SÉCURITÉ de l'information
Sécurité Informatique / Numéro 11 ////// Mars 2011

Éditorial

Les clefs de la confiance

JOSEPH ILLAND
Fonctionnaire de Sécurité de Défense du CNRS

Les clefs USB font partie de notre quotidien, elles se glissent furtives et discrètes dans notre portefeuille, au fond d'un cartable ou d'un sac à dos, sur un coin de bureau ou même en pendentif.

« Pratiques mais risquées », c'est ce que nous démontre Luc Vallée, adjoint au chef du CERTA (Agence Nationale de Sécurité des Systèmes d'Information), dans un article de mise en garde sur les multiples dangers encourus, que la clef soit la victime ou au contraire le vecteur d'une attaque ou encore qu'elle soit perdue ou volée.

Elles sont si pratiques, qu'on leur confie tout... nos secrets professionnels comme nos fichiers familiaux, tant la confusion des sphères privée et professionnelle se retrouve aussi dans une simple clef USB.

Isabelle Benoist de la direction des affaires juridiques du CNRS attire pour sa part l'attention sur quelques risques juridiques attachés à la perte de cet objet devenu incontournable.

Attacher du prix à l'information oblige à la protéger. Le chiffrement s'impose pour se prémunir contre la compromission des données. Celle-ci peut résulter d'une perte involontaire (mais dans quelles mains l'information va-t-elle finalement aboutir ?) ou pire encore d'un vol ciblé. De manière beaucoup plus insidieuse, une simple aspiration des données fera l'affaire... au hasard d'un branchement sur un poste non digne de confiance.

Pierre Barthélemy de l'Institut de Mathématiques de Luminy à Marseille en tandem avec Robert Rolland de l'association Acrypta ainsi que Loïc Duflot, Olivier Levillain et Alix Cazenave de l'ANSSI nous proposent leurs visions respectives et recommandations en matière de chiffrement.

On retiendra la complexité du problème et l'illusion de la confiance aveugle. On notera aussi l'importance des conditions d'implémentation et d'utilisation, le diable se cachant à son habitude dans les plus petits détails de chacune des solutions disponibles sur le marché.

Il reste que le choix d'une solution passe par la « confiance » et rien ne vaut en la matière l'avis de nos experts nationaux. On s'attachera donc à se fier de préférence aux produits évalués et certifiés par l'ANSSI en notant que lorsqu'il s'agit de données très sensibles dites de « diffusion restreinte », la recommandation se mue en obligation réglementaire.

La question est d'importance ; on ne saura trop remercier les auteurs des présentes contributions et tout particulièrement l'ANSSI pour son investissement significatif dans ce bulletin.

joseph.illand[à]cnrs-dir.fr

>>>> *suite page 1*

Clefs USB : pratiques mais risquées

Luc Vallée
ANSSI

Par leurs formats et la généralisation rapide de l'interface USB, les clefs sont rapidement entrées dans les habitudes des utilisateurs de l'informatique. La lourdeur des contenus (ex. : vidéo) a rendu les disquettes, de capacité réduite, inadaptées au point de faire disparaître les lecteurs de disquettes des ordinateurs. Comme ces dernières, les clefs servent au transport et au stockage, et, comme elles, leur utilisation présente des risques qu'il convient d'anticiper pour rester serein. C'est toujours le soir, quand le support informatique n'est plus là, à dix minutes de l'échéance pour un rapport crucial, que les données sont perdues car la clef USB défaille, est infectée ou introuvable. Cet article balaye certains risques et propose des pistes pour les amoindrir, pistes à adapter aux contextes d'utilisation.

Utilisation sans limite ?

Cet idéal est mis à mal par les lois de l'électronique et par le quotidien.

Durée de vie

La mémoire de la clef USB est un circuit électronique qui supporte un nombre déterminé d'écritures. Ce nombre s'exprime généralement en dizaines ou en centaines de milliers.

La longévité de la mémoire est augmentée par un algorithme de gestion de l'espace qui répartit les écritures pour uniformiser le « degré d'usure ». Cette grandeur apparente est modulée par des écritures masquées à l'utilisateur. Ainsi, quand l'utilisateur travaille avec un traitement de texte sur le fichier présent sur la clef, des fichiers temporaires et des copies de sauvegarde peuvent être créés sur cette clef,

A nos lecteurs

Créé en 1994 par le service du Fonctionnaire de Sécurité de Défense du CNRS, le bulletin « Sécurité de l'Information » paraît ici pour la dernière fois sous la responsabilité directe de ce service.
Avant de passer la main, je tiens à remercier les lecteurs de leur fidélité et de leur continuelle confiance.

Joseph Illand
Fonctionnaire de Sécurité de Défense du CNRS

>>>> *suite page 2*

induisant des écritures (à la création) et des effacements (si nécessaire) qui réduisent la longévité de la clef.
Il faut donc prendre en considération la durée de vie finie d'une clef. Comme il n'y a pas de jauge permettant d'indiquer à l'utilisateur la proximité de la fin de vie, il faut toujours considérer que la copie sur la clef ou le travail direct sur la clef peut déboucher sur une panne, une indisponibilité de la clef. Bien sûr cette mise en garde prend plus de sens avec l'âge grandissant d'une clef et avec la lourdeur des fichiers qu'elle est amenée à contenir.
En fin de vie, il est préférable de procéder à une destruction physique de la clef USB.

Mauvaises habitudes
Certains utilisateurs, par ignorance, ne déconnectent pas proprement leur clef de l'ordinateur sur lequel elle est branchée. Ceci présente deux risques principaux.
Le premier est lié à la coupure électrique brutale sur le port USB, qui peut se répercuter sur les composants électroniques qui constituent la clef et les endommager.
Le second tient au système d'exploitation des ordinateurs dont la configuration standard tend généralement à économiser les transferts USB. Il gère sur la mémoire du poste de travail les écritures sur la clef et ne procède au transfert réel que sur certains critères : taille suffisante, débranchement propre de la clef, ordonnancement des tâches, utilisation des DMA,...
Ce faisant, entre l'écriture « logique » vers la clef et l'écriture physique réelle (après transfert USB), il existe une période de désynchronisation. La conséquence est qu'une clef arrachée brutalement ne sera pas correctement synchronisée. Il se peut alors que des fichiers de la clef soient et restent verrouillés, ou présentent des incohérences de contenu. L'incident est souvent apparent lors du branchement suivant de la clef, donc trop tard.
Pour prévenir ces désagréments, il suffit simplement d'utiliser les commandes de déconnexion propres des supports USB. Une icône, dans la barre de tâche de Windows XP ou sur le bureau de certaines distributions Linux, rend cette opération rapide et ergonomique. Les amateurs de la commande en ligne de Linux utiliseront par exemple les commandes sync et umount.

Accidents et disparitions
La clef USB est généralement petite. On la glisse partout, mais elle peut glisser, être perdue ou détruite accidentellement de multiples façons. Perdue, elle l'est alors avec son contenu. Il est donc illusoire de considérer une clef USB utilisée au quotidien comme une sauvegarde. Au contraire, le contenu de cette dernière doit être régulièrement sauvegardé sur un support plus pérenne pour atténuer le risque de disparition de la clef.
La disparition de la clef peut provenir d'un vol, simplement de l'objet ou pour capter l'information présente sur la clef. À la perte du contenu s'ajoute donc son accessibilité par un tiers hostile. En octobre 2010, une clef USB contenant des informations en clair sur une centrale nucléaire anglaise a ainsi été trouvée dans un hôtel (1). Une autre clef, contenant des informations sur la lutte contre le terrorisme, en clair également, a été trouvée dans la rue à Manchester en septembre 2010 (1).
Le chiffrement des données sur les supports amovibles, dont les clefs USB, offre l'avantage de créer un obstacle à la lecture non autorisée du contenu. D'autres articles de ce numéro y sont consacrés. Ces systèmes de chiffrement doivent évidemment être maintenus à jour, sous peine de voir leur efficacité anéantie (1).

Flux d'information incontrôlé
La clef USB peut être donnée aux participants d'une réunion avec les présentations et les documents de travail. C'est aussi est une forme répandue de cadeau publicitaire. La possibilité que cet objet soit infecté sera traitée dans la section sur la malveillance. Ce cadeau représente un risque pour celui qui l'offre, si un processus qualité et sécurité adéquat n'accompagne pas la production en série de l'objet, souvent l'affaire de sous-traitants spécialisés.

Utilisation en « Bureau mobile »
Le possesseur de la clef peut induire un risque en utilisant la clef « bureau mobile ». Des annonces promeuvent auprès des travailleurs nomades informatiques ces clefs qui contiennent une batterie de logiciels : bureautique, navigation, messagerie, etc. L'argument principal pour ces clefs, c'est d'assurer à cet utilisateur de retrouver « ses » logiciels, dans les bonnes versions, quel que soit l'ordinateur sur lequel il travaille.
Un premier problème est la compatibilité de l'utilisation de ces logiciels avec la politique du système d'informations hôte.
La crainte supplémentaire est, comme pour tous les nomades, l'absence de mises à jour immédiates de ces logiciels donc la présence de vulnérabilités devenues publiques, dans la clef USB. Le déploiement de cette solution doit donc s'accompagner d'instructions d'utilisation (et de non-utilisation) et de procédures de maintien à un niveau de sécurité convenable (1).
Enfin, les fichiers de ces clefs, dont beaucoup d'exécutables, peuvent être vecteurs d'infections, ce qui sera détaillé par la suite.

Malveillance
La mobilité des clefs USB est un trait qui n'a pas échappé à la face obscure de l'Internet. Elles sont utilisées pour des malversations qui leur sont spécifiques ou bien pour des attaques en compléments des réseaux. La clef peut être **la cible de l'agression** comme elle peut être **le vecteur de l'attaque**. Ces deux aspects seront successivement abordés.

Attaques contre les clefs USB
La destruction malveillante, tant de la clef, support, que de son contenu, est possible. Pour sa part et jusqu'à présent, le CERTA n'a pas été informé par ses correspondants ou dans sa veille, de tels agissements. Cela ne signifie pas que ce risque doive être balayé d'un revers de main. Comme pour la destruction accidentelle, la sauvegarde des données qui se trouvent sur la clef est une précaution indispensable.

Vol de la clef USB
L'attaque la plus radicale est le vol de la clef pour l'utiliser (vol crapuleux) ou pour en utiliser le contenu (menace stratégique). La taille réduite des clefs rend leur disparition difficile à remarquer rapidement. Quand l'incident est découvert, le coupable est loin. Le chiffrement permet de retarder la divulgation du contenu. Il ne prévient pas le vol simple, pour utilisation du support.

Copie du contenu de la clef USB
Il existe des logiciels dont la seule finalité est de copier insidieusement l'intégralité des fichiers présents sur les clefs USB branchées sur l'ordinateur.
Un chercheur est amené à faire une présentation à une conférence. La clef USB sur laquelle il emporte le diaporama à l'appui de son exposé contient également des travaux en cours. En effet, passionné par ses travaux, il continue à travailler à ses recherches pendant le trajet depuis son laboratoire et à l'hôtel. Arrivé à la salle de conférence, il branche sa clef à l'ordinateur dédié aux orateurs pour y déposer sa présentation. Pendant qu'il transfère explicitement son diaporama, le contenu de sa clef est intégralement et silencieusement copié sur l'ordinateur. Lui qui voulait rester discret sur l'avance qu'il avait par rapport à ses concurrents, tant que son brevet n'était pas déposé, ne s'apercevra pas ou trop tard de la manœuvre.
Il existe souvent des LED sur les clefs qui clignotent lors de transferts entre clef et ordinateur. Ce clignotement peut mettre la puce à l'oreille du possesseur de la clef quand aucun transfert légitime n'a lieu. Elles sont hélas de peu de secours lorsque le pillage des données s'exécute en parallèle avec un transfert légitime.

Pour parer à ce pillage de données, l'ANSSI a édité, avec l'aide d'utilisateurs, un passeport de conseils aux voyageurs (1). Ce qui est mentionné pour les ordinateurs portables est vrai pour les clefs USB. Par ailleurs, dans sa note d'information sur les clefs USB (1), le CERTA préconise la surcharge totale de la clef avant l'écriture des fichiers qui seront transportés, et la séparation des usages : dans l'exemple précédent, une clef pour la présentation publique, une clef pour les travaux de recherche non publics.

▪ *Injection de contenu dans la clef USB*

Dans le premier scénario, le possesseur d'une clef USB peut l'avoir quittée des yeux ou l'avoir branchée sur un ordinateur envers lequel il n'aurait pas dû avoir confiance. Pendant cette période de baisse de vigilance, des fichiers compromettants sont installés sur sa clef USB. La présence de ces fichiers sera ensuite signalée à qui de droit pour monter une opération de déstabilisation du possesseur et de son organisme de rattachement.
Cet incident n'a rien de technique et, de ce fait, n'a pas été signalé à l'ANSSI. Toutefois, des services de renseignement, d'intelligence économique, d'expansion économique ou contre-espionnage peuvent avoir rencontré ou avoir été informés de cette situation.
Le second scénario fait la transition avec la section suivante. Connecter une clef USB à un poste non maîtrisé ou à un ordinateur en libre service c'est prendre le risque d'infecter cette clef. Elle n'est pas réellement la cible de l'attaque, mais elle en est le vecteur.
Des modèles de clefs USB proposaient un commutateur physique qui autorise ou interdit l'écriture sur le support. Cette solution est en voie de disparition au profit de solutions purement logicielles dont l'efficacité reste à prouver.

Attaques utilisant les clefs USB

Si ces clefs n'ont pas la continuité de connectivité des réseaux, et donc ne permettent pas de lancer une attaque en temps réel, elles présentent l'avantage de se brancher sur des systèmes qui ne sont pas reliés aux réseaux publics ou très indirectement. Les automatismes dont l'utilisateur est friand ont fait le reste. Les cas d'infection par clefs USB les plus médiatisés sont Conficker (depuis décembre 2008) et Stuxnet (depuis juin 2010).

▪ *Attaques générales*

Ces attaques sont celles qui utilisent les clefs USB comme n'importe quel support de fichiers. L'histoire étant un éternel recommencement, le scénario existait déjà avec les disquettes.
Les fichiers qui se trouvent sur la clef USB, programmes exécutables et documents (présentations PPT, document DOC ou PDF,...) peuvent être infectés par les programmes malveillants qui se trouvent sur les ordinateurs auxquels elle est branchée. La clef sert d'agent de transmission pour l'infection comme peut le faire un courriel ou un partage réseau.
Comment limiter cette utilisation de clef USB comme vecteur d'infection ? La première question à se poser est l'utilité des fichiers présents sur une clef qui a été branchée sur un ordinateur non maîtrisé.
S'ils étaient copiés uniquement pour une exportation ou si une copie fiable, dans tous les sens du terme, est disponible sur le système d'information, le plus sage est d'éliminer les fichiers de la clef, devenus douteux et de travailler sur des versions de confiance. Si aucune version n'est disponible sur le SI, ce qui est imprudent, en raison de la perte possible de la clef USB, alors la vérification d'intégrité des fichiers s'impose. Elle doit s'effectuer sur un poste dédié, un sas. Une voie possible est la consignation d'une empreinte (comme un condensé SHA256) au moment de la copie sur la clef. Au retour, et avant de réintroduire ces fichiers sur le SI, le condensé est calculé à nouveau et comparé au condensé initial, conservé sur le SI. Un fichier n'est rapatrié que s'il y a coïncidence. Il y a la possibilité d'utiliser un ou plusieurs antivirus, mais il faut rester réaliste sur les limites de ces derniers.
Si les fichiers doivent être impérativement réintégrés au SI, par exemple parce qu'ils ont été modifiés dans une séance de travail ou parce que ce sont des documents donnés par un partenaire, alors la vigilance est de mise. Sur un sas, encore, il est intéressant d'analyser chaque fichier à la recherche d'anomalies ou d'objets dangereux.
Ce qui vient d'être signalé pour des clefs qui sont sorties du SI pour y retourner ensuite est également vrai pour des clefs publicitaires. Le CERTA a eu à traiter le cas de clefs publicitaires neuves contenant des fichiers infectés. L'une des causes est souvent la répartition des tâches dans l'entreprise. L'achat de ces objets publicitaires est souvent piloté par le service de communication ou des relations extérieures. Le service informatique et/ou le service en charge de la sécurité ne sont que rarement informés et sollicités. Il est indispensable que les objets publicitaires fassent l'objet d'un contrôle qualité, comprenant l'absence de danger informatique.
Doit-on accuser la société qui fait le packaging, et qui imprime le logo de l'entreprise ? Pas forcément. Des clefs neuves sont parfois infectées. La chaîne d'approvisionnement représente une source de menaces de plus en plus importante.

▪ *Attaques spécifiques aux clefs USB*

Les clefs USB dans les environnements informatiques actuels ont des fonctions attractives : la possibilité d'amorcer un système (*boot*) ou de lancer une exécution automatique, soit d'un programme sur la clef, soit d'un logiciel sur le poste.

▪ Clefs USB amorçables

La clef amorçable permet des intrusions discrètes sur un poste de travail, en l'absence de son utilisateur légitime. L'incident peut passer très longtemps inaperçu. Cette voie n'est pas de la science fiction : des clefs USB amorçables en Linux contournent le contrôle d'accès Windows. Mieux, une clef USB a été conçue spécialement pour le recueil d'information (1).
Pour réduire la possibilité d'amorcer un système à partir d'une clef USB, cet amorçage doit être désactivé au niveau du BIOS et cette configuration défensive doit elle-même être protégée par un mot de passe, le plus fort possible, compte tenu des protections rudimentaires des BIOS.

▪ Exécution automatique à l'insertion des clefs

L'exécution automatique à l'insertion de la clef, autorun, permet de lancer un programme automatiquement, par exemple l'installation d'un pilote de périphérique ou d'une application (1). Mais le logiciel installé peut être un virus ou un ver, comme Flyhigh, Palevo ou Conficker.
Conficker, apparu en décembre 2008, illustre cette possibilité. Il s'est d'abord propagé par les réseaux, utilisant une vulnérabilité du serveur SMB de Windows, pourtant corrigée par Microsoft dès la fin octobre dans une mise à jour exceptionnelle. Mais cela le « limitait » à l'espace des réseaux reliés entre eux : Internet et les intranets connectés, excusez du peu. Une version enrichie de Conficker est alors apparue, à peine un mois après. Un poste infecté tentait d'infecter par le réseau, mais installait aussi sa charge sur tout support amovible qui lui était connecté, comme une clef USB. Celle-ci, quand elle était branchée sur un autre ordinateur fonctionnant sous Windows, potentiellement sur un réseau isolé, infectait cet ordinateur, donc propageait l'infection à un réseau dont l'isolation pouvait donner l'illusion de la protection. Le CERTA s'est fait écho de la propagation de Conficker (1) mais aussi d'autres programmes malveillants.
Une parade est présente dans Windows Vista : la fonctionnalité d'exécution automatique est

inhibée dans la configuration de base. L'infection est certes possible, mais avec le concours de l'utilisateur imprudent. Étrangement, cette désactivation n'avait pas été proposée pour XP comme mise à jour de sécurité par l'éditeur, alors qu'il avait publié un programme réalisant cette désactivation de manière simple et rapide (1), ce qu'il a corrigé ce 8 février.
Même une distribution Linux conviviale avec une configuration laxiste autorise l'exécution automatique et l'aperçu du contenu des fichiers de la clef USB, avec possibilité d'infection. (1).

■ Clefs U3

Mais, pour le malheur des RSSI, il existe des clefs USB, dites clefs U3, qui, lorsqu'elles se connectent à un ordinateur, se font passer pour des cédéroms et contournent la protection précédente. La désactivation de l'exécution automatique doit être étendue à tous les supports amovibles. Autant l'exécution automatique pour installation est rarement utilisée avec une clef USB, autant elle est courante pour les cédéroms et les dévédés d'installation des logiciels. La pénalisation par la désactivation totale n'est toutefois que d'un clic. Un petit clic qui vaut mieux qu'un grand choc.

■ Lecture automatique à l'insertion des clefs

Cette fonction autorun n'est pas le seul automatisme utilisé par les codes malveillants. La fonction voisine autoplay a pris la relève puisque la désactivation d'autorun se généralisait. Cette exécution automatique est légèrement différente : il s'agit de lancer automatiquement un programme présent sur l'ordinateur lorsque la clef contient un fichier d'un type donné. Par exemple, la présence d'images, lance l'aperçu, celle d'un fichier MP3 lance un lecteur multimédia.
Le scénario d'attaque est le suivant : un fichier malveillant est mis sur la clef USB. Il contient le code d'exploitation d'une vulnérabilité présente dans le programme lancé. Lorsque le fichier est un « raccourci » (extension LNK), c'est l'explorateur de fichier qui est lancé. La vulnérabilité, depuis corrigée, était exploitée par Stuxnet. Stuxnet comportait plusieurs étages. Cette propagation par clef USB lui permettait d'atteindre une cible sur des réseaux de production industrielle, très souvent déconnectés d'Internet.

■ Simulation par clef USB

Les clefs U3 décrites brièvement ci-dessus simulent des cédéroms. Ce n'est pas le seul déguisement possible. Cela tient à la polyvalence de l'interface USB.
Deux chercheurs ont montré, lors de la conférence BlackHat de janvier 2011, comment faire passer un périphérique de stockage USB (téléphone mobile ou clef USB) pour un clavier, et entrer des commandes hostiles sur l'ordinateur.

▸ Recommandations

Quelques règles doivent donc accompagner l'utilisation de ces objets pratiques.
En tant que possesseur et utilisateur d'une clef USB :

- ne pas considérer une clef USB comme fiable à 100 %, ni éternelle ;
- ne pas laisser ses clefs USB sans surveillance ;
- débrancher correctement la clef USB ;
- ne pas en faire un support d'archivage, mais, au contraire, avoir une sauvegarde du contenu de la clef USB ;
- utiliser des clefs USB différentes pour des usages différents ou des documents de sensibilité différente ;
- chiffrer les données sensibles et surcharger la totalité de l'espace libre de la clef si elle doit être branchée sur un système non maîtrisé.

En tant que possesseur d'un ordinateur ou d'un système d'information sur lequel des clefs USB peuvent se brancher :

- avoir les réflexes sécuritaires de base : mise à jour des systèmes, des logiciels et des greffons, cloisonnement, journalisation et surveillance de l'activité, travail quotidien sans droits d'administration ;
- désactiver les automatismes (autorun, autoplay) et durcir les configurations des ordinateurs (BIOS, système d'exploitation,...) ;
- analyser la clef et son contenu avant de le copier. ■

communication[à]ssi.gouv.fr

(1) Bibliographie : pour les renvois mentionnés, on se reportera utilement aux documents du CERTA traitant de ces points spécifiques (http://www.certa.ssi.gouv.fr/)

L'emploi de la cryptographie pour la sécurisation des données sur clés USB

Pierre Barthélemy
Ingénieur de recherche à l'UMR6206 Institut de Mathématiques de Luminy à Marseille

Robert Rolland
Consultant ERISCS (groupe d'Études et Recherche en Informatique des Systèmes Communicants Sécurisés) et expert Acrypta.

▸ Problématique

Avec le développement de l'Internet à partir du milieu des années 1990, assurer la sécurité d'un système d'information a longtemps consisté à sécuriser le point de connexion entre le réseau local et l'Internet par des règles de filtrage et à améliorer le niveau de sécurité des protocoles et des serveurs. Plus tard est apparue l'idée de défense en profondeur : les postes de travail eux-mêmes devaient être mieux sécurisés par des mises à jour des systèmes, des applications et des anti-virus. On considérait à juste titre que l'information se trouvait sur des postes de travail physiquement connectés au réseau local et donc situés à l'intérieur d'un périmètre sécurisé, ou sur des serveurs, plus exposés mais sécurisés par diverses techniques adaptées.
Mais avec le développement du nomadisme dans les années 2000, divers objets portables ont proliféré :

- ordinateurs portables ;

- assistants personnels (PDA) ;
- téléphones portables ;
- tablettes ;
- smartphones ;
- clés USB.

Ces divers objets présentent de nouveaux risques qui souvent s'additionnent. Outre le problème des mises à jour de sécurité, le risque le plus fréquent est qu'ils soient volés ou perdus, alors qu'ils contiennent des données professionnelles ou privées, souvent importantes ou confidentielles, rarement sauvegardées par ailleurs et dont la divulgation peut être très néfaste, voire fatale. Selon une étude de la société Dell et de l'Institut Ponemon publiée en 2008, environ 12 000 ordinateurs portables seraient égarés chaque semaine dans les aéroports américains, dont le tiers seulement sont récupérés. Les téléphones portables, devenus des smartphones en intégrant des fonctions qui étaient auparavant celles des PDA (Personnal Digital Assistant) cumulent tous les risques. Les objets « passifs », comme tous les supports externes (clés USB, CD-ROM, DVD, disques durs amovibles) présentent le seul risque de perte ou de vol mais, selon la nature des données stockées, ce risque ne peut pas être négligé.

Force est donc de constater qu'une grande partie des données du système d'information se trouve maintenant en dehors du périmètre de sécurité, stockées sur des objets dont le niveau de sécurité est faible. La question est de savoir si la cryptographie, précédemment utilisée pour sécuriser les services de l'Internet et l'information contenue sur des serveurs, peut maintenant aider à sécuriser l'information stockée sur ces objets.

Nous montrerons dans cet article, en nous limitant au cas des clés USB, en quoi la cryptographie peut être une réponse à ces problèmes de protection des données et comment cette réponse peut être mise en œuvre.

Solutions cryptographiques

Les fonctionnalités cryptographiques

La protection de la confidentialité des données contenues sur une clé USB, un disque externe et plus généralement sur tout support qu'on peut perdre ou se faire voler, requiert au moins les fonctionnalités suivantes :

- chiffrement des données ;
- contrôle d'intégrité ;
- authentification ;
- éventuellement masquage de l'existence même de données sur le support.

Ces fonctionnalités sont assurées par des systèmes cryptographiques. Pour cette application particulière, on a au moins besoin :

- d'une fonction de chiffrement par bloc à clé secrète dans un certain mode d'utilisation ;
- d'un système de gestion et de protection de la clé secrète qui s'appuie sur une fonction de hachage ;
- d'un système de contrôle d'intégrité (Message Authentication Code).

Bien évidemment on ne saurait se passer non plus d'un générateur de nombres aléatoires utilisé pour la génération des clés.

En ce qui concerne le chiffrement par bloc on peut distinguer deux niveaux de sécurité :

- le premier niveau utilise des chiffrements par bloc ayant une clé de 128 bits et des tailles de données (en entrée et en sortie) de 128 bits ;
- le niveau plus sécurisé utilise des chiffrements par bloc ayant une clé de 192 bits ou 256 bits et des tailles de données (en entrée et en sortie) de 128 bits.

L'utilisation de chiffrement à flot (stream cipher) n'est pas recommandée. En général les circuits choisis sont AES (que l'on retrouvera dans les produits cités plus loin), TwoFish, Serpent.

Chiffrement par hardware

Cette solution est évidemment la plus performante. Les modes d'utilisation en hardware sont déterminés par la disponibilité sur le marché d'un circuit correspondant et on retrouve le plus fréquemment AES en mode CBC. Le mode CBC ("Cipher Block Chaining") est défini dans "NIST Special Publication 800-38A 2001 Edition". Notons que lorsque la valeur initiale est prévisible, le mode CBC peut être sensible à l'attaque dite "watermarking attack".

Les clés USB couramment disponibles sur le marché utilisent un circuit AES. Parmi ces produits, on peut citer :

- la clé IronKey : elle embarque une puce AES 256 bits, elle est conforme à la norme FIPS 140-2 niveau 3 et dispose d'une procédure d'effacement des données en cas de tentatives répétées de saisies erronées du mot de passe, mais la fiabilité de cet effacement reste à valider ;
- la clé SanDisk Cruzer Enterprise (dont la taille varie de 1Go à 8Go) embarque une puce AES 256 bits. Un driver sous Windows et Mac OS X (10.4 Tiger et 10.5 Leopard) permet d'activer et de désactiver le chiffrement, de changer et de gérer les mots de passe. Le rôle de ce driver est crucial et peut empêcher le chiffrement s'il est compromis ;
- la clé Corsair, préconisée par le CNRS (note DGD-R du 16 janvier 2011 et qui utilise elle aussi AES 256 bits).

Ces clés USB auto-chiffrantes sont plutôt destinées à un usage personnel.

Chiffrement par software sur le poste de travail

Cette solution consiste à utiliser un logiciel de chiffrement sur le poste de travail, c'est-à-dire à chiffrer en amont, avant d'écrire les données sur la clé USB.

Pour ces implémentations logicielles les choix sont plus ouverts. Outre le mode CBC, d'autres modes sont sans doute mieux adaptés, par exemple les modes XTS ou GCM.

Le mode d'opération XTS (Xor encrypt xor Tweakable block cipher with ciphertext Stealing), défini dans le document "NIST Special Publication 800-38E January, 2010", transforme le chiffrement par bloc sous-jacent (AES par exemple) en système de chiffrement par bloc paramétrable.

Le mode GCM ("Galois Counter Mode"), très peu connu pour le moment dans le monde industriel, serait utilement employé dans ce contexte.

En effet, le mode GCM fournit à la fois un chiffrement en mode Counter (CTR) et un code d'intégrité et d'authentification. Au chiffré vient se rajouter un bloc qui montre que le chiffré n'a pas été modifié et qui n'a pu être produit que par quelqu'un connaissant la clé secrète (ce tag de vérification d'intégrité dépend de la même clé secrète que le chiffré).

De nombreux logiciels existent, qui ne sont nullement spécifiques aux clés USB, mais plutôt destinés au chiffrement de disques durs d'ordinateurs de bureau ou portables. La notion de containers permet de copier sur des clés USB des données chiffrées.

De tels systèmes logiciels, souvent assez complets, sont sûrs sous réserve d'une implémentation non naïve, c'est-à-dire qui prenne en compte la possibilité de fuites mémoire ou de rétention des informations sensibles par le système, la mise en cache de données, les attaques par des programmes malveillants, ...

Un autre problème plus ou moins bien résolu est celui de la gestion des mots de passe et du séquestre des clés. En effet, l'utilisation du chiffrement dans une organisation peut aboutir à l'impossibilité d'accéder aux informations en cas d'absence ou de disparition de l'utilisateur, ou plus simplement en cas d'oubli du mot de passe. Les logiciels les plus professionnels gèrent les certificats, ce qui permet de s'appuyer sur les fonctions d'une PKI (Public Key Infrastructure) afin de faciliter la gestion des clés et le recouvrement. C'est le cas des logiciels cités ci-après, à l'exception de TrueCrypt.

Les logiciels les plus connus sont :

- ***TrueCrypt***

Le logiciel TrueCrypt est un exemple significatif de ce que peuvent être les

constituants et les fonctionnalités de base d'un système de chiffrement d'un volume à la volée. TrueCrypt utilise au choix AES256, Serpent256, twofish256, ces primitives étant éventuellement cascadées. Le mode d'utilisation est XTS. Les volumes peuvent être cachés, c'est-à-dire qu'il sera impossible de prouver que le support contient des données. Concrètement, TrueCrypt permet de fabriquer des containers dont le contenu (répertoires ou fichiers) n'est pas visible. Il utilise la parallélisation lorsque plusieurs processeurs sont disponibles.
TrueCrypt fonctionne sous Windows, Linux, et MacOS X et il a été certifié par l'ANSSI (qualification niveau élémentaire). TrueCrypt est connu au CNRS et a fait l'objet d'une fiche Plume. L'échange de données entre Windows, Linux, et Mac OS X se fait en copiant sur une clé USB au format FAT un container chiffré.

▪ *ZoneCentral*

Le logiciel ZoneCentral, de la société Prim'X Technologies, fonctionne sous Windows et a été certifié par l'ANSSI (qualification niveau standard et critères communs EAL2+). ZoneCentral est utilisé dans quelques structures du CNRS (une centaine de licences environ) et un bulletin Sécurité de l'Information (le numéro 5 de septembre 2009) a été consacré à son utilisation par la Délégation Régionale Midi-Pyrénées à Toulouse. ZoneCentral inclut l'outil Zed destiné à la fabrication de containers et qui fonctionne aussi sous Linux, ce qui permet de relire un container sur un autre poste de travail (Windows ou Linux). Contrairement à Truecrypt, les noms des répertoires et des fichiers d'un container ZoneCentral sont visibles, ce qui rend son utilisation plus simple et plus transparente mais aussi moins discrète, car le nom d'un fichier est en soi une information et mieux vaut alors ne pas être trop explicite.

▪ *Security BOX*

Security BOX, de la société Arkoon Network Security, est un ensemble de composants logiciels sous Windows partiellement certifiés par l'ANSSI au niveau standard EAL4+ permettant de protéger des données sur tous les types de supports : clés USB, PDAs, smartphones, et bien sûr disques durs d'ordinateurs portables, postes de travail et serveurs de fichiers. L'un des composants logiciels (Security BOX Disk) assure le chiffrement des données sur des périphériques amovibles tels que les clés USB.

▪ *ACID Cryptofiler*

Le logiciel Acid Cryptofiler a été développé au CELAR (Centre d'Electronique de l'Armement) de la DGA (Direction Générale de l'Armement). C'est une solution complète de cryptographie logicielle sous Windows dont la particularité est d'être entièrement sous maîtrise étatique. Pour ce qui est des caractéristiques techniques qui nous intéressent dans le cadre de cet article, Acid Cryptofiler permet de fabriquer des containers sur des clés USB et il s'appuie sur une PKI.

▸ Conclusion

Les logiciels de chiffrement disponibles (TrueCrypt, ZoneCentral, Security BOX, ACID Cryptofiler et d'autres encore) permettent de chiffrer les données sur des périphériques amovibles tels que les clés USB. Ces solutions peuvent s'intégrer à la politique de sécurité d'une organisation, notamment pour la gestion des clés et des mots de passe dans un contexte multi-utilisateurs, ce qui ramène au cas général le cas particulier des clés USB. Pour la plupart d'entre eux, ces logiciels peuvent s'appuyer sur la PKI existante au sein de l'organisation.

En complément, mais plutôt pour un usage personnel, il est aussi possible d'utiliser des clés USB auto-chiffrantes disponibles dans le commerce.

Dans les deux cas, la cryptographie est une réponse efficace au problème de la protection de l'information et permet d'éviter la fuite d'informations en cas de perte ou de vol du support contenant des données qui peuvent être sensibles ou confidentielles.

p.barthelemy[à]univmed.fr
et robert.rolland[à]acrypta.fr

Chiffrement de supports : principe, intérêt et limites

Loïc Duflot, Olivier Levillain et Alix Cazenave
Agence Nationale de la Sécurité des Systèmes d'Information

Procéder au chiffrement d'un support amovible s'impose dès que celui-ci contient des données sensibles. Mais tous les procédés ont leurs caractéristiques et leurs limites. Il est donc important d'en être conscient afin de pouvoir estimer le niveau de sécurité qu'ils procurent.

▸ Menaces sur les supports et objectifs du chiffrement

Dans le cas des supports de stockage amovibles, la menace principale que l'on considère est généralement celle de la perte ou du vol.
Les conséquences peuvent être multiples :

1. atteinte à la confidentialité des données : le vol d'un support peut engendrer la compromission de données sensibles (il s'agit souvent de la conséquence la plus évidente) ;
2. atteinte à l'intégrité des données, qui est souvent considérée, à tort, comme secondaire : l'altération des données contenues peut avoir des conséquences sur les systèmes ou applications qui les utilisent ;
3. atteinte à la disponibilité des données : la perte du support entraîne directement la perte des données qu'il contient.

Le chiffrement d'un support amovible permet de protéger la confidentialité (1) et (parfois) l'intégrité (2) des données qui y sont stockées. Concernant la perte des données (3), seule la réalisation régulière de sauvegardes permet de s'en prémunir. Quelle que soit la méthode de chiffrement employée, les mécanismes cryptographiques utilisés requièrent un élément secret pour fonctionner (la clé). Il est impératif que seul l'utilisateur légitime ait accès à cette clé pour assurer la protection des données. Habituellement une clé a une taille de quelques centaines de bits complètement aléatoires, ce qui la rend très difficile à retenir par cœur. C'est pourquoi les produits proposent des mécanismes

d'authentification pour déverrouiller l'accès à la clé, et donc à la ressource (mot de passe, utilisation d'une carte à puce, etc.).

Scénarios de vol de support

Supposons qu'un utilisateur a mis en place un mécanisme de chiffrement d'un support, et qu'un attaquant accède à ce support et cherche à extraire les données qu'il contient. Dans le cas le plus favorable à l'attaquant, il a accès au support alors que ce dernier est actif, c'est-à-dire qu'il est connecté à une machine informatique sur laquelle le propriétaire légitime du support a débloqué l'accès aux données (en fournissant le secret d'authentification). Dans le cas le moins favorable pour l'attaquant, le support est inerte et l'attaquant n'a pas accès au secret d'authentification.

Une variante de cette menace est le vol dit **« avec remise ».** Dans ce cas, l'attaquant a ponctuellement accès au support et le rend à son propriétaire légitime après d'éventuelles modifications. Les modifications peuvent notamment avoir pour objet de récupérer le secret d'authentification de l'utilisateur au moment où ce dernier s'en sert. Notons qu'en règle générale, les produits de chiffrement ne permettent pas de contrer l'intégralité des attaques reposant sur un vol avec remise. Un exemple de scénario de vol avec remise ainsi qu'une description détaillée de l'attaque sont donnés dans [RW09] ; cet article prend comme exemple TrueCrypt, mais le procédé peut être adapté à de nombreux systèmes de chiffrement.

Différents types de chiffrement

Le chiffrement peut s'effectuer à différents niveaux, en fonction du produit de chiffrement utilisé :

- le chiffrement de fichier : dans ce cas, chaque fichier est chiffré indépendamment et stocké sur le disque. Il est également possible de créer un conteneur chiffré regroupant plusieurs fichiers. Cette solution présente l'avantage d'être souple et permet souvent de gérer le partage d'un fichier entre utilisateurs. Cependant, la couverture offerte est limitée (voir ci-dessous pour plus de détails sur les copies temporaires) et le chiffrement nécessite une action explicite de l'utilisateur ;
- le chiffrement de partition : dans ce cas, une partition (ensemble cohérent de fichiers) est chiffrée intégralement. Le déchiffrement est effectué à la volée lorsque le poste informatique accède au système de fichiers. Ce fonctionnement est transparent pour l'utilisateur, et couvre systématiquement l'ensemble de la partition, mais la gestion du partage entre utilisateurs est généralement difficile ;
- le chiffrement intégral du support. Dans ce cas, le chiffrement est généralement effectué par un mécanisme matériel interne au support (on parle alors de support chiffrant) – ou à la machine sur lequel le support est connecté. Là encore, le mécanisme est transparent et généralement systématique, mais la question de la gestion de l'authentification par l'équipement demeure importante.

Limites classiques des mécanismes de chiffrement

Authentification

De nombreux mécanismes de chiffrement reposent sur l'utilisation d'un mot de passe ou une « *pass phrase* » dont la connaissance permet le déchiffrement. Les données sont alors chiffrées par un procédé mettant en œuvre une clef dérivée du mot de passe. Bien entendu, si le mot de passe choisi est un mot de passe faible, il est possible pour l'attaquant d'essayer toutes les possibilités jusqu'à trouver le mot de passe correct. On parle dans ce cas d'attaque par force brute. Par ailleurs, le mot de passe de certains supports USB chiffrants doit être entré au clavier depuis la station à laquelle le produit est connecté. Sur d'autres, il peut être entré directement sur le support. Cette dernière solution est beaucoup plus satisfaisante du point de vue de la sécurité puisque le mot de passe est entré directement par le support, et ne peut être récupéré par un éventuel attaquant qui aurait piégé le poste de l'attaquant à l'aide d'un *key logger* (enregistreur de frappe).

Cryptographie

Si le mécanisme de chiffrement en lui-même a été mal spécifié ou mal implémenté, l'attaquant peut espérer obtenir l'accès aux données sans même rechercher le mot de passe utilisé pour le chiffrement.

Mécanismes de secours

Quel que soit le support mis en œuvre, une panne matérielle de ce support peut rendre inaccessibles les données et ce même si le support n'est pas chiffré. L'utilisateur est donc fortement encouragé à effectuer une copie de ses données sensibles dans un endroit sûr.

Cependant, lorsque le chiffrement est effectué par un mécanisme matériel, la panne d'un composant extérieur au support peut également entraîner la perte des éléments sensibles. En cas de panne du dispositif matériel, les données sont irrémédiablement perdues. Certaines solutions proposent donc des mécanismes de secours permettant l'accès aux données même en cas de panne. Ces mécanismes supposent que la clef de chiffrement du support a été sauvegardée (sur un serveur, sur un support en clair, sur un papier,...). Si ces mécanismes sont utiles en pratique, voire nécessaires dans certains contextes opérationnels, ils représentent un facteur d'affaiblissement global de la sécurité du dispositif et doivent à ce titre être pris en compte dans l'analyse des risques.

Confiance dans le poste de travail

Il est important de noter que les mécanismes de chiffrement, quels qu'ils soient, ne fournissent aucun mécanisme de protection au cas où le poste informatique sur lequel l'utilisateur légitime les met en œuvre est compromis par un attaquant. Lorsque l'on déchiffre ses données sur un poste qui ne peut être considéré de confiance, les données doivent être considérées comme compromises.

Impossibilité de garantir l'absence de données en clair sur le support

Dans le cas où le produit mis en œuvre effectue un chiffrement de fichier (ou un chiffrement de partition sur un support comprenant plusieurs partitions), il est en pratiquement impossible de garantir que le fichier ne sera jamais présent en clair sur le support. En effet :

- le système d'exploitation du poste dispose d'un mécanisme de gestion de la mémoire qui l'amène à écrire temporairement sur le disque le contenu de certaines zones mémoire. Sur l'extrême majorité des systèmes, cette écriture s'effectue en clair dans une zone d'échange (*swap*) ;
- les applications (et en particulier les suites de bureautique ou les clients de messagerie électronique classiques) effectuent de nombreuses copies locales temporaires en clair des documents auxquels elles accèdent. De plus, ces copies ne sont pas systématiquement effacées lors de l'arrêt de l'application ou de la fermeture de la session de l'utilisateur. Par ailleurs, l'effacement présente d'importantes limitations (voir ci-dessous) ;
- si le chiffrement de fichier est effectué en place, l'original peut être toujours présent sur le support ou ne pas avoir été correctement effacé.

Bonnes pratiques

Produits qualifiés par l'ANSSI

L'utilisation de produits qualifiés par l'ANSSI permet de garantir la robustesse des

mécanismes cryptographiques mis en œuvre. Il est bien entendu impossible de garantir l'absence de bogue dans les produits évalués, mais le processus d'évaluation permet de vérifier la bonne implémentation des mécanismes de sécurité les plus importants et d'analyser la robustesse du produit vis-à-vis des objectifs de sécurité principaux. La liste des produits qualifiés est disponible à l'adresse suivante :
http://www.ssi.gouv.fr/qualification.

Effacement ou chiffrement ?

Comme nous l'avons vu, le chiffrement est le seul moyen de garantir la confidentialité d'une information. En particulier, l'effacement d'un fichier au moyen des mécanismes classiques des systèmes d'exploitation (clic droit suivi de « Supprimer », formatage rapide) n'efface en pratique pas le fichier du disque, mais supprime simplement la référence de ce document depuis le système de fichiers. De nombreux outils disponibles sur Internet permettent à toute personne ayant accès au support de récupérer les documents ainsi effacés.

Il existe des mécanismes dits d'**« effacement sécurisé »** permettant d'effectuer une surcharge logique d'un support. Cependant, ces mécanismes présentent des limitations importantes dues à la diversité des matériels existants. L'effacement ne doit donc être envisagé qu'en complément d'un chiffrement systématique des données sensibles. On pourra se référer à la page web suivante pour plus d'informations sur les limites de ces procédés :

http://www.ssi.gouv.fr/site_article172.html.

Conclusion

Il existe de nombreux cas où il est indispensable de protéger les données numériques. Pour cela, l'utilisation du chiffrement est nécessaire, mais ne fournit pas en soi une sécurité absolue. En effet, il est essentiel d'utiliser des produits **évalués et certifiés**, mais également d'en comprendre le fonctionnement et les limites.

communication[à]ssi.gouv.fr

[RW09] Evil Maid Goes after Truecrypt, J. Rutkowska et R. Wojtczuk, 2009.

Clés USB : quelques risques juridiques...

Isabelle Benoist
Direction des Affaires Juridiques du CNRS

Détournant une citation du Prix Nobel de Littérature de 1911, nous dirions aujourd'hui qu'*il n'y a rien de plus beau qu'une clé, tant qu'on ne sait pas ce qu'elle contient*[1].

Au moins deux grandes catégories de risques juridiques ressortent de l'utilisation des clés USB : ceux liés à la clé elle-même et ceux liés à son contenu.

Pour la 1re catégorie, pour qualifier les malveillances touchant les clés USB (attaques contre les clés ou les utilisants[2]), le juriste se placera sur le terrain des articles 323-1 et suivants du code pénal portant sur les atteintes aux systèmes de traitement automatisé de données punies des peines maximales de 5 ans d'emprisonnement et 75 000 € d'amende pour certaines de ces infractions dites « STAD ».

Pour la 2nde, la qualification juridique des faits dépendra des données contenues dans la clé perdue ou volée, dès lors que ces données ont été peu ou pas protégées.

Imaginons que la clé contienne des dossiers de candidature à un concours organisé par le CNRS. Certaines des données sont *a fortiori* des données à caractère personnel au sens de la loi dite « CNIL ». Or, au titre de son article 34, le responsable de traitement est tenu de prendre toutes précautions utiles pour préserver la sécurité de ces données. Il y a, tout d'abord, un risque de sanction pécuniaire prononcée par la CNIL, jusqu'à 150 000 € pour un 1er manquement. Plus grave encore le manquement à l'obligation de sécuriser les données pourrait être sanctionné sur le fondement de l'article 226-17 du code pénal (peines maximales : 5 ans d'emprisonnement et 300 000 € d'amende).

Prenons maintenant l'hypothèse que la clé appartienne à un chercheur et qu'elle contienne des résultats susceptibles de faire l'objet d'un dépôt de brevet. Cette clé est perdue à l'occasion d'un colloque et récupérée par un individu averti qui s'empresse de l'utiliser. L'atteinte au patrimoine scientifique du CNRS est évidente. Plusieurs actions sont envisageables pour le CNRS :

- action en revendication de brevet (art. L.611-2 du code de la propriété intellectuelle),
- action en concurrence déloyale (art. 1382 du code civil).

Pour autant, la tâche sera particulièrement délicate et complexe pour le CNRS car lui revient la charge de la preuve.

Cette brève présentation ne prétend pas à l'exhaustivité, l'environnement juridique d'une clé USB étant aussi vaste que la variété des supports qu'elle peut contenir. Pour aller plus loin : http://www.dgdr.cnrs.fr/daj/Default.htm

isabelle.benoist[à]cnrs-dir.fr

1. Et non « *ce qu'elle ouvre* » dans la citation originale.
2. Cf. article de L. Vallée de ce numéro

SÉCURITÉ DE L'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[à]cnrs-dir. fr
http ://www.sg.cnrs.fr/fsd

Rédacteur en chef :
Joseph Illand
Fonctionnaire de Sécurité de Défense
Courriel : joseph.illand[à]cnrs-dir.fr

Impression : Bialec, Nancy (France) - D.L. n° 75649

ISSN 1257-8819