The Intel® Converged Security and Management Engine IOMMU Hardware Issue – CVE-2019-0090 and CVE-2020-0566

White Paper

Version 1.1
June 2020

Legal Disclaimer

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

The products described might contain design defects or errors known as errata, which might cause the product to deviate from published specifications. Current, characterized errata are available on request.

Intel technologies might require enabled hardware, software, or service activation. Some results have been estimated or simulated. Your costs and results might vary.

No product or component can be absolutely secure.

Contents

Revision History:

Revision	Date	Description
1.0	4/14/2020	Initial Release
1.1	6/9/2020	Added CVE-2020-0566 related details, added Intel CPU-based security technologies that are not impacted by CVE-2019-0090

Purpose of the white paper

The purpose of this white paper is to provide technical details to help understand the Intel® Converged Security Management Engine (CSME) IOMMU (Input Output Memory Management Unit) Hardware issue (CVE-2019-0090), how it could be potentially exploited, and the resulting impact of a successful exploitation.

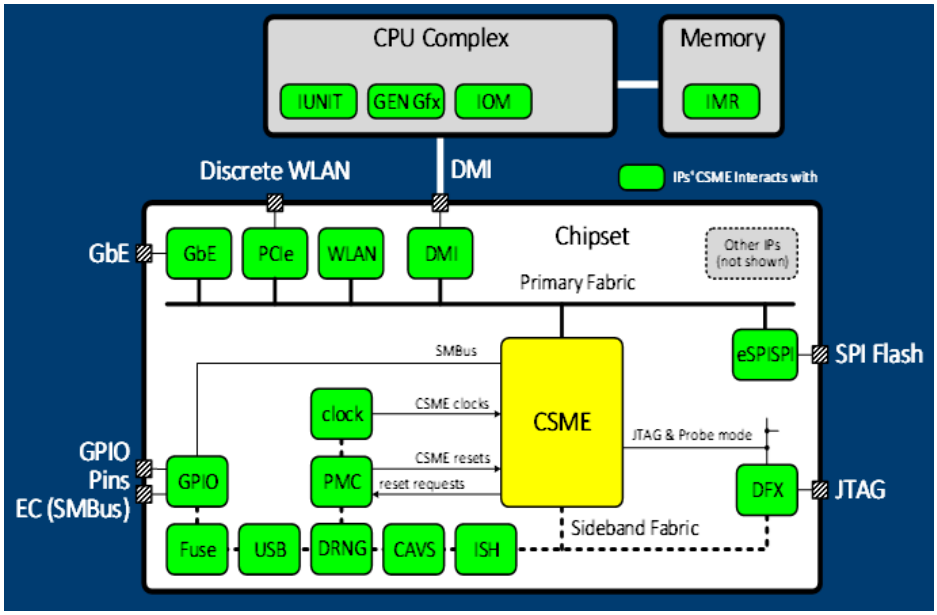
The white paper also discusses the different CSME Firmware workarounds made to help prevent exploitation of CVE-2019-0090 and what steps are recommended to protect systems against potential attacks.

CVE-2019-0090 is the original CVE that describes the CSME IOMMU HW vulnerability and provides initial mitigations. CVE-2020-0566 provides mitigation for additional attack vector on specific platforms.

While most of the technical information contained in this white paper was already documented publicly as part of a Black Hat presentation on CSME in August 2019 by Intel security researchers, the intent of the white paper is to augment that information further in light of recent public disclosures regarding the security of the CSME on certain Intel products.

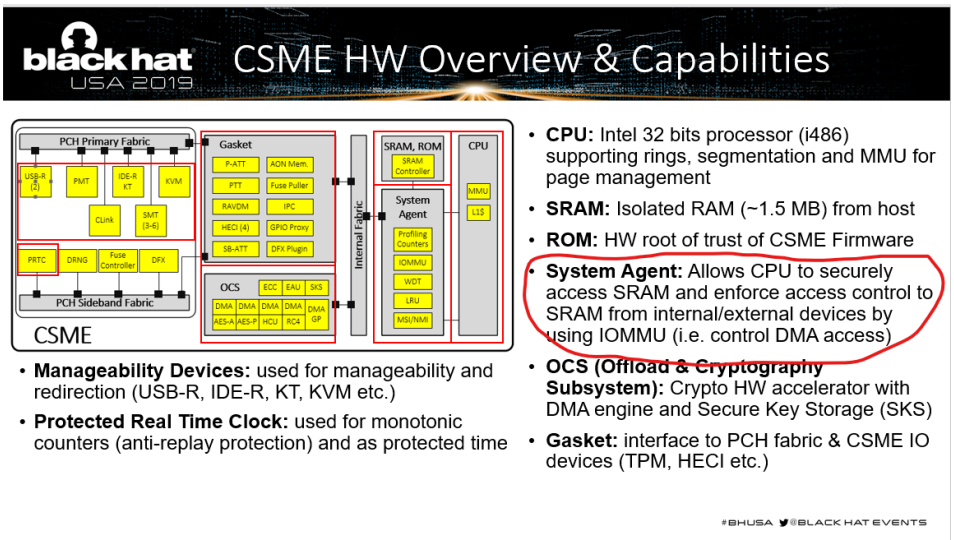
Background

The Platform Controller Hub (PCH)/SoC consists of a set of hardware blocks (aka IP or IPs) connected by an internal fabric, as illustrated in figure hereafter. The CSME is one of those hardware blocks. It is important to note that this figure is for illustrative purposes only and does not reflect the exact hardware block diagram for PCH and SoC products.



One of the main roles of the CSME in the PCH/SoC is to authenticate and load Intel and System Manufacturer Firmware (FW) into relevant IPs such as the Power Management Controller (PMC) and Integrated Sensor Hub (ISH). This requires the CSME to communicate over the fabric with other IPs. This communication is done with a transaction type known as Root Space 1 (RS1); each IP's transactions are tagged by hardware with the IP's identifier. This is known as the Security Attribute of Initiator (SAI). One class of transactions is Direct Memory Access (DMA) transaction types to/from CSME.

The CSME has a dedicated, access-control logic in the Input-Output Memory Management Unit (IOMMU) that controls which IPs can send DMA transactions to specific areas in CSME SRAM. This access control is based on IP SAI and is controlled solely by CSME ring 0 Firmware components: ROM, RBE (ROM Boot Extension – first Firmware component executed by ROM), and Kernel. The CSME Hardware block diagram below highlights the IOMMU inside CSME and its main security role therein.



CVE-2019-0090

By default, when CSME is out of reset, the IOMMU is disabled, and there is a small window of several hundred microseconds that allows RS1 DMA transactions to reach CSME SRAM before CSME ROM turns on the IOMMU protection. This window can be used by an IP having RS1 DMA capability to read and write to CSME SRAM during CSME ROM execution, potentially compromising confidentiality of the CSME SRAM or integrity of the CSME ROM through other techniques such as Return Oriented Programming (ROP).

In order to mount a successful attack, an attacker would need to do one of the following:

1. Compromise Firmware of an IP having RS1 DMA capability, i.e., Integrated Sensor Hub (ISH) on Cannon Point (CNP) PCH
2. Bypass Root of Trust (RoT) protection, install and run attacker's own Firmware in an IP having RS1 DMA capability on a system that has not had End of Manufacturing (EOM) applied. Firmware that can be customized by system manufacturers (i.e., ISH, Audio DSP) is authenticated by CSME Firmware using a manufacturer's public key hash, which is stored in SPI flash. Note that when EOM is successfully applied by a system manufacturer, fuse emulation in flash is disabled and instead Field Programmable Fuses (FPF) in PCH/SoC would be used by CSME Firmware to authenticate and load customized, system manufacturer's Firmware IP.
3. Achieve direct access to RS1 DMA capability

A successful attack would also require that the attacker's IP firmware executes while CSME is coming out of reset, for example during system boot or resume from CSME low-power mode (aka Power Gating) if supported by Firmware SKU or CSME reset.

Positive Technology's security research team utilized a Cannon Point (CNP) PCH-based platform with no EOM applied. Onto this platform, they loaded their own ISH Firmware by storing the hash of their public key in fuse emulation in SPI flash. Then they either triggered a CSME reset using CSME manufacturing command or waited for the CSME to resume from low-power state. Under these limited conditions, they were then able to trigger an RS1 DMA transaction targeting CSME SRAM during the small window where CSME IOMMU is not enabled yet by CSME ROM.

The Mitigation

Intel has mitigated CVE-2019-0090 in newer systems by making the IOMMU enabled by default in CSME Hardware, so when CSME ROM starts executing, RS1 DMA transactions are blocked until the CSME Firmware grants access to specific SRAM area. The following systems already include the hardware fix:

1. Icelake (ICP-LP and ICP-N PCH)
2. Cometlake (CMP-LP, CMP-H and CMP-V PCH)
3. Tigerlake (TGP-LP and TGP-H PCH)
4. Lakefield (LKF SoC)
5. Whitley (LBG-R PCH)
6. Idaville (CDF PCH)
7. Jacobsville (CDF PCH)
8. Eagle Stream (EBG PCH)
9. Tatlow (TGP-H PCH)

On other systems, where the CSME ROM is integrally part of the PCH/SoC Hardware and does not have any patching mechanism, the IOMMU is potentially vulnerable. In these cases, CSME Firmware updates have been released to help prevent RS1 DMA transaction from reaching CSME SRAM while the IOMMU is disabled.

There is a limited list of IPs that have RS1 DMA capability to read and write to CSME for PCH and SoC, which are impacted by CVE-2019-0090. This list differs from one PCH / SoC generation to another.

For CNP-based systems, the CSME Firmware update blocks RS1 DMA transactions to the CSME at the PCH fabric level before the CSME enters low-power mode (aka Power Gating) or initiates a CSME reset. Once resuming from Power Gating or CSME reset is completed and once the IOMMU is enabled, the CSME Firmware is designed to reconfigure the PCH fabric to unblock RS1 DMA transactions. Note this change relies on PMC Firmware's control of power management flows in the PCH/SoC and ability to reset individual IPs like the CSME.

CVE-2020-0566

For BXT-P and GLK-based platforms, the CSME Firmware change consists of disabling USB DbC (debug capability) interface when end of manufacturing has been applied to the system and SoC debug interface is closed. The goal of the firmware update is to prevent an attacker with physical access to a system from connecting to that system via a USB DbC interface and issuing an RS1 DMA transaction when the CSME resumes from Power Gating or a CSME reset has been completed, as described in CVE-2020-0566.

For other systems, the latest CSME Firmware version can prevent known attack vectors (except for physical rollback to CSME Firmware versions previously vulnerable to Intel-SA-00086).

Hardware-based Anti-rollback (ARB)

In order to properly mitigate physical attack vectors, the CSME Hardware-based, Anti-rollback capability (ARB) must be supported by the PCH/SoC and enabled by system manufacturers. This capability will prevent a physical rollback of the CSME Firmware in flash and provide assurances that the system remains protected against known vulnerabilities that have been mitigated in the most recent CSME Firmware release.

This table summarizes in which PCH/SoC and under which conditions Hardware-based ARB is supported.

	PCH / SOC							
	BXT-P	GLK	SPT	KBP	LBG	DNV	DNV-AD	CNP
Hardware based ARB supported	Yes	Yes	No	No	No	No	Yes	Yes
Required enablement during system	Yes	Yes	N/A	N/A	N/A	N/A	Yes	No

manufacturing by manufacturers								
Required support in manufacturers BIOS	Yes	Yes	N/A	N/A	N/A	N/A	Yes	Yes

The Impact of CVE-2019-0090

CVE-2019-0090 might allow an attacker to assert control of the CSME ROM execution and gain access to CSME chipset and attestation keys: the Intel® Enhanced Privacy ID (EPID) private key and the Intel® Platform Trust Technology (PTT) Endorsement Key (EK). Those keys are unique to a given system. Refer to later sections to understand the role played by chipset key and EPID private key in CSME. In addition, CVE-2019-0090 might allow an attacker to load their own CSME Firmware and compromise the CSME use-cases on the system.

The table hereafter lists the different use cases supported by CSME and how they could be potentially impacted by CVE-2019-0090.

Use case	Description	Potential Consequence
Silicon Enabling	Base initialization of PCH/SoC including clocks and GPIOs	Denial of service.
Intel Boot Guard	Authenticate BIOS - prevents SW update and simple physical attack to install unauthorized BIOS	Unauthorized BIOS compromises OS loader and OS integrity.
Intel PTT – Integrated TPM 2.0	Integrated TPM to support UEFI secure boot, disk encryption, virtual smart card, remote attestation	All use cases / user secrets protected by Intel TPM are compromised.
Protected Audio Video Path (PAVP) / Digital Rights Management (DRM) on client platform only	Hardware-based DRM, HDCP link protection	Use case no longer trusted by Content Provider with no recovery. DRM keys can be exposed. Downgrade content playback from UHD/HD to SD.
Intel® Active Management Technology (AMT) on client platform only	Remote management, assistance, recovery, of enterprise PCs	Reveals corporate secrets stored on AMT, access to corporate network, compromise boot, and OS integrity.
Intel® Dynamic Application Loader (DAL) on client platform only	Secure loading and execution of Intel signed DAL applet like Intel® Authenticate, Intel® Identity Protection Technology, Intel® Software Guard Extensions (SGX) Time and Monotonic Counter Services (for SGX DRMs), and more.	Loading of unsigned DAL applet Use cases no longer trusted.
Firmware Authentication for IPs	Secure loading of Power Management Controller, Integrated Sensor Hub, Audio DSP, Image Processing Unit (IPU) Firmware	Unauthorized control of these IPs
PCH/SoC Debug	Authorize and configure debug policies that can unlock the PCH / SoC in various modes (Green, Orange, Red)	Unauthorized reverse engineering and debug of

		Intel and OEM intellectual property
Intel Node Manager on server platform only	Platform-level, power management and telemetry	Platform power policies configured by the administrator are not obeyed. Telemetry data are not trusted.
Hardware "health" check	Periodic Hardware "health" check as part as Functional Safety (FUSA) requirement	Hardware failure will not be detected by FUSA check.

The latest CSME Firmware includes mitigations for the CSME IOMMU Hardware issue against known attacks. When Hardware-based ARB capability is supported and enabled by system manufacturer (including BIOS support), the CSME will only accept the latest CSME Firmware, mitigating against physical FW-rollback attacks.

In addition, EOM should have been applied by system manufacturer before shipment, as specified in Intel guidelines to system manufacturers. EOM specified the following:

1. SPI descriptor, containing access control list on different region (i.e., BIOS, CSME), is locked and cannot be changed by Software. The access control is then enforced by SPI controller.
2. SPI Flash-based fuse emulation is disabled and Field Programmable Fuses in PCH or SoC are used instead.
3. CSME Manufacturing API is disabled.

It is important to note that the following Intel CPU-based security technologies are not impacted by CVE-2019-0090:

1. Intel® Trusted Execution Technology (TXT), if used with a discrete TPM and not Intel PTT. TXT in this white paper refers to Intel CPU Dynamic Root of Trust for Measurement (DRTM) that establishes a new Trusted Computing Base (TCB) starting from the CPU micro-code and not a specific TXT usage by a specific Measured Launched Environment (MLE) or Virtual Machine Manager (VMM).
2. Intel SGX, except the secure time and monotonic counter provided by CSME DAL only on client platform
3. Intel® Virtualization Technology for Directed I/O (VT-d): proper configuration of Intel VT-d prevents rogue DMA access to system memory via a compromised CSME, because such memory access conforms to Peripheral Component Interconnect (PCI) memory transactions, which include CSME devices' PCI Bus/Device/Function (BDFs) that can be managed by VT-d.

Use Case Support per SoC / PCH

The table below lists which use case is supported on which SoC / PCH:

Use Case	PCH / SoC							
	BXT-P	**GLK**	**SPT**	**KBP**	**LBG**	**DNV**	**DNV-AD**	**CNP**
Silicon Enabling	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Boot Guard	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Intel Platform Trust Technology	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Hardware DRM	Yes	Yes	Yes	Yes	No	No	No	Yes

Intel Active Management Technology	No	No	Yes	Yes	Yes[2]	No	No	Yes[2]
Intel Dynamic Application Loader	Yes	Yes	Yes	Yes	Yes[2]	No	No	Yes[2]
Firmware Authentication for IPs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCH/SoC Debug	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel Node Manager	No	No	Yes[3]	No	Yes[3]	Yes[1]	No	No
Hardware "health" check	No	No	No	No	No	No	Yes	No

Yes[1] – Intel Node Manager functionality provides telemetry only, no system power management.

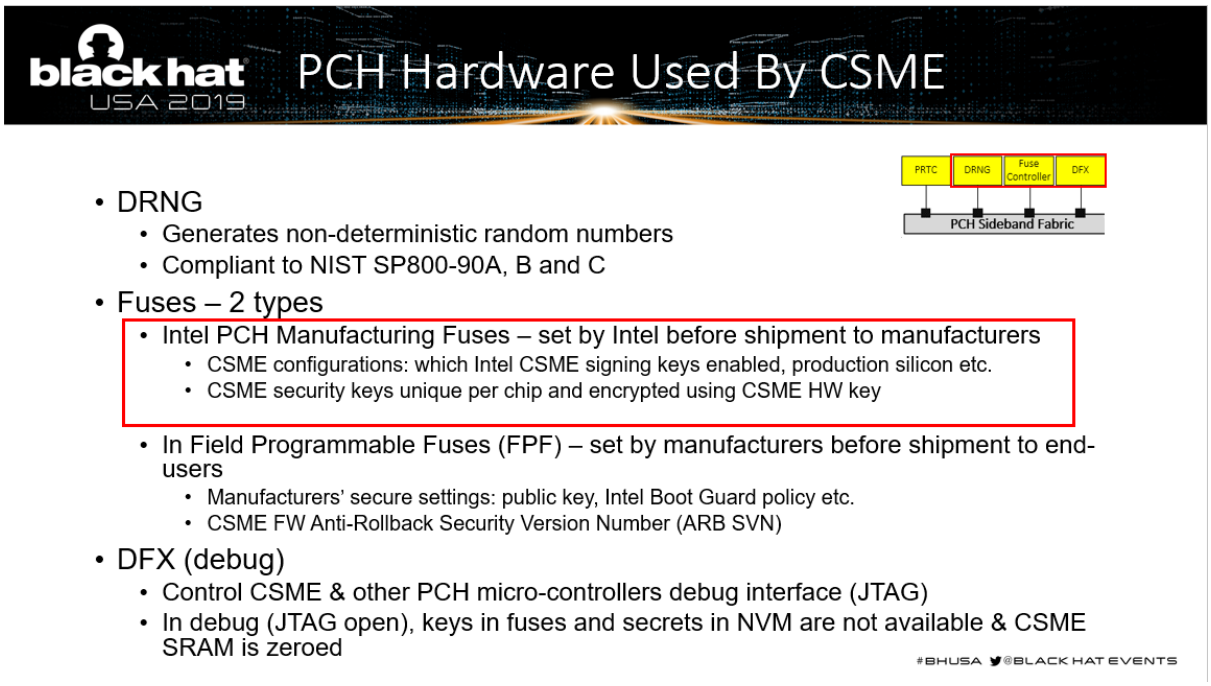
Yes[2] – Use case is supported only on Intel® Workstations Systems that run CSME Firmware. On Server (Intel® Server Platform Services Firmware), the use case is not supported.

Yes[3] – Use case is supported only on Server that runs Intel® Server Platform Services (SPS) Firmware. On Workstation or Client (CSME Firmware), the use case is not supported.

The "Firmware authentication for IP" use case might also differ between client and server. For example, even though ISH Hardware exists in CNP-H PCH used on server platform, SPS Firmware does not support loading of ISH Firmware.

The Chipset Key and the Fuse Encryption Hardware Key

The CSME Chipset Key is the master of all keys generated by the CSME ROM and by CSME Firmware at runtime. All chipset keys are randomly generated by Intel's Key Generator Facility (KGF) for PCH and SoC products, encrypted with a PCH/SOC family Hardware Key (the Fuse Encryption Hardware Key), and sent to Intel Assembly facilities for final programming with other security keys in the PCH/SOC manufacturing fuses before shipment to system manufacturers.



The table below lists the security fuses that get programmed during Intel Manufacturing:

Name	Length in bits	Encrypted with Fuse Encryption Hardware Key

Chipset Key	256	Yes
EPID 1.0 Private Key	256	Yes
EPID 1.0 Group ID	32	No
EPID 2.0 Private Key*	256	Yes
EPID 2.0 Group ID*	32	No
PTT EK Counter	32	No
Debug Enabled Chipset Key	128	No

*Present only starting CNP PCH.

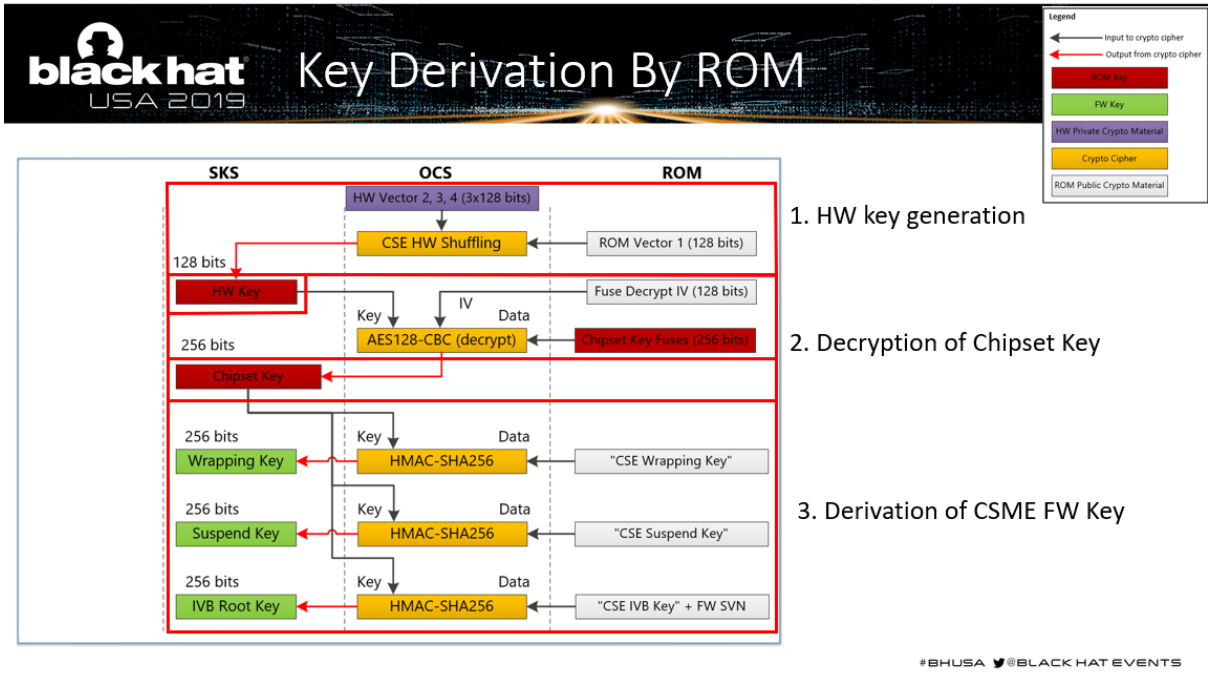
The Fuse Encryption Hardware Key serves to prevent CSME security keys from being exposed, should they be successfully extracted from the fuses.

Note the Fuse Encryption Hardware Key is not meant to protect chipset key and EPID private key from the CSME ROM. More explanations on that are provided in later sections.

Usage of the Chipset Key and Fuse Encryption Hardware Key by the CSME ROM

When the CSME ROM starts executing, it will perform the following sequence:

1. ROM requests from the Crypto Hardware accelerator to generate the Fuse Encryption Hardware Key
2. ROM sets up Secure Key Storage (SKS) slot attributes (privilege level, secure mode, and lock) before loading the Fuse Encryption Hardware Key into the SKS Hardware.
3. ROM pulls security keys from fuses into the CSME SRAM. Once complete, security key fuses are locked. Thereafter, security keys cannot be retrieved until the next CSME reset, thereby providing assurances that only the CSME ROM can retrieve the security keys.
4. ROM decrypts the chipset key encrypted with the Hardware Key from CSME SRAM into SKS
5. ROM can use the chipset key to derive additional keys using HMAC-SHA256 as a Key Derivation Function and hard-coded string (different per key) and CSME Firmware Security Version Number after the CSME Firmware manifest has been verified by CSME ROM.



Several keys are created by ROM using the Chipset Key:

1. Wrapping Key – this key is used to wrap key in SRAM and to ensure the key is unwrapped into SKS before it can be used. Once a key is wrapped, it is bound to the CSME Hardware and cannot be used outside CSME.
2. Memory Guard Key – this key is used to wrap and unwrap key in SRAM. This key is typically used to protect attestation keys like EPID or EK that cannot be stored in SKS, which supports only AES or HMAC key type.
3. Suspend Key – this key is used to generate one-time keys that would allow to save and restore CSME Firmware context while CSME enters Power Gating or when platform goes into standby on client system only. This key is critical to guarantee CSME execution integrity upon resume.
4. Intel Root Key – this key is the master key for the CSME firmware. For example, it is used to generate storage keys that would protect CSME data in NVM.
5. IVB Root Key – this key is used to protect the Integrity Protection Key (IPK) and the CSME Firmware modules' ICVs (Integrity Check Value calculated using IPK and Crypto Hardware accelerator AES-Paging engine over CSME Firmware module's 4KB pages) in NVM. The ICVs allow faster boot of CSME Firmware and to securely page out and page in CSME code and data from CSME SRAM to SPI flash/DRAM. IPK and ICV are invalidated upon CSME Firmware update or an ICV integrity failure. This key is critical to guarantee CSME execution integrity during boot and runtime.
6. Provisioning Key – this key is used by the CSME Firmware to retrieve a new EPID private key from Intel server when a TCB Recovery is required, because the CSME EPID attestation key has been compromised. The Provisioning Key is based on CSME Firmware SVN. The usage of this key is relevant only when the SVN is greater than 1.
7. PTT EK Root Key – this key would be exported by CSME ROM, encrypted with Memory Guard key, and used by Intel PTT to generate its Endorsement Key using the PTT EK counters also exported by CSME ROM to Intel PTT.

Once the CSME ROM generates all keys, it will zero and lock the Chipset Key and the Fuse Encryption Hardware Key before executing CSME Firmware. This is done to ensure these two keys cannot be used outside the CSME Firmware.

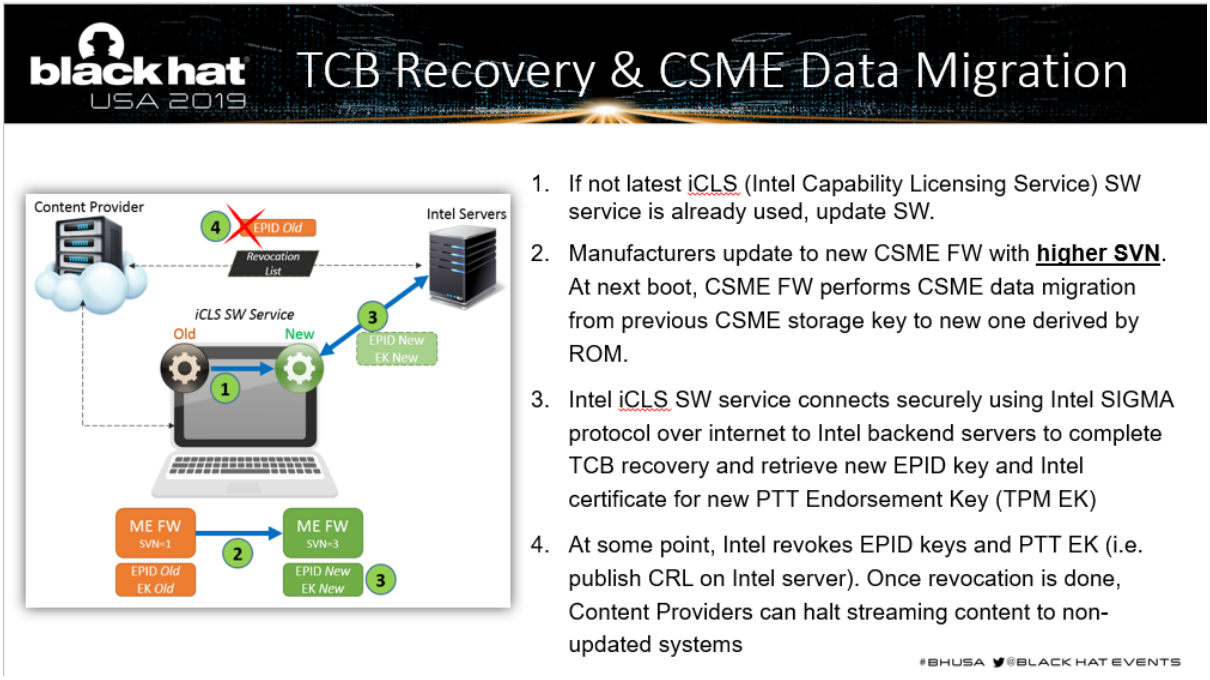
As shown above, CSME execution integrity and data security rely on the chipset key and keys created from it by the CSME ROM.

The EPID Private Key

The KGF is responsible for generating all CSME EPID private keys, group public keys, and associated certificates. During Intel manufacturing of the PCH or SoC, the CSME is provisioned with its unique EPID private key encrypted with the Family Fuse Encryption Key and the EPID group ID.

At CSME boot, the EPID private key is decrypted by the CSME ROM and exported to the CSME Firmware, where the key is managed by the SIGMA module. Then, PAVP, DAL, and PTT can utilize the SIGMA protocol to prove to a server (i.e., content provider) they are running inside a genuine CSME Firmware. The EPID private key is used to generate an EPID signature to prove membership in an EPID group to a verifier (i.e., content provider server). The verifier authenticates a member (the CSME Firmware) by checking the member's signature with the group certificate.

If EPID private key is compromised, then the CSME Firmware can be potentially impersonated, and verifiers' ability to guarantee that they are communicating with a genuine CSME Firmware is compromised. In such a scenario, new EPID private keys can be issued, and the compromised EPID private key or its associated EPID group can be revoked by Intel. This procedure is called TCB recovery and has coincided with the mitigation of a particular vulnerability undermining the CSME Firmware TCB or exposing the EPID private key itself. Examples include those vulnerabilities documented in Intel-SA-00086 (CVE-2017-5705, CVE-2017-5706, and CVE-2017-5707). The figure hereafter highlights the steps required to successfully complete the TCB recovery.



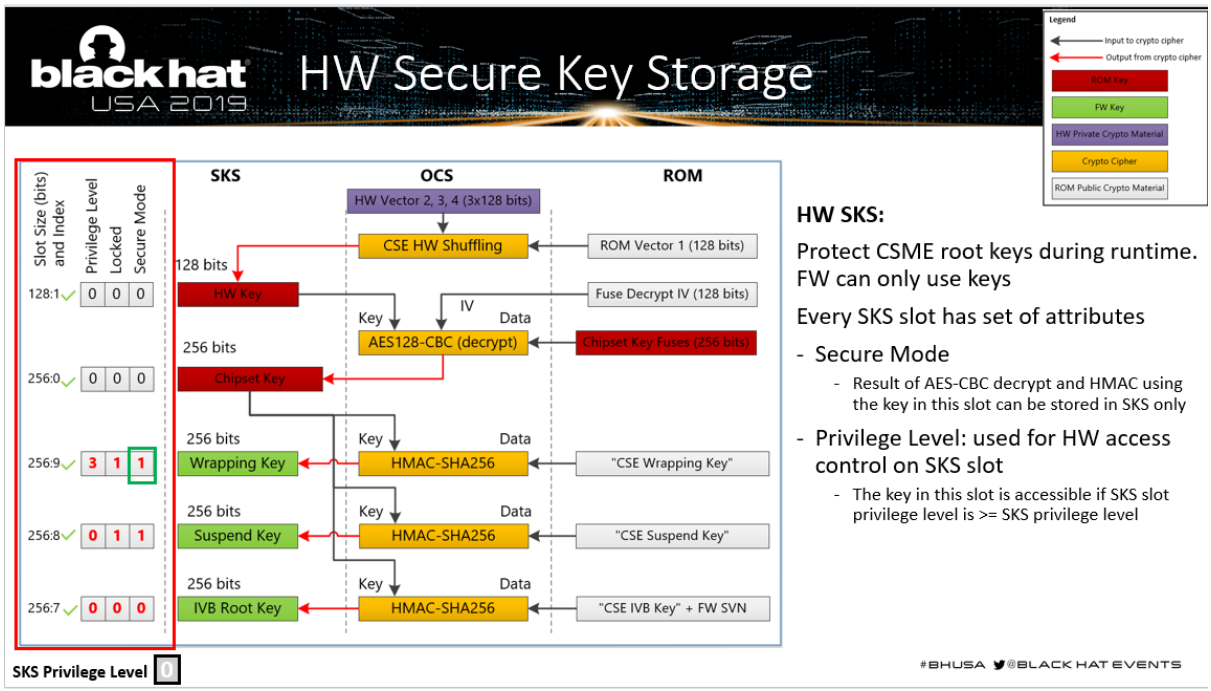
KGF will have to generate new EPID private keys and send them to Intel server. Intel server will deliver the new EPID private key only to the new CSME Firmware with higher SVN. This is achieved

by using the Provisioning Key generated by ROM using the CSME Firmware SVN as explained in previous section. It is important to note that if the CSME ROM is also compromised, then TCB recovery cannot be done securely anymore.

Usage of Secure Key Storage (SKS) Hardware

The CSME ROM also uses the SKS Hardware to protect keys from potential leakage from CSME SRAM, while CSME Firmware runs, and to ensure CSME Firmware can use keys without knowing their actual plaintext values. Note, the CSME ROM cannot make use of an SKS slot with secure mode set for the Fuse Encryption Key and Chipset Key for the following reasons:

1. The EPID private key stored in fuse is not an AES or HMAC key and, as a result, cannot be loaded in SKS. Therefore, the key needs to be decrypted using the Fuse Encryption Hardware Key in CSME SRAM where it gets wrapped by CSME ROM with Memory Guard Key before it gets exported to CSME Firmware.
2. The chipset key is also used to generate an EPID random value that would be used by the CSME Firmware to generate the final EPID private key using the EPID private key. The EPID random value is also wrapped by CSME ROM with Memory Guard Key before it gets exported to CSME Firmware.



Impact of CVE per of Client/Server system

This table lists client systems for CSME and Intel® Converged Security Engine (CSE):

CSME & CSE Version	PCH/SOC	Platform code name	CVE-2019-0090	CVE-2017-5705 CVE-2017-5707	CVE-2020-0566
CSME 15	TGP	Tigerlake	Not affected	Not affected	Not affected
CSME 13.30	LKF	Lakefield	Not affected	Not affected	Not affected
CSE 13.50	JSL-N	Jasperlake	Not affected	Not affected	Not affected

CSME 14.5	CMP-V	Cometlake-V	Not affected	Not affected	Not affected
CSME 14	CMP	Cometlake	Not affected	Not affected	Not affected
CSME 13	ICP	Icelake	Not affected	Not affected	Not affected
CSME 12	CNP	Cannonlake Coffeelake Whiskeylake Mehlow Workstation	Affected	Not affected	Not affected
CSE 4	GLK	Geminilake	Affected	Not affected	Affected
CSE 3	BXT-P	Apollolake Gordon Peak	Affected	Affected	Affected
CSME 11	SPT KBP LBG	Skylake & Amberlake Kabylake & Basin/Glacier Falls Purley Workstation	Affected	Affected	Not affected

This table lists server systems for SPS Firmware and Intel® Advanced Driver Assistance Systems (ADAS) Management Engine Firmware:

SPS / ADAS Version	PCH/SOC	Platform code name	CVE-2019-0090	CVE-2017-5706
SPS E3_06.00	TGP-H	Tatlow	Not affected	Not affected
SPS E5_06.00	EBG	Eaglestream	Not affected	Not affected
SPS SoC-X_05.00	CDF	Idaville	Not affected	Not affected
SPS SoC-A_05.00	CDF	Jacobsville	Not affected	Not affected
SPS E3_05.00 **SPS E3_05.01**	CNP-H	Mehlow Mehlow Refresh	Affected	Not affected
SPS E5_04.04	LBG-R	Whitley	Not affected	Not affected
ADAS_ME_54	DNV-AD	Carlake	Not affected*	Not affected
SPS SoC-X_04.00	SKL-D	Bakerville	Affected	Affected
SPS SoC-A_04.00	DNV	Harrisonville	Affected	Affected
SPS E3_04.00 **SPS E3_04.01** **SPS E3_04.08**	SPT-H	Greenlow Greenlow Refresh Montevista	Affected	Affected
SPS E5_04.00 **SPS E5_04.01**	LBG	Purley Purley Refresh	Affected	Affected

*CVE-2019-0090 exists in SoC/PCH, however there is no path for exploitation as of today.

**None of the systems listed in this table are affected by CVE-2020-0566