Mathrice, 16 mars 2011, Dijon

# Protection des ordinateurs Portables

Bernard Perrot - CNRS - UMR6205
<bernard.perrot@univ-brest.fr>

# Précaution

Les propos tenus ici n'engagent que leur auteur
(et encore...;-) qui n'est pas mandaté pour intervenir
sur le dispositif dont il est question.

# Contexte

- Sujet à l'étude sous l'égide du service du FSD depuis déjà plusieurs années
  - Évaluation de la solution de disques chiffrant sur portables par F. Morris et T. Mouthuy
  - Expérimentaion pilote à l'IN2P3
  - Préoccupation du Ministère depuis 2009 à propos des vols de portables
- Relance récente via la note « *Not11Y159DSI* » du DGDR Xavier Inglebert
  - C'est en raison de cette préoccupation du Ministère que cette note à été émise sous cette forme (envoi aux DU's)
- Dossier officiellement suivi par :
  - Jean-Marc Voltini (cf. la note)
  - François Morris (DSI) dans la pratique

# Contexte

- Constats à cette occasion :
  - La SSI est désormais dans le giron de la DSI
    - Cf *décision n° 100170DAJ* portant organisation de la DSI
    - François Morris a rejoint la DSI
  - Le service du FSD ne semble plus être dans la boucle...(note non diffusée par son service)
    - Sauf pour ce qui relève des informations classifiées ? (cf 2-b)
  - Note non diffusée/relayée via le réseau des CRSSI...
    - C'est un oubli...
    - Les CSSI ne savent donc pas comment la traiter...
    - Cela devrait être réparé avec la publication du guide d'utilisation
    - Ce « guide d'utilisation » n'existe pas encore, dommage qu'il n'ai pas été diffusé en même temps...

# Mise en œuvre

- Sera détaillée dans le *guide d'installation* à venir...
  - Rédaction F. Morris, et d'autres.
  - Une première version devrait être prête dans les prochains jours
- Attention à la nécessité du séquestre/recouvrement des secrets d'accès !
- Pas de difficulté technique majeure, mais du temps, forcément...
  - le recouvrement devrait imposer de fait l'intervention d'un CSSI, l'utilisateur ne peut pas mettre celui-ci complètement en œuvre lui-même

# Dispositif

- Deux niveaux de protection :
  - Premier niveaux : applicable à tous les ordinateurs portables
  - Deuxième niveau : applicable aux données sensibles
    - Le niveau encore supérieur « classifié » est à étudier avec le FSD
- Deuxième niveau :
  - Containers *TrueCrypt*
  - Pas d'alternative citée (n'est-ce pas trop restrictif ?)
  - Pas dit dans la note, mais il faut sans doute comprendre que le niveau de sensibilité est formalisé après une étude PSSI
    - ce qui n'empêche pas de le connaitre déjà... et en tenir compte
  - En l'absence de guide de mise en œuvre, pas facile de comprendre l'apport et le but de cette protection supplémentaire à la seule lecture de la note (même si nécessaire).

# Chiffrement de surface

- Il s'agit du premier niveau du dispositif de la note
- Il est écrit « *applicable à **tous** les ordinateurs portables* »
- Je ne suis pas en mesure de spécifier mieux la portée de ce « tous », mais… :
  - Cette mesure est bonne, alors pourquoi tergiverser sur le parc concerné
  - Elle est peu contraignante, donc, même remarque
  - Se pose la question des portables qui ne sont pas CNRS dans une UMR
    - Administrativement, la question se pose…
    - Techniquement (au regard de la sécurité), il n'y a aucune raison de les exclure, sauf à rendre le dispositif incohérent à l'échelle de l'Unité.
- Rappel : le chiffrement de surface ne protège qu'un ordinateur éteint !
  - Une compromission par logiciel et/ou réseau restera possible

# Chiffrement de surface (portables anciens)

- *nb : pertinent aussi pour les neufs, mais moins performants (au sens I/O).*
- Sauf pour les supports amovibles, il n'y a pas nécessité pour le chiffrement du disque interne d'une solution interopérable entre OS's
- *Macintosh's* (neufs et anciens) : pas de solution matérielle, recourir à une solution native (*FileVault*), ou bien *TrueCrypt*.
- *PC/Linux* : la solution native *dm-crypt* est satisfaisante, et la plus facile à mettre en œuvre.
  - sinon, *TrueCrypt* peut également être utilisé
- *PC/Windows* (XP, Vista, 7) : préconisation de *TrueCrypt* (totalité du disque, pas seulement un container).
- *PC mixte Windows/Linux* : utiliser *dm-crypt* pour Linux, et *TrueCrypt* pour Windows (seulement sa partition).

# Chiffrement de surface (portables PC neufs)

- cf. note : « *Recours **systématique** aux disques chiffrants* »
- Solution « simple » et efficace
- Pas de perte de performances I/O
- Disponibles au marché CNRS avec Dell :
  - Possible sur tous les *Latitude*, mais pas forcément accessible au configurateur en ligne (`dell.quadrem.net`), demander alors un devis au commercial
- Sur Dell Latitude :
  - SSD jusqu'à 128 Go
  - HDD jusqu'à 250 Go (existe en 500 Go, mais pas encore au marché Dell ?)
  - Surcoût d'environ 30€ (négligeable)

# Latitude avec disque FDE

- On parle de disque « FDE » = *Full Disk Encryption*
- Obligation d'un logiciel tiers pour mettre en œuvre et configurer le chiffrement (mode *Trusted Drive*)
- Dell fourni *Wave Embassy* (qui s'intègre à *Dell Control Point*).
  - *Wave Embassy* ne fonctionne que sous Windows
  - En conséquence, pour un PC exclusivement Linux, il faudra au moins un disque externe bootable (sur port eSata par exemple) dans le labo, avec Windows installé pour effectuer cette configuration
- Si pas « initialisé », le disque FDE se comporte comme un disque « normal », donc pas de contrainte initiale suite à l'achat
- Plusieurs (4) utilisateurs configurables : permet de ne pas partager le secret si plusieurs usagers

# Latitude avec disque FDE

- Incompatible avec le mode « veille » (en mémoire vive) : seule la «veille prolongée » (image mémoire écrite sur disque) reste possible
- Terminologie (*Wave Embassy*):
  - *Initialiser* le disque : mettre en œuvre la protection *Trusted Drive*
  - *Désinitialiser* : supprimer cette protection (les données sont conservées)
  - *Effacer la clé* : le contenu du disque est perdu (effet instantané, et supprime la nécessité du Wipe pour recycler un portable)
- *Wave Embassy* ajoute un préboot :
  - Sous Windows seul, pas de contrainte (possible de lier cette authentification initiale et le login Windows)
  - Sur un PC Linux seul ou bi-boot, incompatible avec *Grub legacy* (sans doute aussi avec *Grub 2*, mais pas testé);

# Latitude avec disque FDE et Linux

- J'ai effectué de nombreux tests, mais ai fini par identifier une solution très simple et sans véritable inconvénient :
- Il suffit de remplacer le boot via *Grub legacy* par *Grub4DOS*
  - Cela prend moins d'une minute supplémentaire à l'installation de Linux
  - Est pérenne (*Grub4DOS* est plus dynamique que *Grub legacy*)
  - Donc, à ce jour, pas de problème en fait pour un support Linux qui fonctionne (j'utilise au quotidien désormais...)
- nb : il est prudent d'installer Linux sur un disque *non-initialisé* (pré-boot pas installé)
- Le *guide d'installation* à venir mentionné par la note détaillera j'espère la procédure...
  - dans l'attente, possible de me contacter si aide nécessaire...

# Disques FDE

- Censés être très sûr vis à vis d'un vol, même ciblé
  - à la condition quand même que le mot de passe ne soit pas trivial…
- Ne protège sans doute pas des agences gouvernementales étatsuniennes
  - doit donc protéger des autres, sauf celles et ceux qui savent quand même faire…
- Il est possible d'en installer un dans un Latitude pas trop ancien (vérifier compatibilité et si Wave Embassy intégré à DCP est proposé sur le site de Dell) : compter environ 100€ pour un *Seagate ST9500422AS* (500 Go), et environ 70€ pour un *Seagate ST9250412ASG* (250 Go).

# Clés USB

- Il est très facile de perdre une clé USB, y compris si elle contient des données privées et/ou confidentielles et/ou sensibles
- Rappel : une clé USB ne convient pas au stockage (pas fiable dans le temps), mais seulement au transport de données...
- Solution simple et sans surcoût :
  - Container *Truecrypt* sur clé standard
    - Compatible et interopérable entre Windows, Linux et MacOSX (formater le container en FAT32 est préférable)
  - Pour Windows, on peut embarquer les clients nécessaires sur la même clé à coté du container (en mode « portable » pour ne pas avoir à installer de logiciel sur un poste client)
    - mais il faut quand même que TrueCrypt (le driver) réside sur la machine cliente...
  - Pour Linux, il faudra autoriser le montage avec un « sudo »

# Clés USB

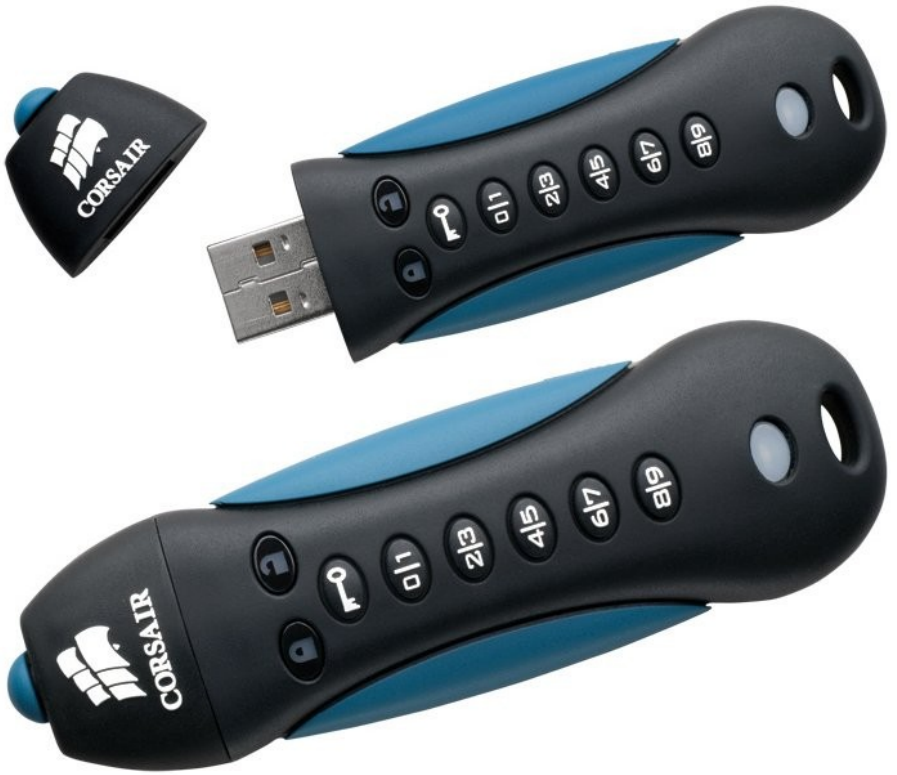
- Sinon, la difficulté est d'avoir une solution compatible et interopérable entre les différents systèmes d'exploitation
  - Cela exclu les clés nécessitant un logiciel propriétaire (en général seulement sous Windows) sur l'ordinateur
- La seule façon de résoudre ce problème est d'avoir la crypto embarquée sur la clé;
  - Il faut donc un dispositif permettant d'entrer le secret indépendamment de l'OS :
- Clés biométriques :
  - *M700 bio USB drive* (MXI Security)
  - À l'exclusion de toutes les autres (lecteur biométrique sur la clé et crypto dans le PC) !
  - Chère, pas de revendeur en France… dommage… j'aimais beaucoup !

# Clés USB

- Clés chiffrantes avec dispositif mécanique :
  - Clé Thomson ? (roues codeuses)
    - Très chère, pas pour nous...
  - *Corsair Padlock-2*
    - Attention, modèle précédent « Padlock 1 » non fiable
  - Autres ? (je ne connais pas...)
    - La rareté du choix n'est pas enthousiasmante..

# Cle USB Corsair Padlock-2

- Vente sur Internet… (cf note de Inglebert)
  - Pas simple dans un labo (compatible procédure d'achat ?)
- Relativement chère :
  - 8Go ~ 50€
  - 16Go ~ 80€
- Relativement grosse (masque le connecteur USB proche…)
- Plein de défaut…
  - … mais pas mieux sur le marché ?



# Cle USB Corsair Padlock-2

- On rentre le code, et on a 20s pour brancher la clé :
  - Pour cette autonomie, la clé contient une pile rechargeable...
  - ... en toute logique, cette accu va défaillir un jour (sera alors toujours utilisable, mais il faudra brancher d'abord...)
- « clavier » 5 touches (ne pas se fier à la sérigraphie qui n'est que mnémonique)
- Code PIN de 4 à 10 chiffres
  - base 5, donc entropie limitée à 12206875 (~ 20 bits, pas énorme)
  - Sans donc craquable rapidement en force brute pour qui peut monter un petit dispositif électronique pour entrer les codes
- Sera efficace en cas de perte fortuite
- Ne sera probablement pas efficace contre un vol ciblé par des personnes très motivées à récupérer le contenu.

# Cle USB Corsair Padlock-2

- La notice (sur le site Corsair, pas celle fournie sous blister) parle d'un *Master PIN* permettant de débloquer la clé sans perte des données, mais cela ne fonctionne pas : recouvrement pas possible
- Dispositif pour effacer le PIN, en perdant les données (il faut reformatter) : efficace si on a perdu le code PIN, mais donc, la clé volée conserve sa valeur marchande brute.
- Il y a eu un grave bug, signalé en juin 2010 : semble résolu, mais n'y en a/aura-t-il pas d'autres ? (la Padlock-1 n'était pas fiable)
- Sans doute des codes ou manipulations obscures...
- Pas certifiée FIPS
- Corsair pas vraiment connu pour son expérience en sécurité, alors ?
- Alors... on n'a pas vraiment d'alternative à ce jour... !

# Notes

# Des questions ?