Avec Uniflow, Canon invente la photocopieuse qui espionne, refuse et dénonce

En l'absence de l'habituel maître des lieux
Les lutins du Framablog font bien de leur mieux
Écumant le web, en quête de sujets sérieux
Ils espérent que ces billets vous rendront joyeux
À défaut de nous aider à ouvrir les yeux
Sur des technologies qui derrière un vœu pieu
Menacent nos libertés et nos échanges précieux

« *On arrête pas le progrès* » aimait à répéter mon grand père, mais aujourd'hui, je me demande ce qu'il aurait pensé des dernières inventions de Canon…

En effet, si l'esprit du hacker est de bidouiller une technologie pour en trouver de nouveaux usages, les grandes firmes s'ingénient elles bien souvent à limiter les possibilités de leurs produits, pour créer une illusion de contrôle.

Dans notre cas, Canon a créé des photocopieuses qui inspectent au plus près les documents qu'on leur donne à reproduire, et s'y refusent si ces derniers contiennent l'un des mots de la liste noire située sur le serveur central des installations Uniflow.

Tout d'abord, ces photocopieuses illustrent exactement la menace qui plane sur la neutralité d'Internet. Imaginez qu'il ne soit plus possible de se parler qu'à l'aide de textes

envoyés d'une photocopieuse à une autre et vous aurez un bon aperçu de comment fonctionne Internet. En effet, chaque message y circule, par petits bonds, d'un ordinateur à un autre entre votre machine et celle à laquelle vous tentez d'accéder de l'autre côté du réseau. Chaque machine rencontrée photocopie simplement les messages qu'elle reçoit vers la sortie qui les rapprochera de leur destination. Pour l'instant, les routeurs de l'Internet transportent les messages de manière aussi neutre qu'une simple photocopieuse, sans le moindre soupçon d'analyse de contenu. Mais Canon vient donc de briser la neutralité des photocopieuses, en créant un système de « deep photocopy inspection » bien sûr associés à un système centralisé de censure.

Ensuite, comme le remarquait Benoit Sibaud sur Identi.ca, nous nous trouvons là devant un cas concret d'informatique déloyale, telle que définie par l'April, où des utilisateurs se trouvent confrontés à des systèmes soit-disant « de confiance », et qui sous prétexte de sécurité ne remplissent tout simplement plus la tâche pour laquelle ils sont conçu si les conditions arbitraires d'une entité tierce de contrôle ne sont pas réunies.

Je parlais d'une illusion du contrôle, car comme toujours le moyen mis en œuvre pour « sécuriser l'usage » est aisément contournable, les documents n'étant (pour l'instant) analysés qu'à l'aide d'un logiciel OCR, incapable donc de percevoir les notes manuscrites, ou les mots (volontairement) mal orthographiés.

Alors à quoi bon mettre en place des systèmes aux performances finalement ridicules au regard du niveau stratégique de l'objectif ? Et quel peut être l'objectif d'imprimantes allergiques à certains mots ?

Tout d'abord, déployer un système à l'efficacité embryonnaire c'est toujours faire un premier pas, ça finance la génération suivante et ça piège les non avertis… [1] Ensuite dans le cas

présent, on peut pallier les manques du système en contraignant le reste de l'environnement, et si on trouve une application admise par les contrôleurs et les contrôlés ça pourrait même rendre service.

Mais pourquoi empêcher d'imprimer ? Pour pallier, d'une certaine manière, au « trou analogique ». Le trou analogique c'est le nom donné à un phénomène simple : aussi sophistiqué que puisse être le système de protection d'un fichier (chiffrement, DRM), pour qu'il soit lu il faut bien à un moment le rendre présentable pour un humain. Et à partir de là, il est toujours possible de renumériser les données… Un MP3, même plombé par un DRM, quand il finit par être lu, rien ne m'empêche de l'enregistrer avec un dictaphone, si j'ai peur de ne pas m'en souvenir tout seul. Dans notre cas, l'intérêt est donc de combler en partie le trou analogique, en évitant que des copies papiers de documents identifiés comme « secrets » ne soient créées.

Toutefois, ça peut vite devenir comique, si une entreprise empêche l'impression de documents contenant le nom de ses clients par exemple, espérons qu'ils ne traitent pas avec Apple, Orange ou même Canon, sinon ils vont vite finir par ne plus pouvoir imprimer grand chose.

Néanmoins, après les imprimantes qui mentent sur leur niveau d'encre et les imprimantes qui laissent des micro-traces pour s'identifier sur toutes leurs copies, Canon invente aujourd'hui les imprimantes qui choisissent ce qu'elles impriment… [2]

Canon promet une sécurisation à base de mots-clés pour ses scanners et imprimantes

Canon promises keyword-based document scanning and printing security

Alan Lu – 12 octobre 2010 – ITPro.co.uk
Traduction Framalang : Siltaar, Julien R., KooToX, Daria

Canon a fait une démonstration d'Uniflow 5, la dernière version de son système de gestion de documents, capable d'empêcher les utilisateurs d'imprimer ou de copier des documents contenant certains mots, grâce à un système de sécurité intelligent basé sur des mots-clés.

Uniflow est un système de gestion de documents qui permet, depuis longtemps, de contrôler imprimantes, scanners et photocopieurs de manière centralisée. Cela permet de conserver le compte des impressions de chaque utilisateur à des fins de facturation. C'est indispensable dans les professions qui facturent les clients à l'heure ou à la quantité de travail, comme les avocats et les architectes. Le système requiert à la fois un serveur Uniflow sur votre réseau et des périphériques d'imagerie Canon, compatibles Uniflow.

La dernière version d'Uniflow possède un système de sécurité intelligent, basé sur des mots-clés. Une fois configuré par un administrateur, le système peut empêcher un utilisateur d'imprimer, scanner, copier ou faxer un document contenant un des mots-clés prohibés, tel que le nom d'un client ou le nom de code d'un projet.

Le serveur enverra alors par courriel à l'administrateur une copie PDF du document en question, au cas où un utilisateur s'y essaie. Le système peut aussi optionnellement informer l'utilisateur par courriel que sa tentative a été bloquée, mais sans identifier le mot-clé responsable, maintenant ainsi la sécurité du système.

La détection des mot-clés d'Uniflow 5 se base sur un système de reconnaissance optique de caractères (OCR), dont la licence est détenue par la firme belge Iris. Cette technologie est plus communément utilisé pour retranscrire des documents scannés en textes éditable sur ordinateur. Canon Angleterre a

confirmé qu’un utilisateur éclairé et déterminé ayant repéré un des mots-clés peut contourner le système en remplaçant une lettre par une autre ou un chiffre ressemblant comme avec « z00 » au lieu de « zoo ».

Néanmoins, l’intérêt de cette fonctionnalité est immédiatement perceptible pour les secteurs traitant des documents sensibles, que se soit pour des raisons légales, concurrentielles ou commerciales. Les représentants de Canon n’ont pu avancer de date quant à la commercialisation des produits Uniflow 5.

Notes

[1] Toute ressemblance avec une loi visant à contrôler les usages sur Internet serait fortuite.

[2] Crédit photo : Timshell (Creative Commons Attribution NoDerivs).