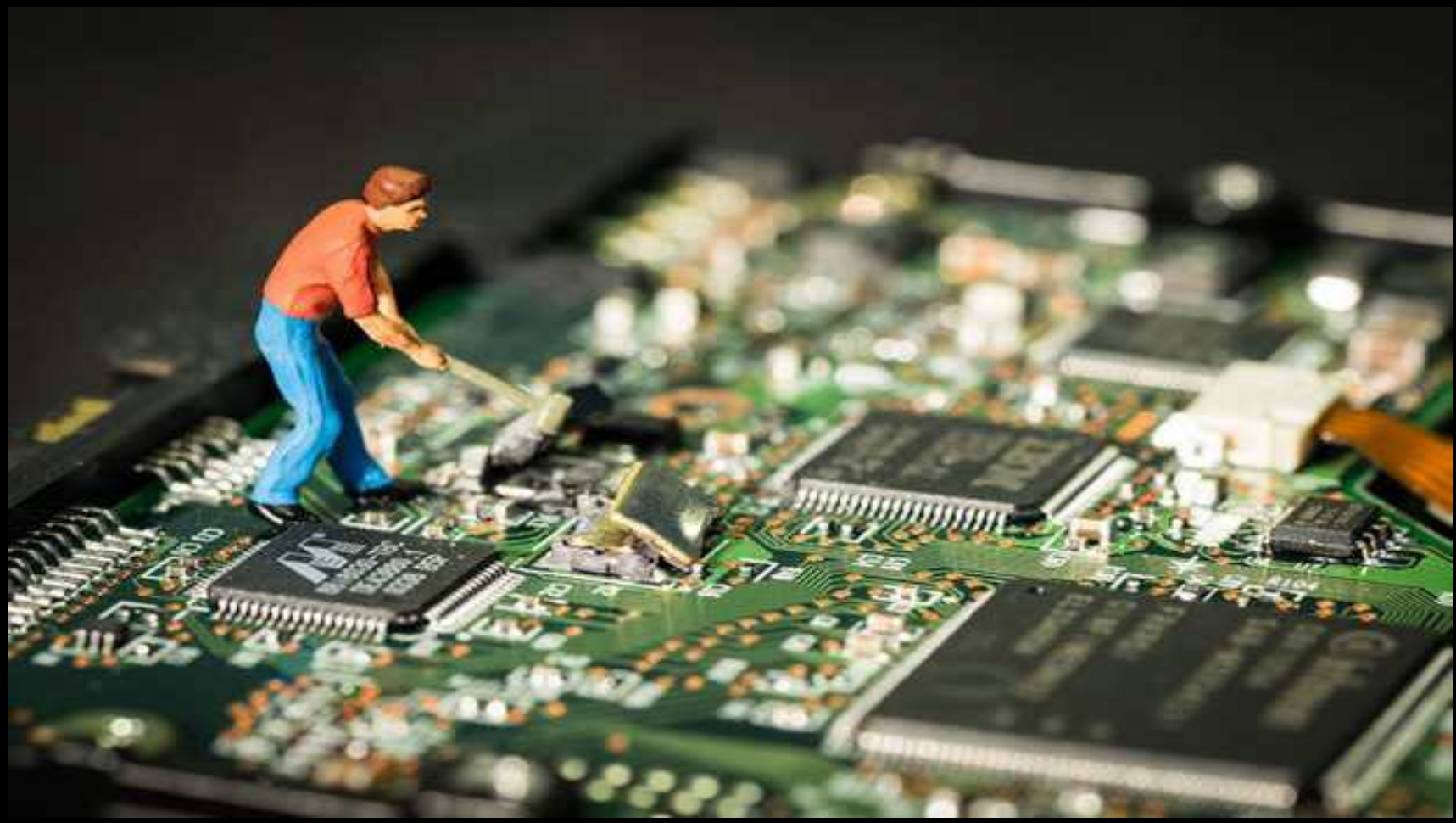
1. Bypass Authentication
   - ID/PW bypass
   - …
2. Information Gathering
   - Exploit Code + Socket Function
   - …
3. Remote System Control
   - Hidden Command / RCE
   - …

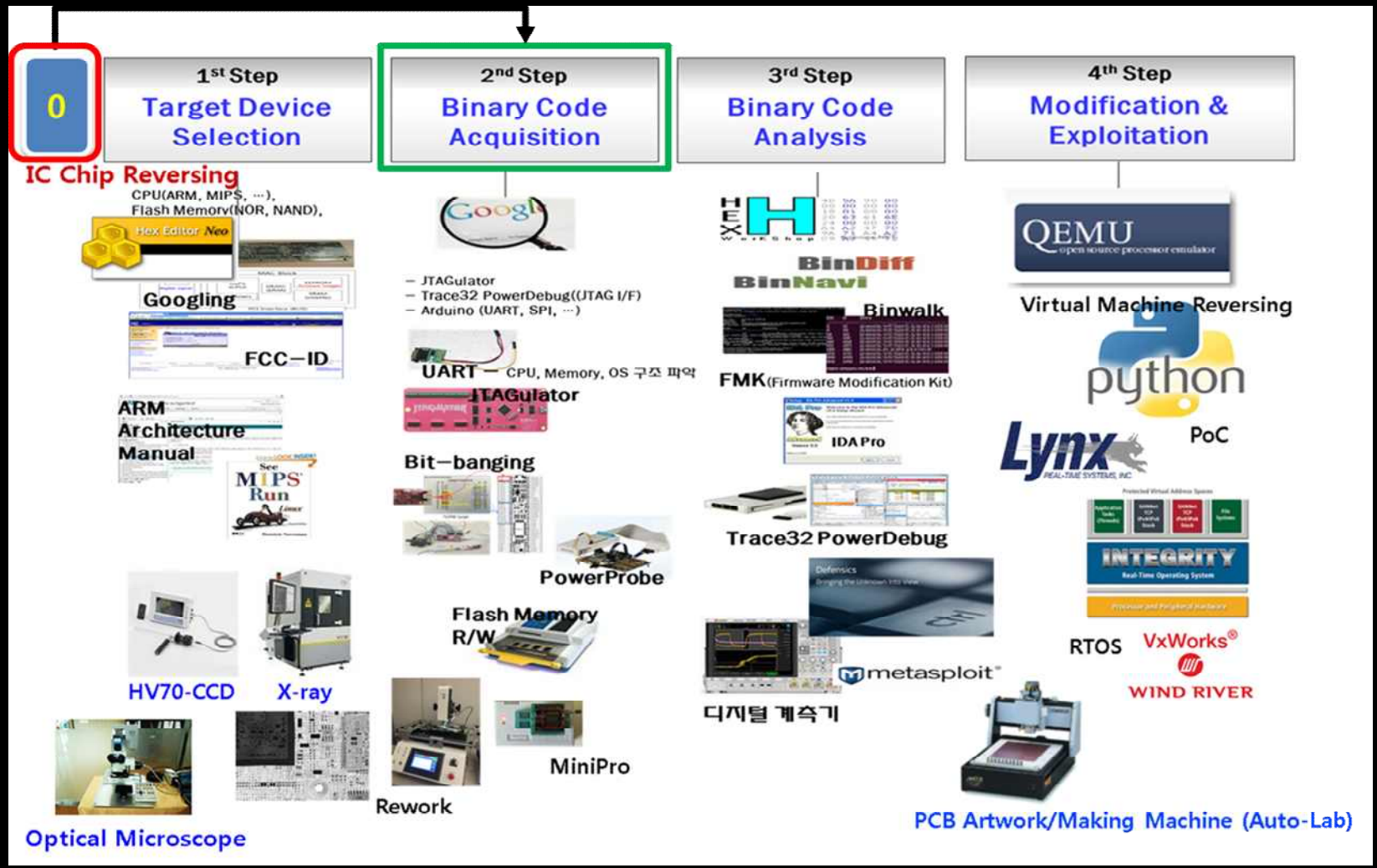
Core Tech.

IC 칩 / PCB / FW 단계의 고수준 분석 기술 요구



Strategy




0
1st Step
Target Device Selection
2nd Step
Binary Code Acquisition
3rd Step
Binary Code Analysis
4th Step
Modification & Exploitation
IC Chip Reversing
CPU(ARM, MIPS, …),
Flash Memory(NOR, NAND),
Hex Editor Neo
Googling
FCC-ID
ARM Architecture Manual
See MIPS Run Linux
HV70-CCD
X-ray
Optical Microscope
Google
– JTAGulator
– Trace32 PowerDebug((JTAG I/F)
– Arduino (UART, SPI, …)
UART – CPU, Memory, OS 구조 파악
JTAGulator
Bit-banging
PowerProbe
Flash Memory R/W
MiniPro
Rework
HEX Workshop
BinDiff
BinNavi
Binwalk
FMK(Firmware Modification Kit)
IDA Pro
Trace32 PowerDebug
metasploit
디지털 계측기
QEMU
open source processor emulator
Virtual Machine Reversing
python
PoC
Lynx
INTEGRITY
RTOS
VxWorks
WIND RIVER
PCB Artwork/Making Machine (Auto-Lab)

(Step 0) IC Chip Reversing

- **Hardware/Firmware Analysis**
  - If) 중요한 Binary가 Flash Memory가 아닌 MCU의 ROM 안에 존재
- **IC Rework ➔ 시편 제작 (Microscope 및 SEM 영상 촬영 가능)**
  - 칩 화학처리 ➔ Metal Layer 및 Poly Silicon Layer 분리
- **IC Chip 시편에 대한 SEM 영상 패턴 분석**
  - 0, 1 패턴 추출 ➔ 패턴 결합 ➔ Binary화
- **최종 추출된 Binary 검증**
  - IDA pro : Instruction 기반 Function Prologue & Epilogue 확인
  - Hex Viewer : 문자열 확인

(Step 1) Basic Analysis

◆ Hardware Analysis

- **Device & Board Scanning** (using X-ray, HV70-CCD, …)
- **Device Information Gathering** (from FCC-ID, Googling)
- **UART/JTAG Pin Map Finding** (by JTAGulator, Logic Analyzer(Saleae), …)
- **CPU (Core) Types** (ARM, MIPS, PowerPC, SuperH(SH), ColdFire, 8051/PIC, …)
  - † Security Enhanced CPU/MPU (최근)
- **Flash Memory Types** (EEPROM, NOR(BootSectorFlash, Secure NOR Flash), NAND, eMMC(e-NAND), …)
- **FPGA, CPLD** (Secure CPLD), …

◆ Software Analysis

- **Device Specification**
- **Firmware Information**

(Step 2) Binary Acquisition

- ◆ Rework Devices
  - – Rework System (예: BK-i310, ...)
  - – HAKKO Soldering Iron & Heat Gun
- ◆ Reball System
  - – Electron microscope, Hot-Plate, Oven, Experimental Desk
- ◆ Flash Memory용 Test-JIG
- ◆ Read & Write Flash Memory
  - – FlashPAK III
    - † Read & Write Flash Memory
    - † High Price
    - † Various Interface Sockets
  - – Etc.
    - † MiniPro : Low Price
    - † Bit-banging (SPI or I2C Serial Interface) : Low Price

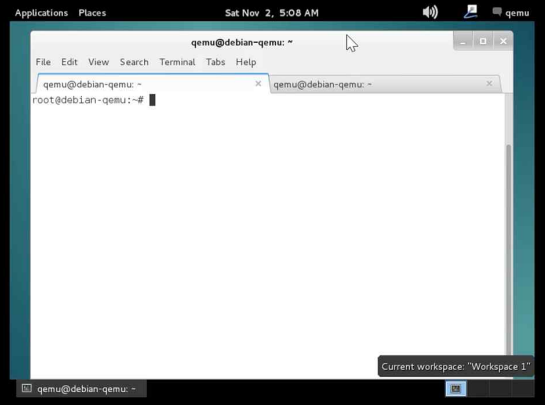
(Step 3) Binary Analysis (Static & Dynamic)

- **KALI Linux**
  - 다양한 공격 도구 탑재
- **Binwalk**
  - 바이너리 또는 펌웨어 기초 분석에 유용
- **Hex Viewer**
  - Hex Workshop, Hex Editor, 010 Editor, …
- **IDA-pro & Hex-ray Decompiler**
  - IDA pro : 거의 모든 Core에 대한 Instruction 해석
  - Hex-ray Decompiler : X86/64(32bit/64bit), ARM(32bit/64bit), PPC 지원
- **SW-based Debugging**
  - QEMU 기반 가상화 환경 구축
    - † QEMU-ARM/MIPS/PowerPC/SuperH 등
    - † gdb(Host)와 gdbserver(Target) 연동 동적 디버깅
  - SM(Set Memory) / DM(Dump Memory) for RTOS Debugging
- **HW-based Debugging (by JTAG Emulator)**
  - Trace32-PD 등을 이용하여 동적 메모리 디버깅 가능

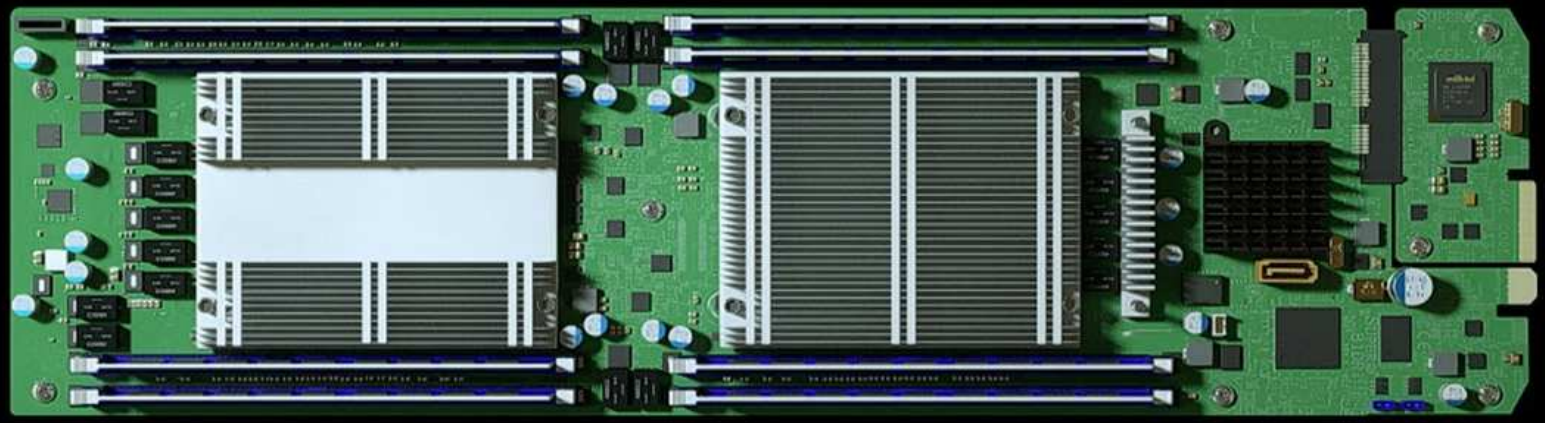
(Step 4) PoC (Proof-of-Concept)

- **Firmware/Binary Modification**
  - **CRC 우회**
  - **Signature 우회**
    - HW Hacking에 의한 Memory Flashing 작업 필요
  - **File System 수정**
    - rcS 수정 (init.d), nc(reverse shell 활성화), gdbserver 삽입, busybox 활용 등)
    - Firmware & Binary Unpack/Patch/Repack
- **Exploit PoC Code Generation**
  - **QEMU 기반 가상화 환경 구축**
    - QEMU-ARM/MIPS/PowerPC/SuperH 등
    - Exploit PoC 코드 제작
  - **C(+Inline-Assembly Code) & Python 코드 생성 및 동작검증**
- **(HW+SW) Binary Patch & Flashing & Rework**
  - **Binary Patch, Flashing (FlashPAK, MiniPro)**
  - **Rework (BK-i310), Reballing**

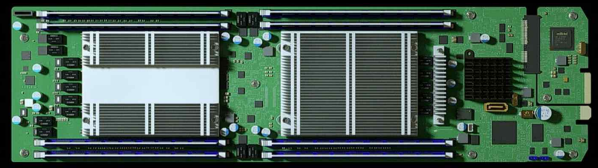

Data I/O
FlashPAK III
Ready
Busy
Error


Applications Places
Sat Nov 2, 5:08 AM
qemu
qemu@debian-qemu: ~
File Edit View Search Terminal Tabs Help
qemu@debian-qemu: ~
qemu@debian-qemu: ~
root@debian-qemu:~#
Current workspace: "Workspace 1"
qemu@debian-qemu: ~

Case Study

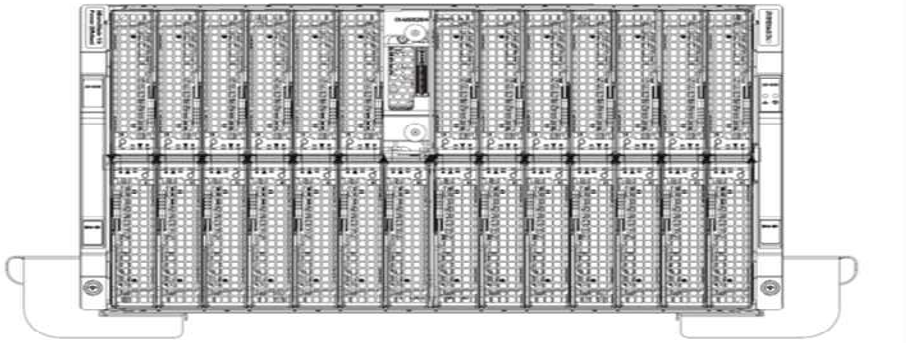


Analysis (1)

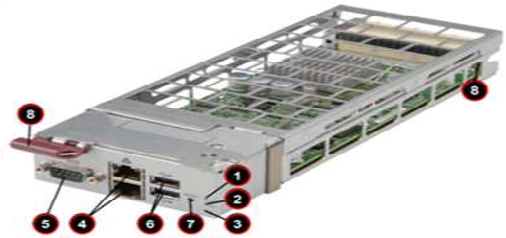


Supermicro MicroBlade

Model : MBI – 6xxx



Enclosure	MBE-628E-420 and MBE-628E-820 rack mount blade enclosures Dimensions: (HxWxD) 10.43 x 17.67 x 36.1 in. (265 x 449 x 917 mm)
Blade Module Support	Up to 28 hot-plug blade modules Supports Intel® based blades, optimize design for Intel E3 and E5 based processor blades
GbE Switch/Pass Through Module	Supports up to two hot-plug MBM-GEM-001 (IntelFM5224) with 56x 1Gbps downlinks; 2x 40Gbps QSFP or 8x 10Gbps SFP+ uplinks and 1Gbps RJ45 Also supports MBM-XEM-001 pass-through module and MBM-GEM-003i/S switch modules
Management Module	Supports up to two hot-plug Chassis Management Modules (CMM) providing remote KVM and IPMI 2.0 functionalities Management module not included in the enclosure
Power Supplies	Either four (MBE-628E-420) or eight (MBE-628E-820) hot-swap High-efficiency 2000W, N+1 or N+N redundant power supplies depending upon enclosure model selected
System Cooling	Up to eight cooling fans

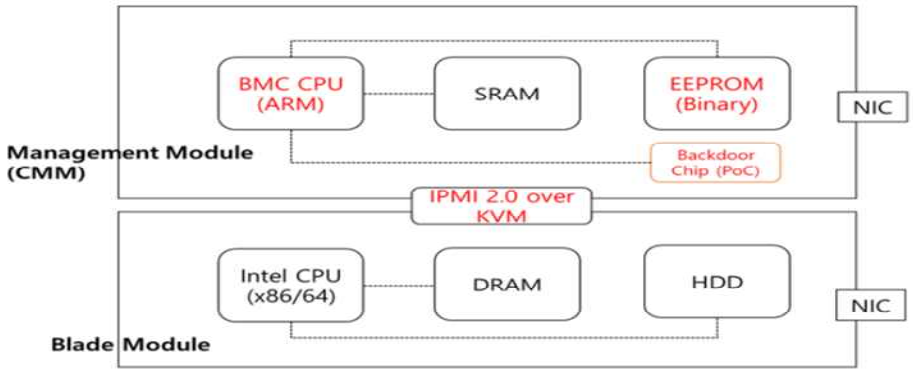


Remote KVM and IPMI 2.0 functionalities

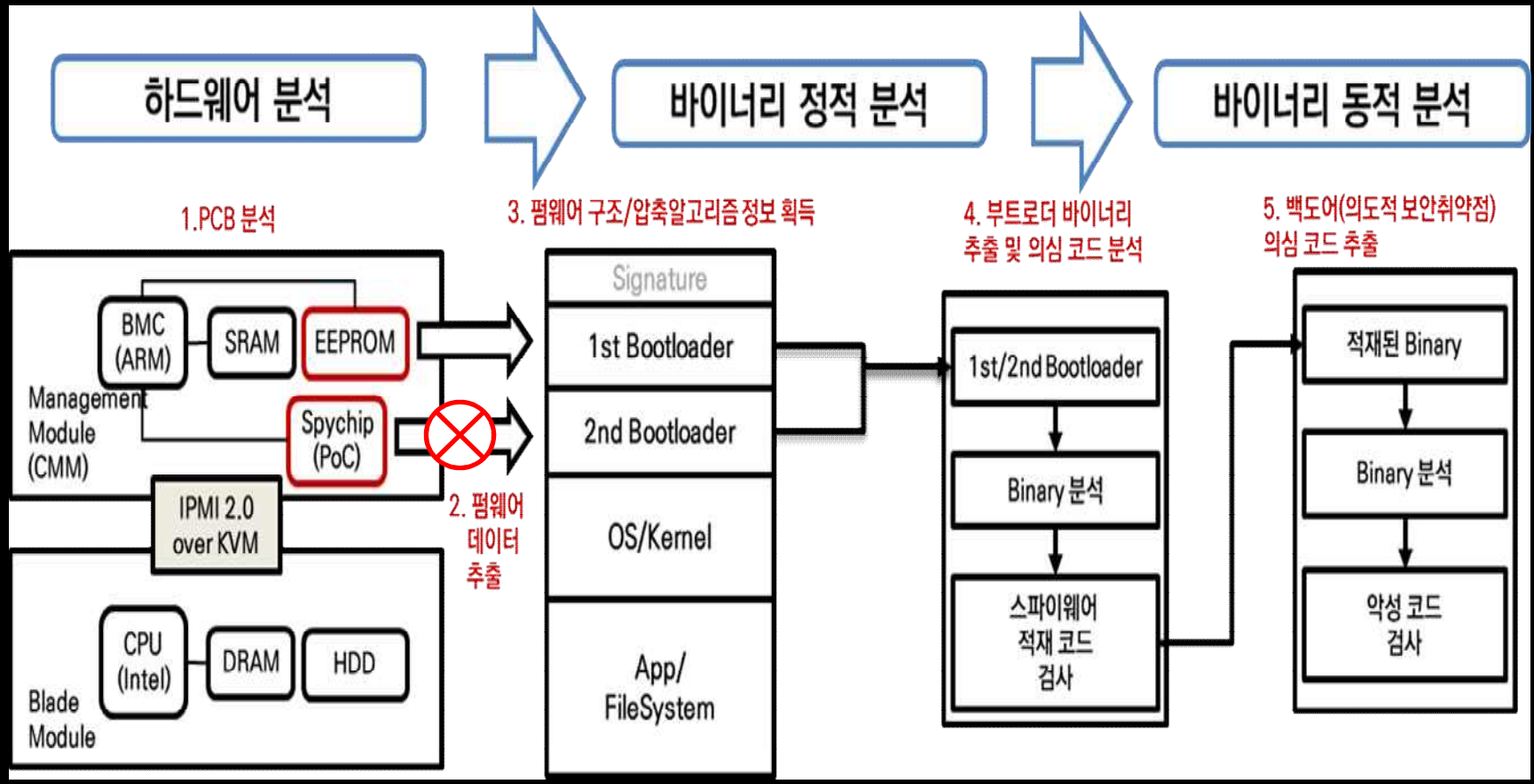
Analysis (2)

중국이 미국 서버 제조업체 **슈퍼마이크로 공급망**을 통해 아마존, 애플을 비롯한 **미국 회사 30여 곳을 공격**했고, 이 때문에 애플은 데이터센터에서 슈퍼마이크로 서버 7천대를 파기하고 아마존은 중국 데이터센터를 매각 (블룸버그, 2018)

해당 공급망 장비의 보안 취약성 배치 구조



Analysis (3)


하드웨어 분석
바이너리 정적 분석
바이너리 동적 분석
1.PCB 분석
3. 펌웨어 구조/압축알고리즘 정보 획득
4. 부트로더 바이너리 추출 및 의심 코드 분석
5. 백도어(의도적 보안취약점) 의심 코드 추출
BMC (ARM)
SRAM
EEPROM
Management Module (CMM)
Spychip (PoC)
IPMI 2.0 over KVM
CPU (Intel)
DRAM
HDD
Blade Module
2. 펌웨어 데이터 추출
Signature
1st Bootloader
2nd Bootloader
OS/Kernel
App/ FileSystem
1st/2nd Bootloader
Binary 분석
스파이웨어 적재 코드 검사
적재된 Binary
Binary 분석
악성 코드 검사

Thank You !

Any Questions ?

Email : corea@etri.re.kr