A BAD DREAM: SUBVERTING TRUSTED PLATFORM MODULE WHILE YOU ARE SLEEPING

Seunghun Han, Wook Shin, Jun-Hyeok Park, and HyoungChun Kim, National Security Research Institute

BACKGROUND

- Trusted Computing Group (TCG)
  - Trusted Platform Module (TPM) is the core technology that provides an anchor of trust
  - Standardize the TPM Technology
    - Security related function
    - APIs
    - Protocols

BACKGROUND - TPM

- TPM is a tamper resistant device that stores RSA encryption keys associated to the system for hardware authentication
- Ensure integrity of a platform (server, laptop, tablet, etc.)
- Contains several Platform Configuration Registers (PCRs) that allow secure storage and security metrics
  - Metrics used to detect changes to previous configurations
  - Use Case: Cryptographically record (measure) software state

BACKGROUND - TPM

- Used to determine credibility of system by checking the values stored in PCRs
- Access control with secret data
  - Seal – an operation to encrypt data using PCRs
  - Sealed data can only be decrypted by the TPM when the PCR values match specified values

BACKGROUND – RTM

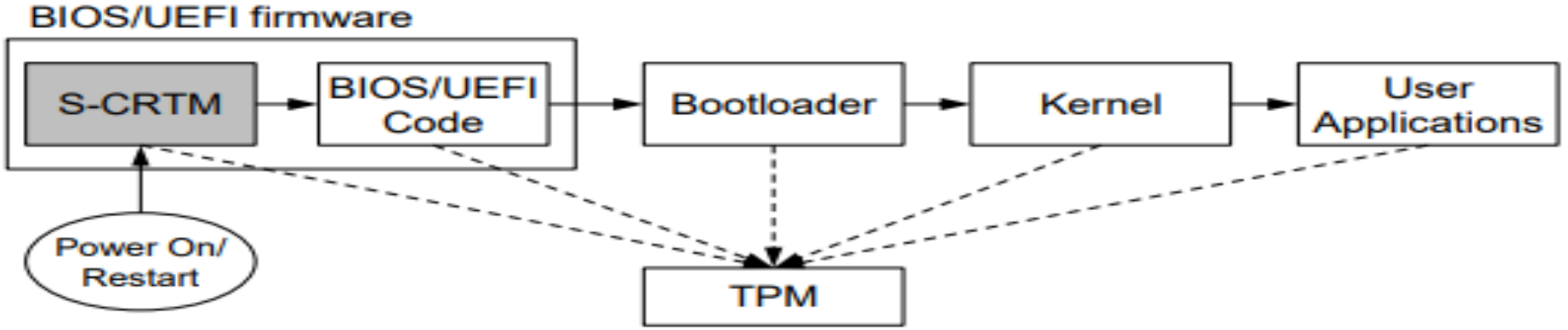
- Root of Trust for Measurement
- Initiating measurement is done by a trusted software component called the core RTM (CRTM)
  - Stored in ROM to protect against attacks
  - First set of instructions when chain of trust is established
- Trust Anchor
  - Trust is assumed and not derived
  - Trustworthiness of whole chain depends on this element

BACKGROUND – RTM

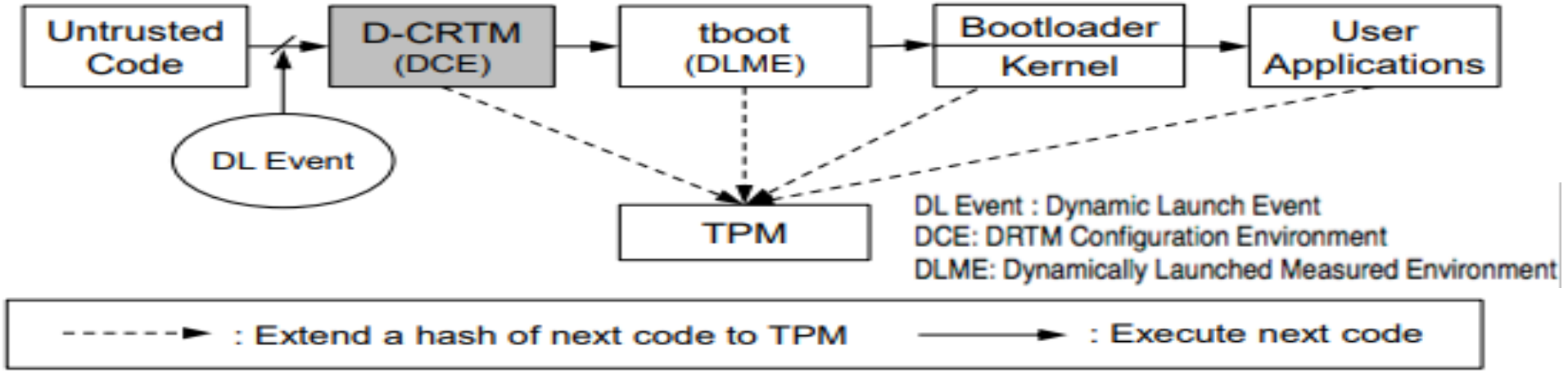
- SRTM is the trust anchor initialized by static CRTM when the host platform starts a power-on or restart

- DRTM is started by dynamic CRTM and launches a measured environment at runtime without platform reset

Static Root of Trust for Measurement



Dynamic Root of Trust for Measurement
(Intel Trusted Execution Technology)



BACKGROUND – ACPI

- Advanced Configuration and Power Interface
  - Global Power States
    - Working (G0 or S0)
    - Sleeping (G1)
    - Soft-off (G2)
    - Mechanical off (G3)

BACKGROUND – ACPI

- Sleeping States
  - S1 – Power on Suspend
    - CPU stops executing instructions (all devices like CPU and RAM are powered)
  - S2 – CPU is powered off
  - S3 – Sleep – All devices powered off except for RAM
  - S4 – Hibernation – All devices powered off
    - Platform context in RAM is saved to disk

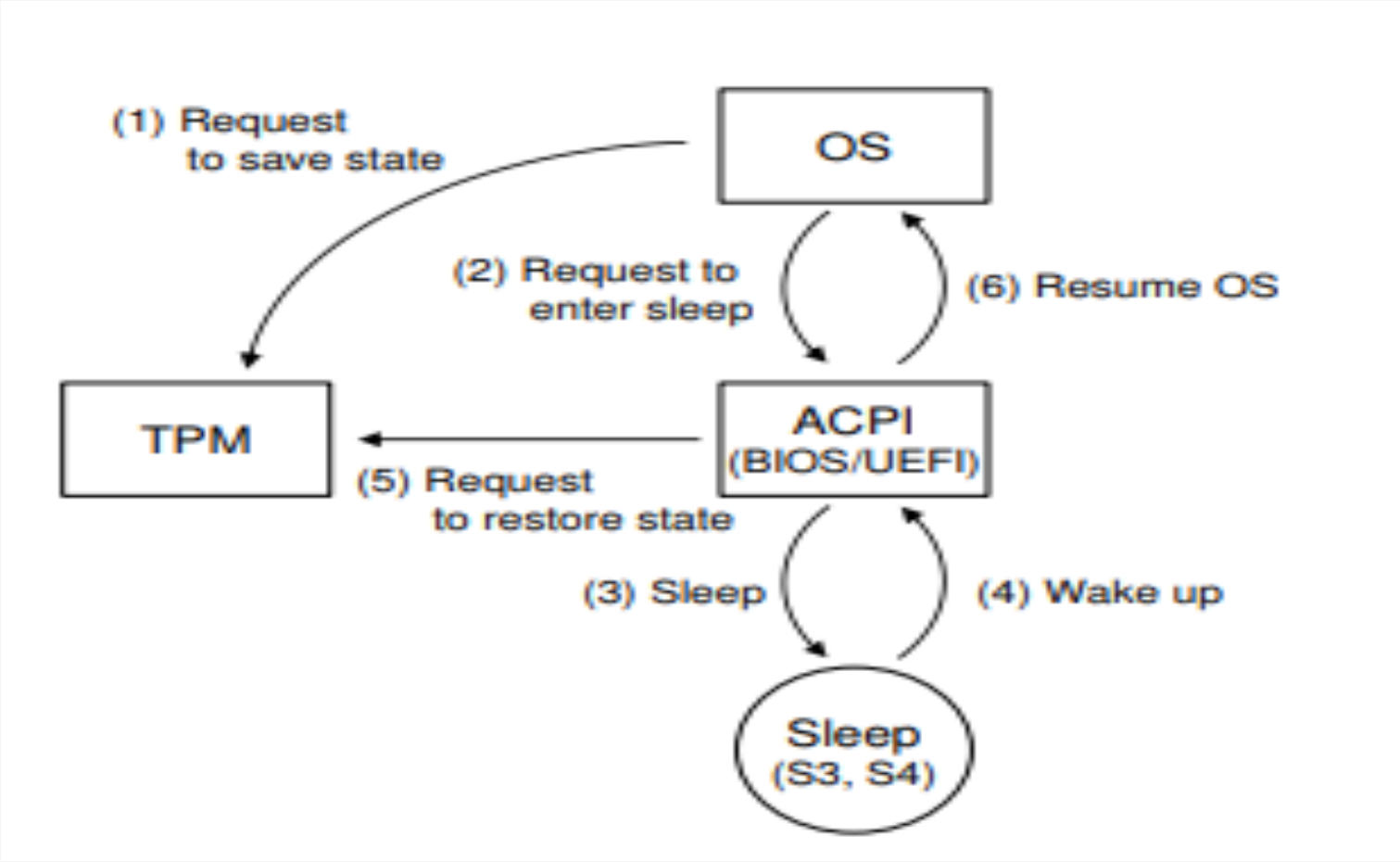
ASSUMPTIONS

- System measures the boot components using TCG's SRTM and DRTM
- The stored measurements in TPM are verified by a remote verifier
- When modifications are made to the components they are detected

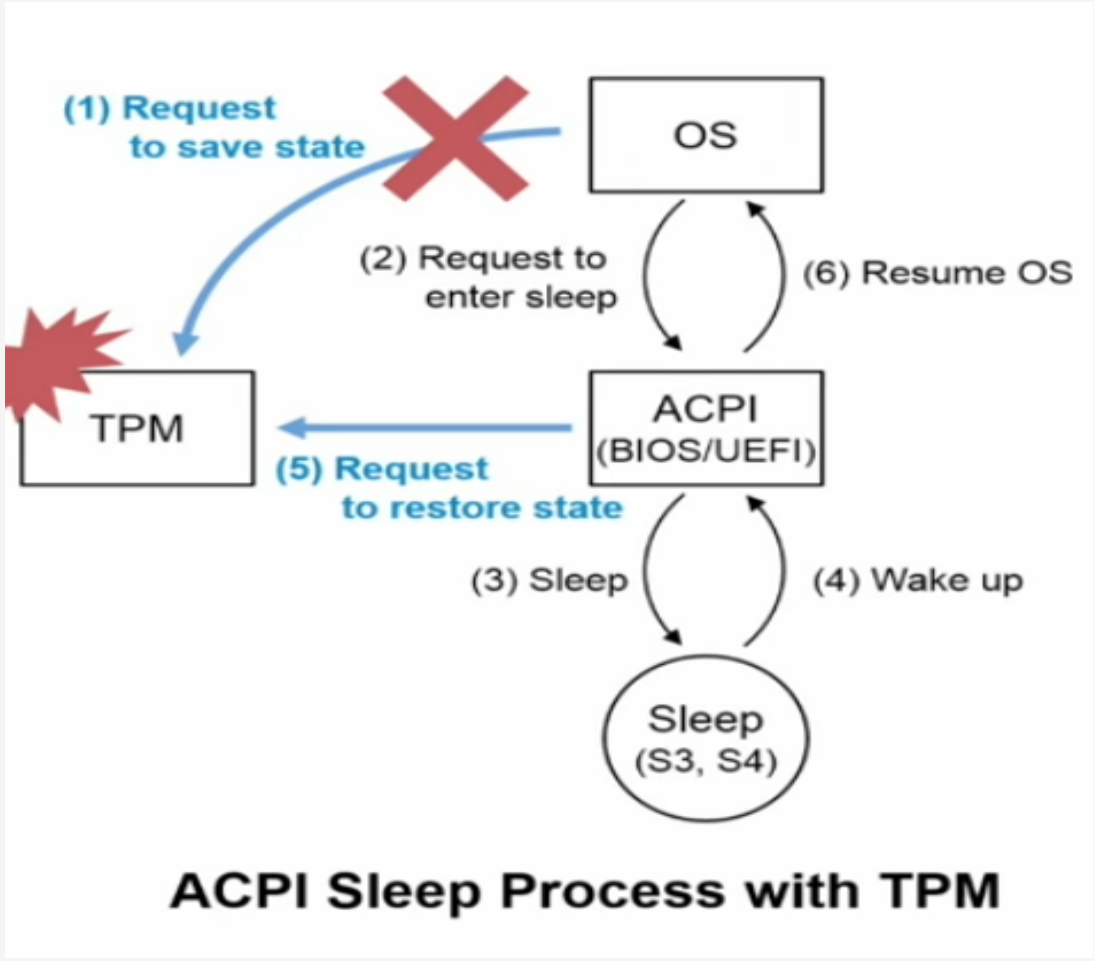
THREAT MODEL

- Consider an attacker who has already acquired the Ring-0 privilege
  - Has admin access to:
    - Firmware
    - Bootloader
    - Kernel
    - Applications
  - He or she cannot flash the firmware with arbitrary code
  - Cannot rollback to an old version of the firmware, where the attacker can exploit a known vulnerability.

ACPI SLEEP PROCESS WITH TPM

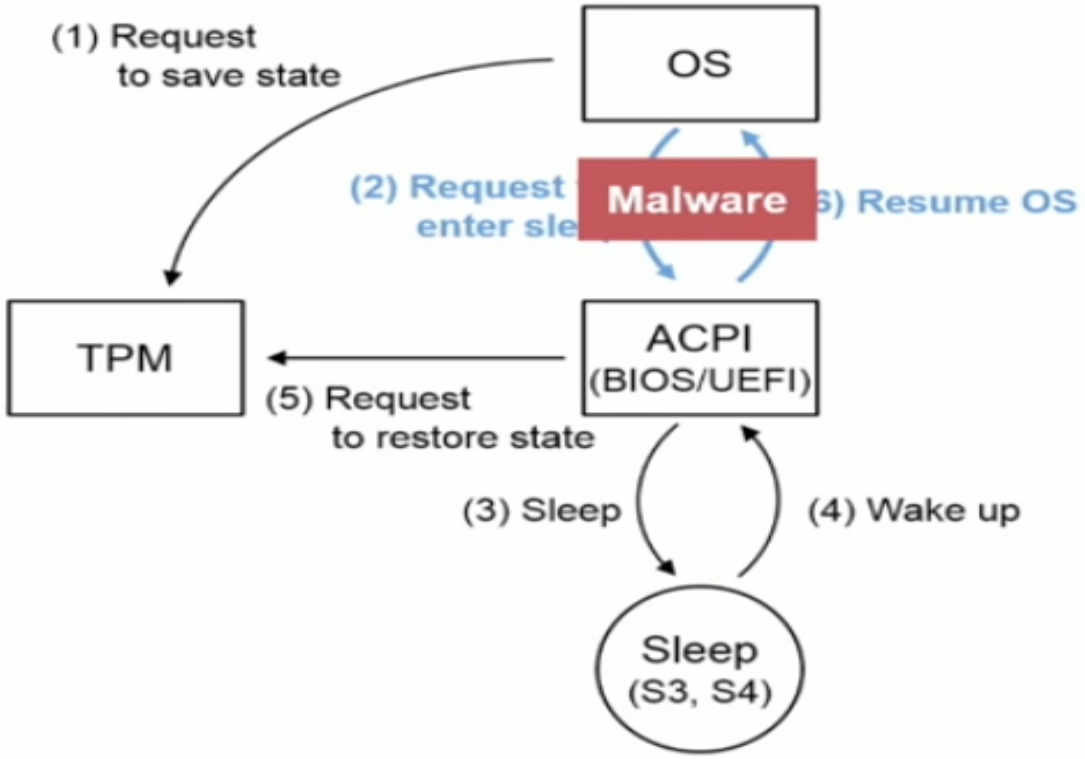


WHAT IF OS IS COMPROMISED AND DOESN'T NOTIFY THE TPM OF SLEEP?



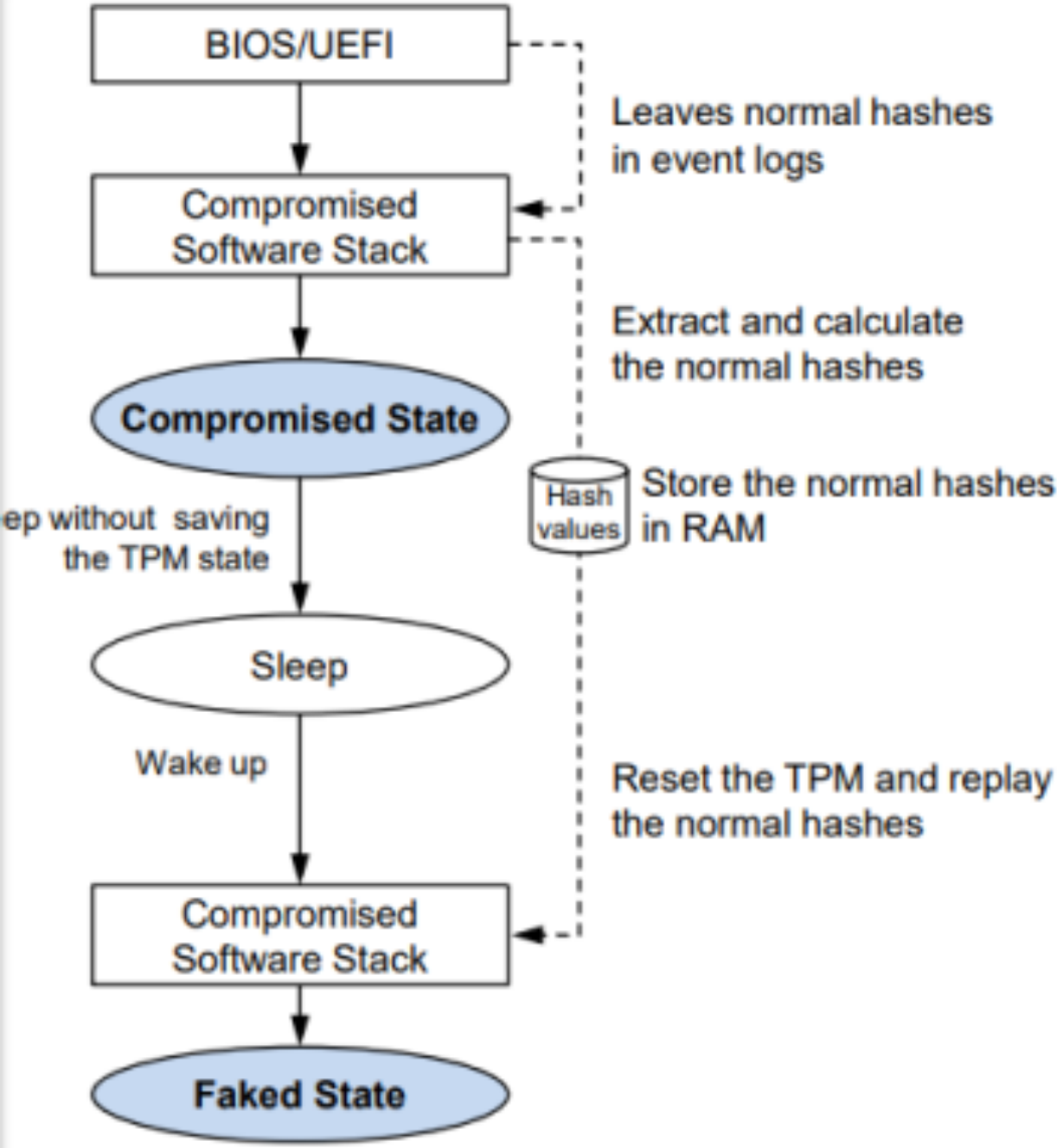
ACPI Sleep Process with TPM

WHAT IF MALWARE INTERCEPTS THE COUNTERFLOW BETWEEN ACPI AND OS?

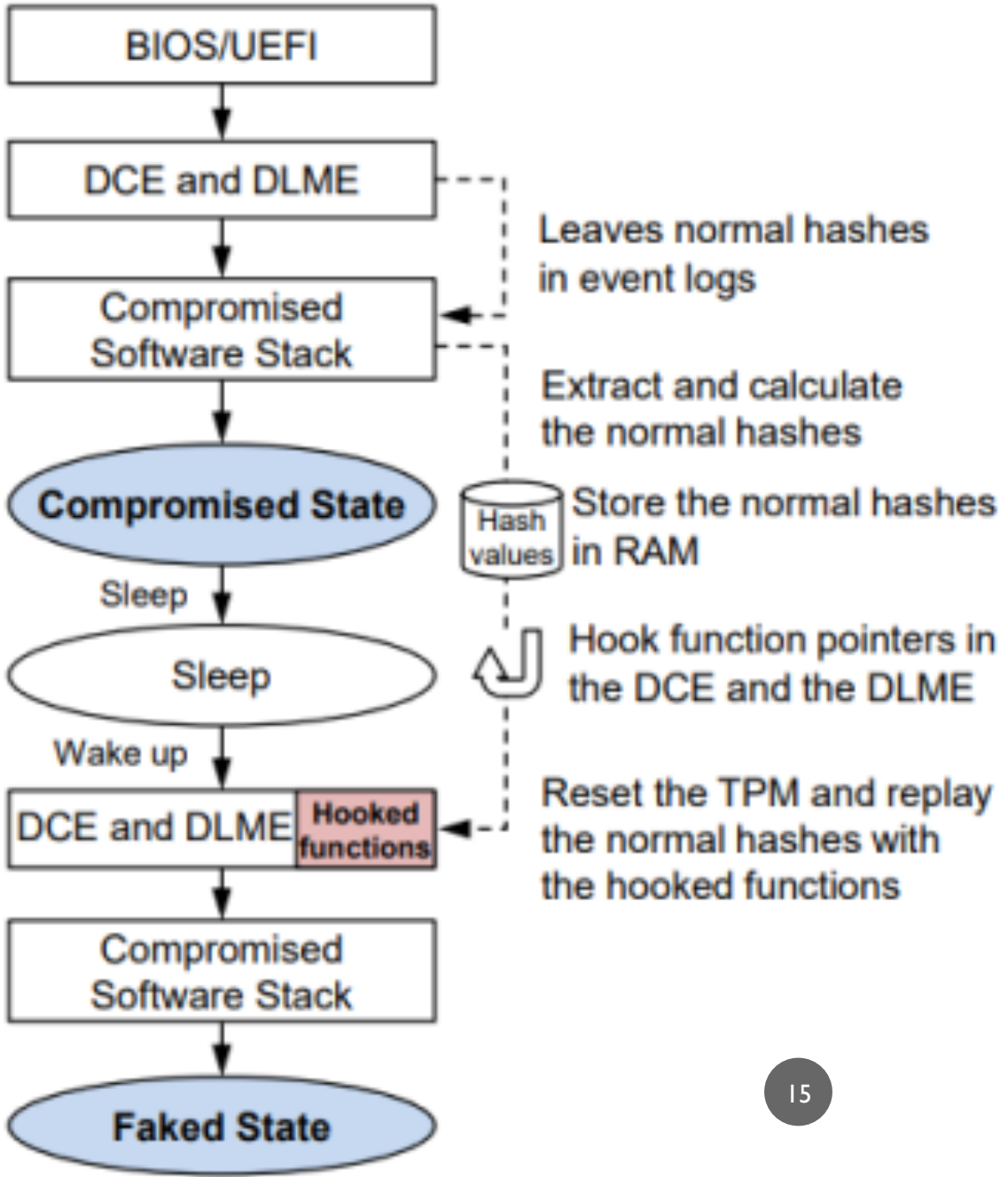


ACPI Sleep Process with TPM

Exploit of the Grey Area Vulnerability



Exploit of the Lost Pointer Vulnerability



EVALUATION

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 [2], 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 [3]
8	Lenovo	Core i5-4570T	ThinkCentre m93p	FBKTCPA, 2017.12.29	1.2	STMicroelectronics, 13.12	N [3]
9	Dell	Core i5-6500T	Optiplex 7040	1.8.1, 2018.01.09	1.2	NTC, 5.81.2.1	N [4]
10	HP	Xeon E5-2690 v4	z840	M60 v02.38, 2017.11.08	1.2	Infineon, 4.43	N [3]
11	GIGABYTE	Core i7-6700	H170-D3HP	F20e, 2018.01.10	1.2	Infineon, 3.19	N [3]

Table 4: List of PC and mainboard models and results of the SRTM attack

PCR VALUES

PC No.	TPM Ver.	PCR No.	PCR values [5] of the ORIGINAL system	PCR values of the COMPROMISED system	PCR values after the SRTM attack
1-7,	1.2,	4	1C2549F2...	DF5AD048...	1C2549F2...
9-11	2.0	9	7767E9EB...	DA28F689...	7767E9EB...
8 [6]	1.2	4	849162AD...	9966FE5A...	849162AD...
		9	7767E9EB...	DA28F689...	7767E9EB...

Table 5: Forged PCR values after the SRTM attack

COUNTERMEASURES

- Grey Area Vulnerability
  - Disable S3 sleeping state in BIOS
  - Revise TPM 2.0 to enter failure mode if there is no state to restore
- Lost Pointer Vulnerability
  - Update tboot
  - Apply researchers patch to tboot

CONCLUSION

- Two vulnerabilities found to undermine TPM with the S3 sleeping state
  - Flaw with TPM 2.0 specification
  - Flaw in implementation flow of tboot
  - Flaw in open source implementation of Intel TXT