A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping

Seunghun Han
National Security Research Institute

Outline

- Background
- Assumptions and Threat Model
- Vulnerabilities and Exploits
  - CVE-2018-6622
  - CVE-2017-16837
- Evaluation
- Countermeasures
- Conclusion

Trusted Computing Group (TCG)

- Defines global industry specifications and standards
- Is supportive of a hardware root of trust
  - Trusted Platform Module (TPM) is the core technology
  - TCG technology has been applied to Unified Extensible Firmware Interface (UEFI)

Trusted Platform Module (TPM) (1)

- Is a tamper-resistant device
- Has own processor, RAM, ROM, and non-volatile RAM
  - It has own state separated from the system
- Provides cryptographic and accumulating measurements functions
  - Measurement values are accumulated to Platform Configuration Registers (PCR #0~#23)

Trusted Platform Module (TPM) (2)

- Is used to determine the trustworthiness of a system by investigating the values stored in PCRs
  - A local verification or remote attestation can be used
- Is used to limit access to secret data based on specific PCR values
  - “Seal” operation encrypts secret data with the PCRs of the TPM
  - “Unseal” operation can decrypt the sealed data only if the PCR values match the specific values

Root of Trust for Measurement (RTM)

- Sends integrity-relevant information (measurements) to the TPM
  - TPM accumulates the measurements to a PCR with the previously stored value in the PCR

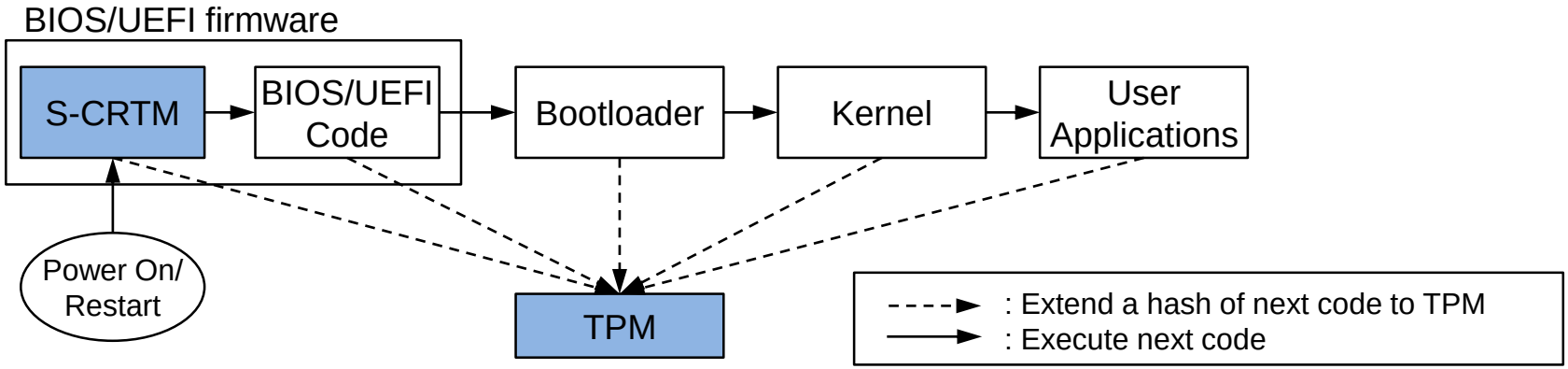
Extend: $PCR_{new} = Hash(PCR_{old} \,||\, Measurement_{new})$

- Is the CPU controlled by Core RTM (CRTM)
  - The CRTM is the first set of instructions when a new chain of trust is established

Static and Dynamic RTM (SRTM and DRTM)

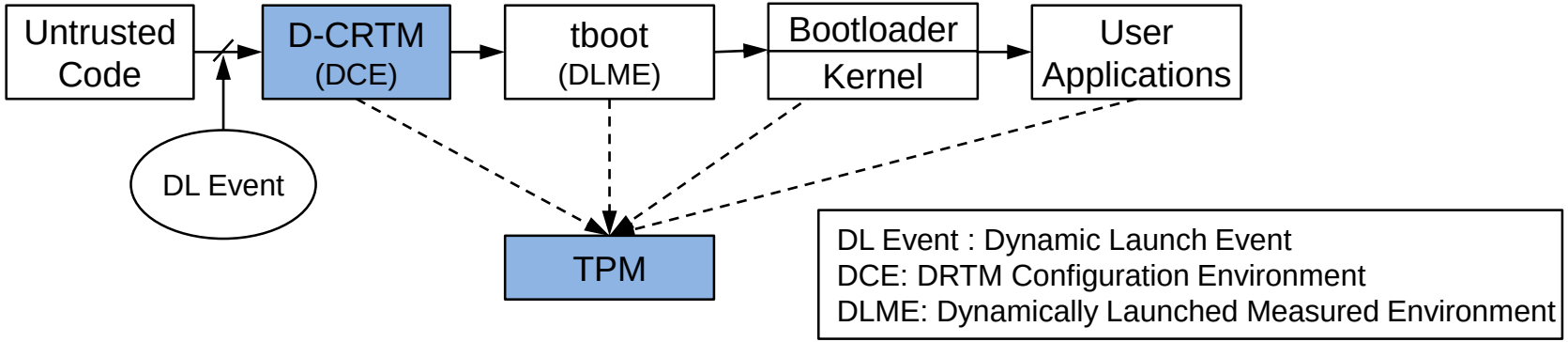
- SRTM is started by static CRTM (S-CRTM) when the host platform starts at **POWER-ON** or **RESTART**
- DRTM is started by dynamic CRTM (D-CRTM) at runtime **WITHOUT** platform **RESET**
- They extend measurements (hashes) of components to PCRs **BEFORE** passing control to them

Static Root of Trust for Measurement



Dynamic Root of Trust for Measurement

(Intel Trusted Execution Technology)



PCR Protection

- PCRs contains measurement results of a system
- They **MUST NOT** be reset by disallowed operations
  - Static PCRs (PCR #0~#15) can be reset only if the host resets
  - Dynamic PCRs (PCR #17~#19) can be reset only if the host initializes the DRTM
- If PCRs are reset by attackers, they can reproduce specific PCR values by replaying hashes
  - They can steal the secret and deceive the local and remote verification

PCR protection mechanisms work properly

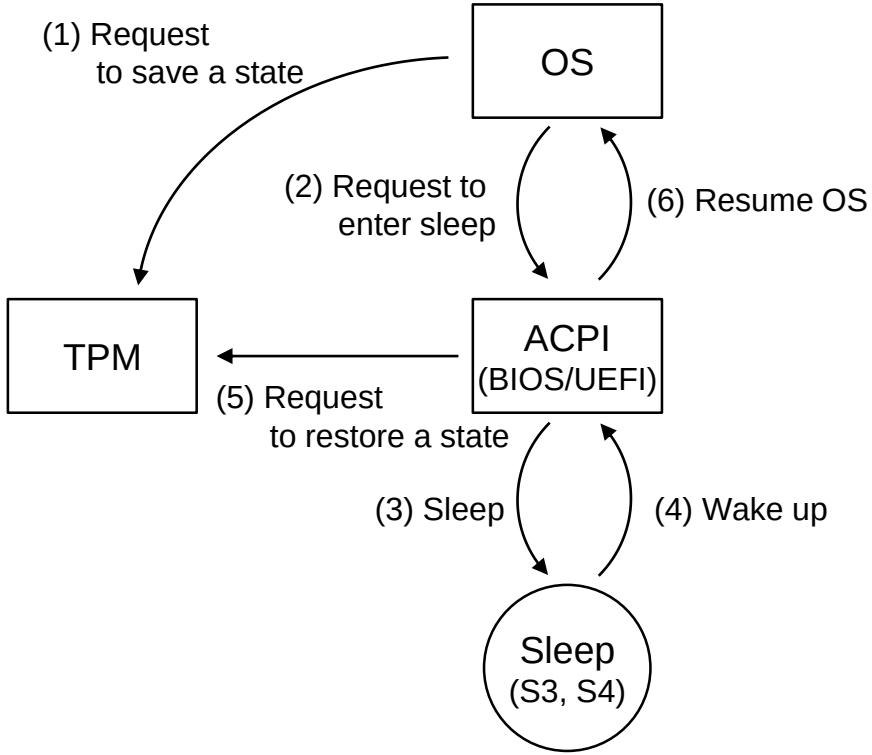
UNTIL YESTERDAY

Assumptions and Threat Model

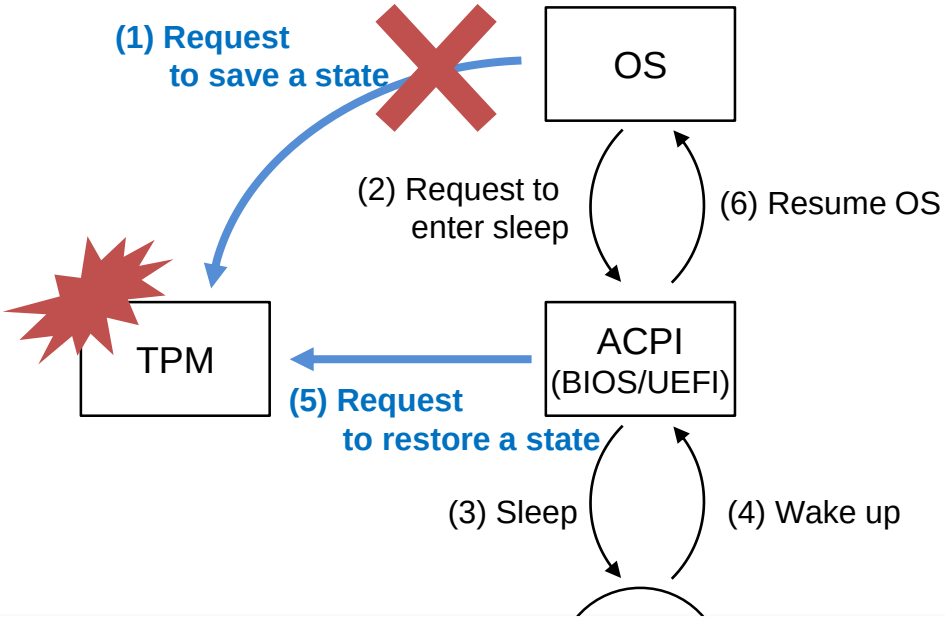
- The system measures boot components using the SRTM and DRTM
  - The measurement results stored in PCRs are verified by a remote verifier
  - The modifications of boot components are detected
- The attackers already gain a root privilege and try to compromise the whole system
  - They try to hide the breach and retain the root privilege
  - They cannot access the system circuit physically
  - They cannot flash the firmware with arbitrary code

Advanced Configuration and Power Interface (ACPI)

- Defines power states and hardware register sets
  - Global states
    - G0 (Working), G1 (Sleeping), G2 (Soft-off), G3 (Mechanical-off)
  - Sleeping states
    - S0 and S1: Working and Power on Suspend
    - S2: Same as S1, CPU is powered off
    - S3: Sleep, **All devices are powered off except RAM**
    - S4: Hibernation, All devices are powered off



ACPI Sleep Process with TPM



The Grey Area vulnerability (CVE-2018-6622)

The Grey Area Vulnerability (CVE-2018-6622)

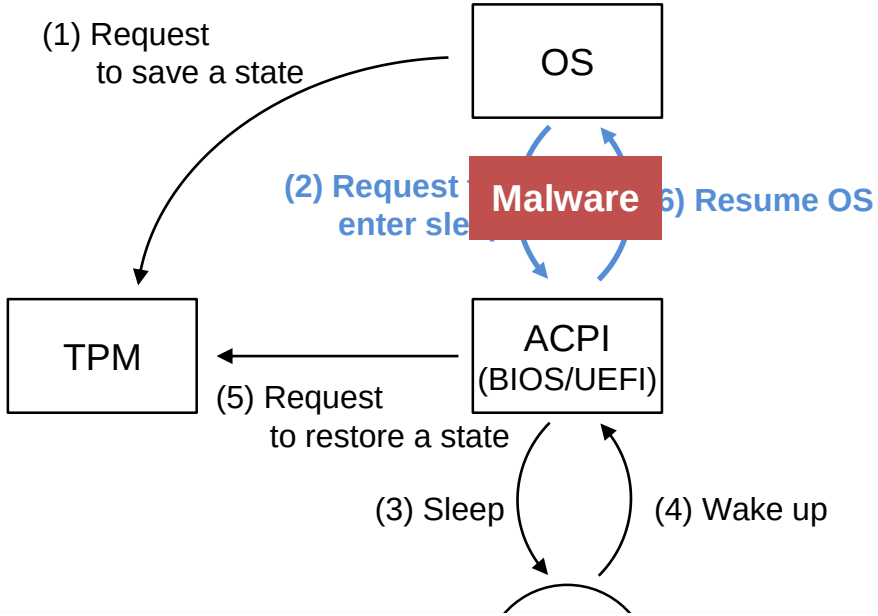
What is the "corrective action"?

If the TPM receives Startup(STATE) that was not preceded by Shutdown(STATE), then there is no state to restore and the TPM will return TPM_RC_VALUE. The CRTM is expected to take corrective action to prevent malicious software from manipulating the PCR values such that they would misrepresent the state of the platform. The CRTM would abort the Startup(State) and restart with Startup(CLEAR).

This means "reset the TPM"

The startup behavior defined by this specification is different than TPM 1.2 with respect to Startup(STATE). A TPM 1.2 device will enter Failure Mode if no state is available when the TPM receives Startup(STATE). This is not the case in this specification. It is up to the CRTM to take corrective action if it the TPM returns TPM_RC_VALUE in response to Startup(STATE).

Trusted Platform Module Library Part1: Architecture



The Lost Pointer vulnerability (CVE-2017-16837)

The Lost Pointer Vulnerability (CVE-2017-16837)

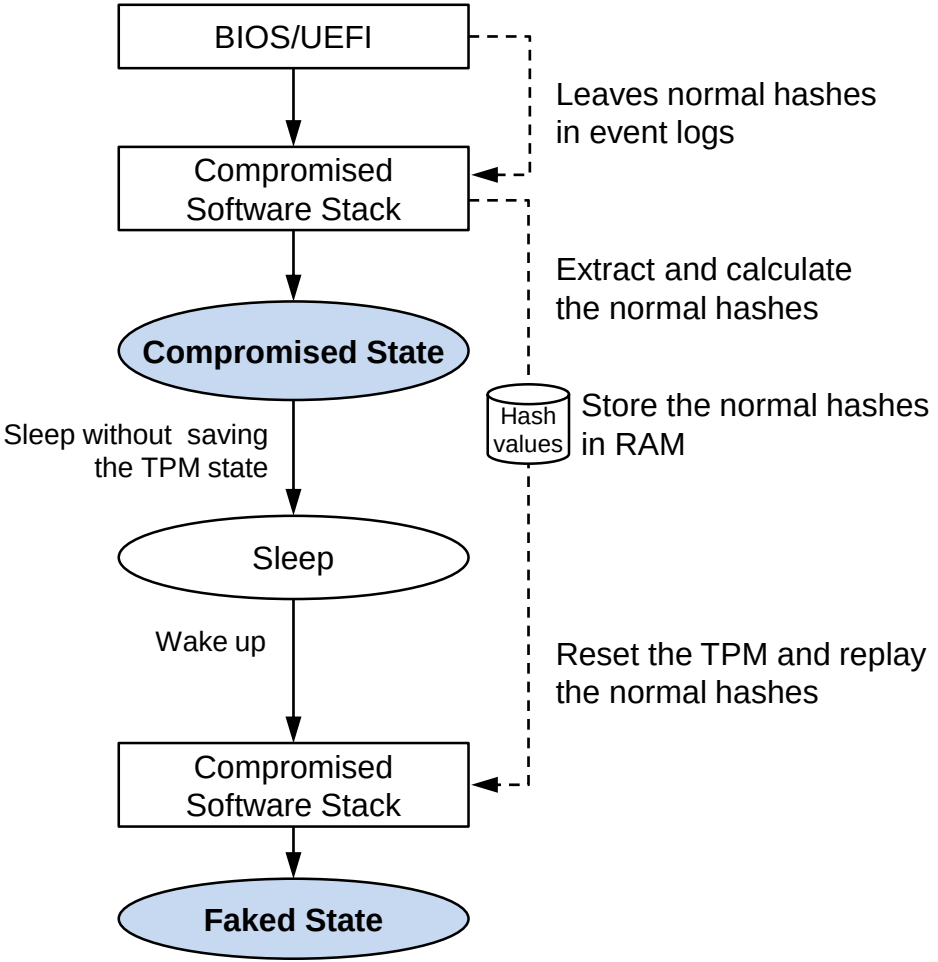
Measured Range

```
SECTIONS
{
  . = TBOOT_BASE_ADDR; /* 0x800000 */

  .text : {
  *(.tboot_multiboot_header)
  . = ALIGN(4096);
  *(.mlept)

  _mle_start = .;          /* Beginning of MLE */
  *(.text)
  *(.fixup)
  *(.gnu.warning)
  } :text = 0x9090

  .rodata : { *(.rodata) *(.rodata.*) }
  . = ALIGN(4096);

  _mle_end = .;            /* End of MLE */

  .data : {                /* Data */
  *(.data)
  *(.tboot_shared)
  CONSTRUCTORS
  }
  ... omitted ...
}
```

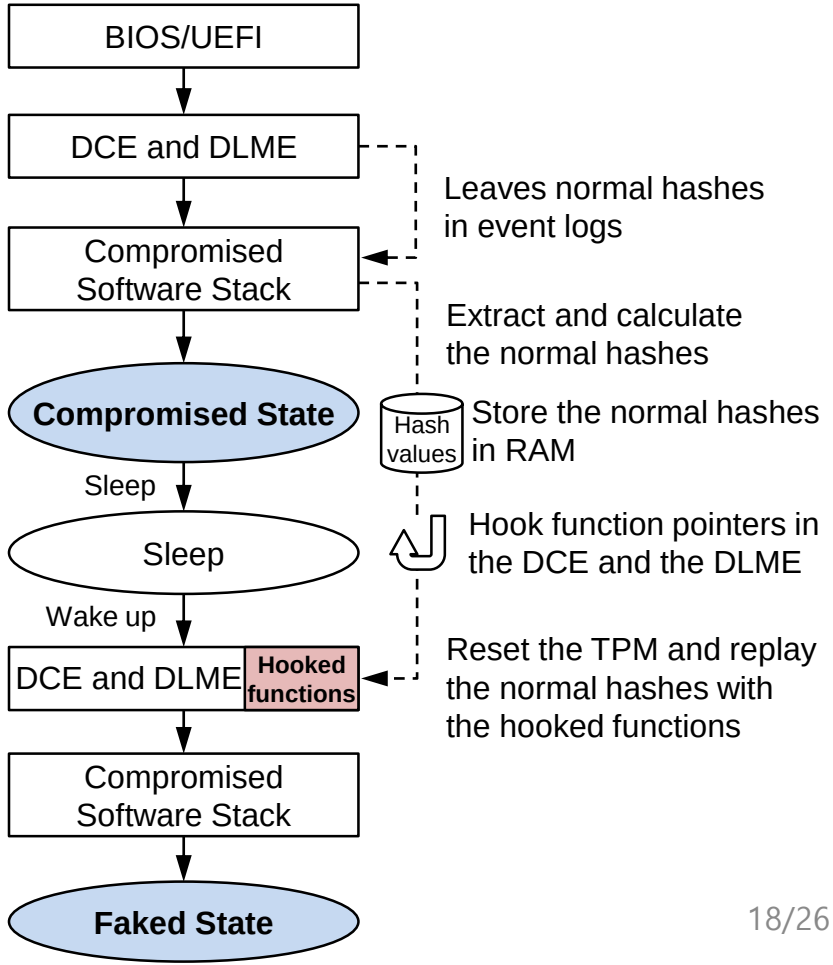
```
/* Beginning of text section (ready-only) */
800000 t multiboot_header
800010 t multiboot2_header
800020 t multiboot2_header_end
801000 t g_mle_pt
804000 T _mle_start /* Beginning of MLE */
804000 T _start
804000 T start
804010 T _post_launch_entry
... omitted ...
83b000 D _mle_end   /* End

/* Beginning of data
83b000 D s3_flag
... omitted ...
83f234 D g_tpm   /* Current TPM interface */
83f238 d num_lines
83f23c d cursor_y
83f23d d cursor_x
83f240 d g_saved_mtrrs
83f260 D g_sinit
... omitted ...
83f2c0 D tpm_12_if  /* TPM interface in */
83f460 D tpm_20_if  /* data section for */
                    /* TPM 1.2 and 2.0 */
... omitted ...
```

Unmeasured Function Pointers

Exploit of the Grey Area Vulnerability



Exploit of the Lost Pointer Vulnerability

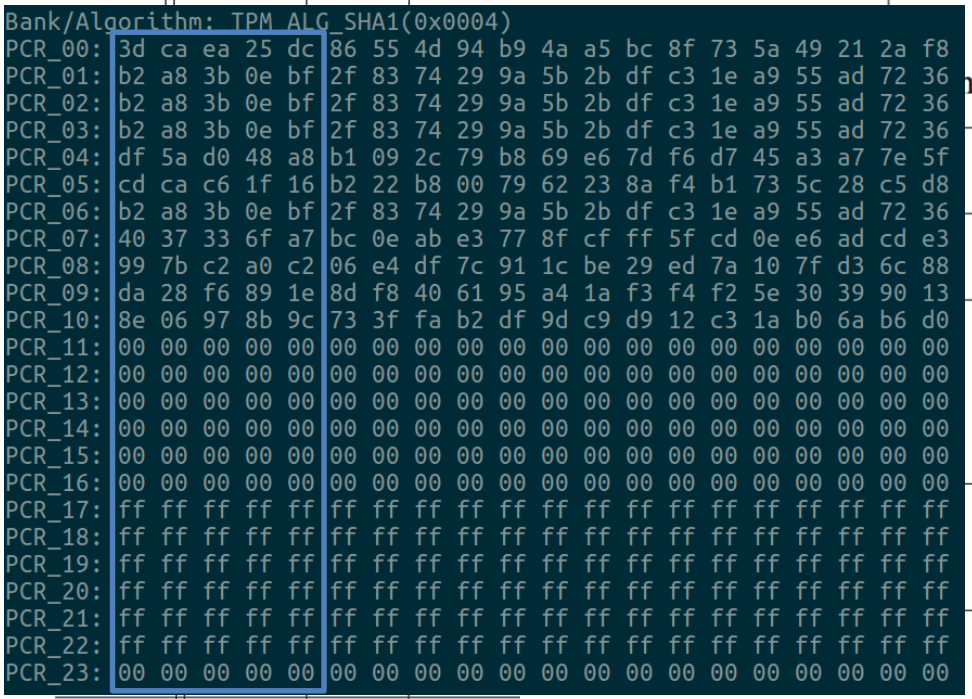


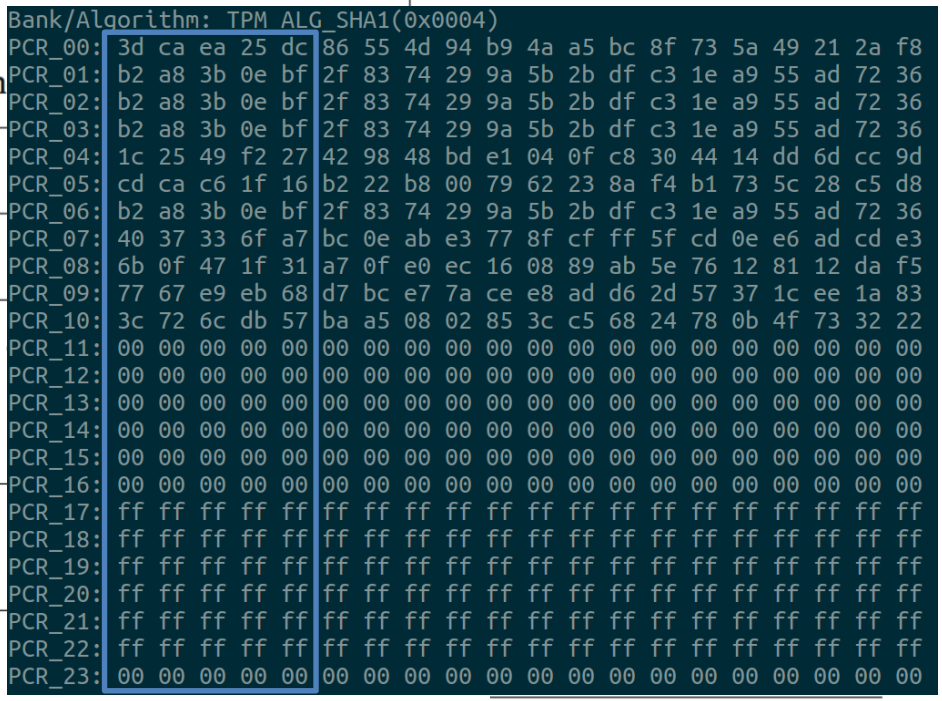
Evaluation – The Grey Area Vulnerability

PC No.	Vendor	CPU (Intel)	PC and mainboard model	BIOS Ver. and release date	TPM Ver.	TPM vendor and firmware Ver.	SRTM attack
1	Intel	Core i5-5300U	NUC5i5MYHE	MYBDEWi5v.86A, 2017.11.30	2.0	Infineon, 5.40	Y
2	Intel	Core m5-6Y57	Compute Stick STK2mv64CC	CCSKLm5v.86A.0054, 2017.12.26	2.0	NTC, 1.3.0.1	Y
3	Dell	Core i5-6500T	Optiplex 7040	1.8.1, 2018.01.09	2.0	NTC, 1.3.2.8	Y
4	GIGABYTE	Core i7-6700	Q170M-MK	F23c, 2018.01.11	2.0	Infineon, 5.51	Y
5	GIGABYTE	Core i7-6700	H170-D3HP	F20e, 2018.01.10	2.0	Infineon, 5.61	Y
6	ASUS	Core i7-6700	Q170M-C	3601, 2017.12.12	2.0	Infineon, 5.51	Y
7	Lenovo	Core i7-6600U	X1 Carbon 4th Generation	N1FET59W (1.33), 2017.12.19	1.2	Infineon, 6.40	N
8	Lenovo	Core i5-4570T	ThinkCentre m93p	FBKTCPA, 2017.12.29	1.2	STMicroelectronics, 13.12	N
9	Dell	Core i5-6500T	Optiplex 7040	1.8.1, 2018.01.09	1.2	NTC, 5.81.2.1	N
10	HP	Xeon E5-2690 v4	z840	M60 v02.38, 2017.11.08	1.2	Infineon, 4.43	N
11	GIGABYTE	Core i7-6700	H170-D3HP	F20e, 2018.01.10	1.2	Infineon, 3.19	N

Evaluation – The Lost Pointer Vulnerability

PC No.	PC and mainboard model	TPM Ver.	Intel TXT support	tboot support	DRTM attack	Note
1	NUC5i5MYHE	2.0	Y	Y	Y	
2	Compute Stick STK2mv64CC	2.0	Y	N	N	The system does not support tboot. It is rebooted while executing the SINIT AC module.
3	Optiplex 7040	2.0	Y	Y	Y	In case of BIOS 1.8.1 version, The system is rebooted while executing SINIT AC module. BIOS 1.4.5 version is used for the DRTM test.
4	Q170M-MK	2.0	Y	N	N	The system does not support tboot. It is rebooted while executing the SINIT AC module.
5	H170-D3HP	2.0	N	N	N	The system does not support Intel TXT.
6	Q170M-C	2.0	Y	N	N	The system does not support tboot. It is rebooted while executing the SINIT AC module.
7	X1 Carbon 4th Generation	1.2	Y	N	N	The system does not support tboot. It is rebooted while executing the SINIT AC module.
8	ThinkCentre m93p	1.2	Y	Y	Y	
9	Optiplex 7040	1.2	Y	Y	Y	For BIOS 1.8.1, The system is rebooted while executing the SINIT AC module. BIOS 1.4.5 is used for the DRTM test.
10	z840	1.2	Y	N	N	The system does not support tboot. It is rebooted while executing the SINIT AC module.
11	H170-D3HP	1.2	N	N	N	The system does not support Intel TXT.





8, 9	1.2	18 19	2E3DC497... F443F487...

Examples of PCR values-Intel NUC5i5MYHE

PC No.	TPM Ver.	PCR No.	PCR values of the ORIGINAL system	PCR values of the COMPROMISED system	PCR values after the SRTM attack
1-7, 9-11	1.2, 2.0	4 9	1C2549F2... 7767E9EB...	DF5AD048... DA28F689...	1C2549F2... 7767E9EB...
8	1.2	4 9	849162AD... 7767E9EB...	9966FE5A... DA28F689...	849162AD... 7767E9EB...

Forged PCR values after SRTM attack

PC No.	TPM Ver.	PCR No.	Before the intrusion	After the intrusion	After the DRTM attack
1	2.0	17	821701E9...	FC8AD796...	821701E9...
3	2.0	17	257B1024...	E90F27EC...	257B1024...
8, 9	1.2	18 19	2E3DC497... F443F487...	3DC85583... E4C61D2A...	2E3DC497... F443F487...

Forged PCR values after DRTM attack

Countermeasures – The Grey Area Vulnerability

1) **Disable S3 sleeping state** option in BIOS menu
   - Brutal, but simple and effective
2) Revise TPM 2.0 specification to **enter failure mode** if there is no state to restore
3) Revise TPM 2.0 specification to **define "corrective action" in detail**
   - A long time to revise and apply to the TPM or BIOS/UEFI firmware, but fundamental solutions

Countermeasures – The Lost Pointer Vulnerability

- **Apply our patch to tboot**
  - https://sourceforge.net/p/tboot/code/ci/521c58e51eb5be105a29983742850e72c44ed80e/
- **Update tboot to the latest version**

Conclusion

- Two vulnerabilities that can subvert the TPM using S3 sleeping state were found
  - The Grey Area Vulnerability: CVE-2018-6622
  - The Lost Pointer Vulnerability: CVE-2017-16837
- Attackers can deceive the local and remote verification with the vulnerabilities
  - They also can unseal the seal secret and steal it
- We have contacted manufacturers and contributed a patch to tboot project to solve the vulnerabilities

Questions?

Seunghun Han
hanseunghun@nsr.re.kr