TPM-FAIL : des racines de confiance pas si sécurisées

Les TPM, même certifiés, ne sont pas sans faille.

L'un des derniers bulletins de sécurité d'Intel (SA-00241, mis en ligne ce 12 novembre 2019) le rappelle. Tout comme un avertissement (ADV190024) que Microsoft a émis le même jour*.

Ces deux alertes couvrent autant de vulnérabilités, détaillées dans un rapport (PDF, 17 pages) que quatre chercheurs viennent de rendre public.

Leur expérimentation s'est portée sur des TPM issus de quatre fournisseurs : Intel, STMicro, Infineon et Nuvoton.

Machine	CPU	Vendor	TPM	Firmware/Bios	ECDSA (Cycle)	RSA (Cycle)
NUC 8i7HNK	Core i7-8705G	Intel	PTT (fTPM)	NUC BIOS 0053	4.1e8	7.0e8
NUC 7i3BNK	Core i3-7100U	Intel	PTT (fTPM)	NUC BIOS 0076	3.2e8	5.4e8
Asus GL502VM	Core i7-6700HQ	Intel	PTT (fTPM)	Latest OEM	3.5e8	5.9e8
Asus K501UW	Core i7 6500U	Intel	PTT (fTPM)	Latest OEM	3.4e8	5.8e8
Dell XPS 8920	Core i7-7700	Intel	PTT (fTPM)	Dell BIOS 1.0.4	4.7e8	8.0e8
Dell Precision 5510	Core i5-6440HQ	Nuvoton	rls NPCT	NTC 1.3.2.8	4.9e8	1.8e9
Lenovo T580	Core i7-8650U	STMicro	ST33TPHF2ESPI	STMicro 73.04	8.7e7	9.2e8
NUC 7i7DNKE	Core i7-8650U	Infineon	SLB 9670	NUC BIOS 0062	1.4e8	5.1e8

Ces TPM (Trusted Platform Module) constituent chacun une « racine de confiance » sur laquelle un terminal informatique peut s'appuyer pour réaliser des opérations critiques. Ce en générant des signatures cryptographiques.

La clé est dans l'observation

Les failles en question (CVE-2019-11090 et CVE-2019-16863) touchent respectivement des implémentations de STMicro et d'Intel.
La première de ces implémentations exploite une puce à part entière, séparée du CPU. La seconde met en œuvre un TPM « logiciel » qui implique un microcontrôleur x86 32 bits.

Dans l'un et l'autre cas, il est possible de reconstituer les clés dont découlent les signatures cryptographiques. La technique : observer le temps d'exécution des opérations liées à la création desdites signatures.

Sur un poste de travail Linux équipé d'un TPM Intel, les chercheurs ont mis moins de 2 minutes (1 300 mesures) pour arriver à leurs fins. Il leur a fallu environ 40 000 mesures pour faire de même sur un autre poste de travail Linux avec un TPM STMicro.
Les tests avec le TPM Intel se sont aussi révélés concluants à distance, sur un serveur VPN StrongSwan mis en œuvre à l'échelle d'un LAN (il a fallu 5 heures pour récupérer la clé).

Une méthodologie à revoir ?

La certification Common Criteria, censée attester la robustesse des TPM, inclut des mesures de détection des signaux « physiques » susceptibles de révéler des clés. Le temps d'exécution des opérations en est un. La consommation énergétique et le rayonnement électromagnétique en sont d'autres.

Au vu de leurs découvertes, les chercheurs suggèrent de réviser le processus d'évaluation Common Criteria. D'autant plus que les puces vulnérables bénéficient du plus haut niveau de certification (EAL 4+).

Intel a mis à jour le firmware sur lequel repose son TPM. STMicro a pour sa part lancé une nouvelle puce dont la résistance est confirmée en date du 12 septembre 2019.
À noter que les puces Infineon et Nuvoton testées présentent elles aussi des signaux physiques, mais non constants.

** Microsoft précise que Windows n'utilise pas l'algorithme de création de signatures vulnérable sur les puces STMicro.*

Photo d'illustration © Pavel Ignatov – Shutterstock.com