Note numéro 32
janvier 2018

Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

Les failles *Meltdown* et *Spectre*

Thomas Fressin (CREOGN)
Cyril Nalpas (Compagnie Européenne d'Intelligence Stratégique)
Marc Watin-Augouard (CREOGN)

Les chercheurs du programme *Project Zero* de Google, dont la mission est de trouver des vulnérabilités « zero-day »[1], ont révélé, le 3 janvier 2018[2], avoir découvert deux nouvelles failles, dénommées *Meltdown* et *Spectre*. Ces divulgations, largement reprises par la presse et les sites spécialisés en informatique, ont de quoi alarmer.

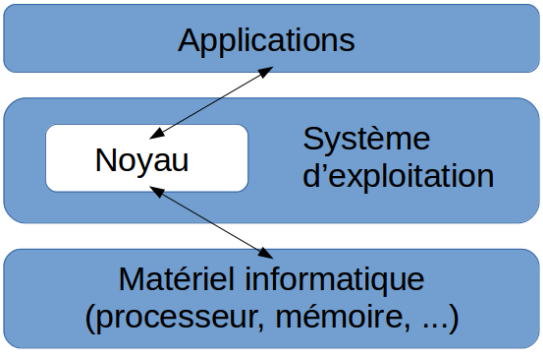
En effet, il ne s'agit pas ici d'erreurs de programmation (où les correctifs logiciels sont faciles à appliquer) mais de vulnérabilités majeures liées aux caractéristiques des microprocesseurs (ce qui est complexe à corriger). Au final, le risque encouru par ces deux failles est simple : la prise de contrôle du matériel par l'attaquant et donc l'accès aux logiciels de la victime, ainsi qu'à la lecture, la modification et la suppression de ses données.

En cause, les microprocesseurs Intel (pour *Meltdown* et *Spectre*) mais aussi ceux des concurrents AMD et ARM (pour *Spectre* uniquement). Et ces puces, utilisées par des particuliers, des administrations ou encore des entreprises, équipent de très nombreux appareils (smartphones, ordinateurs, tablettes, serveurs, etc.), ce qui montre l'ampleur de la vulnérabilité.

Rappelons qu'un microprocesseur permet de traiter des données en temps réel et d'exécuter les instructions que les programmes donnent aux machines. Si l'attaquant peut exécuter un programme sur le système ciblé, via une *exécution spéculative*[3] cumulée à une *prédication de branchement*[4] (pour *Spectre*) ou une *élévation de privilège*[5] (pour *Meltdown*), il est désormais mis en avant qu'il lui est alors possible d'accéder à la mémoire du *noyau*[6] (pour *Meltdown*) ou du processeur (pour *Spectre*), et donc d'accéder à des données considérées en principe comme protégées.

1 Vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.
2 *Reading privileged memory with a side-channel.* Jann Horn, Project Zero, 3 janvier 2018 : https://goo.gl/Vyp7jt Consulté le 11 janvier 2018.
3 Lancement anticipé d'une instruction, c'est-à-dire sans être certain que celle-ci ait réellement besoin d'être exécutée.
4 Fonctionnalité d'un processeur qui lui permet de prédire le résultat d'un branchement et de rendre l'utilisation de sa chaîne de traitement (*pipeline*) plus efficace.
5 Mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement. Cela est utilisé pour lancer des processus sensibles et attaquer un système en vue de prendre son contrôle.
6 Système gérant les ressources de l'ordinateur et permet aux différents composants — matériels et logiciels — de communiquer entre eux.

Tous les systèmes d'exploitation, intermédiaires entre le microprocesseur et les applications, sont donc concernés. Les deux formes d'attaque qui pourraient en découler permettraient de contourner les protections des données et donc d'y accéder pour les extraire.



Parmi ces données récupérables : les mots de passe, les identifiants, les données bancaires, *etc*. Sauf à mettre en place de nouvelles puces, ce qui n'est pas pour demain, seules des solutions de contournement sont envisageables, au risque de perdre en performance.

Après les logiciels malveillants *Wannacry*[7] et *Adylkuzz*[8] en mai 2017 , puis *NotPetya*[9] en juin 2017, *Meltdown* et *Spectre* révèlent, en janvier 2018, la grande fragilité de l'espace numérique hyperconnecté. En l'espèce, les processeurs n'ont pas été sécurisés dès leur conception (*by design*). En effet, les fabricants de processeurs ont longtemps privilégié la vitesse à la sécurité et leur responsabilité est aujourd'hui susceptible de se trouver engagée.

Si le commun des utilisateurs a un risque relatif de se faire attaquer son appareil informatique par ces failles, les hébergeurs informatiques du *cloud*[10] sont eux directement concernés, d'autant plus que le cloisonnement des machines virtuelles, clé de leur modèle économique, est désormais remis en question. De plus, dans le cadre de la correction de ces failles, l'impact sur les performances et donc le coût de ce colmatage les impactera. Octave Klaba, fondateur de l'hébergeur OVH et passé maître en communication de crise informatique, explique en temps réel, sur son compte Twitter[11], comment OVH gère cette situation, ce qui montre qu'au plus haut niveau les risques sont pris en compte.

Pour finir, signalons que certains spécialistes nuancent la gravité de la situation de ces failles. Ryan Kalember, Senior Vice-Président Cybersecurité Stratégie, spécialiste Proofpoint, rappelle, par exemple, que pour « exploiter ces deux failles, un cybercriminel doit en effet être capable d'exécuter leur code directement sur le terminal visé » et « que ces failles ont heureusement été découvertes et révélées de manière responsable par des chercheurs reconnus, au lieu d'être exploitées dans une virulente attaque à très grande échelle. »[12]

7 Rançongiciel (*ransomware*) auto-répliquant ayant touché plus de 300 000 ordinateurs en mai 2017.
8 Logiciel malveillant qui mine une crypto-monnaie, le monero, en utilisant les ressources de la machine infectée. Les gains ainsi générés sont ensuite reversés anonymement à des comptes. Le chiffre du million de dollar de bénéfice pour les pirates a été avancé.
9 Logiciel malevaillant de type *wiper* – qui détruit les données – apparu en juin 2017.
10 Le *cloud* (informatique en nuage) est un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire.
11 https://twitter.com/olesovhcom
12 Kalember, Ryan. *Meltdown & spectre : de la gravité des failles qui restent à nuancer*. Globb Security France : https://goo.gl/CX6Hzh. Consulté le 12 janvier 2018.