

NetSec-KR 2020 제26회 정보통신망 정보보호 컨퍼런스

The 26th Network Security Conference-Korea



NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Cold Boot Attacks

- IoT 디바이스 RAM 메모리 덤프

Yoo-Seung Won
Physical Analysis & Cryptography Engineering Team,
Temasek Laboratories,
Nanyang Technological University

07.17.2020



Table of Contents

(1) What is the Cold Boot Attack?

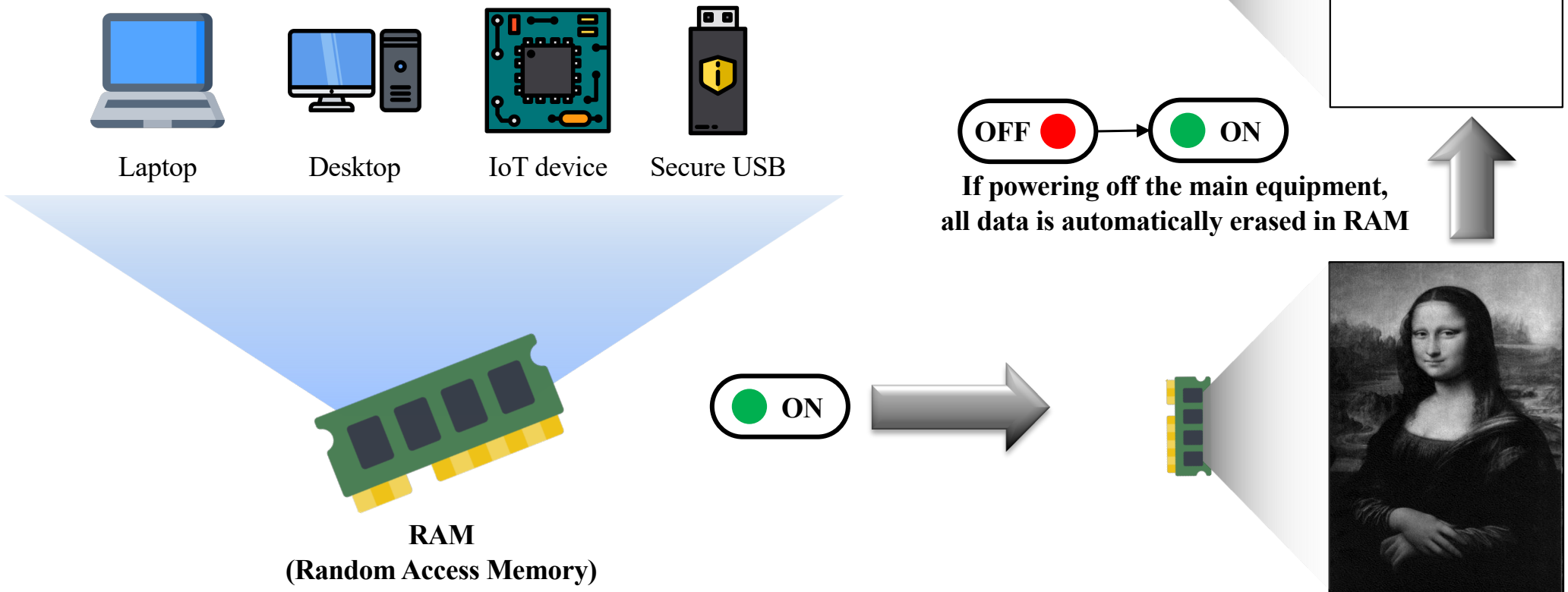
(2) The Outline of Cold Boot Attack

(3) Cold Boot Attack on Practical IoT Device

(4) Conclusion

1. What is the Cold Boot Attack?

- Normal Situation for RAM contents



1. What is the Cold Boot Attack?

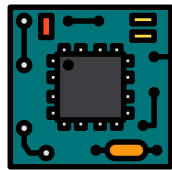
- Cold boot attack for RAM contents



Laptop



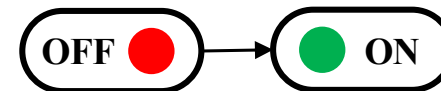
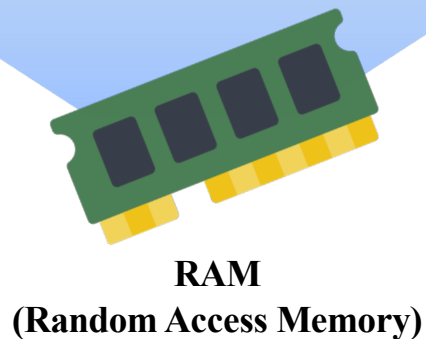
Desktop



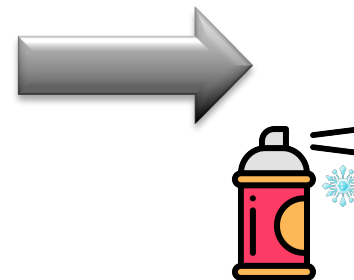
IoT device



Secure USB

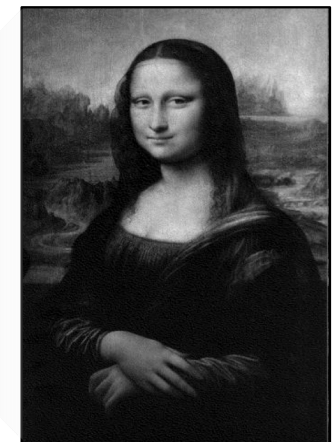
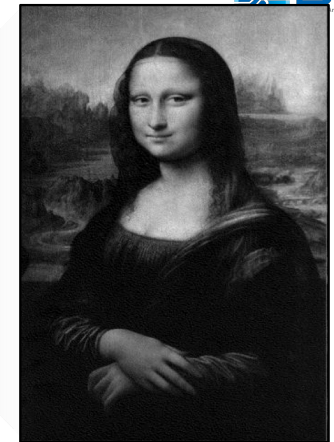


Even though powering off the main equipment,
all data is temporally alive



Air duster (cost under \$10)

-50°C



1. What is the Cold Boot Attack?

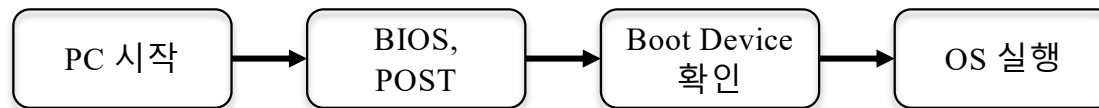
- Cold boot attack for RAM contents

- ✓ **Boot Sequence 에 대한 사전 지식 필요**

- Target이 Booting 될 때의 하는 일?

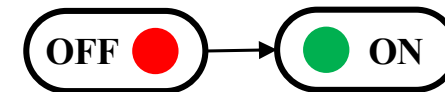
Ex) 하드웨어 초기화 및 제어(BIOS),
하드웨어 Self-test,
운영체제(OS) 로드, 등...

- 언제 RAM 을 읽을 수 있는가?



※ BIOS: Basic Input Output System

※ POST: Power-On Self Test



Even though powering off the main equipment,
all data is temporally alive



-50°C



Air duster (cost under \$10)

Table of Contents

(1) What is the Cold Boot Attack?

(2) The Outline of Cold Boot Attack

(3) Cold Boot Attack on Practical IoT Device

(4) Conclusion

2. The Outline of Cold Boot Attack

USENIX 2008

Target: Laptop

- ✓ 최초 Cold Boot Attack 제안
- ✓ 다양한 RAM에 대한 Cold Boot Attack (DDR / DDR2)
- ✓ Encrypted Disk 솔루션들에 대한 공격
예) dm-crypt, Veracrypt, BitLocker 등...

	Memory Type	Chip Maker	Memory Density	Make/Model	Year
A	SDRAM	Infineon	128Mb	Dell Dimension 4100	1999
B	DDR	Samsung	512Mb	Toshiba Portégé	2001
C	DDR	Micron	256Mb	Dell Inspiron 5100	2003
D	DDR2	Infineon	512Mb	IBM T43p	2006
E	DDR2	Elpida	512Mb	IBM x60	2007
F	DDR2	Samsung	512Mb	Lenovo 3000 N100	2007

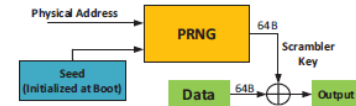
Table 1: Test systems we used in our experiments



IEEE HPCA 2017

Target: DDR3 / DDR4 RAM

- ✓ DDR3/DDR4에 대한 최초 공격
- ✓ Scrambled solution에 대한 Cold Boot Attack
- ✓ Latency가 낮은 Encryption 솔루션 제안



2008

2013

2017

2018

2020



ACNS 2013

Target: Galaxy Nexus

- ✓ 최초 Smart Phone에 대한 공격
- ✓ 공격자 가정: Unlocking the bootloader
- ✓ RAM Dump, 4-dit PIN crack, decrypt user data

State of RAM with power on

1 0 1 1 1 0 1 0 1 0 0 1 1

Freeze + extract RAM

0 0 1 1 0 1 1 1 0 0 1 1

- ▶ DES: (0.5, 0.001) bit flip rate trivially [HSHCPFAF09]
- ▶ AES:
 - ▶ AES-128: (0.7, 0) bit-flip rate in 1 sec on average [KY10]
 - ▶ AES-256: (0.65, 0) bit-flip rate in 90 secs on average [Tso09]
- ▶ RSA (1024-bit modulus): (0.4, 0.001) bit-flip rate in 2.4 secs on average [PPS12]
- ▶ NTRU: (0.01, 0.001) bit-flip rate in minutes to hours on average for the ntru-crypto eps449ep1 parameters ($N = 449, df = 134, dg = 149, p = 3, q = 2048$) [PV17]

Scheme	bit-flip rates		NTT		non-NTT
	ρ_0	ρ_1	cost	rate	cost
Kyber	0.2%	0.1%	$3 \cdot 2^{21.1}$	95%	$2^{38.7}$
Kyber	1.0%	0.1%	$3 \cdot 2^{43.3}$	91%	$2^{70.3}$
Kyber	1.7%	0.1%	$3 \cdot 2^{62.8}$	89%	$2^{100.1}$
NewHope	0.17%	0.1%	$2^{48.7}$	84%	$2^{53.7}$
NewHope	0.25%	0.1%	$2^{60.6}$	81%	$2^{60.0}$
NewHope	0.32%	0.1%	$2^{70.2}$	81%	$2^{66.1}$

CHES 2018

Target: Laptop

- ✓ PQC(Post Quantum Cryptography)의 비밀 키의 NTT (Number Theoretic Transform) encoding 값에 대한 비밀 키 복구 비율
- ✓ Alg.Target: Kyber and NewHope

2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

- Target

	Memory Type	Chip Maker	Memory Density	Make/Model	Year
A	SDRAM	Infineon	128Mb	Dell Dimension 4100	1999
B	DDR	Samsung	512Mb	Toshiba Portégé	2001
C	DDR	Micron	256Mb	Dell Inspiron 5100	2003
D	DDR2	Infineon	512Mb	IBM T43p	2006
E	DDR2	Elpida	512Mb	IBM x60	2007
F	DDR2	Samsung	512Mb	Lenovo 3000 N100	2007

Table 1: Test systems we used in our experiments

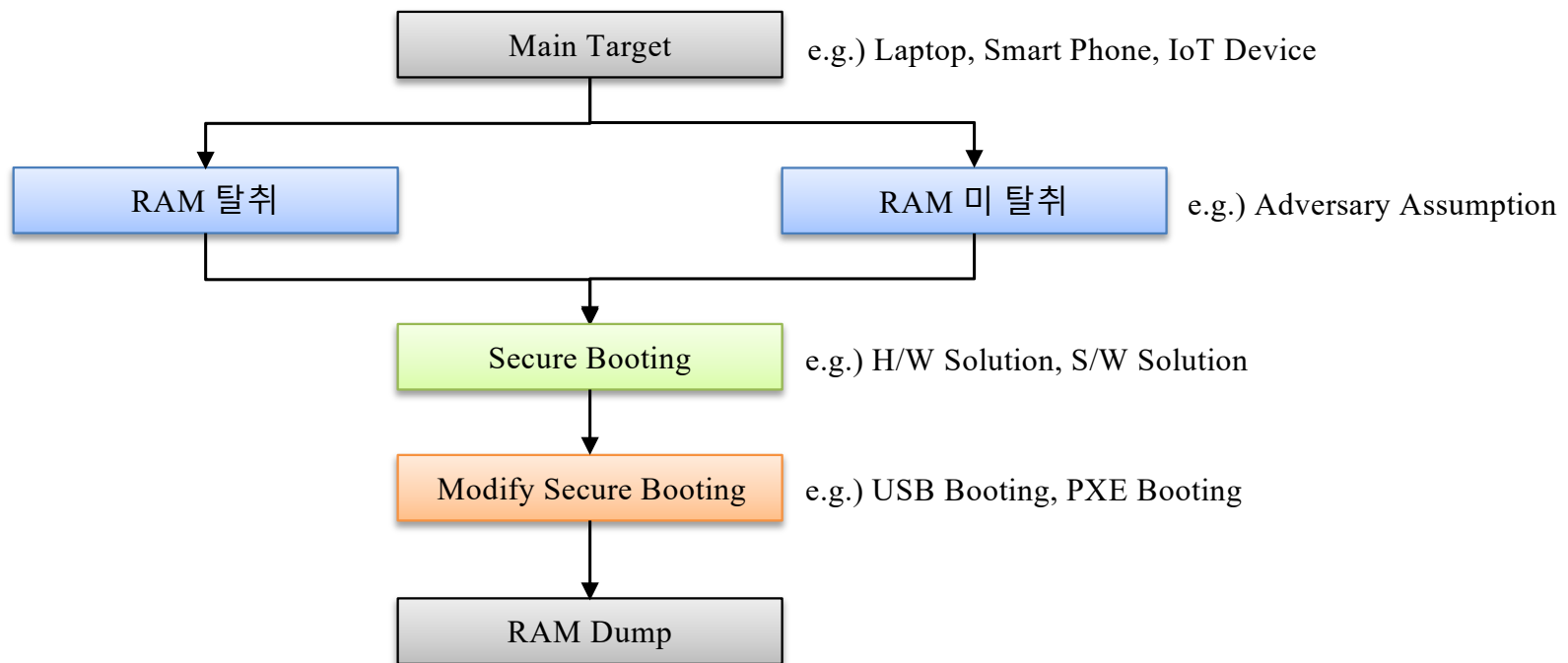
- ✓ Main Target: IBM T43p laptop with 512MB RAM (DDR2)
 - RAM: HYS64T64020HDL-3-7-A (Infineon)



2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

- Flow Chart for Cold Boot Attack against Main Target

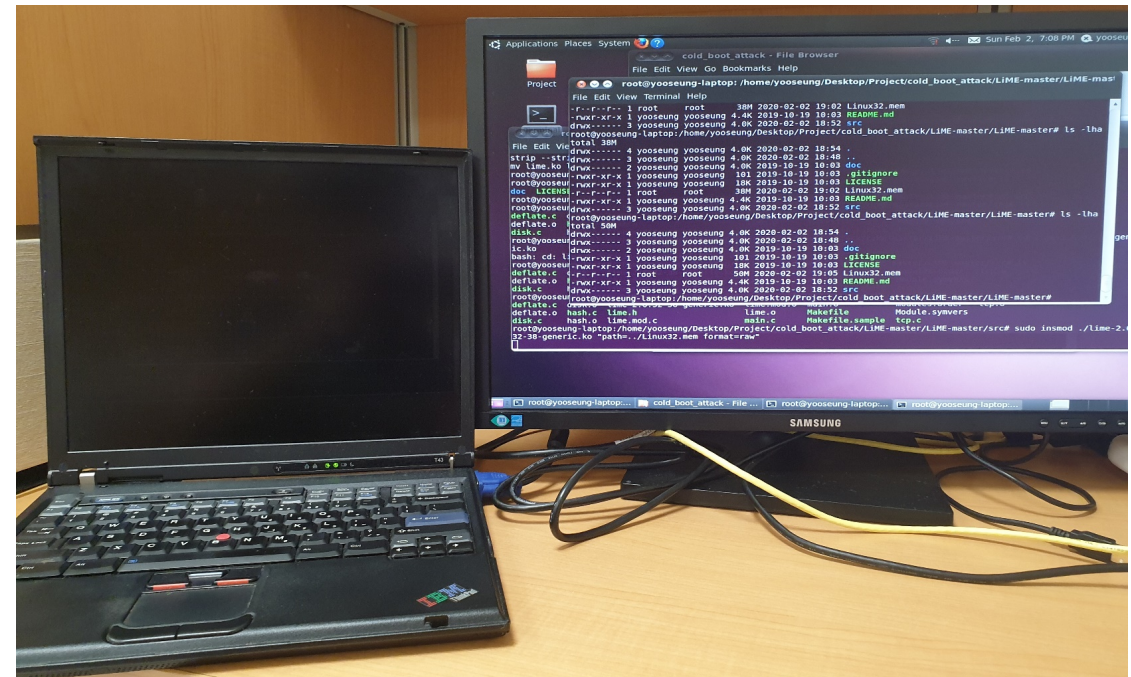


※ PXE: Preboot eXecution Environment

2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

- Main Target
 - ✓ IBM T43p laptop with 512MB RAM (DDR2)
- Open Source Code
 - ✓ <https://citp.princeton.edu/our-work/memory/>

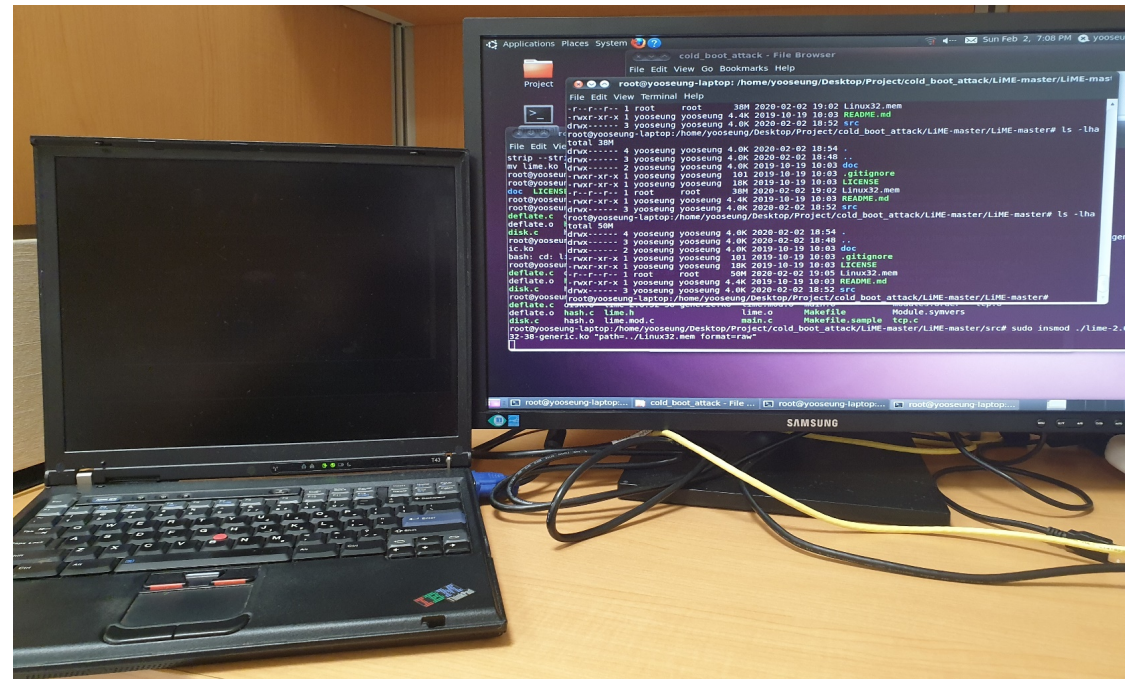


2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

- 공격 방법

- 1) Making Boot USB
- 2) Cold Boot Attack against Victim Laptop
- 3) Obtaining RAM data via USB Memory



2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

• 재연 결과

- ✓ Dumped memory에서
“This is PACE Lab in NTU” hex값 확인

```

007B4090 55 54 68 69 73 20 69 73 20 50 41 43 45 20 4C 61 UThis is PACE La
007B40A0 62 20 69 6E 20 4E 54 55 54 68 69 73 20 69 73 20 b in NTUThis is
007B40B0 50 45 43 45 20 4C 61 62 20 69 6E 20 4E 54 55 54 PECE Lab in NTUT
007B40C0 68 69 73 20 69 73 20 50 41 43 45 20 4C 61 62 28 his is PACE Lab(
007B40D0 69 6E 20 4E 54 55 54 68 79 73 20 69 73 20 50 41 in NTUTHis is PA
007B40E0 43 45 20 4C 61 62 20 69 6E 20 4E 54 55 54 68 69 CE Lab in NTUTHi
007B40F0 73 20 69 73 20 50 41 43 45 60 4C 69 62 20 69 6E s is PACE`Lib in
007B4100 20 4E 54 55 54 68 79 73 20 69 73 20 50 41 43 45 NTUTHys is PACE
007B4110 20 4C 61 62 20 69 6E 21 4E 54 55 54 68 69 77 20 Lab in!NTUThiw
007B4120 69 73 20 50 41 43 45 24 4C 61 62 20 69 6E 20 4E is PACE$Lab in N
007B4130 54 55 54 E8 69 73 20 69 73 20 50 41 43 45 20 4C TUTèis is PACE L
007B4140 61 62 20 6B 6E 20 4E 54 55 54 68 69 73 20 69 73 ab kn NTUThis is
007B4150 20 50 41 43 45 20 4C 61 62 20 69 6E 20 4E 54 55 PACE Lab in NTU
007B4160 56 68 69 77 20 69 73 20 50 41 43 45 20 4C 61 62 Vhiw is PACE Lab
007B4170 20 69 6E 20 4E 54 55 54 68 69 73 21 69 73 20 50 in NTUThis!is P
007B4180 41 43 45 24 4C 61 6A 20 69 6E 20 4E 54 55 D5 68 ACE$LaJ in NTUOh
007B4190 69 73 20 69 73 20 50 49 43 45 20 4C 61 62 20 69 is is PICE Lab i
007B41A0 6E 20 4E 54 55 54 68 69 73 20 69 73 20 50 41 43 n NTUThis is PAC
007B41B0 45 20 4C 61 62 20 69 6E 20 4E 54 55 54 68 69 73 E Lab in NTUThis
007B41C0 20 69 73 20 50 41 43 45 22 4C 61 62 20 69 6E 20 is PACE"Lab in
007B41D0 4E 54 55 54 68 69 73 20 69 73 20 50 41 43 C5 20 NTUThis is PACÂ
007B41E0 4C 61 62 A4 69 6E 20 4E 54 55 54 68 69 73 20 69 Lab*in NTUThis i
007B41F0 73 20 50 41 43 45 E0 4C 61 62 A0 69 6E 20 6E 54 s PACEàLab in nT
007B4200 5D 54 68 69 73 20 69 73 20 50 41 43 45 20 4C 61 ]This is PACE La
007B4210 62 20 69 6E 20 4E 54 55 54 68 69 73 20 69 73 20 b in NTUThis is
007B4220 50 41 43 45 20 4C 61 62 A0 69 6E 20 4E 54 55 54 PACE Lab in NTUT
007B4230 68 69 73 20 69 73 20 50 41 43 45 20 4C 61 62 20 his is PACE Lab

```


2. The Outline of Cold Boot Attack

[USENIX 2008] J.Alex *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”

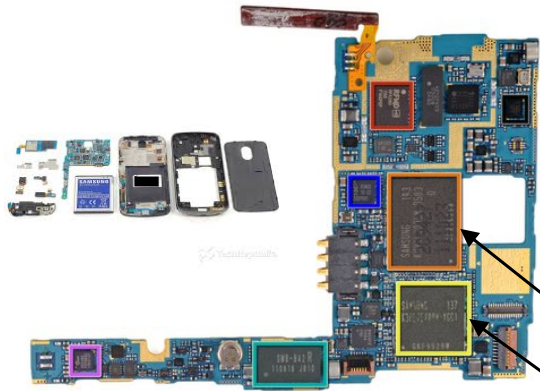
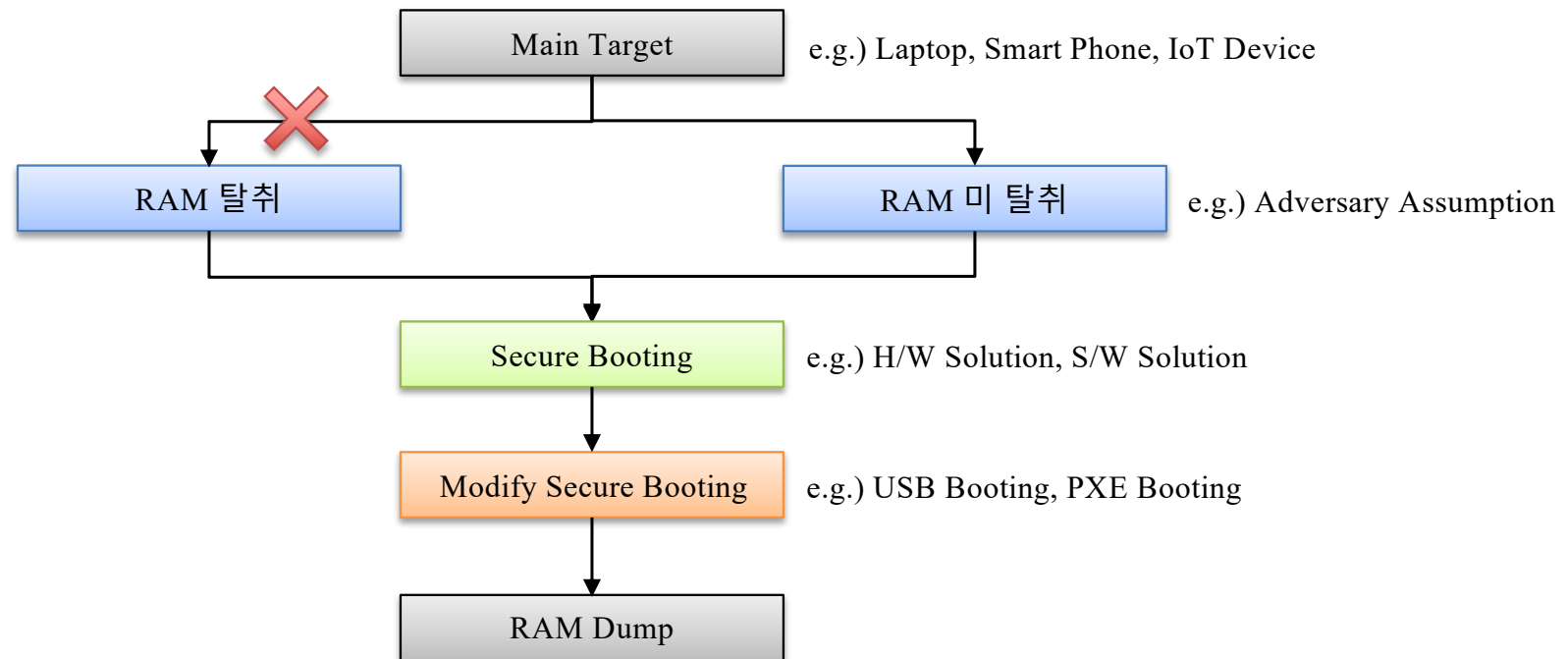
- Encrypted Disk에 대한 Cold Boot Attack
 - ✓ Software Solution for Disk Encryption
 - BitLocker – Windows OS
 - FileVault – Mac OS
 - TrueCrypt – Windows, Mac, Linux OS
 - dm-crypt – Linux OS
 - Loop-AES – Linux OS
 - ✓ Software Solution의 AES 알고리즘의 비밀 키를 Cold Boot Attack을 활용하여 탈취 가능
 - Open Source: <https://citpsite.s3.amazonaws.com/memory-content/src/aeskeyfind-1.0.tar.gz>

2. The Outline of Cold Boot Attack

[ACNS 2013] T.Muller *et al.*, “FROST: Forensic Recovery of Scrambled Telephones”



Samsung Galaxy Nexus
(Android 4.0)



Samsung KMVYL0000LM Multichip Memory
Package with 512MB RAM

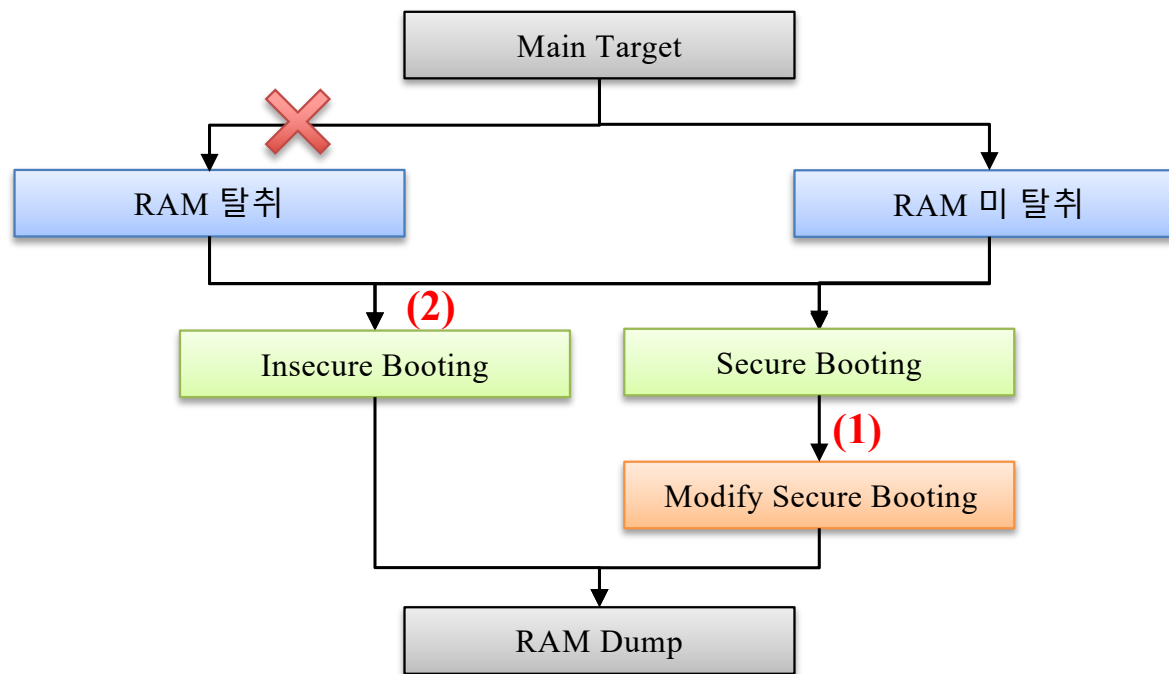
Samsung K3PE7E700M 512MB DDR2 SDRAM

※ Samsung Galaxy Nexus Teardown: <https://ko.ifixit.com/Teardown/Samsung+Galaxy+Nexus+Teardown/7182>

2. The Outline of Cold Boot Attack

[ACNS 2013] T.Muller *et al.*, “FROST: Forensic Recovery of Scrambled Telephones”

※ Unlocking Bootloader: 제조사가 기본 제공하는 Bootloader 소프트웨어의 변경



(1) Locking the bootloader

- ✓ Locking → Unlocking
- ✓ Recent e-mails, photos, visited websites



(2) Unlocking the bootloader

- ✓ Recovery mode에 일부 firmware 삽입
- ✓ AES key 탈취, pin crack, 등... 실행

※ Open Source: <https://www.cs1.tf.fau.de/research/system-security-and-software-protection-group/frost/>

2. The Outline of Cold Boot Attack

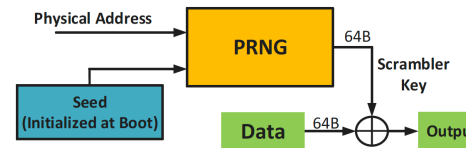
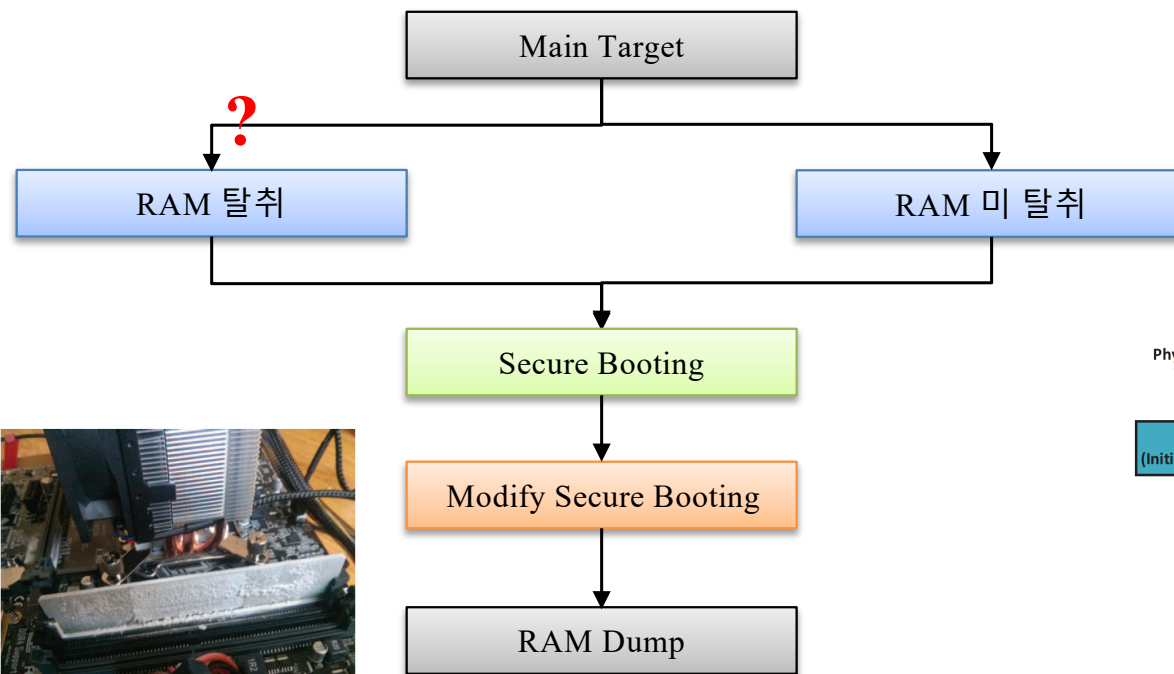
[IEEE HPCA 2013] S. F. Yitbarek *et al.*, “Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors”

(1) DDR / DDR2

✓ Raw 한 형태로 데이터 저장 및 로드

(2) DDR3 / DDR4

✓ Cold Boot Attack에 대한 대응기법으로 Scrambler (64바이트) 적용



DDR4 Scrambler

✓ Scrambler 키 규칙
(16MB로 모든 키 찾을)

CPU Model	Microarchitecture	Launch Date
i5-2540M (DDR3)	SandyBridge	Q1, 2011
i5-2430M (DDR3)	SandyBridge	Q4, 2011
i7-3540M (DDR3)	IvyBridge	Q1, 2013
i5-6400 (DDR4)	Skylake	Q3, 2015
i5-6600K (DDR4)	Skylake	Q3, 2015

Main Target

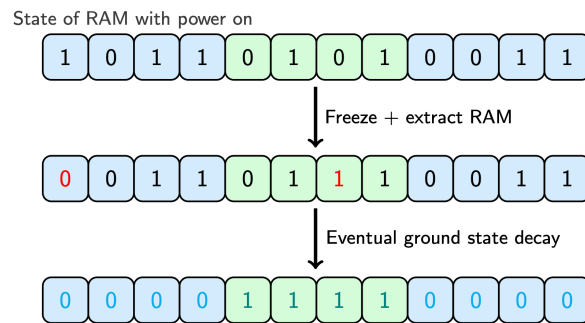
$$\begin{aligned}
 K[i:i+1] \oplus K[i+2:i+3] &= K[i+8:i+9] \oplus K[i+10:i+11] \\
 K[i:i+1] \oplus K[i+4:i+5] &= K[i+8:i+9] \oplus K[i+12:i+13] \\
 K[i:i+1] \oplus K[i+6:i+7] &= K[i+8:i+9] \oplus K[i+14:i+15] \\
 K[i+2:i+3] \oplus K[i+4:i+5] &= K[i+10:i+11] \oplus K[i+12:i+13] \\
 &\text{for } i = 0, 16, 32, 48 \text{ (i.e., for each 16-byte aligned words)}
 \end{aligned}$$

※ DDR SDRAM: Double Data Rate Synchronous Dynamic Random Access Memory

2. The Outline of Cold Boot Attack

[CHES 2018] M. R. Albrecht *et al.*, “Cold Boot Attacks on Ring and Module LWE Keys Under the NTT”

- Cold Boot Attack 환경에서, PQC(Post-Quantum Cryptography)의 비밀키 획득 복잡도



Scheme	bit-flip rates		Average Time
	ρ_0	ρ_1	
DES	0.5%	0.001%	Trivially
AES-128	0.7%	0%	1 sec
AES-256	0.65%	0%	90 sec
RSA-1024	0.4%	0.001%	2.4 sec
NTRU	0.01%	0.001%	1 hour

(ntru-crypto eps449ep1 parameter: N=449, df=134, dg=149, p=3, q=2048)

Scheme	bit-flip rates		NTT	
	ρ_0	ρ_1	cost	rate
Kyber	0.2%	0.1%	$3 \cdot 2^{21.1}$	95%
Kyber	1.0%	0.1%	$3 \cdot 2^{43.3}$	91%
Kyber	1.7%	0.1%	$3 \cdot 2^{62.8}$	89%
NewHope	0.17%	0.1%	$2^{48.7}$	84%
NewHope	0.25%	0.1%	$2^{60.6}$	81%
NewHope	0.32%	0.1%	$2^{70.2}$	81%

※ Reference

- [1] [Communications of the ACM 2009] J. A. Halderman *et al.*, “Lest We Remember: Cold Boot Attacks on Encryption Keys”
- [2] [IEEE 2010] A. A. Kamal *et al.*, “Applications of SAT solvers to AES key recovery from decayed key schedule images”
- [3] [SAC 2009] A. Tsow, “An improved recovery algorithm for decayed AES key schedule images”
- [4] [ASIACRYPT 2012] K. G. Paterson *et al.*, “A coding-theoretic approach to recovering noisy RSA keys”
- [5] [INDOCRYPT 2017] K. G. Paterson *et al.*, “Cold Boot Attacks on NTRU”

Table of Contents

(1) What is the Cold Boot Attack?

(2) The Outline of Cold Boot Attack

(3) Cold Boot Attack on Practical IoT Device

(4) Conclusion

Table of Contents

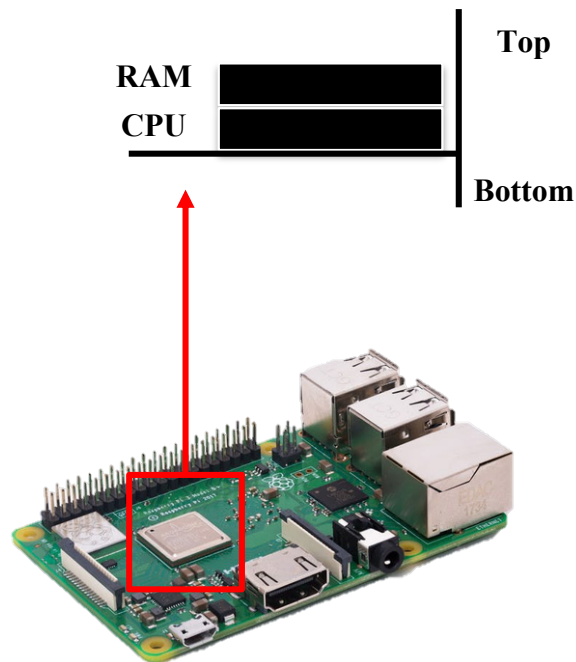
(3) Cold Boot Attack on Practical IoT Device //

- 1) Identifying the Target & Potential Vulnerabilities
- 2) Recovery of image stored in RAM
- 3) Recovery of the dm-crypt master key

3. Cold Boot Attack on Practical IoT device

1) Identifying the Target & Potential Vulnerabilities

✓ Main Target: Raspberry Pi Model B+



Raspberry Pi model B+

Target	Raspberry Pi model B+
SoC	Broadcom BCM2835 (Technology: 65nm)
CPU	700 MHz ARM1176JZF-S single core
GPU	Broadcom VideoCore IV @ 250 MHz OpenGL ES 2.0 (24 GFLOPS) MPEG-2 and VC-1 (with license), 1080p30 H.264/MPEG-4 AVC high-profile decoder and encoder (L2 cache of 128 KB)
Memory (SDRAM)	LPDDR2 512 MB (shared with GPU) (SAMSUNG k4p4g324eq-rgc2)

3. Cold Boot Attack on Practical IoT device

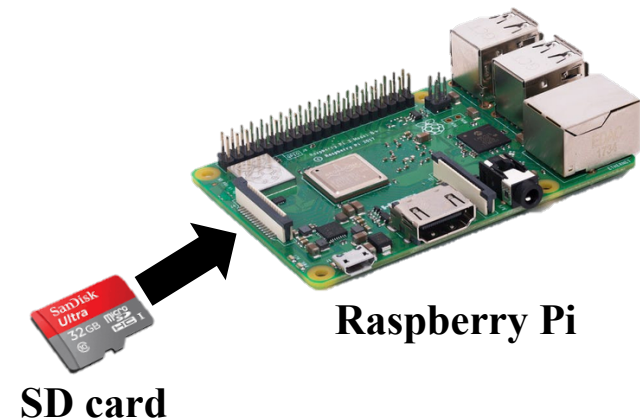
1) Identifying the Target & Potential Vulnerabilities

✓ Raspberry Pi 동작 방법

- OS는 메모리 카드인 SD card에 설치되어 있으며, 이 곳에서 작동한다.

✓ 공격자 가정

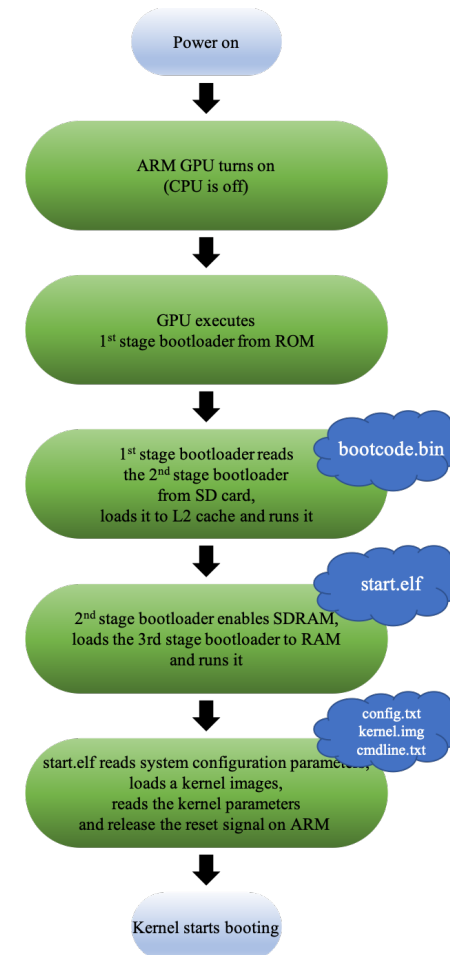
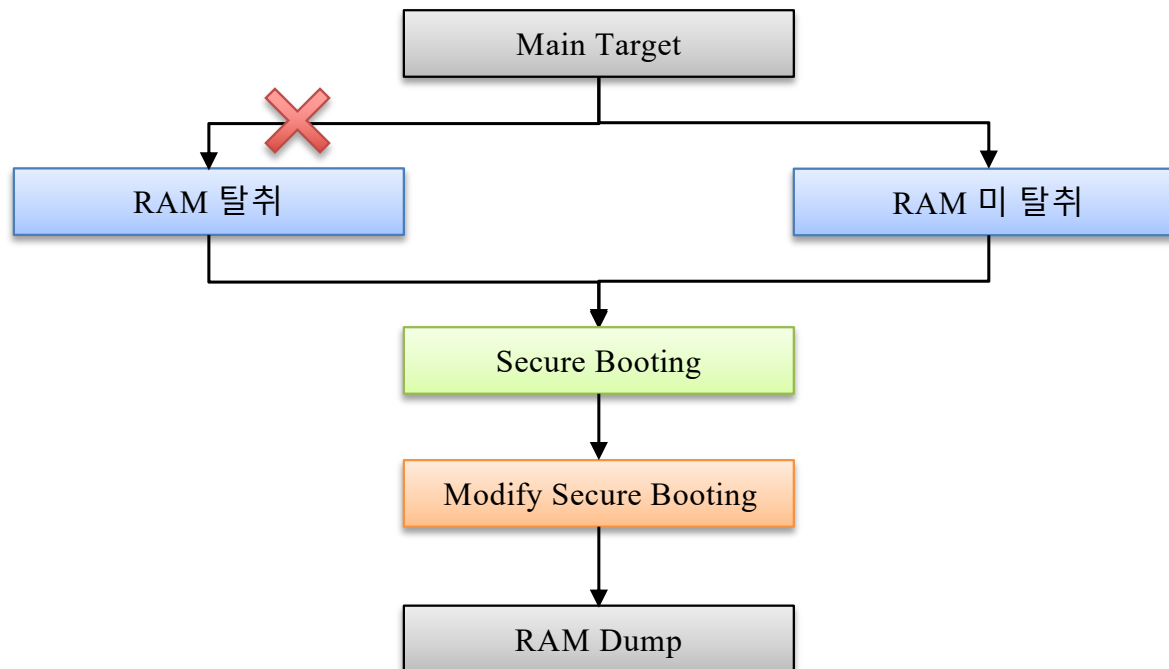
- 권한을 부여 받은 자 이외에 RAM access 불가.
- 공격자는 물리적으로 Raspberry Pi의 SD card를 교체할 수 있다.
- 공격대상자의 SD card로부터 어떠한 비밀 정보도 얻을 수 없다.



3. Cold Boot Attack on Practical IoT device

1) Identifying the Target & Potential Vulnerabilities

✓ Boot Sequence 분석



3. Cold Boot Attack on Practical IoT device

1) Identifying the Target & Potential Vulnerabilities

✓ L2 cache memory

➤ Attack point: Minimum 1st stage bootloader

✓ RAM

➤ Attack point: Minimum 2nd stage bootloader

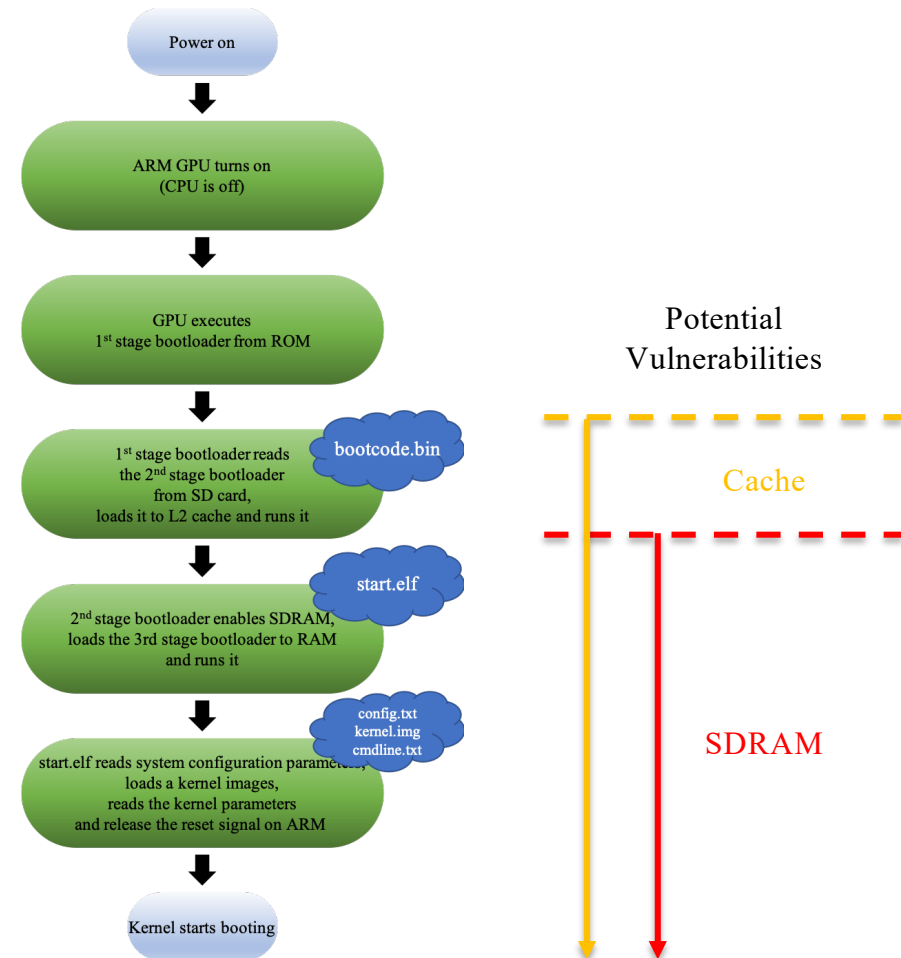


Table of Contents

(3) Cold Boot Attack on Practical IoT Device //

1) Identifying the Target & Potential Vulnerabilities

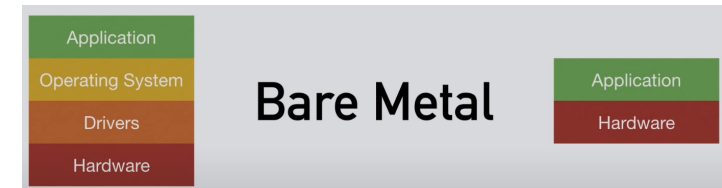
2) Recovery of image stored in RAM

3) Recovery of the dm-crypt master key

3. Cold Boot Attack on Practical IoT device

2) Recovery of image stored in RAM

✓ Bare-metal programming 활용하여, 부팅

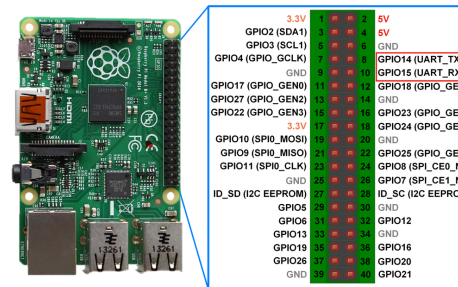


➤ Processor, Clock, Memory 세팅하고, 최소한의 Boot Loader로 OS없이 원하는 기능 프로그래밍

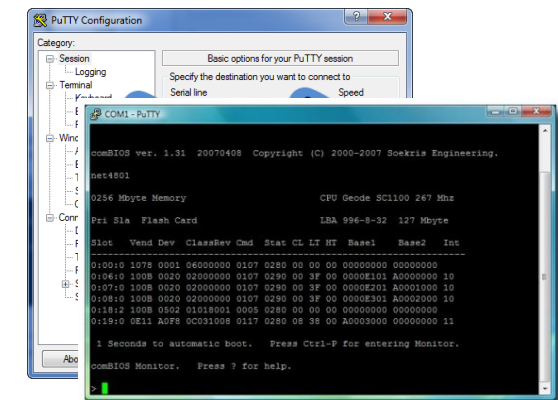
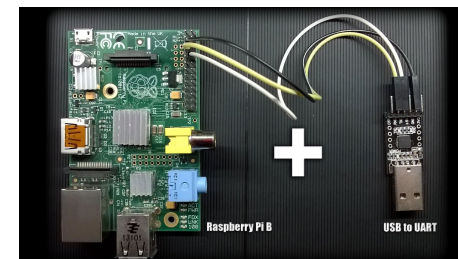
✓ RAM에 저장된 값 읽어오는 방법

➤ UART 통신을 활용한, 부팅 후 RAM 읽음

➤ USB 통신 프로그램 구현



UART to USB 연결



UART Communication Program
(e.g. PuTTY)

3. Cold Boot Attack on Practical IoT device

2) Recovery of image stored in RAM

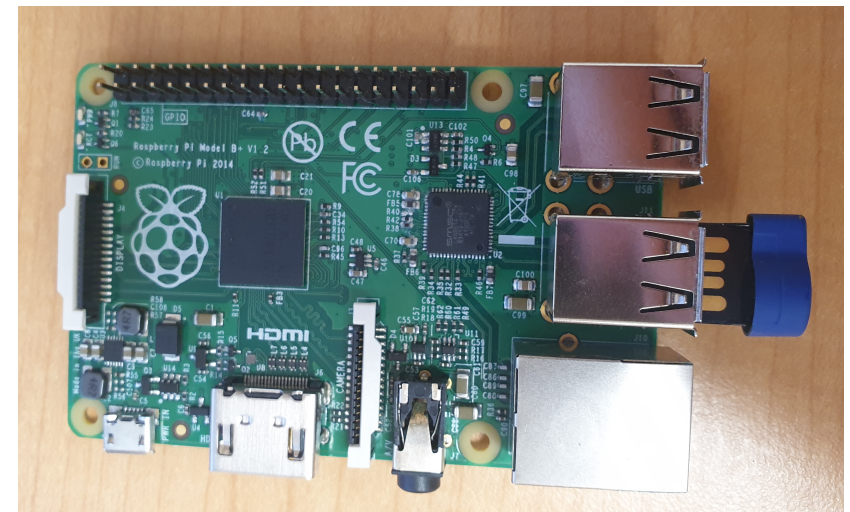
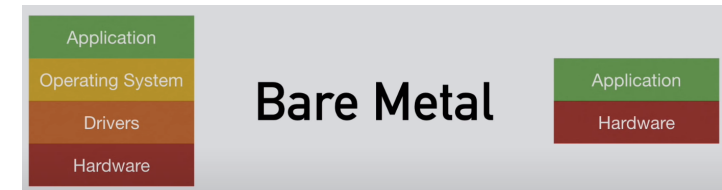
✓ Bare-metal programming 활용하여, 부팅

➤ Processor, Clock, Memory 세팅하고, 최소한의 Boot Loader로 OS없이 원하는 기능 프로그래밍

✓ RAM에 저장된 값 읽어오는 방법

➤ UART 통신을 활용한, 부팅 후 RAM 읽음

➤ USB 통신 프로그램 구현



3. Cold Boot Attack on Practical IoT device

2) Recovery of image stored in RAM

✓ Basic Command for reading the RAM

```
static inline u32 read32 (uintptr nAddress)
{
    return *(u32 volatile *) nAddress;
}
```

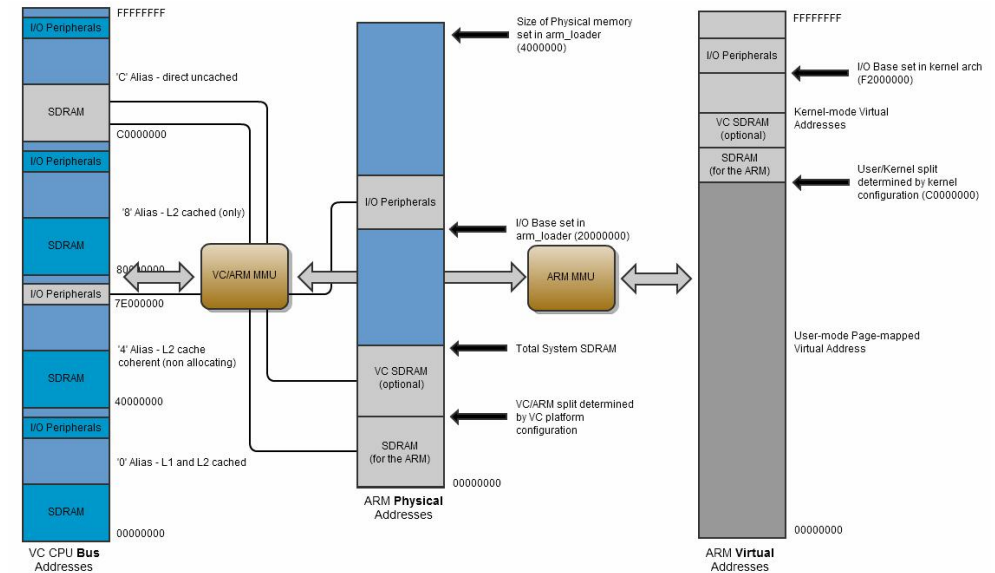
✓ RAM 주소 확인

➤ 0x00000000 ~ 0x20000000 (512MB)

1.2.3 ARM physical addresses

Physical addresses start at 0x00000000 for RAM.

- The ARM section of the RAM starts at 0x00000000.
- The VideoCore section of the RAM is mapped in only if the system is configured to support a memory mapped display (this is the common case).



※ SoC(Broadcom BC2835) Datasheet: <https://www.raspberrypi.org/documentation/hardware/raspberrypi/bcm2835/BCM2835-ARM-Peripherals.pdf>

3. Cold Boot Attack on Practical IoT device

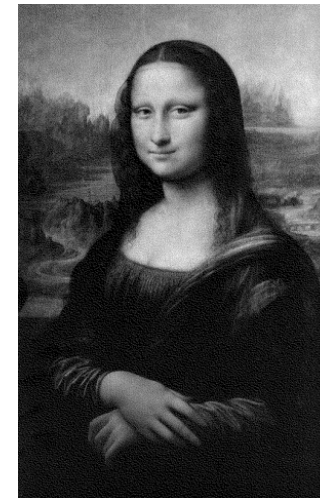
2) Recovery of image stored in RAM

✓ Scenario – Normal situation

1. 모나리자 이미지를 RAM에 업로드
2. Raspberry Pi **OFF** → **ON**
3. RAM을 읽어, 이미지 로드

✓ Scenario – Cold Boot Attack

1. 모나리자 이미지를 RAM에 업로드
2. Air Duster를 활용하여 RAM 온도 낮추기 (약 -35도)
3. Raspberry Pi **OFF** → **ON**
4. RAM을 읽어, 이미지 로드



모나리자 이미지

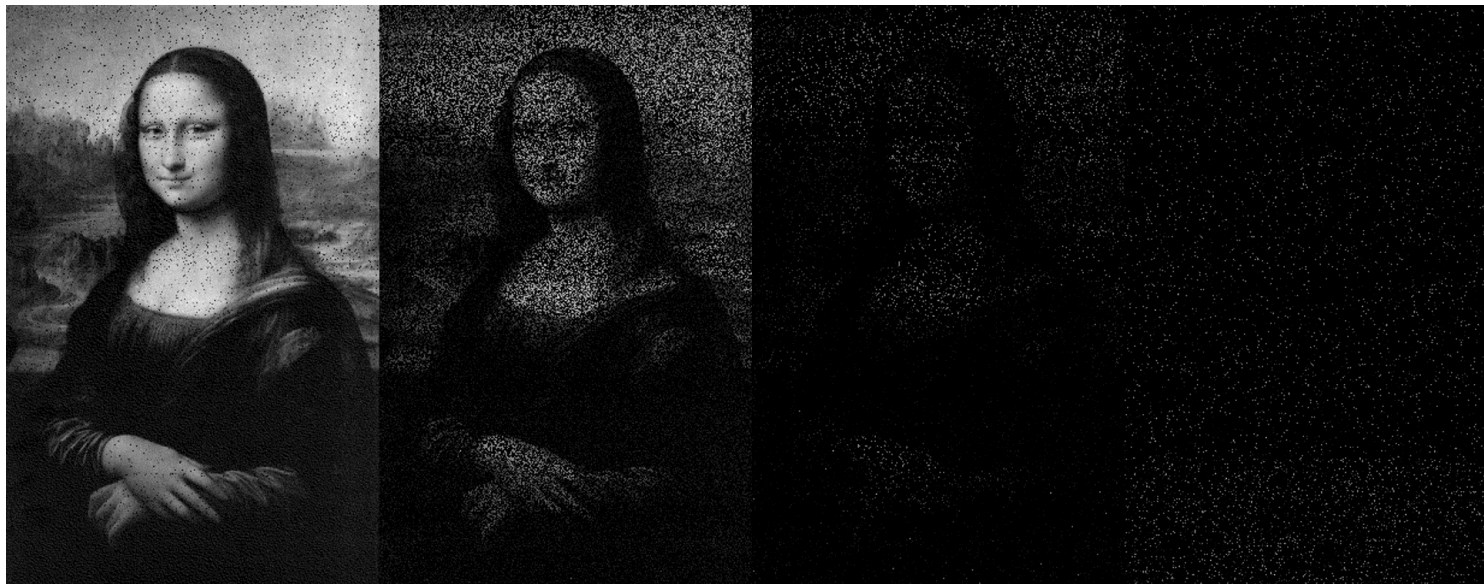


Air Duster

3. Cold Boot Attack on Practical IoT device

2) Recovery of image stored in RAM – Result

✓ Temperature: -35°C



Decay time: 5 seconds 30 seconds 60 seconds 5 minutes

3. Cold Boot Attack on Practical IoT device

2) Recovery of image stored in RAM – Result

- ✓ 이미지 최소 복구율 59.7%
- ✓ Chip 표면 온도: 33.6도
- ✓ -20도 이하에서 99% 복구율 (Decay: 1second)
- ✓ 512MB를 모두 저장하는데 약 5분 소요

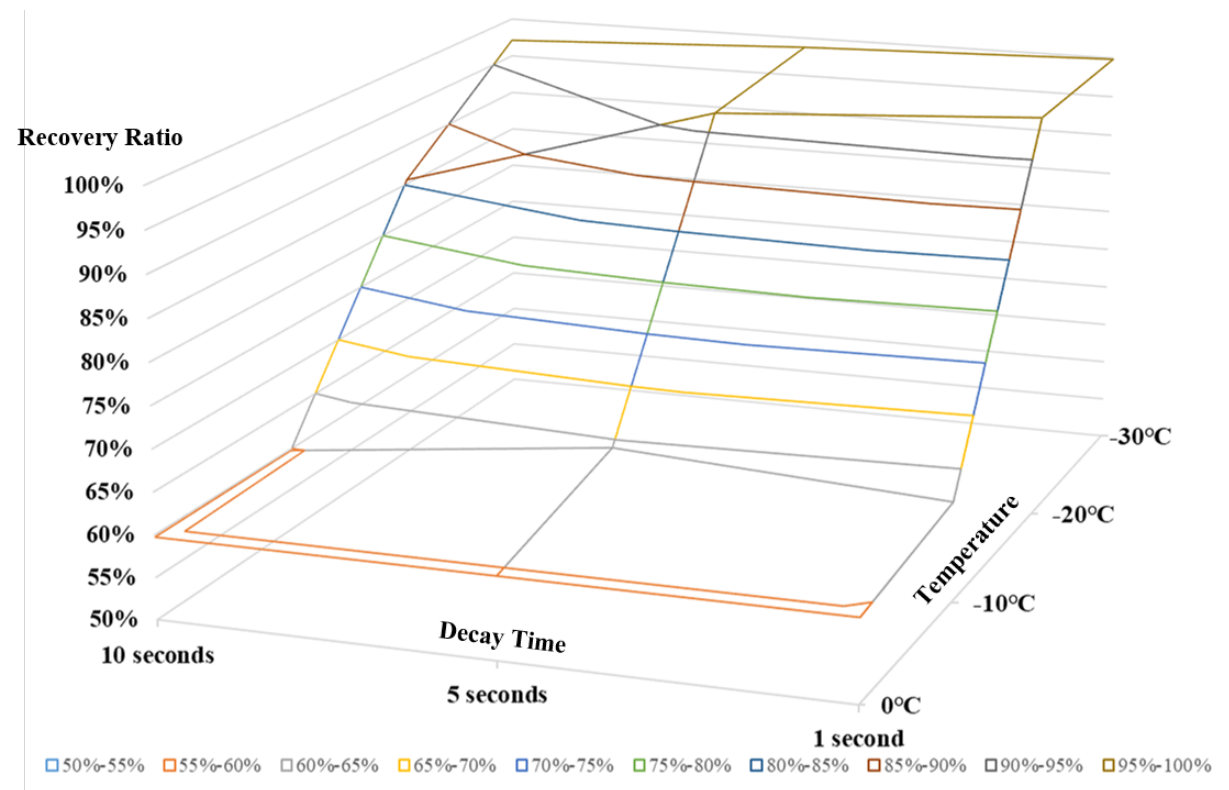


Table of Contents

(3) Cold Boot Attack on Practical IoT Device //

- 1) Identifying the Target & Potential Vulnerabilities
- 2) Recovery of image stored in RAM
- 3) Recovery of the dm-crypt master key

3. Cold Boot Attack on Practical IoT device

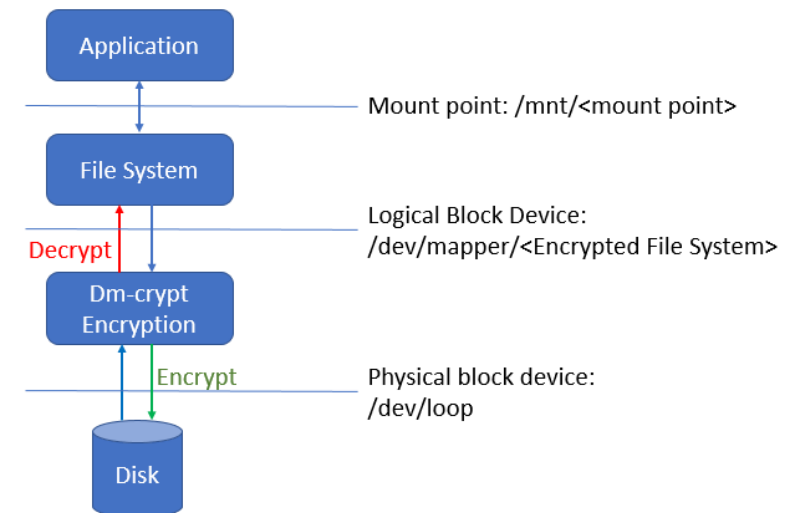
3) Recovery of the dm-crypt master key

✓ Disk encryption system 종류

- BitLocker – Windows OS
- FileVault – Mac OS
- TrueCrypt – Windows, Mac, Linux OS
- dm-crypt – Linux OS
- Loop-AES – Linux OS

✓ Disk encryption system 응용

- Partition encryption/decryption
- USB encryption/decryption



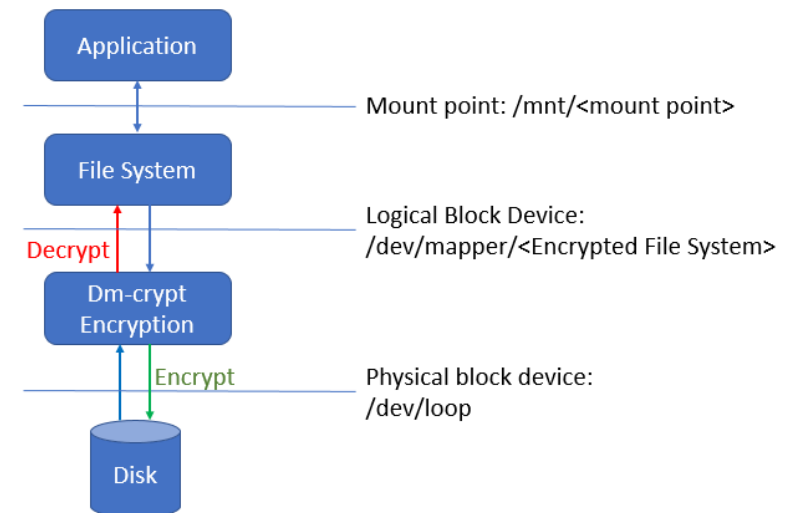
Overview of dm-crypt solution

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ dm-crypt란?

- kernel crypto API를 활용하여 Transparent Encryption을 제공
 - Full disk encryption / File system encryption
- LUKS(Linux Unified Key Setup)* 포맷 지원
- 대칭키, 운영모드, IV 생성 모드 등을 지원



Overview of dm-crypt solution

* LUKS(Linux Unified Key Setup) is a disk encryption specification created by C. Fruhwirh in 2004

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ LUKS Format

start offset	field name	length	data type	description
0	magic	6	byte[]	magic for LUKS partition header, see LUKS_MAGIC
6	version	2	uint16_t	LUKS version
8	cipher-name	32	char[]	cipher name specification
40	cipher-mode	32	char[]	cipher mode specification
72	hash-spec	32	char[]	hash specification
104	payload-offset	4	uint32_t	start offset of the bulk data (in 512 bytes sectors)
108	key-bytes	4	uint32_t	number of key bytes
112	mk-digest	20	byte[]	master key checksum from PBKDF2
132	mk-digest-salt	32	byte[]	salt parameter for master key PBKDF2
164	mk-digest-iter	4	uint32_t	iterations parameter for master key PBKDF2
168	uuid	40	char[]	UUID of the partition
208	key-slot-1	48	key slot	key slot 1
256	key-slot-2	48	key slot	key slot 2
...	...	...	...	...
544	key-slot-8	48	key slot	key slot 8
592	total phdr size			

Figure 1: PHDR layout

offset	field name	length	data type	description
0	active	4	uint32_t	state of keyslot, enabled/disabled
4	iterations	4	uint32_t	iteration parameter for PBKDF2
8	salt	32	byte[]	salt parameter for PBKDF2
40	key-material-offset	4	uint32_t	start sector of key material
44	stripes	4	uint32_t	number of anti-forensic stripes

Figure 2: key slot layout

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ LUKS Format

- Root of trust: passphrase or master key
- Disk layout

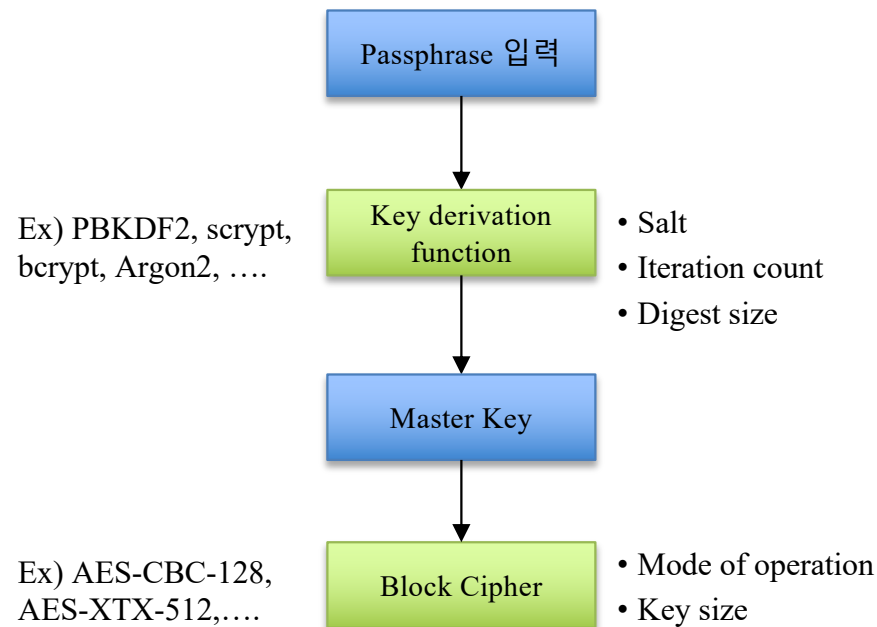


- Phdr: partition header (사용된 암호 종류, 운영 모드, 키길이, 마스터키 체크섬, 키 슬롯 정보)
- KM1~8: key material

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ 암호화 방법



3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ dm-crypt 사용 방법

(1) Connect USB and erase file system

```
mount /dev/sda1 /mnt/tiny_usb
```

```
umount /dev/sda1
```

```
wipefs -a /dev/sda1
```

// sda1의 하드웨어를 linux tiny usb 폴더에 파일 시스템 연결

// mount된 시스템 연결 해제

// sda1의 file system 삭제

(2) Create a LUKS partition

```
cryptsetup luksFormat /dev/sda1
```

(--cipher=aes-ecb --key-size=128과 같은 옵션 가능)

// /dev/mapper/reddrive 파티션에 luks시스템을 연결하고 정의

// (passphrase 입력)

(3) Open the encrypted drive

```
cryptsetup luksOpen /dev/sda1 reddrive
```

// (passphrase 입력)

(4) Create a filesystem

```
mkfs.ext4 /dev/mapper/reddrive -L reddrive
```

(5) Using the encrypted USB

```
mount /dev/mapper/reddrive /mnt/red
```

// reddrive partition을 /mnt/red 폴더에 파일 시스템 연결

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ dm-crypt 사용 방법

(6) Unmount the USB and close LUKS

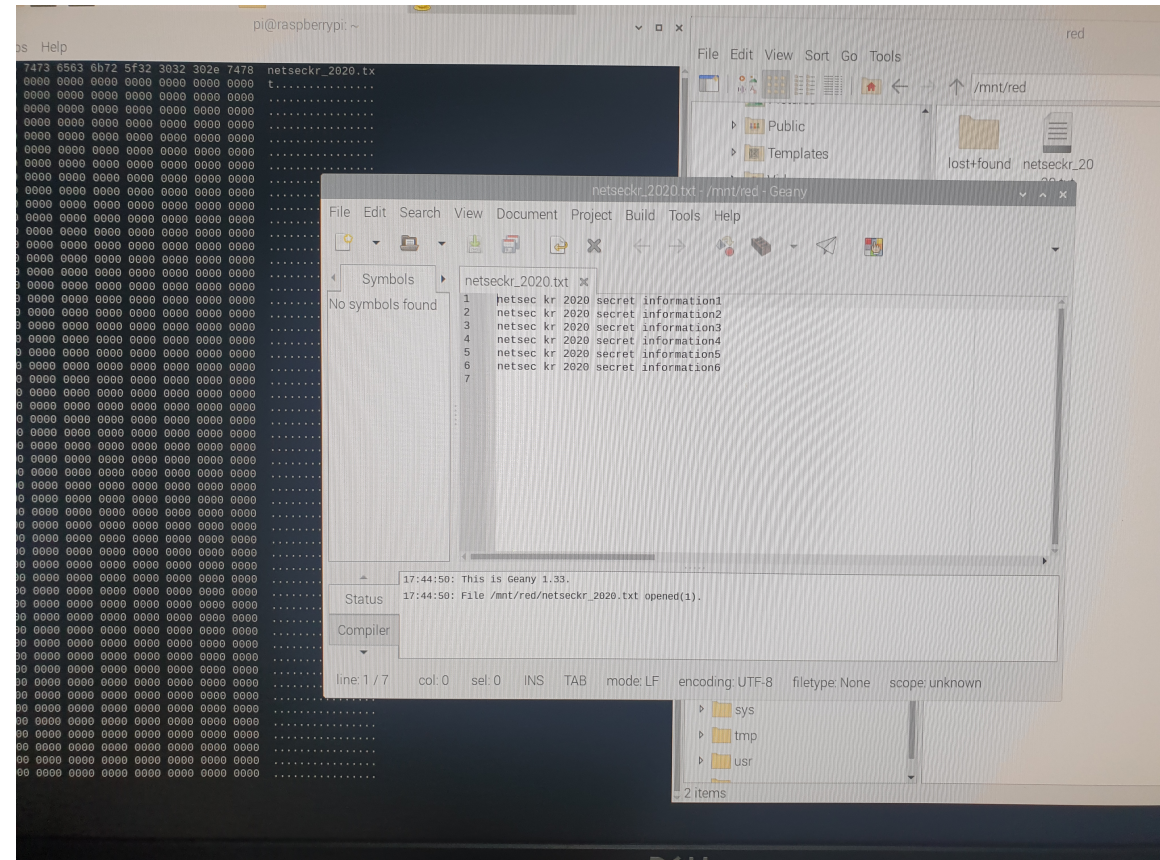
`umount /mnt/red`

`cryptsetup luksClose reddrive`

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

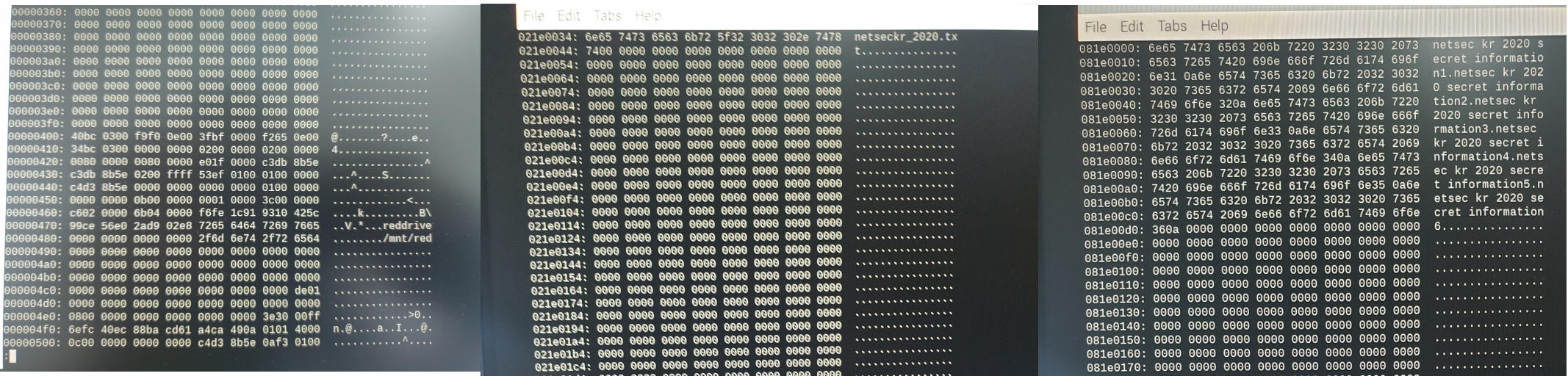
- ✓ dm-crypt로 USB 암호화 진행
 - 모두 default 설정
 - 암호: AES-XTS-512
 - 메모장 (netseckr_2020.txt) 생성하여 저장



3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ /dev/mapper/reddrive 내용 확인



The image displays three sequential screenshots of a terminal window, likely a Windows command prompt, showing the results of a cold boot attack on an IoT device. The terminal output is a hex dump of data recovered from a file named 'netsecr_2020.tx'.

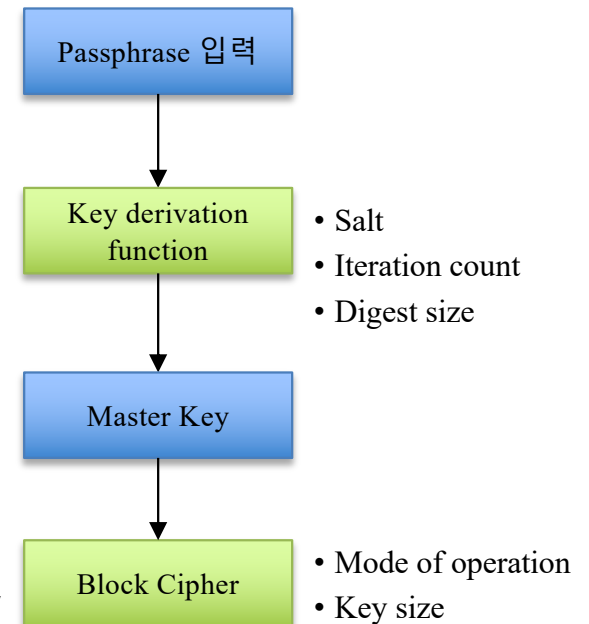
The first screenshot shows the beginning of the hex dump, with addresses ranging from 00000360 to 00000500. The data is displayed in columns of hexadecimal values and their corresponding ASCII representations.

The second screenshot shows the middle of the hex dump, with addresses ranging from 021e0034 to 021e01c4. The data continues to be displayed in columns of hexadecimal values and their corresponding ASCII representations.

The third screenshot shows the end of the hex dump, with addresses ranging from 081e0000 to 081e0170. The data continues to be displayed in columns of hexadecimal values and their corresponding ASCII representations.

- ✓ 탈취된 RAM에서 Master Key 획득 방법

Ex) PBKDF2, scrypt,
bcrypt, Argon2,



3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

- ✓ 탈취된 RAM에서 Master Key 획득 방법

[illegible]

1. 평문, 암호문 쌍을 이용하여, 키 추출
2. 라운드 키를 활용하는 방법

AES-256 마스터 키

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

- ✓ aeskeyfind 로 master key 후보 색출

```

root@ubuntu: /home/yooseung/Desktop/W
File Edit View Search Terminal Help
root@ubuntu:/home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind# ls
20200706_RAM_DUMP_CBA.bin aes.c aes.h aeskeyfind aeskeyfind.c aeskeyfind.o aes.o DATA.BIN LICENSE
root@ubuntu:/home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind# ./aeskeyfind 20200706_RAM_DUMP_CBA.bin
len: 402653184
ccb66669abb81edbb4a70fe8887fc75ce17a2e283c268143eed1870f619f2a19
4b4c20e23c51ee7154c67f9ac2ccd474f2a719c1a83c2a52192bfa12cde2d30d
fa0ffe97d7b696fadc6de0672431ab74fbd495f87762aca507a3b68e059032e5
7e0f01c04bab87656519c10dd26a275ddae4de93f8f70e181660fd5b77cb7ee1
39f8b80dfa81f14ccd2d7c8a1c442fb67c1ff3ca38adc663ffdf8d20bcb463a8
Keyfind progress: 100%
root@ubuntu:/home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind#

```

- ✓ <https://citp.princeton.edu/our-work/memory/>

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

- ✓ 실제 master key 와 비교
(Default: AES-XTS 512)

```
root@ubuntu: /home/yooseung/Desktop/W
File Edit View Search Terminal Help
root@ubuntu: /home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind# ls
20200706_RAM_DUMP_CBA.bin aes.c aes.h aeskeyfind aeskeyfind.c aeskeyfind.o aes.o DATA.BIN LICENSE
root@ubuntu: /home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind# ./aeskeyfind 20200706_RAM_DUMP_CBA.bin
len: 402653184
ccb66669abb81edbb4a70fe8887fc75ce17a2e283c268143eed1870f619f2a19
4b4c20e23c51ee7154c67f9ac2ccd474f2a719c1a83c2a52192bfa12cde2d30d
fa0ffe97d7b696fad6de0672431ab74fbd495f87762aca507a3b68e059032e5
7e0f01c04bab87656519c10dd26a275ddae4de93f8f70e181660fd5b77cb7ee1
39f8b80dfa81f14ccd2d7c8a1c442fb67c1ff3ca38adc663ffdf8d20bcb463a8
Keyfind progress: 100%
root@ubuntu: /home/yooseung/Desktop/WORK/MEM_AES_SEARCH/aeskeyfind#
```

```
root@raspberrypi:/home/pi# cryptsetup luksDump -q --dump-master-key /dev/sda1 | grep -A 3 'MK dump' | sed -e 's/MK du
p://g' -e 's/\s//g' | xxd -r -p > master_key.bin
Enter passphrase for /dev/sda1:
root@raspberrypi:/home/pi# xxd master_key.bin
00000000: 39f8 b80d fa81 f14c cd2d 7c8a 1c44 2fb6 9.....L.-|..D/.
00000010: 7c1f f3ca 38ad c663 ffd6 8d20 bcb4 63a8 |...8...c...c.
00000020: 7e0f 01c0 4bab 8765 6519 c10d d26a 275d ~...K...ee...j']
00000030: dae4 de93 f8f7 0e18 1660 fd5b 77cb 7ee1 .....`.[w.~.
root@raspberrypi:/home/pi#
```

cryptsetup luksDump -q --dump-master-key /dev/sda1 | grep -A 3 'MK dump' | sed -e 's/MK dump://g' -e 's/\s//g' | xxd -r -p > (파일이름).bin

3. Cold Boot Attack on Practical IoT device

3) Recovery of the dm-crypt master key

✓ Passphrase 없이 master key를 사용하여 복호화

➤ cryptsetup --master-key-file (키파일) luksOpen /dev/sda1 reddrive

```

Disk /dev/sda: 3.8 GiB, 4027580416 bytes, 7866368 sectors
Disk model: Flash Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9cd32b8b

Device      Boot Start    End Sectors  Size Id Type
/dev/sda1   *        56 7866367 7866312   3.8G c W95 FAT32 (LBA)

root@raspberrypi:/home/pi# xxd master_key.bin
00000000: 39f8 b80d fa81 f14c cd2d 7c8a 1c44 2fb6  9.....L.-|..D/.
00000010: 7c1f f3ca 38ad c663 ffd5 8d20 bcb4 63a8  |...8..c... ..c.
00000020: 7e0f 01c0 4bab 8765 6519 c10d d26a 275d  ~...K..ee....j']
00000030: dae4 de93 f8f7 0e18 1660 fd5b 77cb 7ee1  .....[w.~.

root@raspberrypi:/home/pi# cryptsetup --master-key-file master_key.bin luksOpen /dev/sda1 reddrive
root@raspberrypi:/home/pi# mount /dev/mapper/reddrive /mnt/red
root@raspberrypi:/home/pi# cd /mnt/red
root@raspberrypi:/mnt/red# ls
lost+found netseckr 2020.txt
root@raspberrypi:/mnt/red# gedit netseckr_2020.txt &

```

Cold Boot Attack으로 찾아낸 키 값
(Hex Value로 기입)

PassPhrase가 아닌 master key 파일로
USB 암호화 해제

```

netsecr_2020.txt
/mnt/red

netsec kr 2020 secret information1
netsec kr 2020 secret information2
netsec kr 2020 secret information3
netsec kr 2020 secret information4
netsec kr 2020 secret information5
netsec kr 2020 secret information6

```

Table of Contents

(1) What is the Cold Boot Attack?

(2) The Outline of Cold Boot Attack

(3) Cold Boot Attack on Practical IoT Device

(4) Conclusion



4. Conclusion

- Cold Boot Attack
 - ✓ 현존하는 RAM에는 Boot Sequence 취약 여부에 따라 공격 가능
 - RAM 내부 하드웨어 대응기법인 Scrambler (DDR3, DDR4)는 어렵지 않게 우회 가능
 - ✓ IoT 장치를 활용한 Security Solution에 대해서 Cold Boot Attack에 대한 대응기법 고려 필요
- Cold Boot Attack에 대한 대응기법
 - ✓ [Disk Encryption 대응기법] RAM을 활용하지 않고,
Register에 Master key를 저장하여 암호화 하는 솔루션이 존재
 - 단, 매번 라운드키 생성 필요
 - ✓ RAM 내부 하드웨어 대응기법은 latency를 고려하여 ChaCha, AES 암호 알고리즘 제안

Q&A

E-mail : yooseung.won@ntu.edu.sg

