Compte-rendu de réunion

Référence RéSIST/2012-01

17 janvier 2012

Table des matières

1 Attaque DMA entre pairs et contre-mesures

La première présentation a été faite par M. Fernand Lone-Sang, du Laas-CNRS (www.laas.fr).
Support de la présentation : www.ossir.org/resist/supports/cr/2012/2012-01-17/F_Lone_Sang.pdf.

M. Lone-Sang a commencé par un rappel général quant à la sécurité d'un système d'informations (au sens large du terme). La surface d'attaque possible a tendance à augmenter, notamment via de nouveaux vecteurs. S'il s'agit d'attaques visant du logiciel, il existe de nombreuses protections qui, bien que parfois imparfaites, ont le mérite d'exister. Le domaines des attaques visant le matériel est nettement moins étudié (même s'il n'est pas vierge).

L'une des explications à cette situation est qu'une attaque matérielle est, par nature, très liée au matériel. De ce fait, elle peut se révéler inefficace sur des matériels très proches mais pour lesquels un composant interne diffère.

Le DMA, pour *Direct Memory Access*, est un mécanisme d'entrées-sorties permettant à un contrôleur d'exécuter des transferts de données sans avoir à gérer le processus de transfert. Les contrôleurs réseau, Wifi, disque ou graphique utilisent beaucoup ce mécanisme.

Une architecture de type PC est généralement composée de deux puces distinctes [1] :

passerelle nord (ou North Bridge) : pour les contrôleurs rapides (cartes graphiques)

1. Même si les architectures actuelles tendent à intégrer la passerelle nord au processeur, cette distinction entre passerelle nord/sud reste valide.

Rédigé par Pierre-Yves Bonnetain -– pyb@ba-consultants.fr
ReSIST -– http://www.ossir.org/resist
Comptes-rendus -– http://www.ossir.org/resist/supports/index.htm

passerelle sud (South Bridge) : pour les contrôleurs lents (disques, USB)

L'attaque DMA la plus classique est une escalade du contrôleur vers la mémoire centrale, et de là vers le noyau système. Cependant, il existe une autre possibilité, d'un contrôleur vers un autre contrôleur. C'est de cette seconde notion que vient l'expression d'« attaque entre pairs ».

Quelques résultats expérimentaux reposent sur l'utilisation du contrôleur FireWire comme source des attaques. Ce contrôleur peut être sur la passerelle nord ou sud, en PCI ou PCI Express. L'équipe projet a réalisé différents tests afin d'évaluer les possibilités d'attaque entre pairs à partir d'un tel contrôleur. Les résultats varient grandement selon les architectures matérielles (puce utilisée et types de passerelles nord/sud).

M. Lone-Sang a présenté une preuve de concept qui, au travers du contrôleur FireWire, permet d'accéder en lecture à la carte graphique et donc au contenu de l'écran. Cette preuve de concept montre qu'il est possible d'« intercepter » tout l'affichage [2].

Après cette démonstration, la présentation a abordé les contre-mesures. Deux grandes possibilités apparaissent :

via l'IOMMU L'*I/O Memory Management Unit* est un composant de gestion de la mémoire dédié aux contrôleurs d'entrées-sorties. Ce composant peut, entre autres, filtrer et/ou bloquer des accès considérés comme non légitimes. Il est à noter que, dans une architecture Intel, l'IOMMU se situe sur la passerelle nord. Des accès entre pairs sur la passerelle sud restent donc envisageables [3].

via les ACS Les *Access Control Services* permettent de définir des points de contrôle sur les bus d'entrées-sorties, ainsi que les composants auxquels ces contrôles sont délégués.

La présentation s'est terminée sur les suites envisagées pour les travaux du Laas. Ils demandent à être approfondis (vulnérabilités d'autres chipsets) et, dans une optique plus élargie, peuvent déboucher sur des outils spécifiques d'attaque. Une carte réalisant du fuzzing sur les entrées-sorties, ou mettant en place une automatisation complète, fait partie des possibilités. Des travaux sont en cours pour généraliser l'attaque afin qu'elle soit moins dépendante d'un matériel particulier (puces et passerelles nord/sud utilisées).

D'après M. Lone-Sang, il sera très difficile de détecter de telles attaques entre pairs, qui sont réalisés complètement « sous » le système d'exploitation.

2. Y compris, comme le montre une vidéo, l'utilisation du « clavier graphique » d'un site bancaire en ligne.

3. Sauf à remonter tous les accès vers l'IOMMU sud, ou à disposer de plusieurs IOMMUs.

2 Infection en naviguant

La seconde présentation a été faite par M. Pierre-Yves Bonnetain, de B&A Consultants (www.ba-consultants.fr).
Support de la présentation : www.ba-consultants.fr/images/articles/ReSIST/Analyse_Malware.pdf.

Le contexte est l'analyse d'un logiciel malveillant qui a fait parler de lui sur la fin de l'année 2011. Ce logiciel se présente comme provenant de la Gendarmerie Nationale et (outre le blocage du poste de travail) menace l'utilisateur des pires désagréments judiciaires s'il ne règle pas scéance tenante une « amende ». Cette menace est motivée par une foule de prétendues actions illégales à partir du dit poste de travail.

L'utilisateur en question a indiqué que le logiciel malveillant est arrivé sur son poste après une recherche sur Google, sans avoir cliqué sur quoi que ce soit au-delà de la validation des mots-clés [4]

Le programme malveillant fait partie d'une « famille » qui a la particularité de géolocaliser la victime afin de présenter un écran de verrouillage approprié (langue, références à la législation et aux forces de police/justice, etc.). Dans le cas rencontré, l'exécutable `explorer.exe` a été remplacé par un programme affichant l'écran de verrouillage en question. Dans d'autres cas, une clé du registre (`...\Winlogon\Shell`) est modifiée pour pointer sur le programme d'affichage de l'écran de verrouillage.

L'analyse de la chronologie d'accès au système de fichiers, et celle de l'historique de navigation de l'utilisateur, confirment l'installation à l'insu de ce dernier du programme malveillant. Cela se fait en plusieurs temps :

1. récupération, après plusieurs rebonds sur des sites de moins en moins légitimes, d'un code Javascript d'énumération de la plate-forme locale.
2. enchaînement de tests et détermination des vecteurs possibles d'infection (via PluginDetect) : Java, Acrobat Reader, HCP, Flash.
3. accès à une URL appropriée, selon les vecteurs identifiés, pour récupérer du code intrusif
4. exécution du code sur l'ordinateur local .

Le code des différentes étapes de l'intrusion est brouillé, pour rendre son analyse plus difficile. Après décodage, le code est un dérivé de BlackHole.

En conclusion, les mécanismes de pré-chargement entre Google et Firefox rendent possibles ce type d'incident sans intervention de l'utilisateur. Cela suppose que le premier site renvoyé par Google sur une certaine requête a été infecté (site légitime exportant, à son insu, du JavaScript aggressif). Comme souvent, une plate-forme non complètement à jour, y compris pour des outils tiers qui ne font pas partie du système d'exploitation, se révèle très vulnérable.

4. Dont il est utile de souligner qu'ils n'avaient rien pouvant diriger le navigateur vers un site « discutable ».