Faille Intel : des processeurs sans défense ?

Mark Ermolov, Dmitry Sklyarov et Maxim Goryachy ont-ils trouvé la « faille ultime » dans les processeurs Intel ?

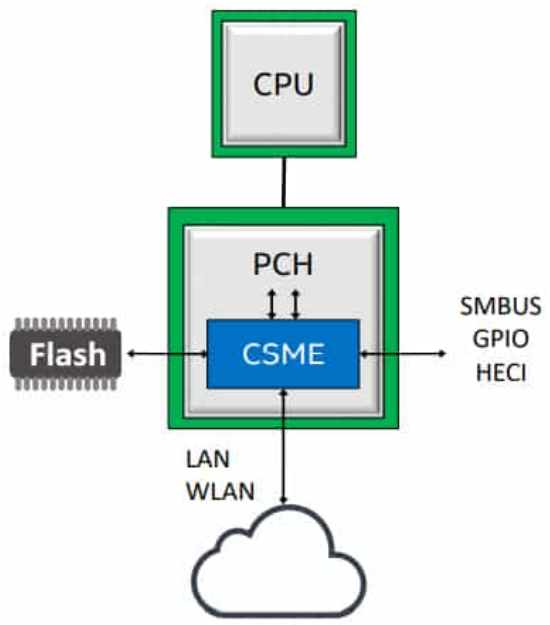
Le groupe américain les remercie, dans son bulletin de sécurité SA-00213, de lui avoir signalé la faille en question.

Leurs noms ne sont mentionnés que depuis quelques semaines, alors même que la publication du bulletin remonte à mai 2019.

La vulnérabilité (CVE-2019-0090) semble avoir fait l'objet d'un embargo à la hauteur de la menace qu'elle paraît représenter. Tout du moins au regard de la description qu'en font les trois chercheurs.

> *So, as Intel dropped embargo, now we can say: the Intel CSME boot ROM bug exists in all their chipsets and SoCs having x86 CSME MCU (except Ice Point and Comet Point).*
> *Let's find it together: pic.twitter.com/nPNHIWkrDi*
>
> *— Mark Ermolov (@_markel___) February 11, 2020*

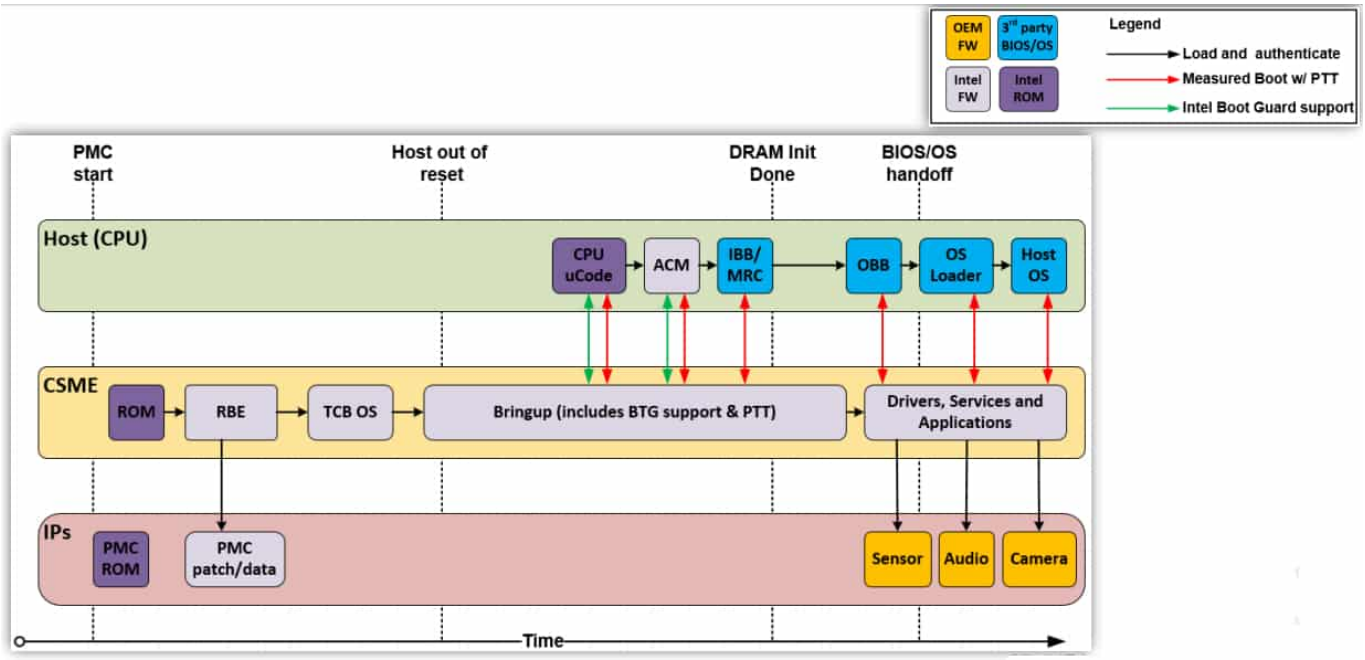
La quasi-totalité des *chipsets* et SoC Intel actuellement commercialisés sont touchés.



Le danger est d'autant plus grand que la faille ne peut être corrigée par une mise à jour : elle est codée « en dur » dans la ROM de masque du CSME (Converged Security and Management Engine).

Ce dernier est intégré dans la puce PCH (Platform Controlled Hub). Il fait office de racine de confiance pour l'ensemble de la plate-forme Intel.

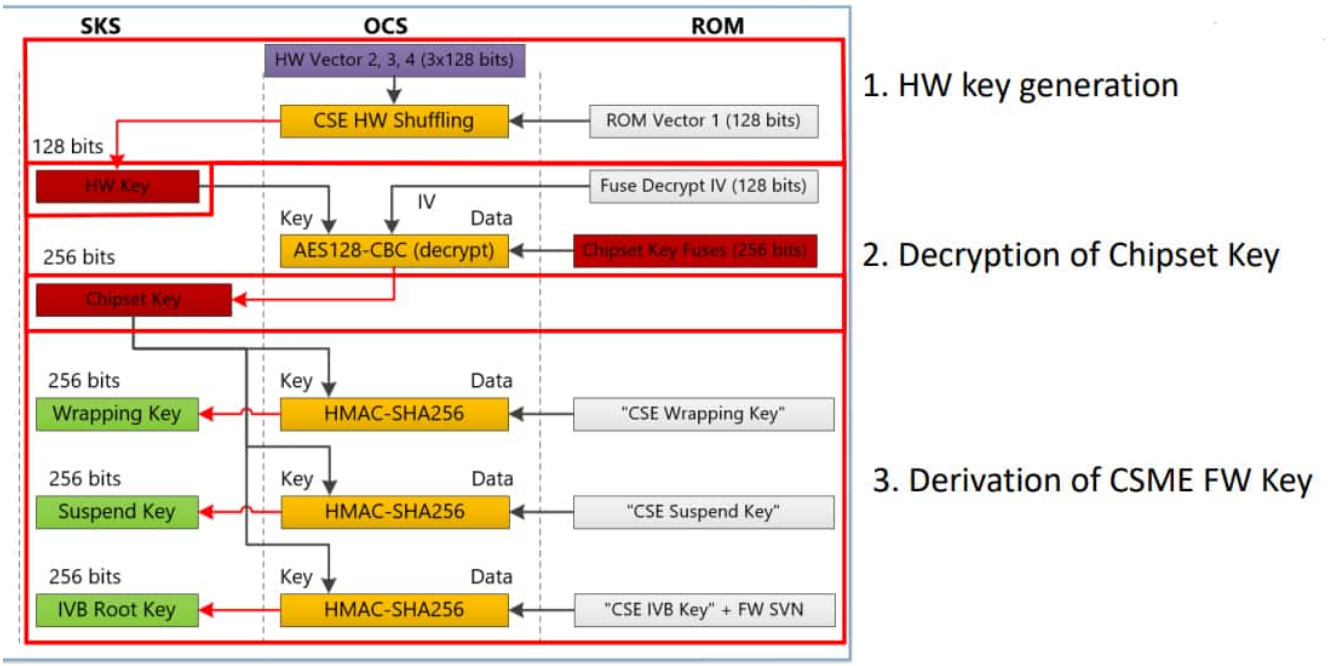
Au démarrage de la plate-forme, il vérifie l'authenticité de différents composants : UEFI/BIOS, *firmware* du gestionnaire d'alimentation…



Les clés du CSME

Le CSME sert également de base cryptographique pour diverses fonctions de sécurité.
Il implémente notamment EPID (Enhanced Privacy ID), algorithme destiné à authentifier – de manière anonyme – des systèmes de confiance. Mais aussi les TPM (Trusted Platform Module) logiciels, pour le stockage de données sensibles.

Intel a fait en sorte que la compromission d'un module du CSME ne mette pas en danger la clé maîtresse du *chipset*.
Preuve en fut d'une vulnérabilité d'exécution distante de code trouvée en 2017 dans le module d'initialisation *hardware* BringUp. Il a suffi à Intel d'utiliser le mécanisme SVN (Security Version Number) pour générer de nouvelles clés.



La faille CVE-2019-0090 pose toutefois un souci : elle permet de lire la clé maîtresse tout en contrôlant la création des autres clés.

Parmi ces autres clés, l'une permet de modifier le code de tout module du CSME sans que cela soit détecté.

Dans l'absolu, il existe un rempart : la clé maîtresse, logée dans une ROM en lecture seule, est elle-même chiffrée par une clé *hardware* (cf. schéma ci-dessus).

Problème : la faille s'enclenche à un stade suffisamment précoce pour permettre d'extraire cette clé *hardware*. Ermolov et al. estiment qu'il ne faudra pas longtemps pour que quelqu'un y parvienne.

Les clés *hardware* ne sont pas spécifiques à chaque système. Elles sont partagées entre plusieurs générations de *chipsets*. En combinaison avec EPID, leur fuite pourrait avoir de lourdes conséquences, estiment les chercheurs. Entre autres, un déchiffrement massif de disques durs.

Du côté d'Intel, on assure qu'il faut mettre en œuvre « des moyens considérables » pour pouvoir exploiter la faille.

Illustrations issues d'une présentation Intel réalisée à la Black Hat USA 2019