NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

FDTC 2021 Fault Diagnosis and Tolerance in Cryptography

PACE

Are Cold Boot Attacks Still Feasible:
A Case Study on Raspberry Pi With Stacked Memory

Yoo-Seung Won and Shivam Bhasin

PACE Lab, Temasek Laboratories,

Nanyang Technological University

14:00~14:15 (CEST), 17.Sep.2021.

Table of Contents

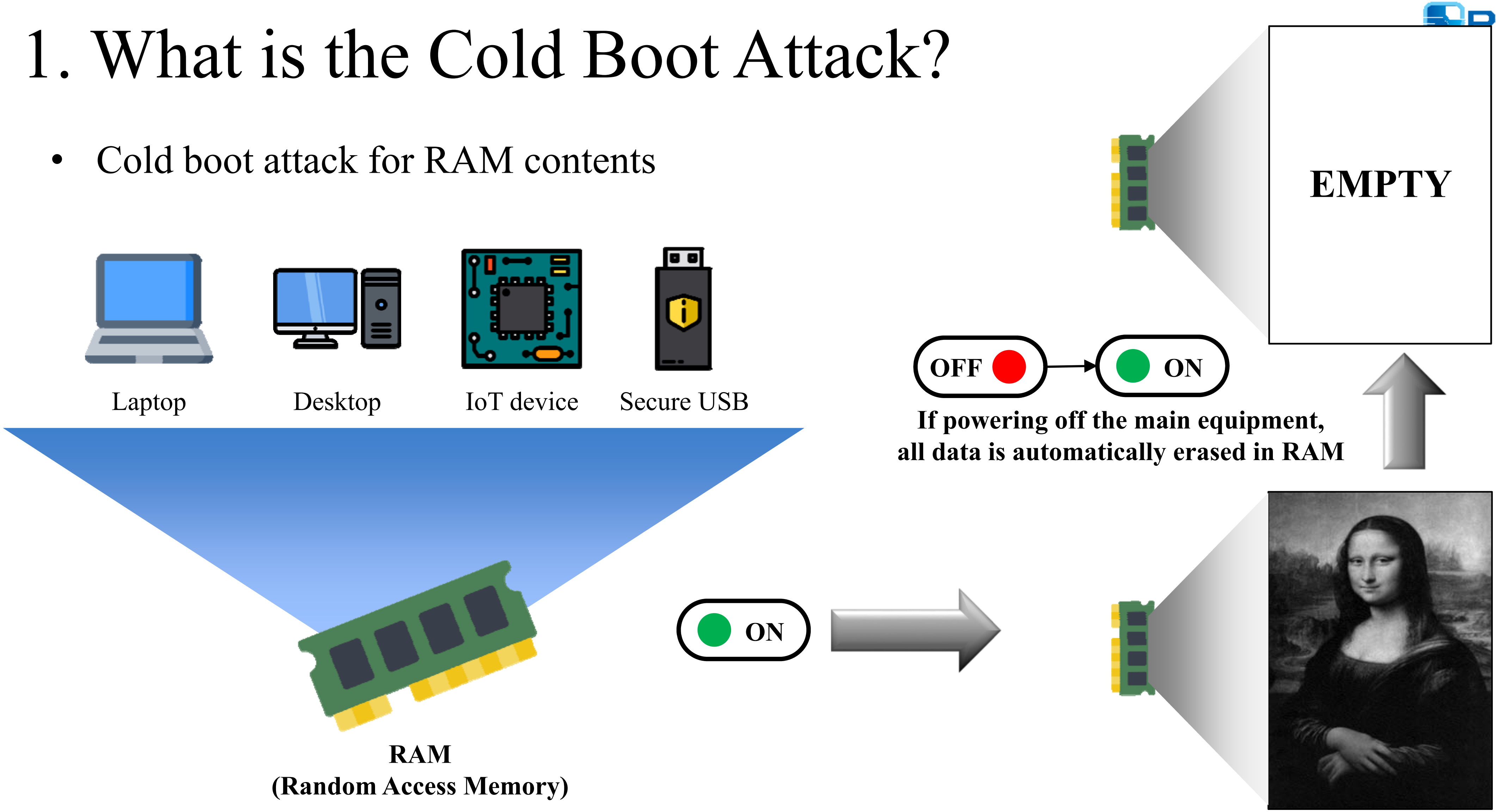
(1) What is the Cold Boot Attack?

(2) Cold Boot Attack on Raspberry Pi

(3) Conclusion & Mitigation

1. What is the Cold Boot Attack?

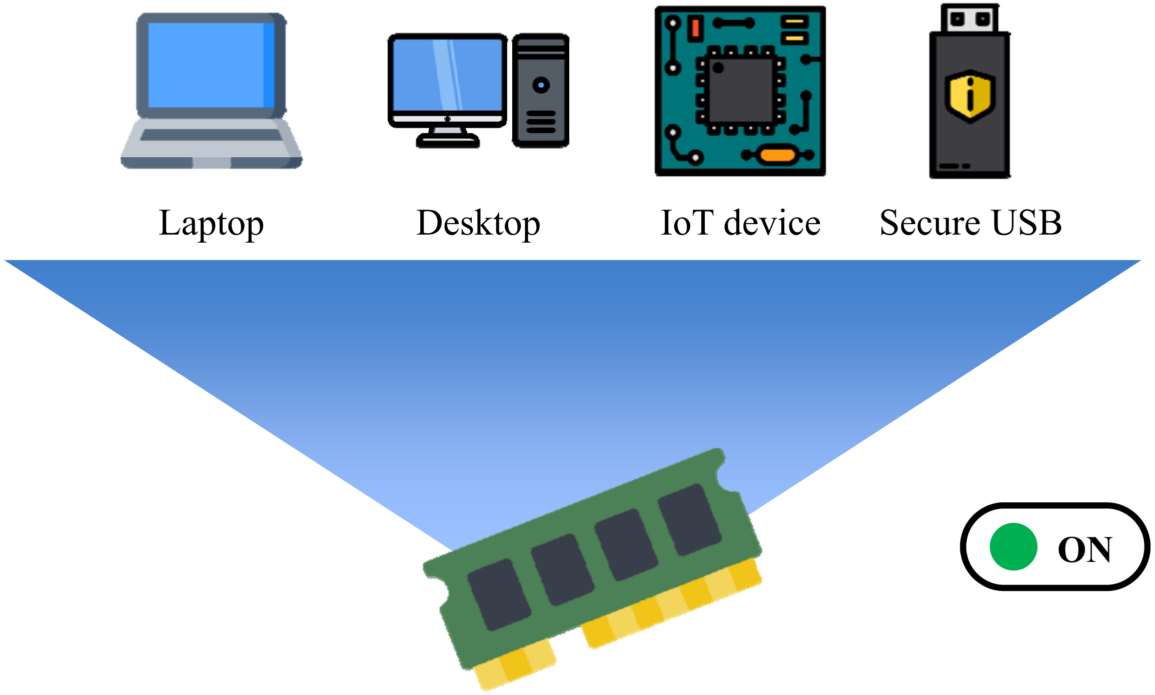
- Cold boot attack for RAM contents



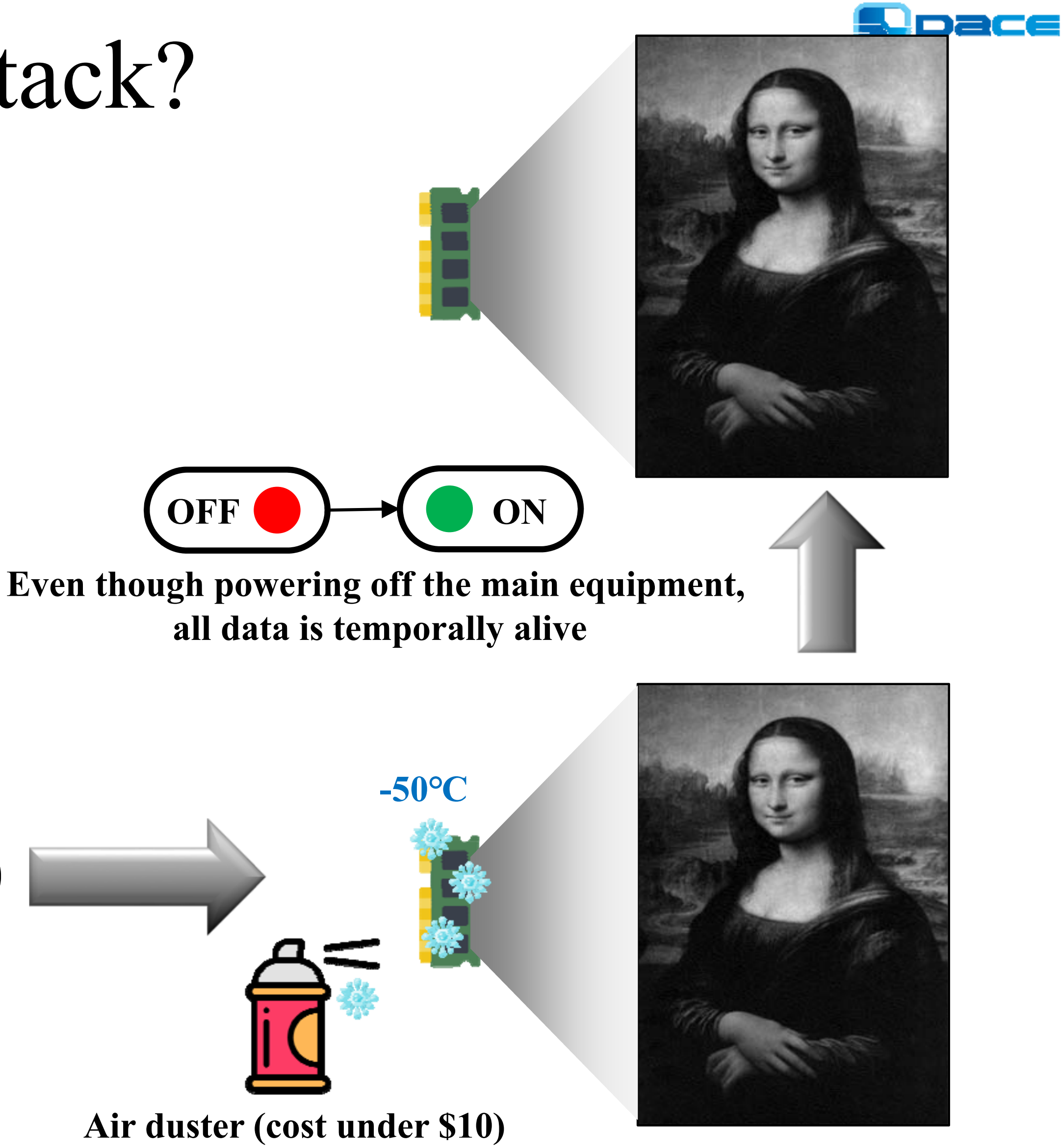
If powering off the main equipment, all data is automatically erased in RAM

1. What is the Cold Boot Attack?

- Cold boot attack for RAM contents



RAM
(Random Access Memory)



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

Air duster (cost under $10)

Table of Contents

(1) What is the Cold Boot Attack?

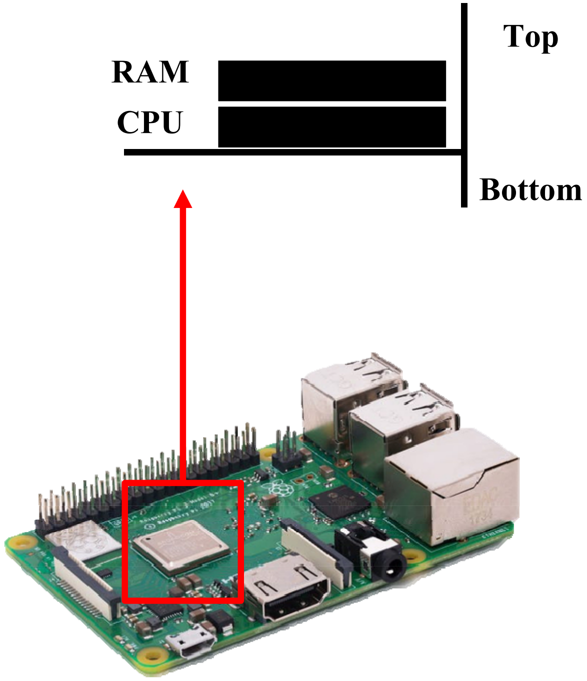
(2) Cold Boot Attack on Raspberry Pi

(3) Conclusion & Mitigation

2. Cold Boot Attack on Raspberry Pi

1) Identifying the Target & Potential Vulnerabilities

✓ Main Target: Raspberry Pi Model B+



Raspberry Pi model B+

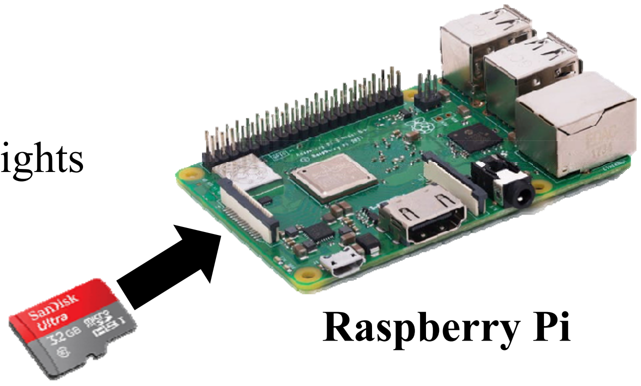
Target	Raspberry Pi model B+
SoC	Broadcom BCM2835 (Technology: 65nm)
CPU	700 MHz ARM1176JZF-S single core
GPU	Broadcom VideoCore IV @ 250 MHz OpenGL ES 2.0 (24 GFLOPS) MPEG-2 and VC-1 (with license), 1080p30 H.264/MPEG-4 AVC high-profile decoder and encoder (L2 cache of 128 KB)
Memory (SDRAM)	LPDDR2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

2. Cold Boot Attack on Raspberry Pi

1) Identifying the Target & Potential Vulnerabilities

✓ Adversary Assumption

- No one can access the RAM while victim's program (burned on a SD card) is in operation except for an authorized person
- An adversary can physically access the Raspberry Pi and can replace the victim's SD card by adversary SD card and vice versa
- Victim's SD card reveals no sensitive information owing to lack of access rights

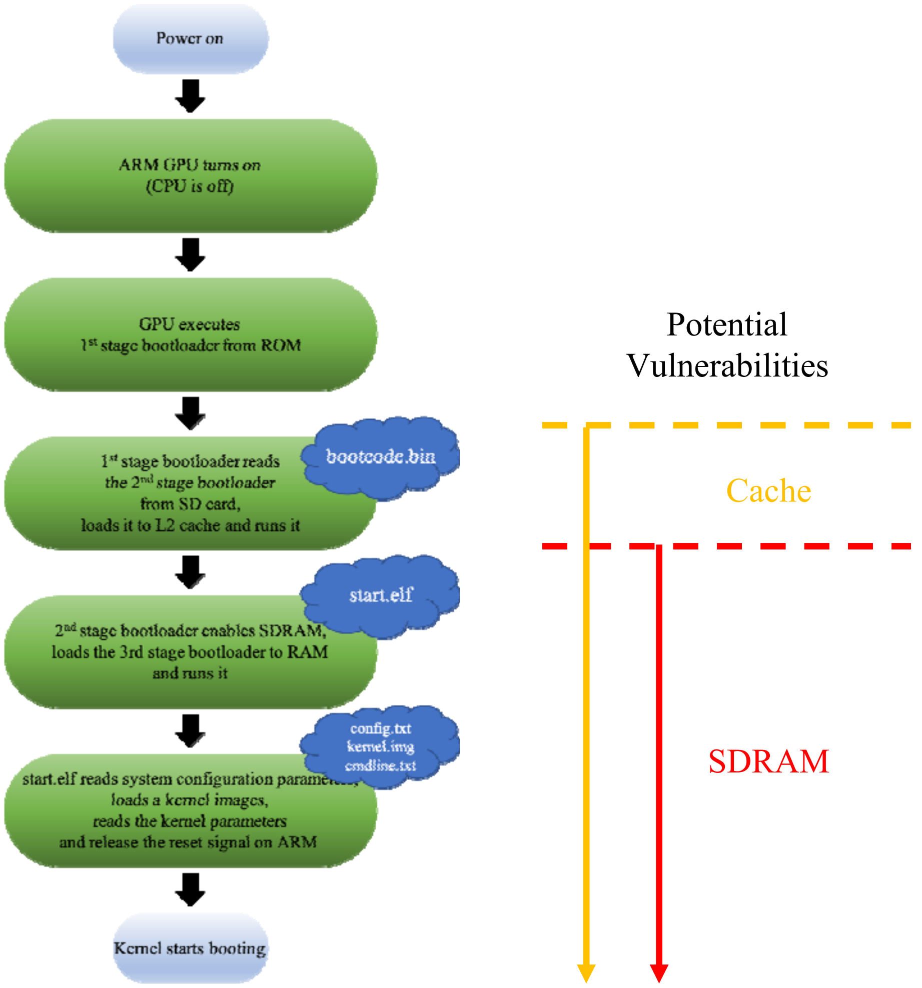


2. Cold Boot Attack on Raspberry Pi

1) Identifying the Target & Potential Vulnerabilities

- ✓ L2 cache memory
  - Attack point: Minimum 1st stage bootloader

- ✓ RAM
  - Attack point: Minimum 2nd stage bootloader



Power on

ARM GPU turns on
(CPU is off)

GPU executes
1st stage bootloader from ROM

1st stage bootloader reads
the 2nd stage bootloader
from SD card,
loads it to L2 cache and runs it

bootcode.bin

2nd stage bootloader enables SDRAM,
loads the 3rd stage bootloader to RAM
and runs it

start.elf

start.elf reads system configuration parameters,
loads a kernel images,
reads the kernel parameters
and release the reset signal on ARM

config.txt
kernel.img
cmdline.txt

Kernel starts booting

Potential
Vulnerabilities

Cache

SDRAM

2. Cold Boot Attack on Raspberry Pi

2) Recovery of image stored in RAM

1) Upload the Mona Lisa figure to RAM

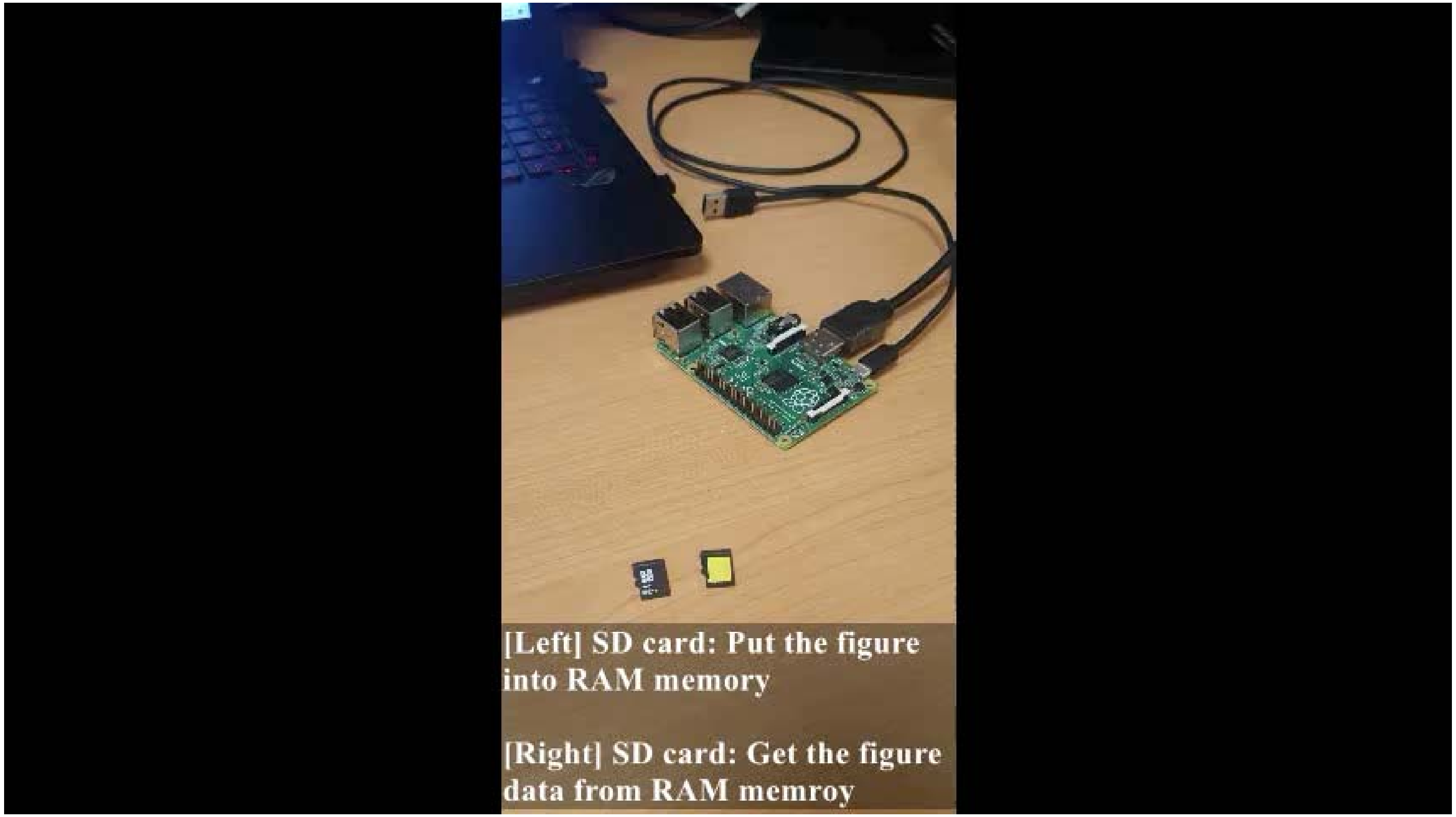
2) Freezing the RAM

3) Turn off and turn on the Raspberry pi

4) Read the RAM to show the figure

2. Cold Boot Attack on Raspberry Pi

2) Recovery of image stored in RAM



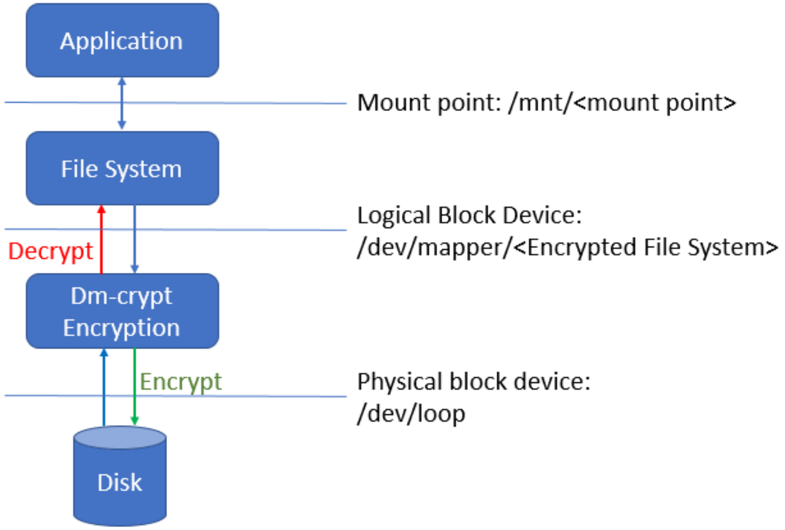
[Left] SD card: Put the figure into RAM memory

[Right] SD card: Get the figure data from RAM memroy

2. Cold Boot Attack on Raspberry Pi

3) Recovery of the dm-crypt master key

- ✓ Type of Disk encryption system
  - ➢ BitLocker – Windows OS
  - ➢ FileVault – Mac OS
  - ➢ TrueCrypt – Windows, Mac, Linux OS
  - ➢ dm-crypt – Linux OS
  - ➢ Loop-AES – Linux OS
- ✓ Application of Disk encryption system
  - ➢ Partition encryption/decryption
  - ➢ USB encryption/decryption

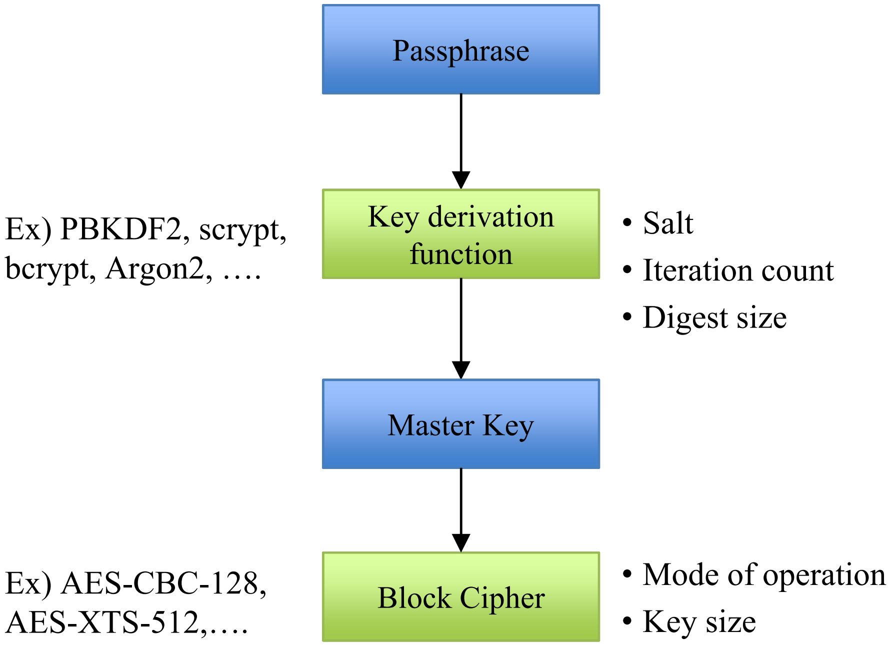


Overview of dm-crypt solution

2. Cold Boot Attack on Raspberry Pi

3) Recovery of the dm-crypt master key

✓ Encryption Method



Passphrase

Ex) PBKDF2, scrypt, bcrypt, Argon2, ….

Key derivation function

- Salt
- Iteration count
- Digest size

Master Key

Ex) AES-CBC-128, AES-XTS-512,….

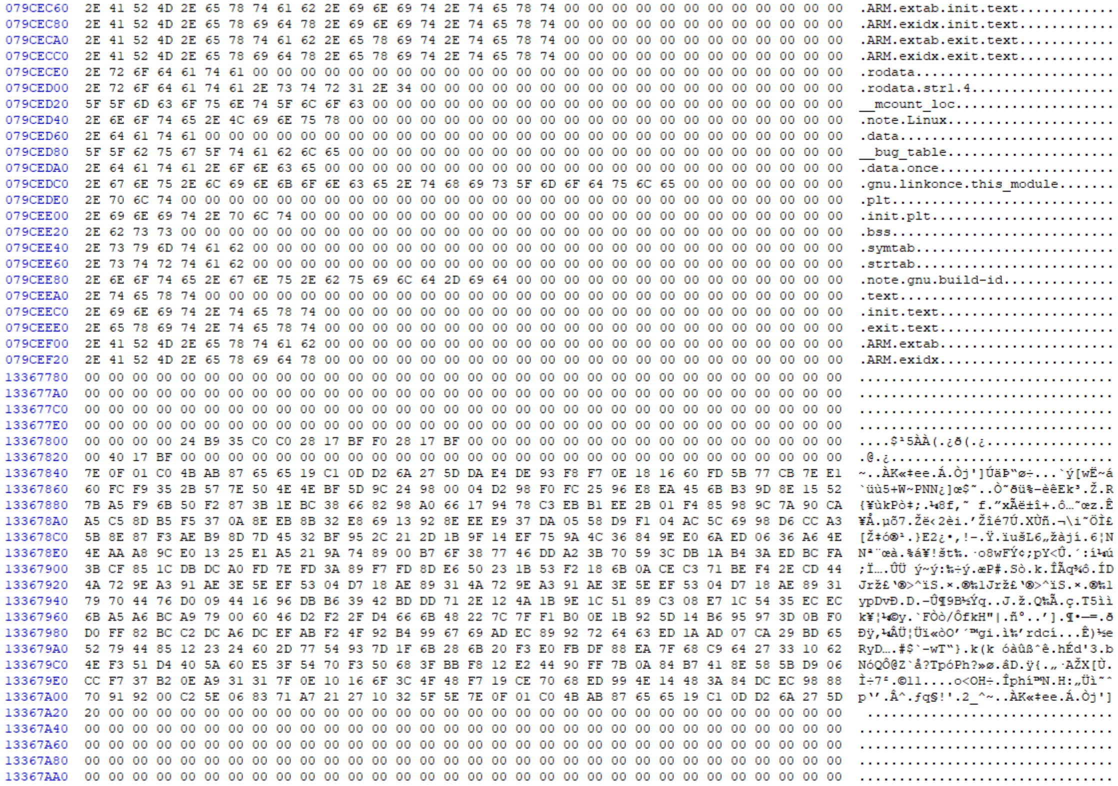
Block Cipher

- Mode of operation
- Key size

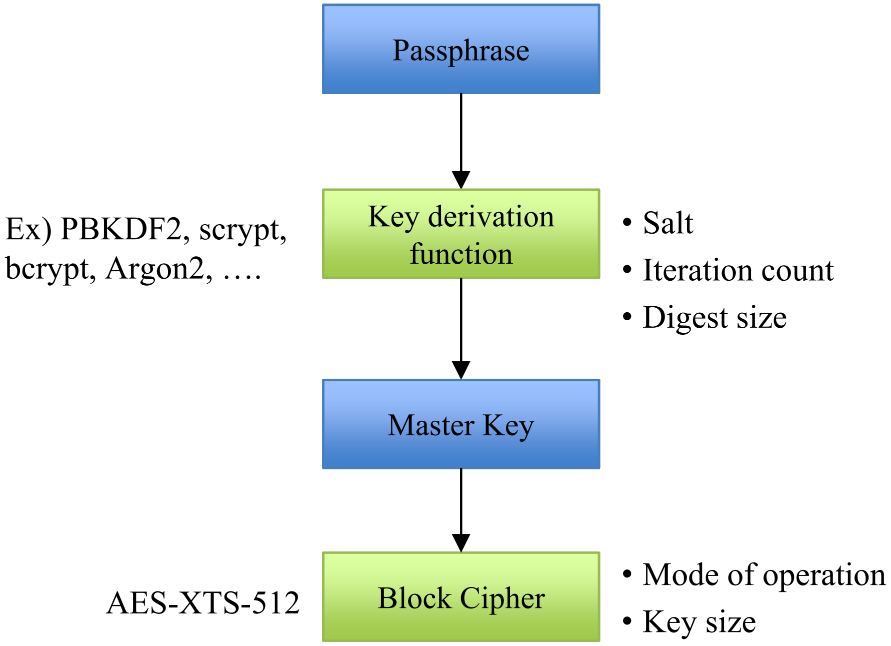
2. Cold Boot Attack on Raspberry Pi

3) Recovery of the dm-crypt master key

✓ Where is the master key in the RAM?



```
079CEC60  2E 41 52 4D 2E 65 78 74 61 62 2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab.init.text............
079CEC80  2E 41 52 4D 2E 65 78 69 64 78 2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx.init.text............
079CECA0  2E 41 52 4D 2E 65 78 74 61 62 2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab.exit.text............
079CECC0  2E 41 52 4D 2E 65 78 69 64 78 2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx.exit.text............
079CECE0  2E 72 6F 64 61 74 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .rodata.........................
079CED00  2E 72 6F 64 61 74 61 2E 73 74 72 31 2E 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .rodata.str1.4..................
079CED20  5F 5F 6D 63 6F 75 6E 74 5F 6C 6F 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  __mcount_loc....................
079CED40  2E 6E 6F 74 65 2E 4C 69 6E 75 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .note.Linux.....................
079CED60  2E 64 61 74 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .data...........................
079CED80  5F 5F 62 75 67 5F 74 61 62 6C 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  __bug_table.....................
079CEDA0  2E 64 61 74 61 2E 6F 6E 63 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .data.once......................
079CEDC0  2E 67 6E 75 2E 6C 69 6E 6B 6F 6E 63 65 2E 74 68 69 73 5F 6D 6F 64 75 6C 65 00 00 00 00 00 00 00  .gnu.linkonce.this_module.......
079CEDE0  2E 70 6C 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .plt............................
079CEE00  2E 69 6E 69 74 2E 70 6C 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .init.plt.......................
079CEE20  2E 62 73 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .bss............................
079CEE40  2E 73 79 6D 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .symtab.........................
079CEE60  2E 73 74 72 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .strtab.........................
079CEE80  2E 6E 6F 74 65 2E 67 6E 75 2E 62 75 69 6C 64 2D 69 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .note.gnu.build-id..............
079CEEA0  2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .text...........................
079CEEC0  2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .init.text......................
079CEEE0  2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .exit.text......................
079CEF00  2E 41 52 4D 2E 65 78 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab......................
079CEF20  2E 41 52 4D 2E 65 78 69 64 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx......................
13367780  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367800  00 00 00 00 24 B9 35 C0 C0 28 17 BF F0 28 17 BF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....$¹5ÀÀ(.¿ð(.¿................
13367820  00 40 17 BF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .@.¿............................
13367840  7E 0F 01 C0 4B AB 87 65 65 19 C1 0D D2 6A 27 5D DA E4 DE 93 F8 F7 0E 18 16 60 FD 5B 77 CB 7E E1  ~..ÀK«‡ee.Á.Òj']ÚäÞ“ø÷...`ý[wË~á
13367860  60 FC F9 35 2B 57 7E 50 4E 4E BF 5D 9C 24 98 00 04 D2 98 F0 FC 25 96 E8 EA 45 6B B3 9D 8E 15 52  `üù5+W~PNN¿]œ$˜..Ò˜ðü%–èêEk³.Ž.R
13367880  7B A5 F9 6B 50 F2 87 3B 1E BC 38 66 82 98 A0 66 17 94 78 C3 EB B1 EE 2B 01 F4 85 98 9C 7A 90 CA  {¥ùkPò‡;.¼8f‚˜ f.”xÃë±î+.ô…˜œz.Ê
133678A0  A5 C5 8D B5 F5 37 0A 8E EB 8B 32 E8 69 13 92 8E EE E9 37 DA 05 58 D9 F1 04 AC 5C 69 98 D6 CC A3  ¥Å.µõ7.Žë‹2èi.’Žîé7Ú.XÙñ.¬\i˜ÖÌ£
133678C0  5B 8E 87 F3 AE B9 8D 7D 45 32 BF 95 2C 21 2D 1B 9F 14 EF 75 9A 4C 36 84 9E E0 6A ED 06 36 A6 4E  [Ž‡ó®¹.}E2¿•,!-.Ÿ.ïušL6„žàjí.6¦N
133678E0  4E AA A8 9C E0 13 25 E1 A5 21 9A 74 89 00 B7 6F 38 77 46 DD A2 3B 70 59 3C DB 1A B4 3A ED BC FA  Nª¨œà.%á¥!št‰.·o8wFÝ¢;pY<Û.´:í¼ú
13367900  3B CF 85 1C DB DC A0 FD 7E FD 3A 89 F7 FD 8D E6 50 23 1B 53 F2 18 6B 0A CE C3 71 BE F4 2E CD 44  ;Ï….ÛÜ ý~ý:‰÷ý.æP#.Sò.k.ÎÃq¾ô.ÍD
13367920  4A 72 9E A3 91 AE 3E 5E EF 53 04 D7 18 AE 89 31 4A 72 9E A3 91 AE 3E 5E EF 53 04 D7 18 AE 89 31  Jrž£‘®>^ïS.×.®‰1Jrž£‘®>^ïS.×.®‰1
13367940  79 70 44 76 D0 09 44 16 96 DB B6 39 42 BD DD 71 2E 12 4A 1B 9E 1C 51 89 C3 08 E7 1C 54 35 EC EC  ypDvÐ.D.–Û¶9B½Ýq..J.ž.Q‰Ã.ç.T5ìì
13367960  6B A5 A6 BC A9 79 00 60 46 D2 F2 2F D4 66 6B 48 22 7C 7F F1 B0 0E 1B 92 5D 14 B6 95 97 3D 0B F0  k¥¦¼©y.`FÒò/ÔfkH"|.ñ°..’].¶•—=.ð
13367980  D0 FF 82 BC C2 DC A6 DC EF AB F2 4F 92 B4 99 67 69 AD EC 89 92 72 64 63 ED 1A AD 07 CA 29 BD 65  Ðÿ‚¼ÂÜ¦Üï«òO’´™gi.ì‰’rdcí...Ê)½e
133679A0  52 79 44 85 12 23 24 60 2D 77 54 93 7D 1F 6B 28 6B 20 F3 E0 FB DF 88 EA 7F 68 C9 64 27 33 10 62  RyD….#$`-wT“}.k(k óàûßˆê.hÉd'3.b
133679C0  4E F3 51 D4 40 5A 60 E5 3F 54 70 F3 50 68 3F BB F8 12 E2 44 90 FF 7B 0A 84 B7 41 8E 58 5B D9 06  NóQÔ@Z`å?TpóPh?»ø.âD.ÿ{.„·AŽX[Ù.
133679E0  CC F7 37 B2 0E A9 31 31 7F 0E 10 16 6F 3C 4F 48 F7 19 CE 70 68 ED 99 4E 14 48 3A 84 DC EC 98 88  Ì÷7².©11....o<OH÷.Îphí™N.H:„Üì˜ˆ
13367A00  70 91 92 00 C2 5E 06 83 71 A7 21 27 10 32 5F 5E 7E 0F 01 C0 4B AB 87 65 65 19 C1 0D D2 6A 27 5D  p‘’.Â^.ƒq§!'.2_^~..ÀK«‡ee.Á.Òj']
13367A20  20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ...............................
13367A40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367A60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367A80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367AA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
```



Ex) PBKDF2, scrypt, bcrypt, Argon2, ….

- Salt
- Iteration count
- Digest size

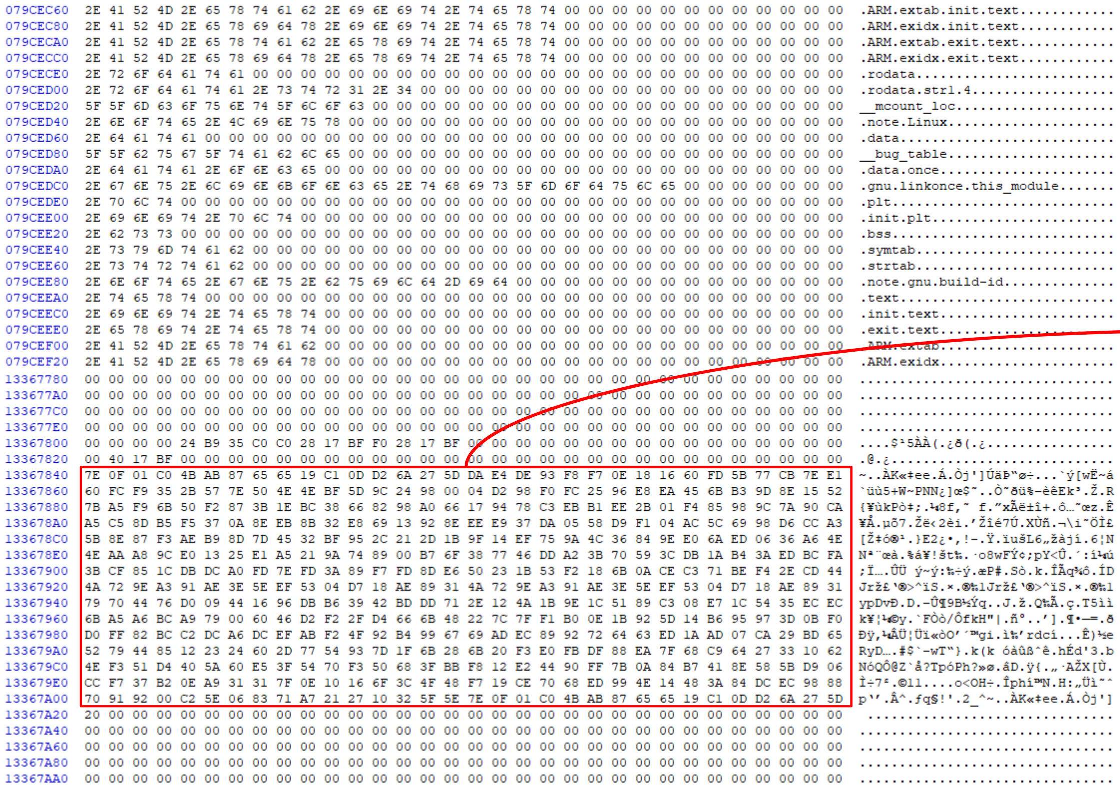
AES-XTS-512

- Mode of operation
- Key size

2. Cold Boot Attack on Raspberry Pi

3) Recovery of the dm-crypt master key

- ✓ Where is the master key in the RAM?



```
079CEC60  2E 41 52 4D 2E 65 78 74 61 62 2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab.init.text............
079CEC80  2E 41 52 4D 2E 65 78 69 64 78 2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx.init.text............
079CECA0  2E 41 52 4D 2E 65 78 74 61 62 2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab.exit.text............
079CECC0  2E 41 52 4D 2E 65 78 69 64 78 2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx.exit.text............
079CECE0  2E 72 6F 64 61 74 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .rodata.........................
079CED00  2E 72 6F 64 61 74 61 2E 73 74 72 31 2E 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .rodata.str1.4..................
079CED20  5F 5F 6D 63 6F 75 6E 74 5F 6C 6F 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  __mcount_loc....................
079CED40  2E 6E 6F 74 65 2E 4C 69 6E 75 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .note.Linux.....................
079CED60  2E 64 61 74 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .data...........................
079CED80  5F 5F 62 75 67 5F 74 61 62 6C 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  __bug_table.....................
079CEDA0  2E 64 61 74 61 2E 6F 6E 63 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .data.once......................
079CEDC0  2E 67 6E 75 2E 6C 69 6E 6B 6F 6E 63 65 2E 74 68 69 73 5F 6D 6F 64 75 6C 65 00 00 00 00 00 00 00  .gnu.linkonce.this_module.......
079CEDE0  2E 70 6C 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .plt............................
079CEE00  2E 69 6E 69 74 2E 70 6C 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .init.plt.......................
079CEE20  2E 62 73 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .bss............................
079CEE40  2E 73 79 6D 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .symtab.........................
079CEE60  2E 73 74 72 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .strtab.........................
079CEE80  2E 6E 6F 74 65 2E 67 6E 75 2E 62 75 69 6C 64 2D 69 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .note.gnu.build-id..............
079CEEA0  2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .text...........................
079CEEC0  2E 69 6E 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .init.text......................
079CEEE0  2E 65 78 69 74 2E 74 65 78 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .exit.text......................
079CEF00  2E 41 52 4D 2E 65 78 74 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.extab......................
079CEF20  2E 41 52 4D 2E 65 78 69 64 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .ARM.exidx......................
13367780  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
133677E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367800  00 00 00 00 24 B9 35 C0 C0 28 17 BF F0 28 17 BF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....$¹5ÀÀ(.¿ð(.¿................
13367820  00 40 17 BF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .@.¿............................
13367840  7E 0F 01 C0 4B AB 87 65 65 19 C1 0D D2 6A 27 5D DA E4 DE 93 F8 F7 0E 18 16 60 FD 5B 77 CB 7E E1  ~..ÀK«‡ee.Á.Òj']ÚäÞ“ø÷...`ý[wË~á
13367860  60 FC F9 35 2B 57 7E 50 4E 4E BF 5D 9C 24 98 00 04 D2 98 F0 FC 25 96 E8 EA 45 6B B3 9D 8E 15 52  `üù5+W~PNN¿]œ$˜..Ò˜ðü%–èêEk³.Ž.R
13367880  7B A5 F9 6B 50 F2 87 3B 1E BC 38 66 82 98 A0 66 17 94 78 C3 EB B1 EE 2B 01 F4 85 98 9C 7A 90 CA  {¥ùkPò‡;.¼8f‚˜ f.”xÃë±î+.ô…˜œz.Ê
133678A0  A5 C5 8D B5 F5 37 0A 8E EB 8B 32 E8 69 13 92 8E EE E9 37 DA 05 58 D9 F1 04 AC 5C 69 98 D6 CC A3  ¥Å.µõ7.Žë‹2èi.’ŽîéÚ7.XÙñ.¬\i˜ÖÌ£
133678C0  5B 8E 87 F3 AE B9 8D 7D 45 32 BF 95 2C 21 2D 1B 9F 14 EF 75 9A 4C 36 84 9E E0 6A ED 06 36 A6 4E  [Ž‡ó®¹.}E2¿•,!-.Ÿ.ïušL6„žàjí.6¦N
133678E0  4E AA A8 9C E0 13 25 E1 A5 21 9A 74 89 00 B7 6F 38 77 46 DD A2 3B 70 59 3C DB 1A B4 3A ED BC FA  Nª¨œà.%á¥!št‰.·o8wFÝ¢;pY<Û.´:í¼ú
13367900  3B CF 85 1C DB DC A0 FD 7E FD 3A 89 F7 FD 8D E6 50 23 1B 53 F2 18 6B 0A CE C3 71 BE F4 2E CD 44  ;Ï….ÛÜ ý~ý:‰÷ý.æP#.Sò.k.ÎÃq¾ô.ÍD
13367920  4A 72 9E A3 91 AE 3E 5E EF 53 04 D7 18 AE 89 31 4A 72 9E A3 91 AE 3E 5E EF 53 04 D7 18 AE 89 31  Jrž£‘®>^ïS.×.®‰1Jrž£‘®>^ïS.×.®‰1
13367940  79 70 44 76 D0 09 44 16 96 DB B6 39 42 BD DD 71 2E 12 4A 1B 9E 1C 51 89 C3 08 E7 1C 54 35 EC EC  ypDvÐ.D.–Û¶9B½Ýq..J.ž.Q‰Ã.ç.T5ìì
13367960  6B A5 A6 BC A9 79 00 60 46 D2 F2 2F D4 66 6B 48 22 7C 7F F1 B0 0E 1B 92 5D 14 B6 95 97 3D 0B F0  k¥¦¼©y.`FÒò/ÔfkH"|.ñ°..’].¶•—=.ð
13367980  D0 FF 82 BC C2 DC A6 DC EF AB F2 4F 92 B4 99 67 69 AD EC 89 92 72 64 63 ED 1A AD 07 CA 29 BD 65  Ðÿ‚¼ÂÜ¦Üï«òO’´™gi.ì‰’rdcí...Ê)½e
133679A0  52 79 44 85 12 23 24 60 2D 77 54 93 7D 1F 6B 28 6B 20 F3 E0 FB DF 88 EA 7F 68 C9 64 27 33 10 62  RyD….#$`-wT“}.k(k óàûßˆê.hÉd'3.b
133679C0  4E F3 51 D4 40 5A 60 E5 3F 54 70 F3 50 68 3F BB F8 12 E2 44 90 FF 7B 0A 84 B7 41 8E 58 5B D9 06  NóQÔ@Z`å?TpóPh?»ø.âD.ÿ{.„·AŽX[Ù.
133679E0  CC F7 37 B2 0E A9 31 31 7F 0E 10 16 6F 3C 4F 48 F7 19 CE 70 68 ED 99 4E 14 48 3A 84 DC EC 98 88  Ì÷7².©11....o<OH÷.Îphí™N.H:„Üì˜ˆ
13367A00  70 91 92 00 C2 5E 06 83 71 A7 21 27 10 32 5F 5E 7E 0F 01 C0 4B AB 87 65 65 19 C1 0D D2 6A 27 5D  p‘’.Â^.ƒq§!'.2_^~..ÀK«‡ee.Á.Òj']
13367A20  20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ...............................
13367A40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367A60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367A80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
13367AA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................
```

AES-256 Round Keys

- ✓ We use *aeskeyfind* program to find round keys.

  https://citp.princeton.edu/our-work/memory/

Table of Contents

(1) What is the Cold Boot Attack?

(2) Cold Boot Attack on Raspberry Pi

(3) Conclusion & Mitigation

3. Conclusion & Mitigation

- The total cost of the reported attack is under $10

- It makes a serious threat against billions of IoT devices deployed into the wild.

- Secure boot process can be put in place to overcome such vulnerabilities, ensuring memory initialization and prevent unauthorized modification of boot sequence/firmware

- Even though the device is vulnerable to cold boot attacks, there are some solutions to protect the disk, utilizing the safe encryption solutions such as TRESOR* and ARMORED**

[*] T. Muller, F. C. Freiling, and A. Dewald, “Tresor runs encryption ¨ securely outside ram.” in USENIX Security Symposium, vol. 17, 2011.

[**] J. Gotzfried and T. M ¨ uller, “Armored: Cpu-bound encryption for ¨ android-driven arm devices,” in 2013 International Conference on Availability, Reliability and Security. IEEE, 2013, pp. 161–168

Q&A

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

The world's top young university
TIMES HIGHER EDUCATION YOUNG UNIVERSITY RANKINGS 2021
NTU SINGAPORE