Une atteinte à la liberté des utilisateurs d'ordinateurs

Extraits traduits et commentés d'un article de la Free Software Fundation :

The Intel Management Engine: an attack on computer users' freedom (Lien vers l'original)

« Intel Management Engine : une atteinte à la liberté des utilisateurs d'ordinateurs »

Avec des problèmes de sécurité tels que la vulnérabilité de « Spectre » et « Meltdown[1] » découverte dans les puces Intel au début de 2018, il est devenu plus important que jamais de parler de la nécessité d'utiliser des logiciels libres dans ces technologies hautement verrouillées.

Le moteur de gestion Intel est un outil (microcontrôleur embarqué exécutant un système d'exploitation micronoyau léger) fourni avec certains chipsets[2] Intel, et censé faciliter le travail des administrateurs système[3]. Il constitue en réalité une restriction supplémentaire (comme les licences propriétaires et les brevets) aux libertés des utilisateurs, restriction imposée par une entreprise (fabricant de votre processeur), et utilisée pour contrôler votre informatique.

Le Management Engine[4], non contrôlable par l'utilisateur (il démarre avant le système d'exploitation) contraint à l'exécution de logiciels non libres intégrés à cet OS qui ne peuvent être modifiés ou remplacés que par Intel (le chemin d'accès est très particulier). Il s'agit d'une atteinte à la liberté, la vie privée et la sécurité des utilisateurs d'ordinateurs.

Le Management Engine a commencé à apparaître sur les ordinateurs Intel vers 2007[5].

Au départ, il a été conçu pour aider les administrateurs système à gérer à distance les ordinateurs[6], et a été présenté comme une fonctionnalité informatique pour les clients professionnels. Il pourrait, par exemple, être utilisé à distance pour :

---

1 https://www.zdnet.fr/actualites/meltdown-et-spectre-intel-promet-des-correctifs-rapidement-39862256.htm

Meltdown présente une faille exclusive à Intel ; elle permet une élévation de privilège autorisant l'accès à des ressources mémoires protégées au niveau du noyau du système d'exploitation ; elle peut ainsi permettre à un attaquant d'accéder à des données confidentielles stockées sur la machine, telles que des mots de passe ou identifiants d'accès …

La faille propre à Spectre n'est pas exclusive à Intel et touche d'autres constructeurs ; elle permet à un programme d'accéder aux espaces mémoires d'un autre programme et donc de récupérer des informations confidentielles.

2 Définition Wikipédia : « ... jeu de composants électroniques inclus dans un circuit intégré préprogrammé, permettant de gérer les flux de données numériques entre le ou les processeur(s), la mémoire et les périphériques ».

3 Il est présenté comme ceci par intel : « Les caractéristiques incluent (mais ne sont pas limitées à) :
- Services de gestion de faible puissance, hors bande (OOB)
- Service de licences de capacité (CLS)
- Protection antivol
- Chemin audio vidéo protégé (PAVP) » ;

vous noterez bien le « (mais ne sont pas limitées à) ».

4 Encore appelé SPS (Server Platform Services) sur certains serveurs, et TXE (Trusted Execution Engine) sur certains mobiles et certains appareils de faible puissance.

5 Pour plus d'informations sur l(histoire du Management Engine, cf pages 27, 28, 29 du livre (en anglais) de 2014 : Platform Embedded Security Technology Revealed, by Xiaoyu Ruan (ISBN 978-1-4302-6571-9), at Springer.

6 La gestion à distance peut se faire à travers une application tournant à l'intérieur du Management Engine. Il existe différentes applications pour cela, la plus connue étant AMT (Active Management Technology).

-Mettre en route et éteindre les ordinateurs.

-Démarrer les ordinateurs à partir d'un stockage distant situé sur la machine de l'administrateur système ou sur un serveur, et prendre ainsi le contrôle de l'ordinateur[7].

-Récupérer et stocker divers numéros de série qui identifient le matériel informatique.

Au fil du temps, Intel a imposé le moteur de gestion sur tous les ordinateurs Intel, supprimé la possibilité pour les utilisateurs et les fabricants d'ordinateurs de le désactiver et a étendu son contrôle sur l'ordinateur à près de 100 % (il a même accès aux données en mémoire RAM).

Il constitue un environnement informatique distinct refusant à l'utilisateur le contrôle complet de son ordinateur. Il peut même exécuter des applications gérant des restrictions numériques (DRM)[8]. Cf « Defective by Design » pour savoir en quoi les DRM sont restrictifs.

L'administration à distance s'effectue via des applications s'exécutant à l'intérieur du moteur de gestion, telles que AMT (Active Management Technology)[9]. AMT donne aux administrateurs système distants le même contrôle qu'ils auraient s'ils étaient assis devant l'ordinateur[10]. AMT peut également contrôler les interfaces Intel Ethernet et les cartes WiFi pour filtrer ou empêcher le trafic réseau d'entrer ou de sortir de l'ordinateur[11].

Intel est allé jusqu'à utiliser un système d'exploitation libre (base Minix) et à le convertir en logiciel non libre pour attaquer la liberté de ses utilisateurs : en effet la licence[12] du système d'exploitation qu'il utilise ne donne pas aux utilisateurs de droits sur le code source (droit qu'on a habituellement sous une licence libre), ni ne garanti le droit aux utilisateurs d'exécuter des versions modifiées de ce code sur le moteur de gestion.

---

7 Cette fonctionnalité est une partie de « AMT » et est connue comme redirection « SOL/IDE ».

8 Pour plus d'informations sur Digital Restrictions Management et sur le Management Engine, cf de la page 191 jusqu'à la fin du chap 8 (Hardware-Based Content Protection Technology) du livre Platform Embedded Security Technology Revealed, by Xiaoyu Ruan (ISBN 978-1-4302-6571-9) at Springer.
Ce chapitre tente de justifier le recours à la « Gestion des restrictions numériques » (DRM). Cette DRM est totalement inacceptable en déniant aux utilisateurs le contrôle de leurs ordinateurs pour les empêcher d'exercer leurs droits légaux (comme un usage normal ou la possibilité de copier des travaux publiés). Ce chapitre montre clairement le lien entre le dénie aux utilisateur du plein contrôle de leur matériel et une DRM efficace.
La campagne de la Free Software Fundation « Defective by Design » a des ressources pour agir contre les DRM.

9 AMT est souvent disponible sur les ordinateurs Intel conçus pour les clients « hommes d'affaires » et pas sur les machines destinées aux clients « standard ». Quand il est disponible, les réglages BIOS ou UEFI sont souvent sur « off », mais comme ces machines sont équipées de logiciels non-libres, il n'y a pas vraiment moyen de savoir ce que ces réglages font réellement, ou de connaître les effets d'une mise sur « on » ou sur « off » de AMT.

10 Cette fonctionnalité est une partie de AMT et est appelée System Defense. Pour plus de détails sur ceci, cf « Intel's System Defense description and Intel's documentation on how it works ».

11 Pour réaliser cela, Intel utilise VNC (Virtual Network Computing), un protocole standard pour gérer à distance les ordinateurs, en pilotant le clavier, la souris et l'affichage par le réseau internet. Plusieurs logiciels libres mettant en œuvre des protocoles similaires peuvent faire la même chose ; on les trouvera dans le « free software directory ».

12 Dans le cas évoqué ici, Intel vient de commencer à utiliser Minix, un logiciel d'exploitation libre publié sous différentes licences BSD ; les licences BSD sont des licences de logiciels libres « faibles », qui n'empêchent pas les logiciels d'être utilisés à l'encontre des utilisateurs (en supprimant les libertés incluses à la base).

Certaines parties de Minix sont publiées sous la licence BSD d'origine ou sous des versions modifiées. Cette façon de procéder rend impossible la combinaison de tels logiciels avec d'autres sous licence GNU GPL. Pour éviter cela, il est préférable de choisir d'autres licences « faibles » comme expliqué dans cet article sur la licence BSD modifiée (https://www.gnu.org/licenses/license-list.html#ModifiedBSD).

Nous pourrions corriger tous ces problèmes si les utilisateurs étaient en mesure d'exécuter des logiciels entièrement gratuits sur ce moteur de gestion, ou au moins avaient la possibilité de faire qu'il n'exécute aucun code, en le désactivant complètement, mais cela est impossible car le moteur de gestion n'exécutera que du code signé cryptographiquement par Intel[13]. Cela signifie qu'à moins que quelqu'un ne trouve une faille dans le matériel, permettant aux utilisateurs [administrateurs] de contourner la vérification de signature, on se voit effectivement refuser la possibilité d'installer le logiciel que l'on souhaite dans le moteur de gestion.

Par ailleurs, pour éviter que les systèmes d'exploitation libres ne soient détournés (comme Minix) en un instrument rendant l'attaque de la liberté des utilisateurs moins chère et plus facile, il est important d'octroyer une licence à leurs composants (sous la GNU GPLv3 ou ultérieure) chaque fois que possible. Cela maintiendra le logiciel libre et interdira aux fabricants de matériel de refuser aux utilisateurs la possibilité d'exécuter des versions modifiées du logiciel.

Découvrez comment choisir une licence pour votre propre travail, afin d'en savoir plus sur les meilleures stratégies d'octroi de licences pour maximiser la liberté des utilisateurs, et dans quels cas des licences autres que la GPLv3 pourraient convenir (https://www.gnu.org/licenses/license-recommendations.html).

Malgré tous les efforts d'Intel pour rendre le moteur de gestion incontournable, des développeurs de logiciels ont réussi à l'empêcher de charger du code ; par exemple, le projet Libreboot désactive le Management Engine en supprimant tout le code qu'il est censé charger sur certains ordinateurs Thinkpad fabriqués en 2008, notamment les R400, T400, T400, T500, W500, X200, X200 et X200T ;

Pour information, de nombreux ordinateurs Intel fabriqués en 2006 ont l'ancêtre du « Management Engine » (désactivé dès le départ), comme les Lenovo Thinkpads X60, X60s, X60 Tablet et T60, et bien d'autres.

En conclusion :

Le « Management Engine » d'Intel (ME) et le « Platform Security Processor » d'AMD (PSP) représentent l'une des pires menaces qui planent sur la sécurité de vos données. Il s'agit d'un système embarqué totalement autonome, niché au cœur même du processeur (chez AMD) ou du chipset (chez Intel). Il est constitué d'un microcontrôleur et d'un **système d'exploitation complet associé (base Minix)**. Il est opérationnel en permanence même quand votre PC est éteint mais relié à EDF (les portables étant toujours alimentés par batteries). Il dispose d'un accès complet à l'intégralité des données qui circulent partout, du CPU jusqu'au framebuffer de la carte graphique en passant par les ports Ethernet ou l'intégralité de la mémoire. Il peut aussi envoyer tous vos petits secrets à quiconque dans votre dos. Le ME sait tout, et de manière invisible pour n'importe quel logiciel qui tourne sur le PC. Même les plus paranoïaques ne peuvent rien lui cacher. Le firmware du ME est mis à jour avec le BIOS. Le ME est évidement impossible à désactiver pour le commun des mortels. Les patchs de BIOS sont disponibles mais rarement mis à jour.

Quelques exemples de failles :
https://www.hardware.fr/news/15102/faille-critique-intel-amt.html

https://www.hardware.fr/news/15297/nouvelle-faille-securite-intel-me.html

13 Cf « intelmetool », un utilitaire pour signaler l'état du Management Engine status ; (https://github.com/zamaudio/intelmetool).

https://blogmotion.fr/internet/securite/importante-faille-de-securite-intel-amt-cve-2017-5689-15938

https://www.touslesdrivers.com/index.php?v_page=3&v_code=6843

Pour en savoir techniquement plus :
https://github.com/platomav/MEAnalyzer

https://github.com/chip-red-pill/IntelTXE-PoC

https://github.com/ptresearch

Désactivation ? : « ... it is possible to partially disable one potentially bad component ...» cf :
https://thinkpenguin.com/gnu-linux/penguin-pro-11-gnu-linux-desktop

For more information on the Intel Management Engine, see:

Intel & ME, and why we should get rid of ME
"Active Management Technology": The obscure remote control in some Intel hardware
https://www.fsf.org/blogs/licensing/intel-me-and-why-we-should-get-rid-of-me