UNIVERSITÉ DE LORRAINE

Institut Jean Lamour

PENSER LES MATÉRIAUX DE DEMAIN

cnrs

Point sur le chiffrement des ordinateurs portables à l'IJL

UIJL - UMR 7198 - CNRS - Université de Lorraine

Journée 2RCE Lorraine - ATILF – Salle LMBS

Retour d'expérience sur le chiffrement des ordinateurs portables

Introduction : pourquoi chiffrer ?

Vols de matériels informatiques en recrudescence ➔ Demande CNRS de chiffrer les postes, notamment ceux mobiles :

- Note de la DGDR CNRS du 16/01/2011 - NOT11Y159DSI
- Note DSI CNRS aux DU – 21/12/2012 – NOT15YDSI-RSSIC

Impacts directs :

- perte d'actifs … et leurs disponibilité, intégrité, confidentialité, traçabilité

Impacts indirects :

- Atteinte au personnes morales/physiques, notoriété, confiance, crédibilité
- Atteinte à des tiers : partenaires, collaborateurs, …

Contextes spécifiques

- Institut Jean Lamour - ~550 pers. - Unité sensible (ex- E.R.R.) sous régime Z.R.R. :
  - PPST renforcée !
  - Accès aux ZRR subordonné à autorisation préalable du HFDS

ZRR : Au Pénal : Est puni de six mois d'emprisonnement et de 7500 euros d'amende le fait […] de s'introduire, sans autorisation à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications.(cf. Article 413-7 du code pénal)

Pourquoi chiffrer ?

Que nous apporte le chiffrement ?

- Données protégées, même lorsqu' éteint …
- Restriction & contrôle de l'accès aux données
- Données protégées si supports démontés/déplacés/volés
- Actif réduit à la valeur matérielle en cas de vol
- En fin de vie : « jeter la clé » suffit
- Et plus ? …

Important

- Ne dispense pas de la sauvegarde !
- Rançongiciels : Cryptowall, TeslaCrypt, CTB-Locker, Locky, … chiffrent aussi ☹

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Sommaire

De l'Informatique de confiance … à la puce TPM

de TCPA à TCG, & Palladium/NGSCB

Solutions matérielles de chiffrement déployées

Disques auto-chiffrants DELL, HP et logiciels associés

Solutions logicielles de chiffrement déployées

Sous MS Windows , Apple OS X , Systèmes Linux

Bilan / Tendances / Conclusion

De l'Informatique de confiance … à la puce TPM

De TCPA … et Palladium

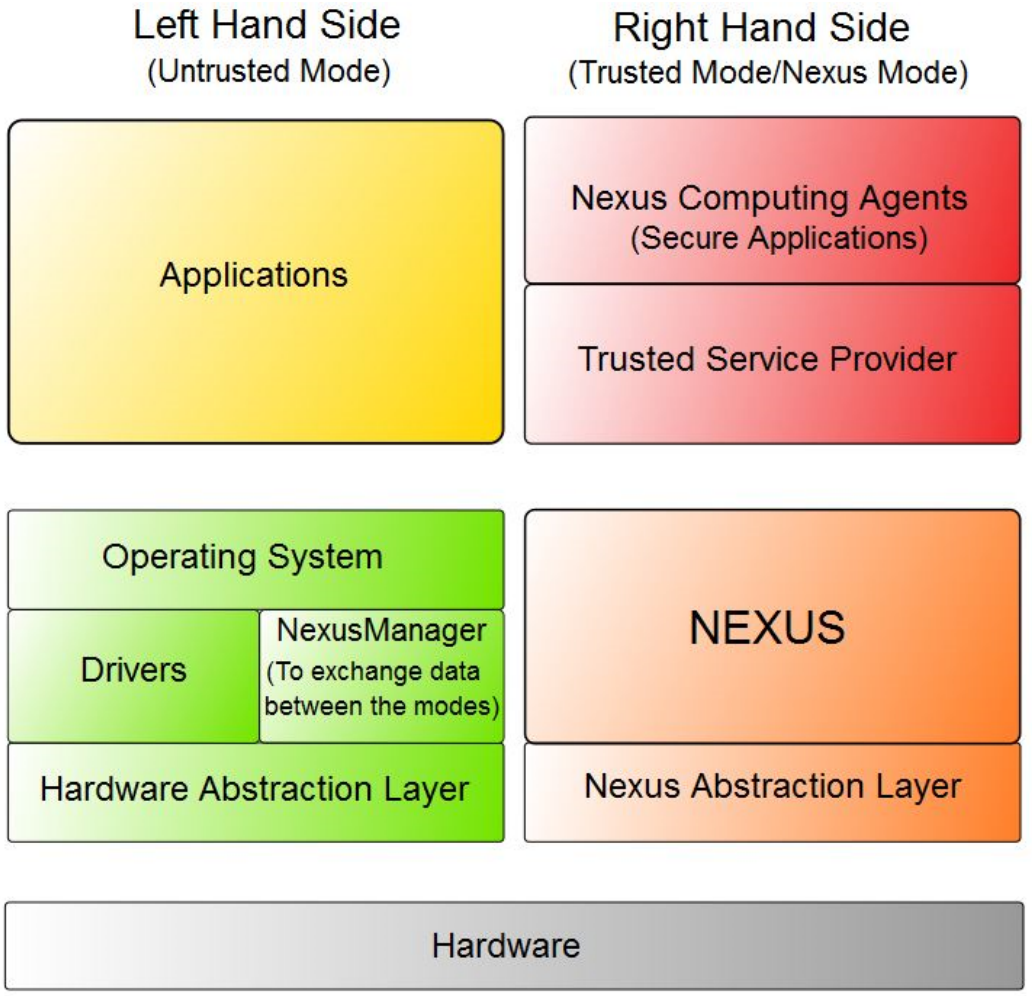
- TCPA Trusted Computing Platform Alliance (1999 – 2002)
  - Fondateurs : Compaq, Hewlett-Packard, IBM, Intel, and Microsoft ... rejoints par ~70 leaders hardware/software
  - **BUT** : promouvoir la confiance en une plateforme informatique et sa sécurité
  - TCPS : Trusted Computing Platform Specifications - V1.0, 1.1a, 1.1b
  - 1ère implantation physique (2002) : IBM Thinkpad T23 : ESC, puis ESS 2.0
  - 1ère implantation physique (2002) : IBM Thinkpad Série 60 : TPM 1.2

    http://www.thinkwiki.org/wiki/Embedded_Security_Subsystem#Models_featuring_this_Technology

- Palladium = Microsoft Trusted Windows
  - Noyau Windows / Applications classiques + Noyau Nexus/Trusted App's
  - Isolation hardware de processus, chiffrement, mesures de l'intégrité, authentification /approbation locale ou distance de la configuration hardware/logicielle, création et distribution de DRM (Gestion des droits numériques / procédés anti-copie/anti-diffusion)

De l'Informatique de confiance … à la puce TPM

Palladium



De l'Informatique de confiance … à la puce TPM

De TCPA à TCG …et NGSCB

- Trusted Computing Group (2003 -)
  - Fondateurs AMD, Hewlett-Packard, IBM, Intel, and Microsoft ... rejoints par les acteurs de la téléphonie mobile/PDA

BUT : créer un circuit intégré conforme aux TCPS - *Trusted Computing Platform Specifications* - pour offrir des services sécurisés sur une plateforme informatique certifiée de confiance

⇒ **Circuit intégré TPM : Trusted Platform Module**
+ TSS : TGC Software Stack :

Spécifications TSS : Version 1.2 (2011)
Spécifications TSS : Version 2.0 (2014)

- Palladium ➔ NGSCB : Next-Generation Secure Computing Base
  - MS Trusted Windows : promis dans Windows Vista (Longhorn)

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

De l'Informatique de confiance … à la puce TPM

Héritage de feu-Palladium ?

- Sujet « Trusted Computing » très controversé : DRM, Appli. non approuvée => non exécutable, … :

  http://www.gnu.org/philosophy/can-you-trust.html

  par Richard Stallman

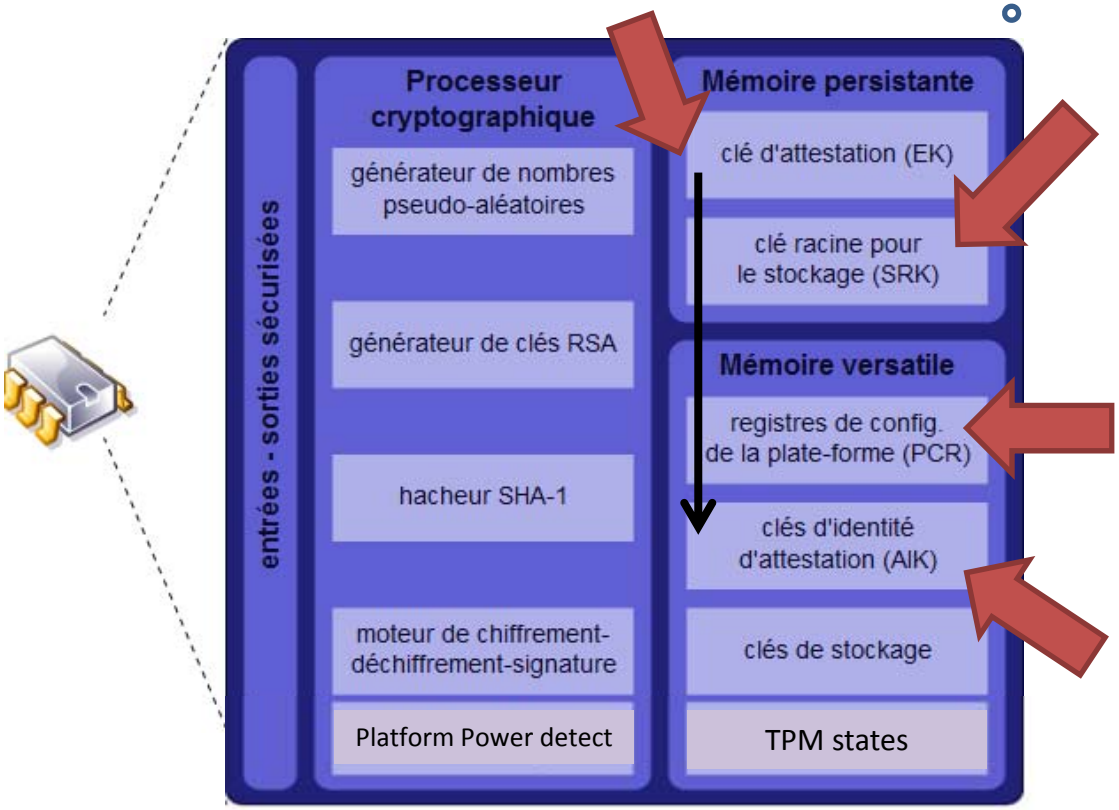
➔ Abandon de l'intégration dans Windows Vista : Oui, mais ….

Quelles fonctionnalités '"restent"' depuis Vista ? Palladium, le retour ?

- BDE : BitLocker Disk Encryption avec/sans puce TPM
- Measurement : Vérification d'intégrité (du BIOS à l'OS startup) par puce TPM
- Measured Boot - Windows 8
  - Vérification d'intégrité de tous les composants du boot, jusqu'à exécution de l'anti-malware
- Certificate Attestation - Windows 8.1
  - Certificats protégés : signés/vérifiés par les clés d'attestations (AIK) "enfermés" dans la puce TPM
- Device Guard - Windows 10
  - Plateforme verrouillée & virtualisée qui n'exécutera que des applications dûment approuvées (signées numériquement par les éditeurs, le Windows Store, ou l'entreprise elle-même)

La puce TPM

EK : Endorsement Key
Racine de Confiance (RoT : Root of Trust)
Paire de clé privée/publique intégrée par le constructeur !
Non modifiable & certificat associé signé par AC constructeur



SRK : Storage Root Key : clé (2048 bits) créée lors de la phase de « prise de possession » du TPM: Take Ownership

Dynamic Root of Trust Measurement (DRTM) ➔Registres PCR
Mémorisent les mesures d'intégrité initiales de la 'plateforme' (160 bits) : imbriquées, SHA1 + Hash

Clés AIK : paires asymétriques à usage d'identification, signatures et, elles-mêmes signées par le certificat constructeur associé à l'EK

La puce TPM

TPM : Static Root of Trust Measurement - SRTM

- Registres PCR : « Measurement & Mémorisation » de l'intégrité de la plateforme :
  à la « prise de possession » du TPM
- Confiance en la « Computing Plateform » ? A chaque reboot : re-mesuré + comparaison

Si TPM réinitialisé : effacement des PCR … et de la SRK + toutes les clés dérivées !!!

En **bleu** : PCR utilisés par Bitlocker

PCR 0	• Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions
PCR 1	• Platform and Motherboard Configuration and Data
PCR 2	• Option ROM Code
PCR 3	• Option ROM Configuration and Data
PCR 4	• Master Boot Record (MBR) Code [bytes 0 – 01B7h]
PCR 5	• Master Boot Record (MBR) Partition Table [bytes 01B8h – 01FFh]
PCR 6	• State Transition and Wake Events
PCR 7	• Computer Manufacturer-Specific
PCR 8	• NTFS Boot Sector
PCR 9	• NTFS Boot Block
PCR 10	• Boot Manager
PCR 11	• BitLocker Access Control
PCR 12-23	• Réservé pour un usage ultérieur

Mémorise l'intégrité hardware + secteur de boot, peu importe l'OS

Mémorise l'intégrité logicielle
+
usages ultérieurs

La puce TPM 

TPM : Dynamic Root of Trust Measurement - DRTM

- Objectif : « démarrage « en toute confiance » d'un OS
  ➔ OS vérifié avant même qu'il boote .. par DRTM
  PCR reset + mesures dynamiques, signées
  ➔ l'OS (voire les App.) peuvent s'autocontrôler à postériori

PCR17 – DRTM and launch control policy

PCR18 – Trusted OS start-up code

PCR19 – Trusted OS (for example OS configuration

PCR20 – Trusted OS (for example OS Kernel and other code)

PCR21 – as defined by the Trusted OS

PCR22 – as defined by the Trusted OS

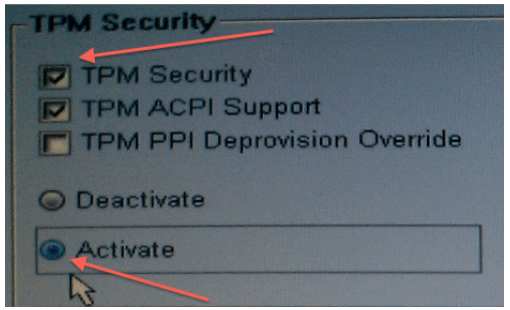
Mémorise l' intégrité du boot

et /ou autres parties de l'OS (au choix)

Réf. : https://en.wikipedia.org/wiki/Trusted_Execution_Technology

La puce TPM

TPM : Gestion d'Etat



- Enabled/Disabled - Config dans le BIOS
  ➔ Electrique : ON/OFF
- Activated/Inactive - Config dans le BIOS
  ➔ prise de possession possible, si pas déjà fait
- +
  Owned/unowned
  ➔ Prise de possession nécessaire pour créer SRK
  ➔ Prise de possession nécessaire pour éval. des PCR

Niveau de confiance à accorder à la puce TPM ?

- Chaque changement d'Etat du TPM est **assujetti à présentiel** : demande de reboot, saisie clavier, …
- Sert à créer les paires "clé privée/publique"
  Une clé privée ne peut jamais sortir de la puce en clair, sort seulement chiffrée avec une clé résidente du TPM

TPM : Platform Power Detection : allumé, veille, hibernation, …

- Selon l'état de la plateforme, fonctionnalités TPM accessibles ou non

La puce TPM 

Microsoft : « Mesures & Chiffrement » 

Microsoft BDE – Bitlocker Disk Encryption

- **Chiffrement de supports amovibles : la puce ne pouvant suivre le support**
  - **Déverrouillage du support chiffré sans TPM ➔ par mot de passe**
    ➔ Bitlocker-To-Go

- **Chiffrement de supports intégrés dans la plateforme : TPM optionnel**
  - **Avec TPM : si Mesures = OK ☺**
    - **Déverrouillage TPM automatique**
    - **Déverrouillage TPM avec code PIN**
    - **Déverrouillage TPM avec support USB bootable (dite « clé USB de démarrage »)**

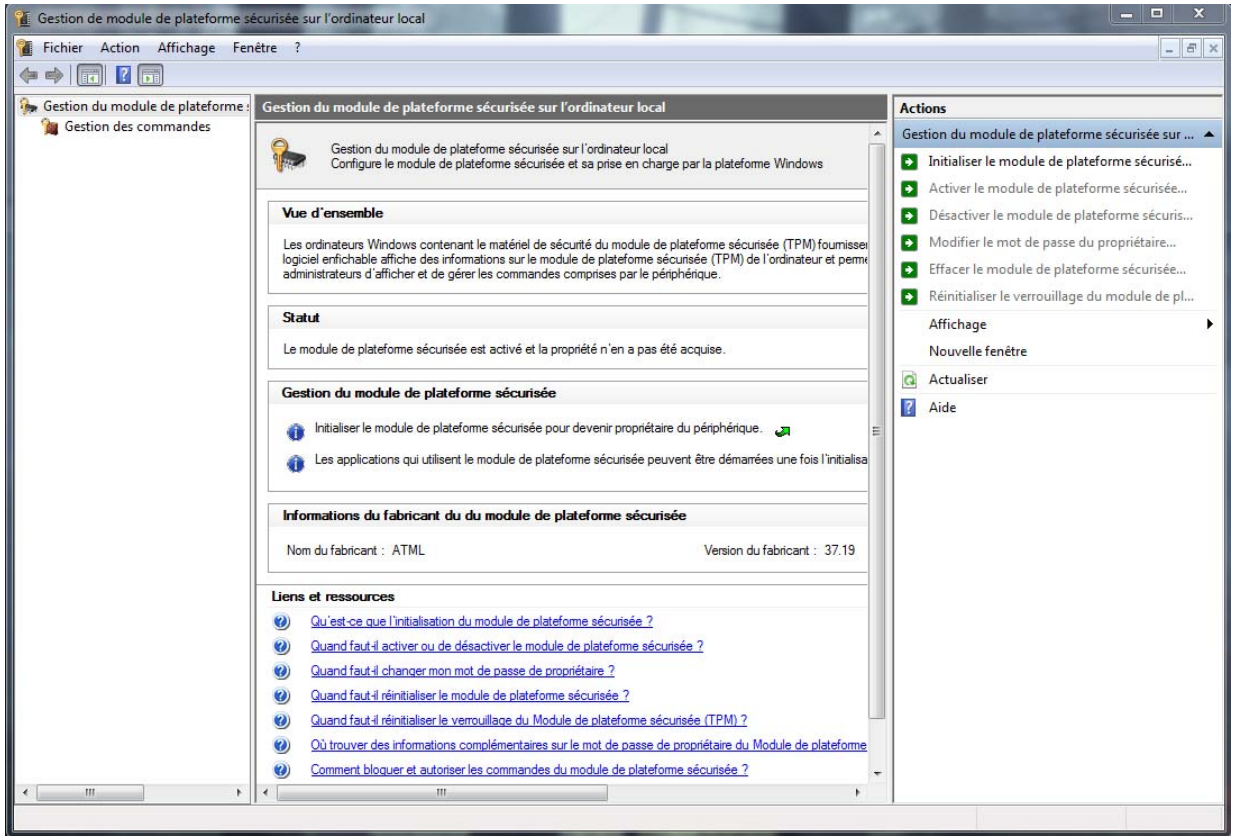
    et si TPM refuse - Mesures = KO ☹
    - **avec la « clé de récupération Bitlocker »**
  - **Sans TPM :**
    - **idem supports amovibles ➔ BitLocker-To-Go**

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

La puce TPM

Autres outils

Console tpm.msc



La puce TPM 

Apple – « Mesures & Chiffrement »

DTRM

- **Sans TPM: SIP - System Integrity Protection – alias ‘rootless’**

Chiffrement

- **Sécurité non basée sur un ‘RoT’ TPM : FileVault / FileVault 2**

Logique constructeur prédominante

- **Plus d’intégration de puce TPM … depuis 2006**
- **Hardware spécifique Apple (ARM A7 intégrant la notion de ‘RoT’)**
- **Gatekeeper (App signées/, Développeurs approuvés), Sandboxing, SIP**

Linux – « Mesures & Chiffrement »

DTRM

- **Possible avec TPM : TrustedGRUB**
  Extension du GRUB boot loader

Chiffrement

- **Pas de recours à un ‘RoT’ de type TPM**
- **LUKS = chiffrement + système de stockage des passphases**
- **Master Key : stockée chiffrée dans le ‘LUKS header’ de la partition chiffrée**

La puce TPM 

TPM : Conclusion & tendances

- **BIOS compatible TCG**
- **INTEL : TXT - Trusted eXecution Technology**
- **MICROSOFT's World :**
  - **Windows / Ordinateurs PC**
  - **Windows RT / 'Surface' … & Mobiles**
- **Autres fonctionnalités:**
  - **Mails sécurisés X.509**
  - **Connexions sécurisées 802.1x**

TCG : autre plateformes de confiance promues

- **Trusted Network Connect : TNC**
- **Trusted Mobility Solutions : TMS**
- **…**
- **Self-Encrypting Drives/Disques auto-chiffrants : SED**

Solutions de chiffrement déployées …

A l'Institut jean Lamour …

Solutions Matérielles de chiffrement

- **SED – PC portables Dell**
- **SED – PC portables Hewlett Packard**

Solutions matérielles

Disques auto-chiffrants DELL & logiciels associés

Pré-requis

- Un PC portable avec TPM allumé et activé
- Un "Self-Encrypting Disk« - Chiffrera TOUT le disque (toutes ses partitions)
- Logiciel DDPA - Dell Data Protection | Access
- Etre le « bon » Administrateur du « bon » domaine pour toute re-configuration :
  - Logiciel exigeant : domaine/workgroup : le même qu'à la 1ère config.

Configuration

1 – Créer le login/domaine/mot de passe « Administrateur du SED »
2 – Créer le/les login/domaine/mot de passe de chaque usager additionnel

NB :

- DDPA peut s'appuyer sur un AD Windows
- Choisir en 1 ou 2 : compte/domaine/passphrase « passe-partout « , ie. de récupération/recouvrement (pour l'Equipe informatique)
- Possibilité de synchroniser mots de passe chiffrement & celui de session Windows

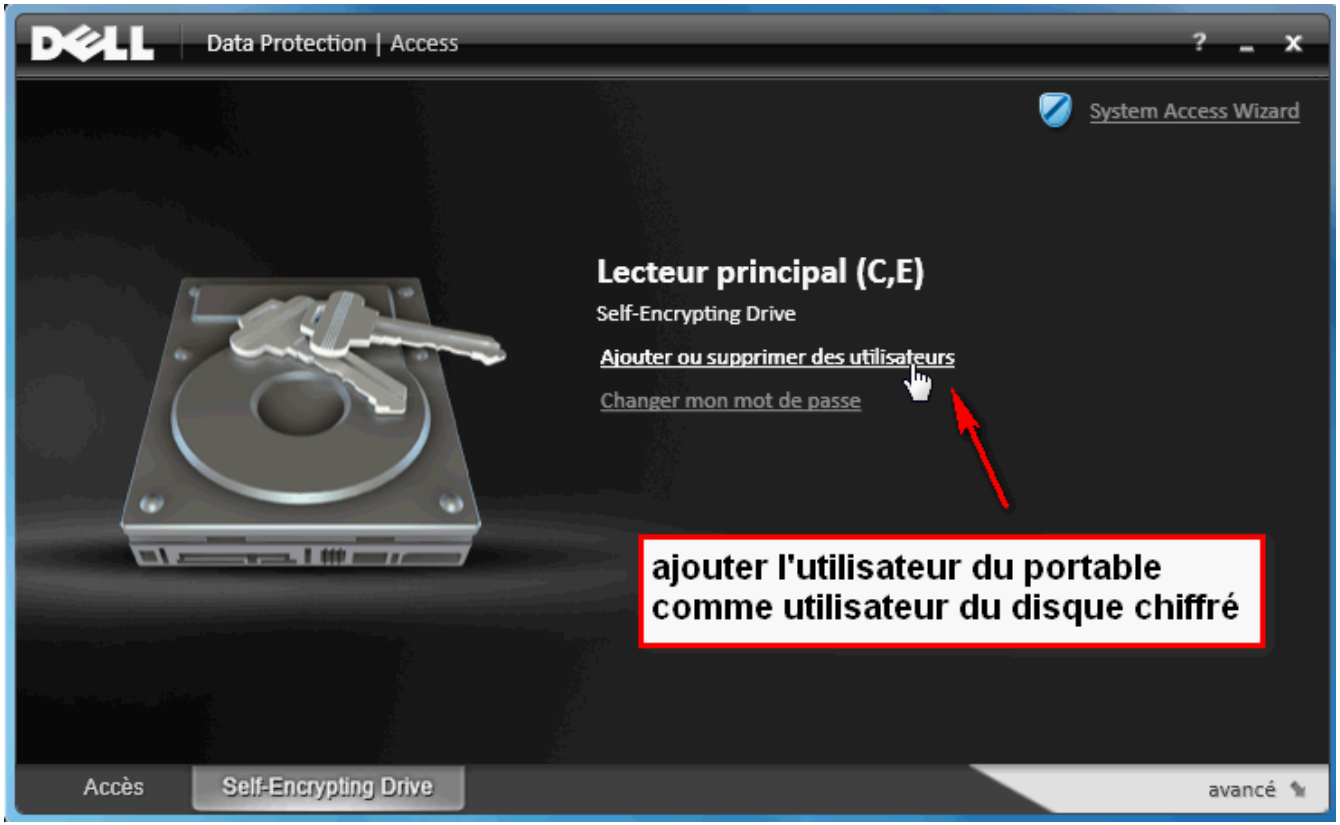
Disques auto-chiffrants DELL & logiciels associés

Logiciel DDPA - Dell Data Protection | Access

Solutions matérielles

Disques auto-chiffrants DELL & logiciels associés

Logiciel DDPA - Dell Data Protection | Access



Solutions matérielles

Disques auto-chiffrants DELL & logiciels associés

- **Pas de séquestre de chaque clé d'usager**
  Séquestrer le « passe-partout » !

Suppression du chiffrement, sans perte des données

DDPA System Reset

- **Advanced > Maintenance > Reset System**
- **"I understand that this will reset my system to factory Dell settings"**
- **Reboot**

Après cette suppression "matérielle"

- **DDPA désinstallable**

Bilan IJL / Disques auto-chiffrants

Retour d'expérience : SED sur PC portable DELL

- **Stabilité bonne**
  - Pas de soucis / variation de versions BIOS
  - Pas de casse disque lors des configurations
  - Tant que OS = MS Windows : OK
  - Linux : update du boot loader ➔ potentiellement : Destruction/altération du pré-boot SED ☹
- **Déverrouillage hors PC d'origine**
  - DELL : possible et correcte
    - Sur tout PC Dell avec logiciel DDPA - Dell Data Protection Access
  - Suppression du chiffrement
    - Simple & efficace
- **Partie Logicielle : DDPA**
  - Logiciel simple et abouti
  - Windows only ☹
  - PC en configuration Linux : aucun moyen de modifier la config DDPA/SED
- **Conseils**
  - Eviter usages : dual boot ; Linux seul

Solutions matérielles

Disques auto-chiffrants HP & logiciels associés

Pré-requis

- Un PC portable … TPM non utilisé (pour SED)
- Un "Self-Encrypting Disk« - Chiffrera TOUT le disque
- Logiciel HP Protect Tools

Configuration

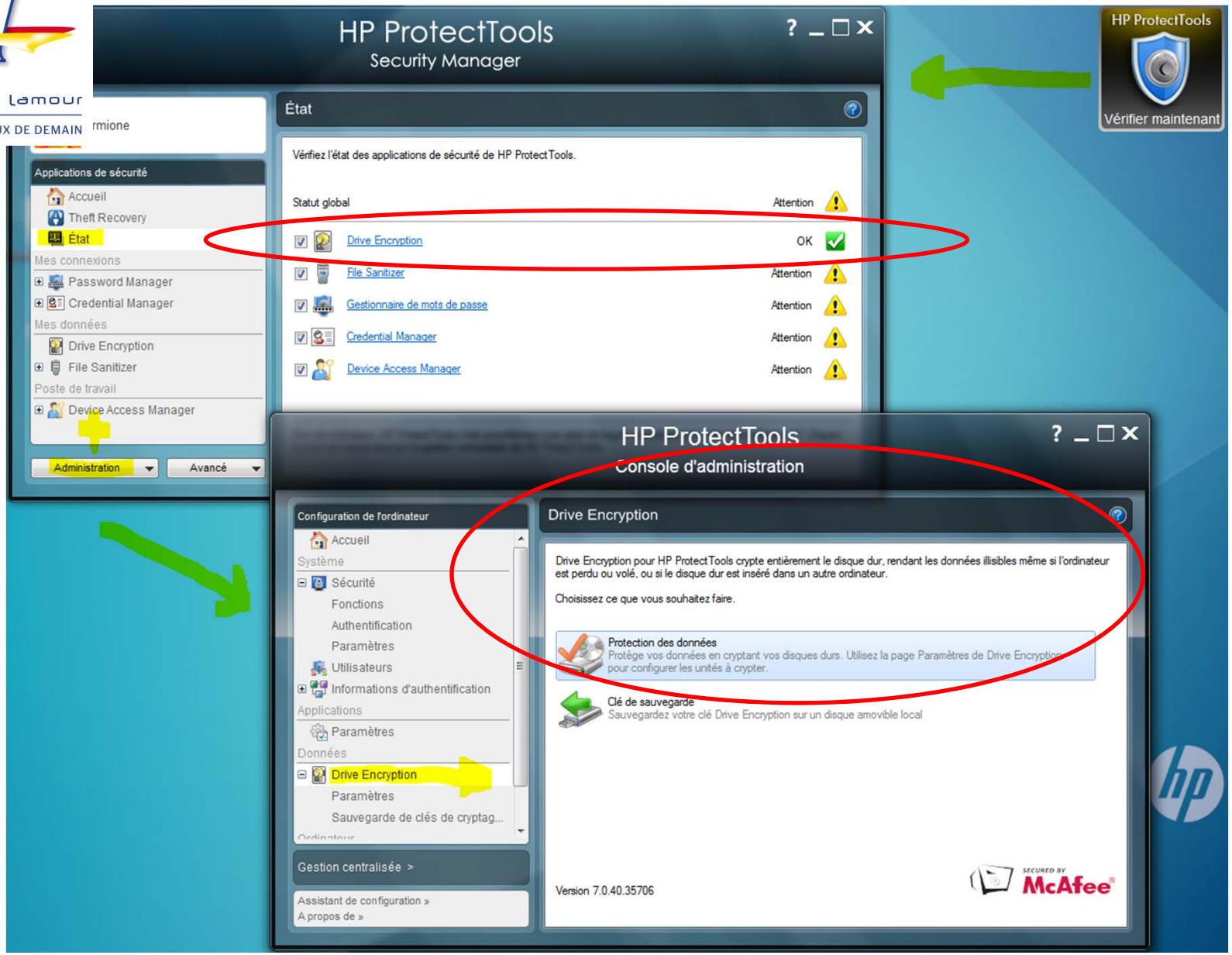
- Définir l'Administrateur HP Protect Tools = Session Admin. Windows
- Activer la fonction de sécurité « Drive Encryption »
- Activer le chiffrement du SED via « Administration => Protection des données »
- **Fichier généré : 'DriveEncryption-nom du pc.dat'** : clé à séquestrer !

Solutions matérielles

Disques auto-chiffrants HP & logiciels associés

Institut Jean Lamour

PENSER LES MATÉRIAUX DE DEMAIN



Solutions matérielles

Disques auto-chiffrants HP & logiciels associés

- **Séquestrer la clé SED, unique : impérativement !**
- **Pas de clé par usager :**
  - **Déverrouillage par ouverture de session**
  - **Mot de passe des comptes windows = la clé usager**

    ➔ **Forte intégration à Windows**

Suppression du chiffrement, sans perte des données

- Idem : via « Administration => Protection des données »

Bilan IJL / Disques auto-chiffrants

Retour d'expérience : SED sur PC portable HP

- **Stabilité aléatoire**
  - Très dépendant de la version du BIOS
  - Dépendant de la version firmware disque
  - Configuration de certains SED …. Casse ☹ ➔ échange Std
- **Déverrouillage du SED hors PC d'origine**
  - Nécessaire si panne : carte vidéo, carte mère, …
  - Médiocre … voire impossible sur un PC 'autre' ☹
    - Solution : posséder chaque PC portable à l'identique, en état & dispo. !
- **Partie Logicielle**
  - Logiciel avec foison d'autres outils de sécurisation
  - Forte intégration à Windows : SED inutilisable avec LINUX ☹
- **Sécurité**
  - la fonction de sécurité « Drive Encryption » n'utilise pas TPM ☹
- **Conseils**:
  - Eviter usages suivants : dual boot ; Linux

Solutions de chiffrement déployées …

… à l'Institut jean Lamour …

Solutions Logicielles de chiffrement

Windows : **BDE – Bitlocker Disk Encryption**

OS X : **FileVault**

Linux : DMCrypt + LUKS

Solutions logicielles

MS Windows

BDE – Bitlocker Disk Encryption

- Chiffrement : clé 512 bits : 256 AES-CBC + 256 diffusion Elephant (distorsion basée sur N° secteur)

Pré-requis

- Un PC portable … avec TPM allumé, et activé
  - Sans TPM : BitLocker To Go : possibilité de lire le support sous Windows XP et Vista
- Windows 7 Pro/Enterprise-Utimate, Windows 8 et ultérieurs

Configuration

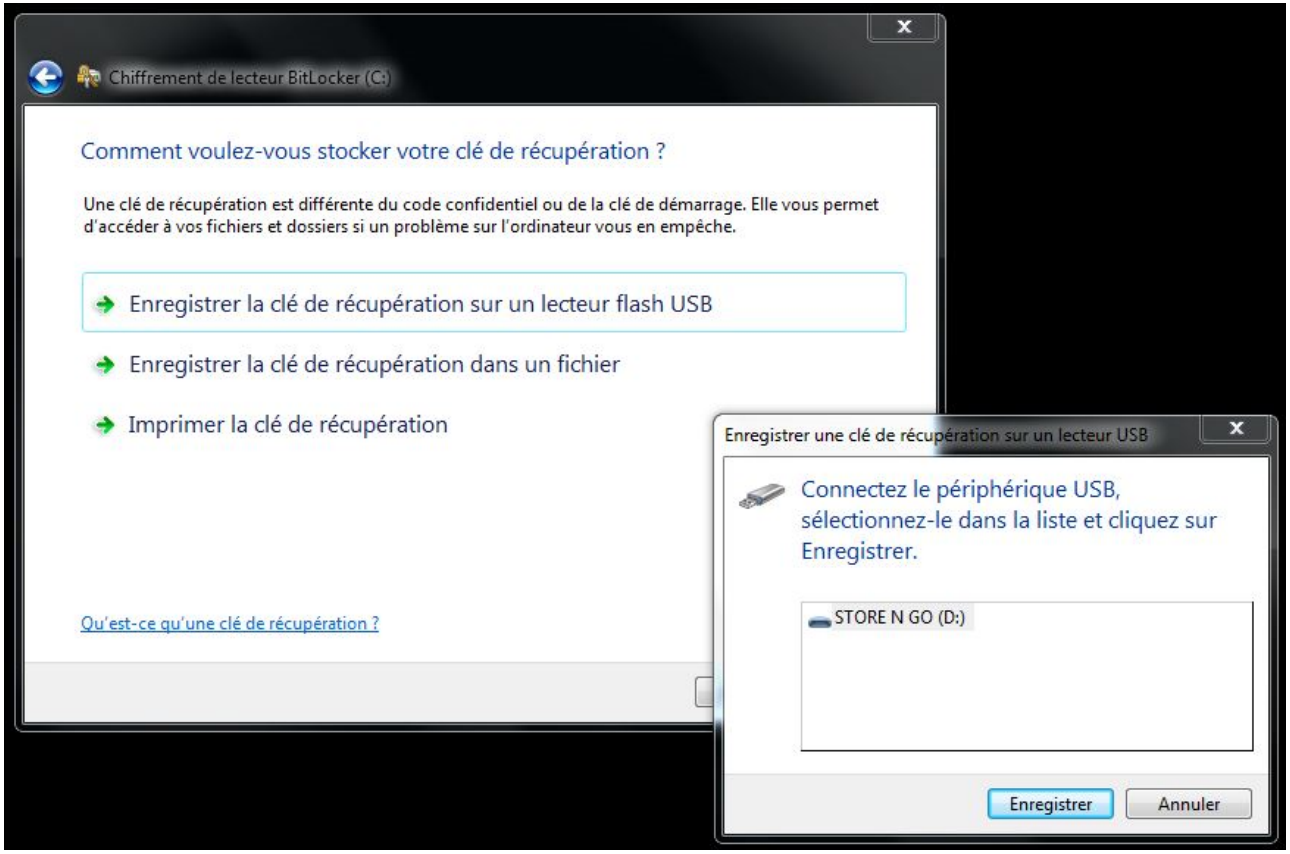
- Sur chaque lecteur logique ➔ Menu « Activer Bitlocker … »

- Pour chaque Lecteur chiffré : séquestrer la clé de récupération Bitlocker !

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

BDE



Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

BDE

Principe

- **Chaque secteur : chiffré/déchiffré avec la FVEK : Full Volume Encryption Key**
- **‘FVEK en clair ’ : jamais écrit sur le lecteur !!!**
- **FVEK : chiffrée/protégée par la VMK : Volume Master Key**
- **‘FVEK chiffrée’ : écrite sur le lecteur (Blob dans le Volume Metadata)**
- **VMK : chiffrée/protégé par un ou plusieurs Protecteurs**
- **‘VMK chiffrée’ : écrite sur le lecteur (Blob dans le Volume Metadata)**

➔ **Pour déverrouiller, il faut présenter un des « Protecteurs »**

Solutions logicielles

BDE

Avec les « Protecteurs »

→ Récup. clé VMK

→ Récup. clé FVEK

→ Accès R/W aux secteurs disques

- **TPM fournit une clé en environnement de confiance avéré 'RoT'**
  - Méthode la plus utilisée
    +
    Génère une « clé de récupération » ➔ Permet de se passer du TPM si problème
- **« Clé de démarrage USB »**
  - Support bootable avec clé de chiffrement)
- **TPM + un code PIN**
- **TPM + « clé de démarrage USB » :**
  - Méthode la plus sûre
  - Pré-boot sur USB →vérification de la plateforme TPM par le code de boot USB ☺

Solutions logicielles

BDE

Bitlocker

Gestion centralisée du séquestre des « clés de récupération » ?

- Sauvegardées dans AD - Windows Server 2003 SP1 et +
- Interactions AD ⇔ TPM …

➔ **MBAM : Microsoft BitLocker Administration and Monitoring**

- BitLocker , et BitLocker To Go

WinRE

Attention à Windows Recovery Environnement (WinRE), si installé

- Déplacé à l'initialisation de Bitlocker vers partition non chiffrée MSR - « Microsoft System Reserved »

Remarques

- Snapshots = en clair : volsnap.sys ⇔ fvevol.sys (Bitlocker) ⇔ volmgr.sys ⇔ disque
- Lancer le Chiffrement au dernier moment … qq heures; ordi '"utilisable"'; si reboot, clé de récupération demandée tant que non terminé

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

BDE

Sensible aux 'Measurements' SRTM du TPM !!!

➔ **Réclamation soudaine de la « clé de récupération Bilocker » … à chaque boot ☹**

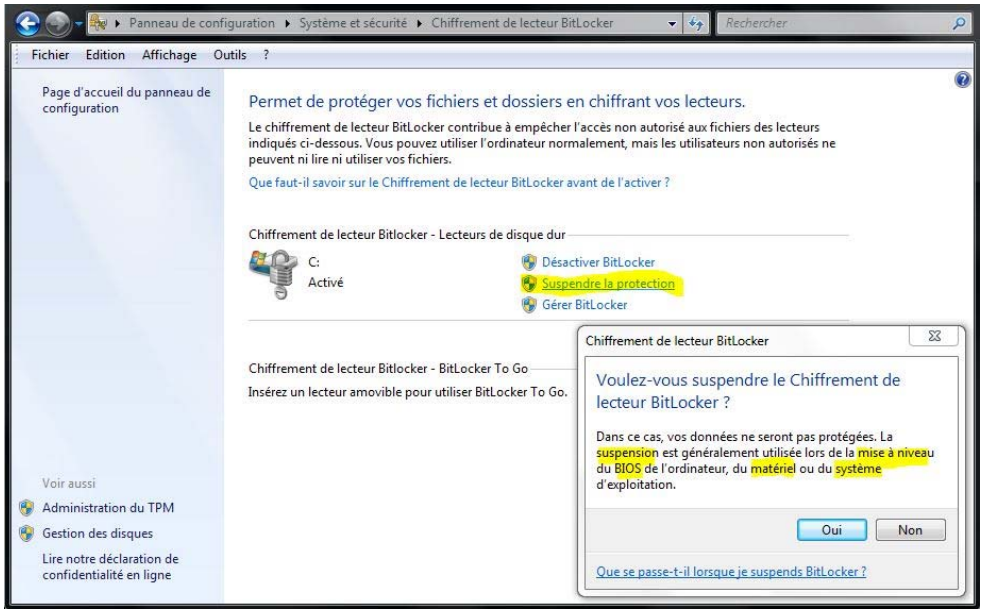
Sources du problème : Cf. page « TPM : Static Root of Trust Measurement : SRTM »

- Update du BIOS
- Modifications : MBR , table de partition, NTFS boot sector/block, Windows boot manager, …
- Certains « Windows Update » (1x/an) ➔ Mauvaise surprise pour l'usager au reboot ☹

Solution

Intégrée à BDE :

1. Suspendre la protection
2. Reboot
3. Rétablir la protection

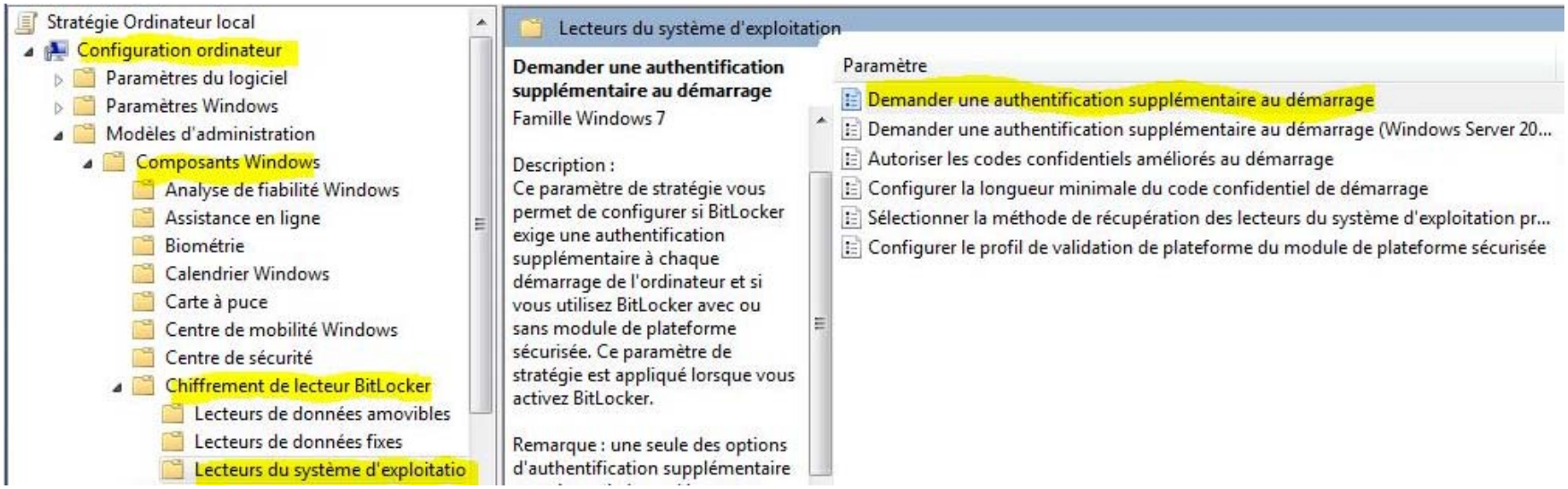


Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

Consoles

gpedit.msc



manage-bde.exe - Sous console de commande

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

Apple OS X

FileVault 2

- *Sous OS X 10.7 (Lion) et +*
- *FDE : Full Disk Encryption - XTS-AES 128 bits*

… versus FileVault ‘’1”

- *OSX 10.6 et antérieur*
- *Chiffrement partiel dossier/fichier*
- *Soucis avec Time Machine*

➔ *Déconseillé*

Pré-requis

- Un Ordinateur Apple sous OS X 10.7 ‘Lion’ … pas de puce TPM
- "Recovery HD" : boot (via ‘cmd + R’) sur partition Apple cachée (depuis “Lion”, plus de DVD)

Configuration

- Tableau de bord « Sécurité et confidentialité » - Onglet « FileVault »
- Création de la « clé Établissement » ➔ la seule à séquestrer
- Diffusion de cette clé sur chaque poste
- Activation de FileVault
- Autoriser chaque compte Utilisateur à déverrouiller (les non autorisés : assujettis à tiers autorisé)

Apple OS X

Activation du compte root

https://support.apple.com/fr-fr/HT204012

Cf. Préférences Système.

- Dans le menu Présentation, sélectionnez Utilisateurs et groupes.
- Cliquez sur l'icône de cadenas et authentifiez-vous avec un compte d'administrateur.
- Cliquez sur Options d'ouverture de session.
- Cliquez sur le bouton « Édition » ou « Rejoindre » situé en bas à droite.
- Cliquez sur le bouton « Ouvrir Utilitaire d'annuaire ».
- Cliquez sur l'icône de cadenas de la fenêtre Utilitaire d'annuaire.
- Saisissez un nom et un mot de passe d'administrateur, puis cliquez sur OK.
- Sélectionnez Activer l'utilisateur root dans le menu Édition.
- Saisissez le mot de passe root que vous souhaitez utiliser dans les champs Mot de passe

Apple OS X

Création de la clé d'Etablissement

Activer le « mot de passe principal »

- Préférences Système ➔ panneau des préférences Utilisateurs et groupes.
- Bouton Services ➔ option « Définir le mot de passe principal... »
- https://support.apple.com/fr-fr/HT202385

➔

2 fichiers créés :

/Library/Keychains/FileVaultMaster.cer (à supprimer)
/Library/Keychains/FileVaultMaster.keychain (= clé Etablissement - protégée par mot de passe)

Ouvrir avec 'Trousseau d'accès' la clé créée

- supprimer le "FileVault Master Password"

➔ **FileVaultMaster.keychain**
= 'Clé d'Établissement' à distribuer … à séquestrer !

Solutions logicielles

Apple OS X

Distribution de la clé d'Etablissement

1 - Copier la 'clé d'Etablissement' sur le Mac à chiffrer

Sous /Library/Keychains/

2 - Rectifier droits et permissions

$ sudo chown root:wheel /Library/Keychains/FileVaultMaster.keychain

$ sudo chmod 644 /Library/Keychains/FileVaultMaster.keychain

3 - Activer 'FileVault 2'

… et associer/autoriser les comptes usagers

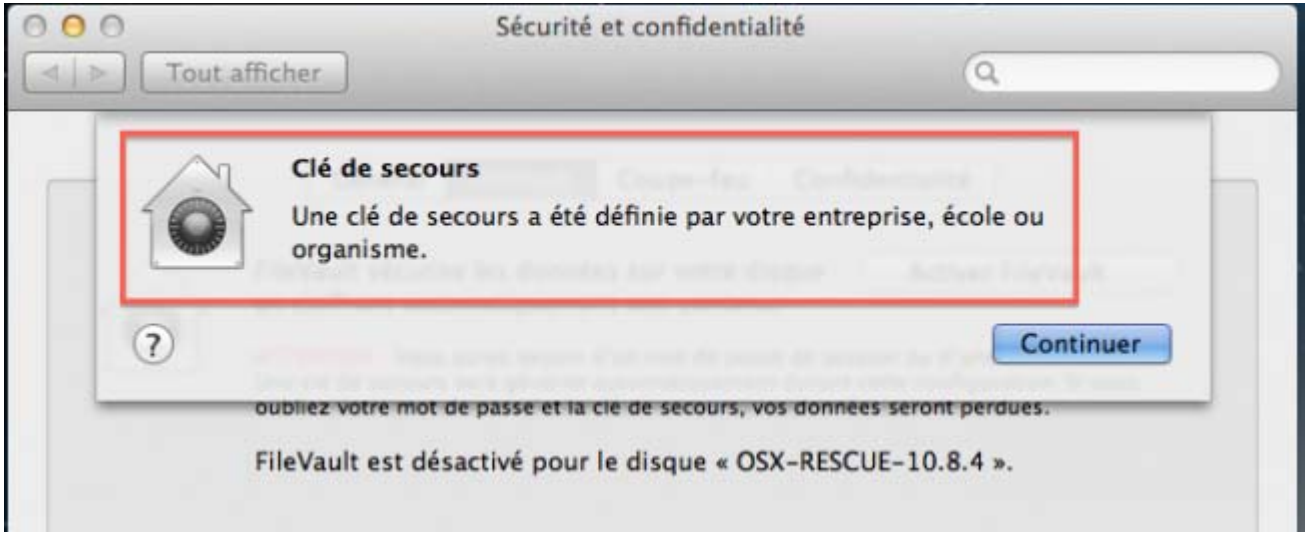
Apple OS X

Activation de FileVault …

Solutions logicielles

Apple OS X

Activation de FileVault …



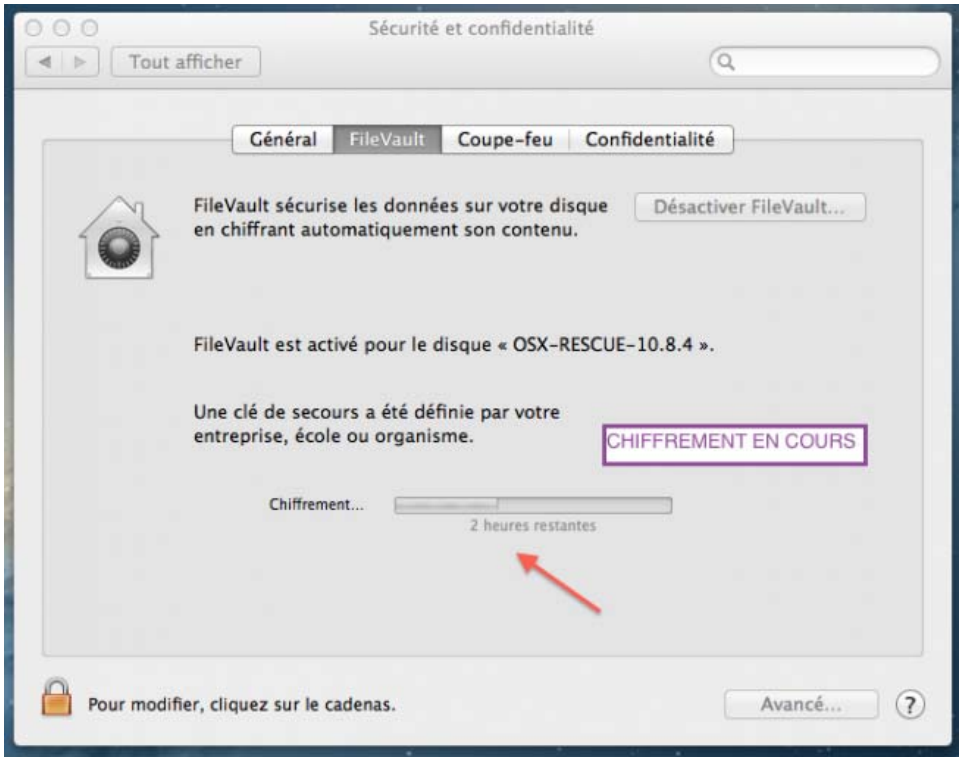
+ reboot exigé

Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

Apple OS X

Ordinateur utilisable pendant le chiffrement, y compris arrêt/suspension, …



Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

Systèmes Linux

… IJL en phase d'apprentissage – consolidation - tests sous UBUNTU …

LUKS

- Gestion du chiffrement et des passphrases (8 Slots maxi)
- Ces Passphrases déchifffrent la "Master Key",
- "Master Key" : stockée dans le LUKS Header
  ➔ LUKS HEADER : à séquestrer AUSSI !

DM-CRYPT

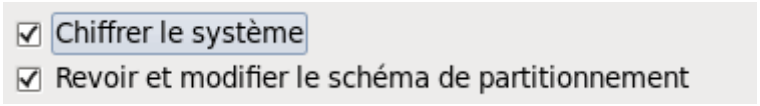
- Périphérique bloc sous /dev/mapper - chiffrement transparent

Outil de configuration dm-crypt/luks

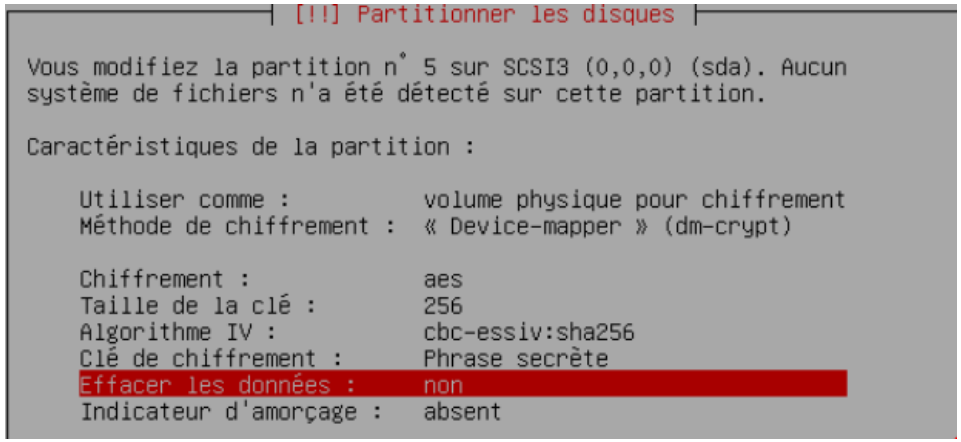
- 'cryptsetup' : configuration du chiffrement - extensions LUKS incluses

Systèmes Linux

- Choix à l'installation d'UBUNTU

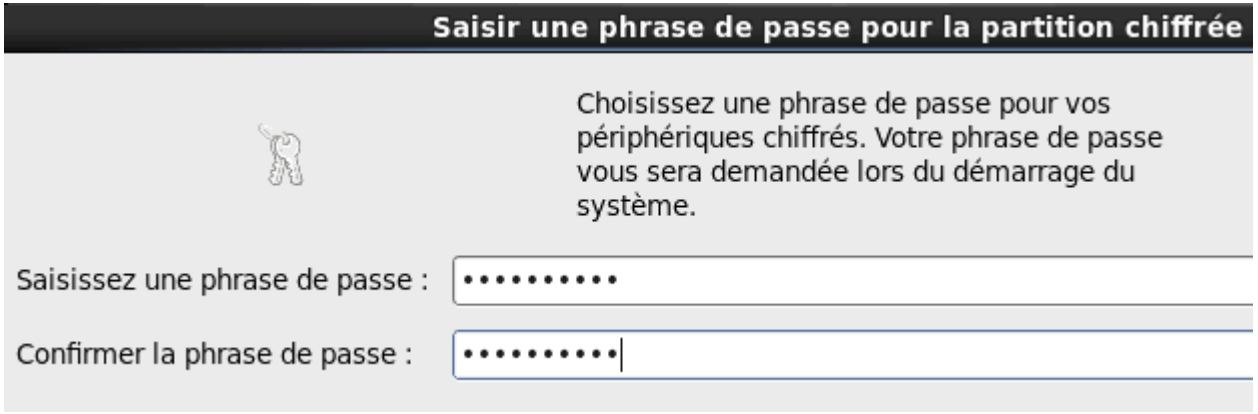


- Sélectionner la/les partitions à chiffrer /configurer (chiffrement via dm-crypt)



Systèmes Linux

- définir la 1ère PASSPHASE (LUKS protège celui-ci dans le slot 0): à séquestrer !



Institut Jean Lamour
PENSER LES MATÉRIAUX DE DEMAIN

Solutions logicielles

Systèmes Linux

- **LUKS : définir la/les PassPhrase Utilisateur: 1 slot = 1 passphase ; 8 slots (0 à 7)**

  # cryptsetup luksAddKey /dev/<*partition*>
  … supprimables …
  # cryptsetup luksKillSlot /dev/<*partition*> 2

- **Liste des Slots LUKS actifs pour une partition chiffrée :** au moins 1 slot actif !

  # cryptsetup luksDump /dev/<*partition*> | grep Slot
  Key Slot 0: ENABLED
  Key Slot 1: ENABLED
  Key Slot 2: DISABLED
  …

- **LUKS HEADER de chaque partition chiffrée** : le générer & le séquestrer !

  # cryptsetup luksHeaderBackup –header-backup-file <*filename*> /dev/<*partition*>

Bilan IJL / Chiffrement Logiciel

Chiffrement Matériel

- Un comble : grande dépendance / logiciels ☹
- Logiciels : oui, uniquement/MS Windows
- Chiffrement : disque entier seulement
- Surcoût ?
- En cours d'abandon/migration à L'Institut

Chiffrement Logiciel

- à préférer aux SED
- Chiffrement par lecteur/partition & par OS (Pb. multi-boot moindre)

Bilan IJL / Chiffrement

Bilan chiffré … en clair ☺

Ordinateurs portables	Actuels		EN FIN DE VIE <= 2011
	Chiffrés	Non chiffrés	Non chiffrés
En service chiffrés	106		
En service non encore chiffré		36	
En fin de service/fin de vie			74
TOTAL	106	36	74

Procédures IJL:

- Chiffrement systématique des ordinateurs portables neufs
- Postes recyclés/réinstallés :
  - Chiffrement systématique
  - Passage du chiffrement SED au chiffrement « Logiciel »

Bilan IJL / Tendances

… Autres …

TPM & Lenovo

- puce chinoise : hors TGC - algorithmes de chiffrement différents

Dislocker

- Driver FUSE pour Linux & Mac OSX pour accès à des volumes chiffrés avec Bitlocker

Conclusion

Tout documenter

Procédures à écrire noir sur blanc : WIKI, …

Séquestre des clés, passphrase de chiffrements ou de recouvrement

Impératif avec Bitlocker, HP Protect, LUKS, … : si pas de passe-partout
Sinon séquestrer uniquement le passe-partout
L'idéal : un clé unique par usager
+ une clé passe-partout pour le service informatique

Panne/SAV : penser aux conséquences :

SAV interne : Lecture des données … « ailleurs » !
SAV externalisé : problématique du déverrouillage par des tiers !

Bref, le chiffrement de volumes de données :

Avec (beaucoup) de (la) méthode, parfaitement maîtrisable !
Votre allié : un système de sauvegarde associé !