Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . N
Direction centrale de la sécurité des systèmes d'information
CERTA

Paris, le 09 novembre 2006
N° CERTA-2006-INF-006-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Risques associés aux clés USB

Gestion du document

Référence	CERTA-2006-INF-006-001
Titre	Risques associés aux clés USB
Date de la première version	09 novembre 2006
Date de la dernière version	14 novembre 2006
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Introduction

Les périphériques USB (pour Universal Serial Bus) occupent actuellement une place prépondérante dans l'univers de l'appareillage informatique. Ils peuvent être de tout type, comme par exemple un support de données amovible (clé USB, lecteur de musique au format `MP3`, etc).

De par leur facilité d'installation, ces périphériques s'échangent très facilement d'une machine à une autre. Cependant, cette opération présente des risques. Nous montrons dans ce document que ces échanges peuvent aussi bien affecter le périphérique que l'ordinateur d'accueil.

Du fait de la simplicité et de la furtivité des attaques basées sur ces échanges, il est important de prendre des mesures préventives. Il n'est bien sûr pas question de remettre en cause l'utilité de l'USB, notamment les différents périphériques de stockage, mais certaines considérations doivent être prises avant leur utilisation, que ce soit pour l'utilisateur ou l'administrateur. Ce document offre donc quelques recommandations à cet égard.

2 Présentation de l'*Universal Serial Bus*

2.1 USB 1.0 et 2.0

L'USB (pour Universal Serial Bus) est une interface de connexion définie dans les années 90 et destinée à remplacer les ports série et parallèle sur les ordinateurs. Elle est utilisée de nos jours pour brancher tout type de périphérique, que ce soient les imprimantes, les scanners, les modems, ou des appareils de stockage, comme les clés USB.

Sans rentrer dans les détails fournis par les documents de référence, il existe, à la date de rédaction de cet article, deux standards distincts, `USB 1.1` et `USB 2.0` :

- L'USB version 1.1 considère deux modes différents, dits lent (1,5 Mbits/s en théorie) et rapide (12 Mbits/s en théorie). Le premier mode, moins sensible aux perturbations électromagnétiques, convient aux petits transferts de données, comme ceux requis par les claviers ou les souris. Le second peut servir dans le cas d'imprimantes, de scanners, de disques durs externes, ou de lecteurs et graveurs CD/DVDs.
- L'USB version 2.0 ajoute un nouveau mode, permettant des échanges théoriques à 480 Mbits/s. La compatibilité entre périphériques USB 1.1 et 2.0 est assurée. Toutefois l'utilisation d'un périphérique USB 2.0 sur un port USB à bas débit limitera celui-ci à 12 Mbit/s maximum. De plus, le système d'exploitation est susceptible d'afficher un message expliquant que le débit est bridé.

Les termes sont parfois utilisés de manière abusive, et la dénomination commerciale `USB 2.0 Full Speed` fait en réalité référence à la version USB 1.1 en mode rapide, tandis que `USB 2.0 High Speed` correspond bien au standard 2.0.

L'architecture de type USB a pour caractéristique de fournir une alimentation électrique aux périphériques qu'elle relie, avec une tension maximale de 5V et un courant d'au plus 500mA. Il est enfin possible de connecter jusqu'à 127 appareils à un Bus USB [1] à un temps donné. L'USB se compose de plusieurs couches de protocoles, ou moyens de communication, qui ne seront pas abordées dans ce document.

L'USB, pour résumer, possède les propriétés suivantes :

- la topologie en arbre dont la racine est normalement une machine hôte (PC, Mac, etc.) ;
- les périphériques peuvent être branchés et débranchés sans arrêter l'ordinateur ;
- les périphériques sont alimentés par un bus ;
- il est possible de chaîner jusqu'à 127 périphériques sur un même bus USB (avec l'utilisation d'un *hub* par exemple);
- les périphériques inutilisés sont automatiquement mis en veille ;
- les périphériques sont identifiés et configurés automatiquement par les systèmes d'exploitation.

2.2 La norme *On-the-Go*

L'USB est contrôlé par un hôte, installé sur la machine d'accueil. L'hôte USB a la charge de mener à bien toutes les transactions et de gérer la bande passante. Cependant, depuis l'USB 2.0, il existe un protocole « au pied levé » (ou *On-the-Go*), qui permet, pour deux périphériques USB, de négocier et d'élire un hôte parmi eux. L'intérêt est le suivant : on peut relier deux périphériques sans ordinateur. Parmi les illustrations les plus courantes, il peut s'agir d'une imprimante et d'un appareil photo numérique reliés entre eux, ou bien d'un lecteur MP3 et d'une clé de stockage USB.

2.3 L'USB sans fil ?

Des projets consistant à porter des caractéristiques de l'USB au domaine du sans-fil tendent à apparaître, l'un en particulier étant déjà très médiatisé : le *Wireless USB* (s'appuyant sur la technologie `UWB`, *Ultra-Wideband*), lancé par un conglomérat de constructeurs, promet des produits commercialisés dans les mois à venir. Nous ne voulons pas nous étendre pour le moment sur cette nouvelle approche USB, mais il sera intéressant, en temps voulu, de vérifier si celle-ci permettra d'éviter les problèmes mentionnés dans les paragraphes suivants et si elle présentera des problèmes spécifiques.

2.4 Génération USB U3

Créée par la société U3 avec le soutien de constructeurs de mémoire flash, cette technologie transforme une clef USB en un système portable contenant des fichiers et des applications favorites.

Une clef USB U3 dispose d'un logiciel, ou `lanceur`, qui s'exécute sur l'ordinateur hôte afin de présenter (le plus souvent) les applications disponibles. Il est facile de gérer son contenu *via* un menu *"Démarrer"* (ou `lanceur`) dédié accessible dans la barre des tâches. Il est alors possible d'afficher à l'écran son *système* personnel sauvegardé sur la clef USB avec son fond d'écran et un accès facile aux différentes applications.

Les inconvénients de la gestion d'applications sur les clefs traditionnelles sont donc effacés : l'accés aux programmes se fait simplement et de manière transparente pour l'utilisateur ; s'appuyant sur un format qui cherche à se standardiser, l'offre logicielle compatible avec U3 ne cesse de se développer.

1. Le bus USB est l'interface matérielle, souvent incluse dans la carte mère d'un ordinateur, permettant de relier l'unité centrale à un périphérique USB.

Autre caractéristique des clefs U3 : elles ne laissent que très peu de traces sur l'ordinateur hôte puisque les documents contenus sur la clef sont ouverts avec des applications elles aussi présentes sur la clef (y compris les cookies récoltés lors d'une navigation sur l'Internet). Les tâches d'écriture se font *via* la mémoire volatile de la machine hôte uniquement, et ces applications ne modifient ni la base de registre, ni la mémoire morte (ROM) de cette dernière.

De nombreuses applications gratuites ou payantes ont désormais des versions compatibles avec U3 : notamment le logiciel de voix sur IP Skype ou le navigateur Firefox. D'autres logiciels sont également disponibles : jeux, bureautique, gestionnaires d'images ou de fichiers audio MP3 ; et cette offre logicielle augmente de jour en jour.

L'USB U3 présente donc un avantage, pour la maîtrise de l'application utilisée ; par exemple, quand une personne est amenée à utiliser un ordinateur dont la configuration et le niveau de sécurité ne sont pas connus (comme dans un cyber-café, un hôtel, un aéroport, etc). Cela permet d'utiliser ses propres applications, plutôt que certaines méconnues, ou aux mises à jour et à la configuration non spécifiées. Elle reste cependant tributaire de la machine d'accueil pour toute communication, toute saisie, et tout transfert de données vers l'extérieur, et cette opération peut l'exposer à certains risques décrits dans les paragraphes qui suivent.

3 Risques associés à l'USB

3.1 Vol d'informations de la clé

Une clé, ou tout autre support de stockage USB, est, une fois branchée sur une machine, à la merci de celle-ci. Un processus fonctionnant silencieusement, peut très bien attendre que la clé soit branchée (information signalée par le système d'exploitation) pour enclencher une procédure de lecture et de copie du contenu de la clé. Un tel processus, comme la plupart des codes malveillants actuels, ne sera pas facilement décelable sur la machine hôte (dissimulation au niveau de la liste des tâches, des appels système, etc.).

Certains outils plus pernicieux permettent même de faire une image complète de la clé. Outre le vol de documents présents dans celle-ci, ce procédé peut également faciliter la récupération de tout ou partie de documents effacés sur la clé.

Les clés disposent de voyants lumineux, montrant les échanges de données. Un clignotement anormal de la clé peut donc être une première indication d'une telle activité de copie. Attention cependant, le voyant peut aussi être manipulé de manière logicielle sur certaines clés. Quelques secondes suffisent enfin pour dérober plusieurs Mo de données avec les performances USB actuelles.

3.2 Exécution d'applications hébergées par la clé

L'action malveillante du paragraphe précédent est perpétrée par la machine d'accueil. Une autre approche, ou action malveillante, se nomme `podslurping` et s'effectue depuis le périphérique. Elle consiste à brancher sur un système un support de stockage, ou aussi un lecteur MP3 (`podslurping` fait référence au produit iPod d'Apple), afin d'en dérober furtivement de l'information.

L'ingénierie sociale, ou la force de persuasion, peut être associée à cette approche, afin de provoquer le branchement, et de perpétrer le vol des informations. Une phrase parmi les dialogues possibles pourrait être :

"Excusez-moi, pourrais-je connecter quelques minutes mon lecteur de musique MP3 sur votre port USB ?... Les batteries sont déchargées, et je ne rentre que demain chez moi. Merci beaucoup !".

Pendant quelques minutes, une partie du disque est copiée sur le lecteur de musique, qui dispose d'un espace de stockage important (de l'ordre de quelques Go à plusieurs dizaines de Go), et dont l'usage ne fait pas obligatoirement penser à un périphérique de stockage.

Ce scénario est aussi valable avec un appareil photo numérique.

Ce problème n'est absolument pas récent, et existait déjà à l'époque des disquettes. Cependant, les supports de stockage ont maintenant une capacité et un débit de transfert beaucoup plus importants, ce qui augmente la quantité de données pouvant être dérobées dans un cours intervalle de temps.

3.3 Problématique des clés USB U3

3.3.1 Mises à jour des logiciels

De nombreux scénarios d'attaques étudiés par le CERTA dans le cadre des incidents qu'il traite au quotidien sont dus à une absence de mises à jour, qui ouvre une brèche au niveau applicatif.

Il en va de même pour clés USB U3, dont le premier point délicat réside dans la maintenance des logiciels compatibles avec U3.

Ces logiciels, comme nous l'avons vu, sont pour la plupart des déclinaisons de ceux manipulés sur des systèmes plus standards (navigateur, client de messagerie, etc). En revanche, ils ont subi quelques modifications pour fonctionner sur le support U3, et quelques sites centralisent ces versions particulières.

Il se pose alors la question des mises à jour de ces dernières. Il n'est pas évident que les sites suivent de manière réactive les modifications des éditeurs officiels. Par ailleurs, la clé ne peut être mise à jour que si l'on dispose d'une connexion Internet.

Imaginons alors le scénario suivant :

1° l'utilisateur possède une clé U3, essentiellement pour un usage bureautique, afin de faire des présentations.

2° l'utilisateur branche sa clé régulièrement pour lire, rédiger et présenter des transparents.

3° la clé n'est pas mise à jour ; elle possède une version du logiciel de bureautique ayant des vulnérabilités permettant une exécution de code arbitraire par le biais d'un document spécialement conçu.

4° la clé peut servir à contaminer les ordinateurs sur lesquels les transparents sont visionnés.

Il est très délicat d'imposer aux utilisateurs d'une clé de se connecter à Internet pour effectuer les mises à jour. Ce n'est pas nécessairement l'usage premier qui est recherché.

Pour résumer, il existe les problèmes suivants, liés aux applications disponibles actuellement :

1. il n'existe pas de mise à jour automatique. Pour effectuer l'une d'elle, il faut supprimer l'application courante, afin d'installer une version plus récente ;
2. les applications compatibles avec U3 sont maintenues par certains sites, mais :
   - les éditeurs légitimes ne donnent généralement aucune garantie sur ces versions ;
   - les versions sont modifiées, et leur configuration est souvent criticable. Par exemple, l'installation d'un navigateur implique une page d'accueil spécifique, une barre de recherche pré-installée et méconnue, une configuration peu regardante sur la sécurité (taille du cache, activation du javascript), des favoris par défaut, etc.
   - certaines applications sont des espiogiciels, voire des troyens. Il peut aussi s'agir de jeux par exemple, compatibles avec U3, mais nécessitant au préalable un enregistrement *via* l'Internet (quel est le but de cette collecte d'information ?).
3. l'utilisateur doit régulièrement surveiller les sites, donc se connecter, pour découvrir les mises à jour.

Il reste possible de développer soi-même les versions de certaines applications (en faisant attention aux problèmes de licences). Plusieurs détails pour opérer se trouvent sur l'Internet, mais cela reste marginal, et nécessite à la fois des connaissances minimales pour compiler du code et une disponibilité des fichiers sources.

3.3.2 Vol d'informations

Compte tenu des applications disponibles, les clés U3 sont susceptibles de contenir des informations personnelles ou confidentielles :

- la configuration du client de messagerie ;
- les contacts stockés par le client de messagerie ;
- les pages en cache du navigateur Internet ;
- les sites favoris installés sur le navigateur ;
- des mots de passe gérés par une application dédiée (application fréquemment offerte par défaut avec la clé).

Le risque du vol de données comme il existe pour les clés classiques reste présent. Malheureusement, l'utilisation d'applications impose de fournir sur la clé U3 un minimum d'informations pour leur bon fonctionnement. D'autres applications U3 incitent également à centraliser des données confidentielles sur le support USB (gestionnaire de mots de passe par exemple). Le vol de celles-ci peut avoir des conséquences variées et génantes.

3.4 Les lanceurs malveillants

Pour finir, il faut noter que les clés U3 sont généralement fournies avec un `lanceur`, qui donne accès aux applications, une fois la clé insérée. Cependant, certains `lanceurs` malveillants sont également disponibles. Ils permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant : de récupérer les tables de mots de passe, d'installer une capture de clavier ou un `rootkit`, difficilement décelables *a posteriori*.

4 Les recommandations du CERTA

4.1 Comptes utilisateurs et droits

La clé ne dispose pas d'autres droits que ceux de l'utilisateur courant sous Windows. Pour limiter les actions que celle-ci peut effectuer sur le système, il est donc important de n'autoriser la connexion de clés que sur des sessions avec des droits limités, et de ne réserver les droits de l'administrateur qu'occasionnellement, pour la maintenance du système. Cette règle de base est également vraie, indépendamment des clés USB.

Sous Windows, pour ouvrir l'outil `Comptes d'utilisateurs`, il faut ouvrir le `Panneau de configuration` à partir du menu `Démarrer`, puis sélectionner `Comptes d'utilisateurs`. La gestion des comptes et des droits associés s'effectue à partir de cette interface.

4.2 Désactivation de la fonctionnalité `autorun`

Les clés U3 profite d'une propriété offerte par les systèmes d'exploitation Windows, nommée `autorun`. Elle consiste à exécuter automatiquement un logiciel lorsqu'un périphérique de stockage qui le contient est connecté. Microsoft autorise par défaut cette fonction pour le périphériques de type CDROM/DVDROM, ou les disques fixes. Cette fonctionnalité est visible, quand, par exemple, à l'insertion de certains CD, une fenêtre de navigation Internet Explorer, ou une application d'installation s'ouvre. Un périphérique USB classique ne permet pas, lors de son insertion dans une machine fonctionnant sous Windows, d'exécuter automatiquement des programmes ou des commandes qu'il peut contenir. Dans l'objectif de faire exécuter automatiquement du code au cours de l'insertion d'un périphérique USB, certains fabriquants de matériels USB ont développé une astuce, qui consiste à faire passer celui-ci auprès de Windows pour un CD ou/et un DVD. Cette technique existe, et c'est elle qui est utilisée par les produits USB U3. Le principe général est que le périphérique, au moment de l'insertion, se présente comme un lecteur de CDROM USB, permettant *a fortiori* l'exécution d'un `autorun`.

La fonction `autorun` n'est généralement pas indispensable. Pour la désactiver sous Windows, il suffit de modifier la clé suivante dans la base de registres :

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/CDRom`

Pour la désactivation de l'`autorun` :

– Autorun = 0

pour l'activation de l'`autorun` :

– Autorun = 1

Cela fonctionne sur les systèmes Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP et Windows 2003.

4.3 Verrouillage des postes

Afin d'éviter des incidents liés à l'insertion de clés USB sur son système, il est également important de verrouiller son poste de travail : sous Windows, cela peut se régler de manière automatique, après un manque d'activité de quelques minutes sur le système (choisir `Propriétés` après un clic droit sur le fond d'écran), ou de manière ponctuelle (appuyer simultanément sur les touches `Ctrl+Alt+Suppr` ou `Windows+L`).

L'insertion d'un périphérique USB sous Windows ne provoque pas son installation quand l'écran est verrouillé. La partition peut être cependant montée (`automount`) sous Linux malgré le verrouillage [2].

4.4 Clés USB de confiance : une clé par usage

Si une clé doit être insérée dans un système critique, il est important de vérifier son origine. Une solution serait de conserver une clé blanchie, régulièrement formatée, et de réserver l'usage de l'USB à cette seule dernière (ajout de nouveaux matériels/périphériques interdits). En d'autres termes, il faudrait considérer une clé par usage, voire interdire son déplacement hors des locaux liés à son utilisation.

4.5 Bloquer la clé en écriture

Certaines clés présentent un interrupteur physique, qui permet de bloquer l'accès en écriture à la clé. Il ne faut donc pas l'oublier. Si cela ne protège pas du vol d'information, et donc des différentes problématiques de confidentialité, cela empêche des éléments extérieurs de modifier le contenu de la clé, ou de l'effacer à l'insu de l'utilisateur.

2. Cette opération est par exemple visible avec l'appel à la fonction `dmesg`.

4.6 Nettoyer proprement le contenu de la clé

Les clés peuvent contenir des données sensibles. Avant de les prêter ou de les abandonner, il est important de bien nettoyer leur espace de stockage, ou d'assurer la confidentialité de leur contenu. En fonction des impératifs et des réglementations, certaines opérations doivent être conduites.

4.6.1 Mesures élémentaires

Il n'est souvent pas suffisant de faire `"supprimer"` pour détruire complétement toute trace d'un document. Des résidus peuvent subsister. Certains outils permettent de faire un nettoyage beaucoup plus complet.

- Sous Windows, il existe par exemple :
  - `eraser`
    http://www.bugbrother.com/eraser
  - `BCWipe`
    http://www.jetico.com/bcwipe.htm
- Sous Linux ou MacOS, il existe entre autres la commande `shred` (`ShredIt` sous Mac OS) ou l'application :
  - `wipe`
    http://wipe.sourceforge.net/

Il faut cependant bien vérifier que tout l'espace de stockage reste inaccessible. Certains outils se contentent d'effacer des fichiers, mais d'autres temporaires peuvent encore subsister sur l'espace de stockage (cas des documents bureautiques avec Microsoft Word par exemple).

4.6.2 Mesures spécifiques

Dans le cas de données plus sensibles, il existe des mesures plus efficaces que celles précédentes. Elles peuvent s'appuyer sur des méthodes de surcharge, de démagnétisation, etc. Enfin, une dernière mesure consiste à détruire le support de stockage USB.

4.7 Chiffrement et intégrité

Nous n'aborderons pas ce point dans ce document, car les questions de chiffrement et d'intégrité se posent pour tout support de stockage, mais il est bien entendu que si la solution de chiffrement nécessite une clé, celle-ci ne doit pas se trouver sur l'appareil USB. De la même manière, le résultat du test d'intégrité ne doit pas être stocké sur le même support.

D'autre part, les clés actuelles offrent comme contrôle d'accès l'utilisation d'un mot de passe pour accéder aux fonctionnalités U3. C'est une première protection contre le vol, mais il faut garder à l'esprit que :

- si le mot de passe est frappé depuis une machine compromise (contenant une capture de frappe au clavier), ce dernier est récupérable. Or le CERTA observe dans le cadre de traitements d'incidents que de tels outils malveillants sont fréquemment installés.
- le mot de passe est stocké sur le support amovible. Il peut donc être récupéré, sous une certaine forme, avec le reste des informations contenues (cf. le chapitre 3.1). Des tentatives de récupération par tests exhautifs reste possible, sans disposer de la clé en permanence.

5 Conclusions

Les périphériques de stockage USB offrent beaucoup d'avantages. Outre leur capacité importante, ils étendent actuellement leur champ d'action pour offrir à l'utilisateur des applications et des fonctionnalités multiples. Cependant, ces mêmes technologies peuvent également être utilisées à mauvais escient pour exécuter des actions malveillantes sur le système. *A contrario*, un système malveillant peut tirer profit de la qualité et la quantité des informations contenues sur ces supports, pour en dérober tout ou partie.

Il est important de considérer tout cela, pour un usage approprié de ces périphériques. Certaines mesures doivent être prises, selon le contexte, pour garantir un niveau de sécurité minimal. Etant donné l'usage répandu de ces appareils, un effort de sensibilisation est également nécessaire.

6 Documentation

- Caractéristiques de l'USB U3 :
  http://www.u3.com
- Comment désactiver la fonction autorun sur une machine Windows :
  http://support.microsoft.com/kb/q155217
- Site du standard USB :
  http://www.usb.org
- Documentation en français sur le fonctionnement de l'USB, par B. Acquier :
  http://acquier.developpez.com/cours/USB/
- Cours de Supélec par J. Weiss, "Le protocole USB' :
  http://www.rennes.supelec.fr/ren/fi/elec/docs/usb/usb.html

Gestion détaillée du document

09 novembre 2006 version initiale.
14 novembre 2006 corrections sur la forme.