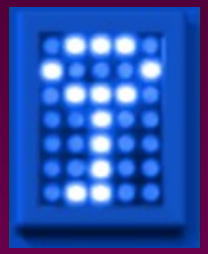
Protection des données et chiffrement



Jacques Beigbeder
Pierre Vincens

Protection des ordinateurs portables

Circulaire CNRS du 16 janvier 2011 de J.M. Voltini / X. Inglebert

- Un constat
  - De nombreux ordinateurs régulièrement volés ou perdus
  - Des informations susceptibles d'être exploitées :
    - Données scientifiques
    - Données à caractères personnels
    - Identifiants
    - Informations privées de l'utilisateur
    - …

→ Postes fixes, serveurs, échanges par messagerie traités ultérieurement

Protection des ordinateurs portables

- L'orientation choisie : le chiffrement
  - Chiffrer tous les ordinateurs portables du CNRS en accord avec la demande du ministère de la Recherche
  - Solution la mieux adaptée à la diversité et à l'envergure de l'environnement informatique du CNRS
    - «*Généralement, il n'y a pas à entrer de mot de passe supplémentaire*»

Protection de base applicable à tous les ordinateurs portables

- Nouveaux Portables :
  - Windows et Linux : solution matérielle disques chiffrants

    → Commander les PC avec l'option «disques chiffrants» via le marché Dell
  - Mac : solution logicielle native Filevault
  - Clefs USB : autochiffrantes recommandées par le CNRS (ex : Corsair)
- Parc existant
  - Windows : solution logicielle Truecrypt (qualifié ANSSI, gratuit)
  - Linux : solution logicielle native dm-crypt
  - Mac : solution logicielle native Filevault
  - Clefs USB : container TrueCrypt

Protection des données sensibles

- Données sensibles «ordinaires»
  - Rajout d'une deuxième couche de chiffrement

    → Container TrueCrypt (qualifié ANSII, certification de sécurité de premier niveau (CSPN))

- Données «classifiées de défense»
  - Règles propres à définir avec le fonctionnaire de défense

Recouvrement des clés

- Un risque majeur du chiffrement :
  - La perte des clés (oubli du mot de passe, absence du détenteur,...)
- Préconisation du CNRS:
  - Mettre en place une solution de secours permettant de récupérer les codes d'accès
  - Séquestre des mots de passe dans un coffre fort physique ou électronique

Avertissement

- Mesure de chiffrement ne dispense pas :
  - Vigilance contre le vol
  - Sauvegarde régulière des données
- Rappel sur
  - Restriction ou interdiction d'usage du chiffrement dans certains pays

    → recommandation d'usage d'une machine dédiée contenant un minimum d'informations réinstallé avant le départ et après le retour (voir Passeport de conseils aux voyageurs)
- Responsabilité du directeur d'unité
  - S'assurer que les mesures de protection des données sont bien mises en place

Des informations techniques

http://www.dsi.cnrs.fr/service/securite/

François Morris

(14/04/2011)

Des questions ?

- Comment faire accepter aux utilisateurs?
- Comment choisir les mots de passe et clés?
- Comment mettre en place le séquestre?
- Comment faire migrer le parc existant?
- Comment gérer les changements d'unité des utilisateurs?
- Comment gérer les mises à jours ?
- Comment « traiter » le problème de la sauvegarde ?
- Comment « gérer » une panne sur un équipement chiffré?

Comment faire accepter à nos utilisateurs ?

- C'est une règle imposée
  - Circulaire CNRS, PSSI, chartes,...

  MAIS:
  - Résistance à une contrainte supplémentaire
    - encore un code! → « post'it » sur la machine
  - Mauvaise compréhension
    - « cela va me protéger des virus! »
  - Crainte face à une « nouvelle » technologie
    - « je vais perdre mes données »
  - Modification des habitudes
    - Prêt d'une clé usb à un tiers pour échange d'informations

  => Comment faire respecter les règles d'usage ?
- Sensibiliser...

Gérer les mots de passe et le séquestre ?

- L'administrateur connaît le mot de passe, mais sans disponibilité du support n'a pas accès réellement à l'information
  - → limite : container sur un disque partagé
- Le(s) mot(s) de passe est(sont) modifiable(s) par l'utilisateur
  - → effacement volontaire ou accidentel par l'utilisateur
  - → remplacement par l'utilisateur
- Le mot de passe peut prendre des formes différentes :
  - → phrase (longueur minimale),..., fichiers
- Les situations de recouvrement sont variables :
  - → personne en déplacement qui a oublié son mot de passe
- Une approche possible :
  - Mots de passe spécifiques à chaque équipement (et non au parc)
  - Clés de recouvrement mis sous enveloppe
    - → écrit sur papier, gravé sur CD
    - → disponibilité d'un coffre (minimiser les ouvertures)

MAIS : l'utilisateur peut initier une solution de chiffrement sans informer l'administrateur. Quid du recouvrement?

Mise en place du chiffrement au niveau système

- Conseiller car chiffrer seulement les données laisse perdurer un risque de fuite
- Cas de nouveau matériel :
  - Étape supplémentaire lors de l'installation
- Matériel ancien :
  - Linux (dm-crypt) : nécessite une réinstallation pour chiffrer le système
  - Windows avec Truecrypt : pas de réinstallation mais temps de chiffrage «long»
  - Disques chiffrants : fonctionnalités activables après l'installation de Windows (type de disques?), mais peut impliquer des modifications du système (ex : version de grub sous Linux).

  → implique de disposer de l'équipement pendant quelques heures (planification,...)

Comment gérer les changements d'affectation ?

- Migration des utilisateurs entre unités
  - Hétérogénéité des méthodologies et des matériels entre unités et organismes français et internationaux.
  - Matériel suit l'utilisateur
    → transfert des clés de recouvrement
    → « neutralisation » du chiffrement
  - Matériel réaffecté
    → changement de la clé utilisateur ?
    → réinstallation complète ?

Sauvegarde

- Le chiffrement diminue les chances de restauration en cas de panne de disques
  - → sauvegarde régulière des données INDISPENSABLE
  - → sauvegarde réalisée avec les données déchiffrées
    - Chiffrement possible de la sauvegarde
- Cas des containers
  - → Sauvegarde du container en tant que fichier
    - En mode incrémental, une modification même mineure du contenu implique une sauvegarde complète du container
      => explosion des volumes de sauvegarde
    - Problème similaire lors de synchronisation d'espace (ex : Unison)
      => explosion des temps de synchronisation

En cas de panne

- Panne de disque
  - Le chiffrement évite la fuite d'information en cas d'échange standard avec retour
- Panne impliquant une expertise externe
  - Les supports techniques ne maîtrisent pas le chiffrement
  - Il y a nécessité de « supprimer » le chiffrement
    - Échange du disque avant renvoi en SAV
    - Réinstallation sans chiffrement de l'OS après sauvegarde de l'image
    - Suppression des données et désactivation du chiffrement

Clés USB Corsair

- Capacité : 8 Go ou 16 Go (32Go annoncé?)
- Un mot de passe « utilisateur » modifiable
  - Mise en place simple (trop : effaçable par accident!)
  - Longueur minimale : 4 soit seulement 625 possibilités
  - Réinitialisation possible avec perte de données (code 911)
    => nécessite un formatage: « mkfs.msdos -I -n MACLE /dev/sdx »
    - => problème de partitionnement
- Un mot de passe « master » non modifiable (?)
  - Permet de supprimer le mot de passe utilisateur sans perte
  - Mise en place un peu « récalcitrante »
  - Suggestion : au moins 7 ou 8 chiffres (max 10)
- Bilan
  - Fonctionnement raisonnable, mais quelques habitudes à changer
  - Déploiement lourd : coût (~ 70€ pour la version 16Go) et manipulations

Filevault

- Chiffrage du home de l'utilisateur
  - Clé = mot de passe de l'utilisateur
  - Séquestre de la « recovery key » (filet de sécurité)
- Chiffrage du disque entier à partir de OS X 10.7 (Lion)
- Facilité de mise en œuvre
- Compatibilité (?) avec Time Machine

Truecrypt

- Support
  - Windows (système et données)
  - Linux et MacOS (données seulement)
  - Chiffrement de partitions ou de « containers »
- À l'usage
  - Mise en œuvre assistée
  - Nécessite les droits administrateurs

    => utilisation de sudo ou runas pour un utilisateur ordinaire
  - Performance raisonnable (utilisation des instructions spécifiques AES des processeurs)

Dm-crypt

- Périphérique bloc : support partitions, raid, lvm
  - Restriction : taille non modifiable
- Support
  - Linux (système et données)
  - Windows (accès aux données) via FreeOTFE
- Fiabilité
  - Portable et serveurs depuis 4 ans sans soucis
- Impact sur les performances
  - Avec les processeurs actuels, non visible sauf dans certaines situations pour le swap
- Gestion des clés
  - 8 différentes, modification possible en en connaissant une seule
- Séquestre (mot de passe et en-tête)
  - En tête : cryptsetup luksHeaderBackup --verbose –header-backup <backup> <device> avec backup le fichier de sauvegarde et device le périphérique chiffré

Chiffrement logiciel d'un PC en dual-boot (méthode 1)

- Prérequis :
  - Windows et /boot de Linux en partition primaire
- Étape 1 : installation de Windows
  - Installation de l'OS
  - Mise en place du chiffrement avec Truecrypt

    => Nombre de systèmes d'exploitation :
    - Amorçage ou Amorçage mutiple : choisir Amorçage
- Étape 2 : installation de Linux
  - Installation de l'OS (cas de Ubuntu : prendre le « alternate CD »)

    => /boot doit être une partition spécifique en ext2 ou ext3

    => créer une partition chiffrée (découpable avec LVM)
  - Faire : « grub-install - -force /dev/sdaX

Chiffrement logiciel d'un PC en dual-boot (méthode 1)

- Le boot :
  - Choix entre
    - Tapez le mot de passe Truecrypt pour décoder la partition Windows et lancer cet OS
    - Tapez « ESC » qui provoque la recherche d'autres partitions bootables
      => grub prend la main et boot linux
- Le piège
  - Lors d'une mise à jour Linux :
    - Contrôler où se fait l'installation de grub (préciser /dev/sdaX et non /dev/sda)
      => si piégé, il faut réinstaller le MBR

Chiffrement logiciel d'un PC en dual-boot (méthode 2)

- Installation similaire des deux OS

  MAIS :

  - Installer grub sur /dev/sda
  - Expliquer à grub de générer la suite nécessaire pour initier le lancement de Truecrypt

    => fonctionnerait avec grub version 1 (chain loader)

    => ? avec grub version 2
- Avantage :
  - Au boot, on retrouve le comportement habituel (panneau grub à choix multiple)

Disques chiffrants

- Disponibilité
  - Capacité limitée (320Go max)
  - Non supporté sur tous les matériels
  - Livraison par Dell sans aucune notice explicative ou logiciel (à télécharger).
- Compatibilité
  - Implique de pouvoir disposer d'un système Windows pour le paramétrage
  - Sous Linux : nécessite quelques ajustements (voir notes de Bernard Perrot)

En conclusion...

- Mise en œuvre sur le nouveau matériel
  - Faible surcharge de travail pour les approches logicielles sur machine monoOS
  - Quelques difficultés en dual boot
  - Sous MacOS, chiffrement limité aux données (avant Lion)
  - Disques chiffrants non encore exploités en tant que tel
- Mise à niveau d'un parc existant
  - Plus contraignant : disponibilité de l'équipement, temps passé
- Fiabilité
  - Pas de soucis liés au chiffrement observé (sauf avec Filevault)
- Quelques contraintes
  - Acceptation par l'utilisateur
  - Implication pour les sauvegardes, les pannes,...

=> Faut-il une formation pour les ASRs et pour les utilisateurs?

Quelques liens...

- Information DSI CNRS
  - http://www.dsi.cnrs.fr/service/securite/
- Truecrypt
  - http://www.truecrypt.org/
  - http://mikenation.net/files/TrueCrypt_on_USB_without_admin_rights.pdf
- Filevault
  - http://support.apple.com/kb/HT4790?viewlocale=fr_FR