CHIFFREMENT DES ORDINATEURS PORTABLES

30 janvier 2014

www.cnrs.fr

Chiffrement, kezako?

« la *science du secret* »

disciplines de la **cryptologie**

Le **chiffrement** est un procédé de **cryptographie** grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

$$C = P(\rho^i D \rho^{-i})(\rho^j M \rho^{-j})(\rho^k G \rho^{-k}) U (\rho^k G^{-1} \rho^{-k})(\rho^j M^{-1} \rho^{-j})(\rho^i D^{-1} \rho^{-i}) P^{-1}$$

Que peut-on chiffrer ?

Transport de données : protocole TLS (successeur de SSL)

https, ssh, openssl, smtps, sftp

Courriels : protocole S/MIME, PGP (implémentation avec certificats électroniques)

Signature numérique, chiffrement intégral du message

Stockage de données : coffre fort numérique

TrueCrypt, Dm-crypt, Filevault, Keepass

UNIVERSITÉ DE STRASBOURG

Jeudi 13 mars 9H - 17H

FORMATION

Echanges sécurisés de documents sensibles

1. **Utilisation du chiffrement lors d'échanges de courriels** (avec certificat électronique)
   a) Certificat électronique : demande et installation
   b) Utilisation de certificat avec les clients de messagerie (outlook, thunderbird,…)
2. **Utilisation de containeur chiffré**
   a. Présentation et installation de Truecrypt
   b. Création de containeur chiffré
   c. Outils d'échanges (messagerie, BFS, Cloud ?,…)
3. **Autres outils d'échanges**
   a. Plate-formes dédiées
   b. Clé USB auto-chiffrantes

Fiabilité du chiffrement …

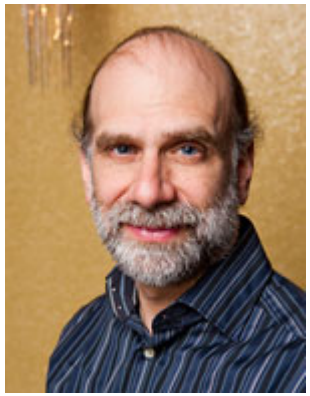
Edward Snowden

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. “

http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower#block-51bf3588e4b082a2ed2f5fc5

“Can the NSA break AES?

My guess is that they can't”



Bruce Schneier

https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html

Pourquoi chiffrer les ordinateurs portables ?

Les postes de travail sont de plus en plus légers et portables, leur exposition au vol a considérablement augmenté ces dernières années.

Le chiffrement d'un ordinateur, d'une clé USB ou d'un disque externe rend les données illisibles et inexploitables en cas de vol du matériel.

Alternative au chiffrement

Ne pas transporter de données confidentielles . Les données restent dans le laboratoire.

Comment ?

Partir avec un ordinateur vierge, accéder à des données soit sur une clé USB chiffré et/ou se connecter à distance son système d'information via VPN

(nécessite une bonne connexion réseau)

Les textes

1ère note du président du CNRS :	16 janvier 2011
2ème note du président du CNRS :	08 janvier 2013

Deux principes pour réduire les risques

1. Protection technique du poste de travail et des périphériques de stockage
2. Sensibilisation du personnel

Règles :

- Achat de disque chiffrant (windows, marché Matinfo 3)
- Chiffrer tous les nouveaux portables dès leur acquisition
- Déploiement terminé au 30 juin 2013

Suivi de la mise en œuvre du chiffrement

Accès réservé aux CSSI

https://extra.core-cloud.net/collaborations/RSSI-CNRS/Lists/Enqute%20chiffrement/AllItems.aspx

Code unité	Sigle		Nb portables	Nb portables chiffrés	Nb fixes	Nb fixes chiffrés	Nb total ordi	Date_de_mise_
UMR7357		Oui	150	1	0	0	150	23/04/2013 13:55
UMR7361		Oui	21	5	210	0	231	
UMR7362			42	6	69	0	111	23/04/2013 11:16
UMR7363			0	0	0	0	0	
UMR7364		Oui	8	1	50	0	58	
UMR7501			47	10	65	2	112	
UMR7504		Oui	150	1	450	6	600	
UMR7509			0	0	0	0	0	
UMR7515			0	0	0	0	0	
UMR7516		Oui	200	2	245	0	445	21/05/2013 09:09
UMR7517			44	0	122	0	166	24/04/2013 15:03
UMR7522		Oui	28	3	90	2	118	
UMR7551			50	0	50	0	100	26/04/2013 15:01
UMS3206			3	2	24	6	27	17/10/2013 09:19

Documents techniques

CNRS/RSSI-FSD :

Recommandations pour la protection des données et le chiffrement

CNRS/DSI/RSSI *juin 2012* - **François MORRIS**

Chiffrement des portables

Mise en oeuvre et utilisation

Les principes

- L'accès aux données chiffrées se fait via une pass-phrase.
- **Chiffrement** = sauvegarde + **recouvrement**
- On peut chiffrer un disque entier (= chiffrement de surface), une partition (= disque virtuel) ou un containeur (= fichier)

Règle 6 - Utilisation de mots de passe robustes, personnels et différents

RAPPEL

- *Une **pass-phrase** doit être suffisamment complexe :*
  - Longueur minimum 10 caractères
  - Caractères spéciaux, majuscule et chiffres

Mot de passe	robustesse	Attaque brut force	commentaire
manganese	36 %	0 s	
25manganese	52 %	22 mn	Rajout de chiffres
25=manganese	70 %	3 ans	Rajout caractère spécial « = »
25 = manganese	84 %	174 000 ans	Rajout caractère spécial <espace>
25 = Manganese	91 %	16 millions ans	Rajout Majuscule
25 = Manganèse	100 %	3 milliards ans	Rajout caractère spécial « è »

Exemple 1 : Le sport, j'aime ça (robustesse = 100 %)
Exemple 2 : Le Racing en Ligue1 (robustesse = 100 %)
Exemple 3 : Le roi, c'est Gauss (robustesse = 100 %)

http://password-checker.online-domain-tools.com/

CHIFFREMENT → **RECOUVREMENT**

Recouvrement
Procédure qui permet d'accéder à une information chiffrée en cas de d'oubli du mot de passe ou de l'indisponibilité de son détenteur.

La méthode la plus simple consiste à stocker le mot de passe en un lieu sûr, on parle alors de séquestre

SAUVEGARDE
procédure qui permet de récupérer les données en cas de vol ou de défaillance du mécanisme de chiffrement.

Types de chiffrement

- **Chiffrement de surface**
  Tout le disque est chiffré
  Pas de chiffrement effectif après le démarrage

- **Chiffrement de partition**
  Seul le disque virtuel est chiffré

- **Chiffrement de conteneurs**
  Utilisation du logiciel Truecrypt pour lire et modifier les éléments chiffrés

Disque entier : facile à réaliser, transparent pour l'utilisateur

Containeur : facile à transporter (clé USB, mail)

Applications pratiques

Windows 7 : TrueCrypt
Chiffrement du disque entier ou d'un conteneur
Utilisation d'un disque chiffrant (marché Matinfo3)

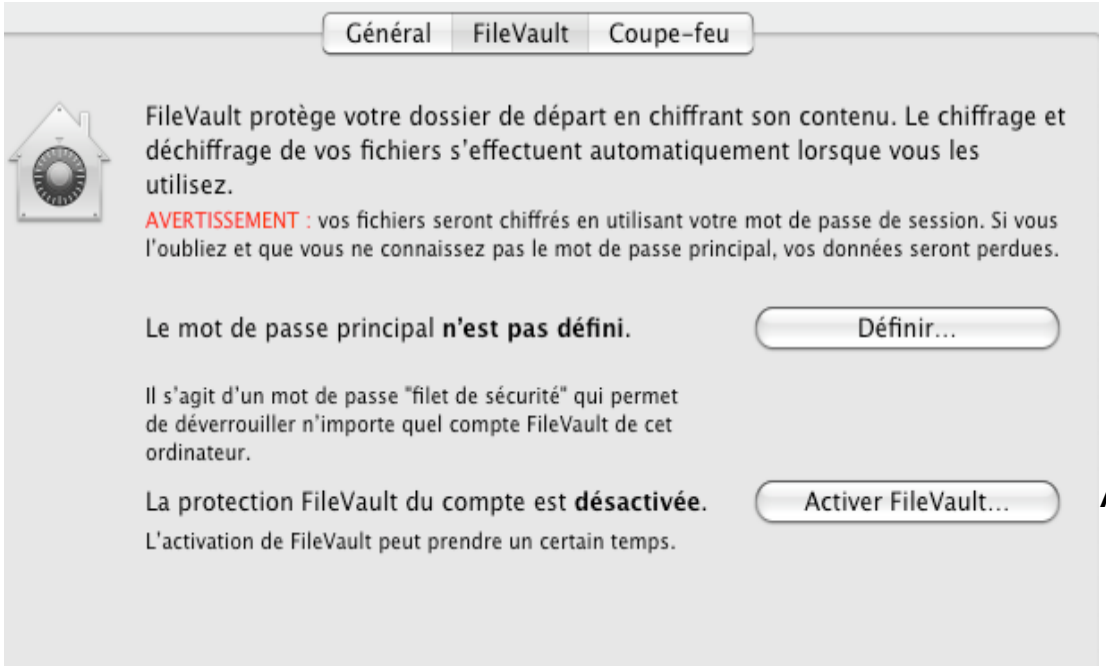
Windows 8 : Bitlocker
Chiffrement de partitions
Utilisation d'un disque chiffrant (marché Matinfo3)

MacOS X : FileVault (intégré à MacOSX)
Chiffrement d'un répertoire
Chiffrement disque à partir de Mac OSX Lion

Linux : Dm-crypt (intégré au système de nombre de Distribution Linux (Ubuntu …) Chiffrement du disque

Mac : utilisation de FileVault

- Protège un compte
- Ce système est natif sur les OS 10.3 à 10.6
- AES 128 bits
- Chiffrement de surface du disque



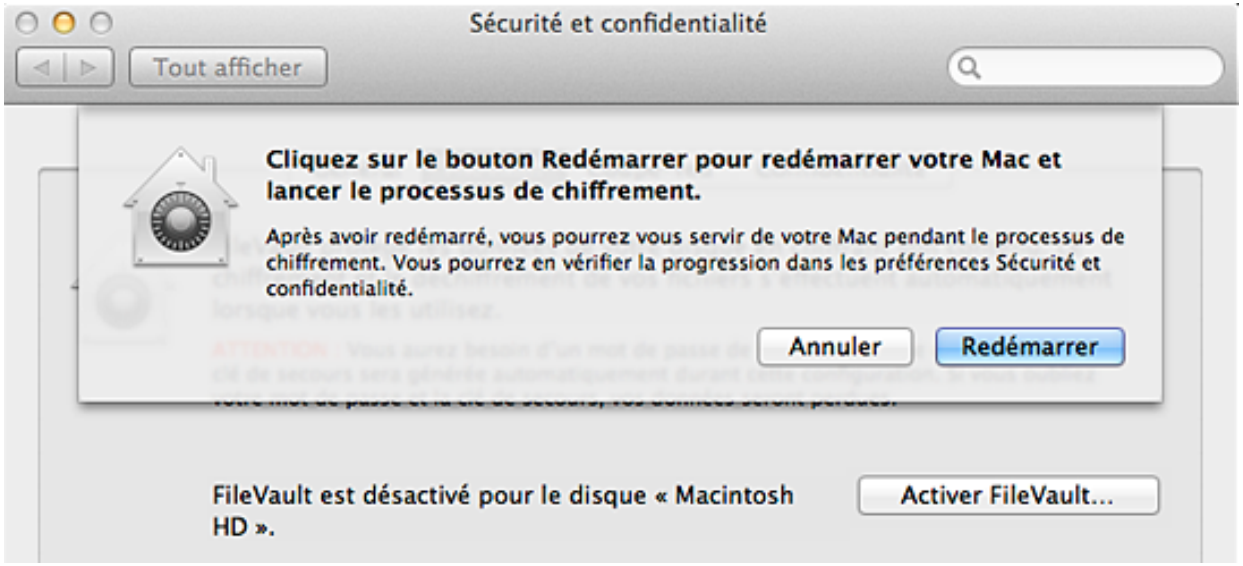
Mot de passe de recouvrement
Valable pour tous les comptes

Activer FileFault pour le compte choisi

Mac : utilisation de FileVault 2

- Ce système est natif sur l'OS 10.7 et suivant
- AES 128 bits
- Chiffrement de surface du disque

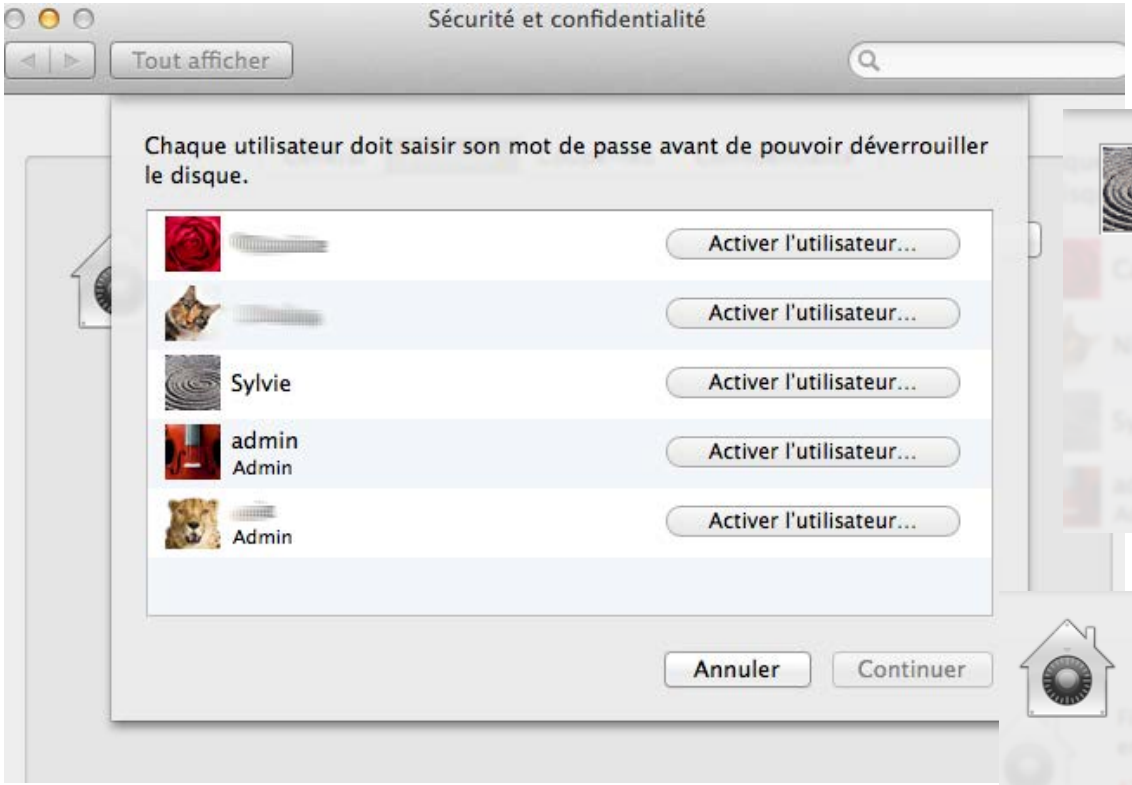
- OS X : à propos de FileVault 2
- OS X : création et déploiement d'une clé de secours pour FileVault 2

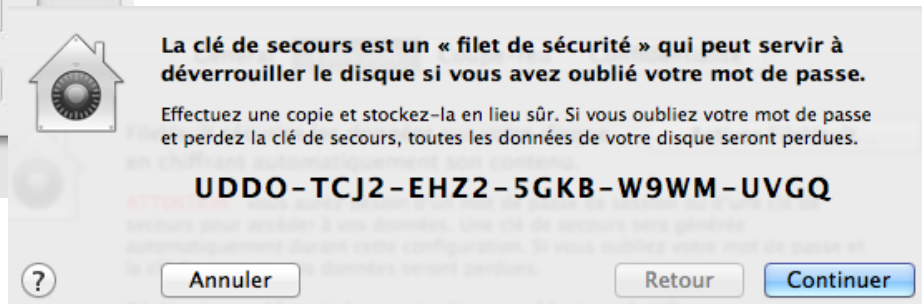


Mac : utilisation de FileVault2

- Nouveauté sur les OS 10.8.5 et plus

on demande de choisir qui peut déchiffrer le disque (indiquer au moins un compte)



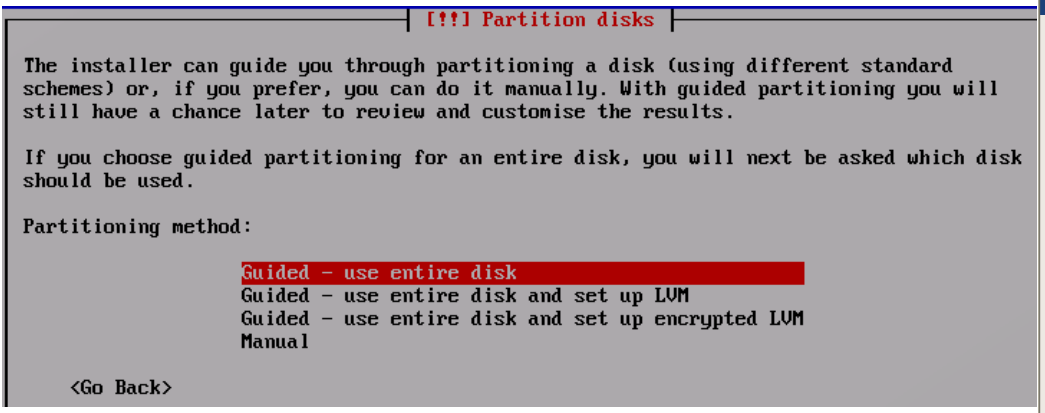


Linux : utilisation de Dm-Crypt

- Solution native sur la majorité des systèmes Linux 2.6.4
- Fait parti de l'infrastructure « device-mapper »
- Permet de chiffrer
  - La partition système (sauf /boot)
  - Les autres partitions
- Les volumes amovibles
- Souvent utilisé avec LUKS (Linux Unified Keys System)

Linux : utilisation de Dm-Crypt

- Facile à mettre en œuvre lors de l'installation du système



- Plus difficile de chiffrer la partition système sur une machine déjà installée

Linux : utilisation de Dm-Crypt

- Mot de passe demandé
  - au démarrage pour la partition système

```
Enter LUKS passphrase for /dev/sda2: _
```

  - au montage des volumes
- On peut définir 8 clés par volume

```
Key Slot 0: ENABLED
        Iterations:             299066
        Salt:                   99 5e d2 83 70 6e dc 8f c7 9e 6a 80 1a e2 e7 69
                                2c 8e 5f b6 81 89 6f d1 cc b7 ef 76 76 1e 64 56
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: ENABLED
        Iterations:             340140
        Salt:                   01 1c c8 8d 26 7f 42 0c e0 45 6d 92 f5 d4 3e f7
                                e5 bb bc 46 d1 63 c6 74 28 95 fd 61 1b 2c 53 83
        Key material offset:    136
        AF stripes:             4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
[root@localhost ~]#
```

- Penser à sauvegarder l'entête du volume

Cryptsetup luksHeaderBackup --verbose –header-backup <*backup*> <*device*>

Windows 8: BitLocker

- Logiciel disponible dans les versions Pro et Enterprise
- Intégration possible avec Active Directory
- Par défaut: AES 128 (mais 256 possible)
- Utilisable avec les puces TPM (Trusted Plateform Module)
  http://fr.wikipedia.org/wiki/Trusted_Platform_Module

Windows : TrueCrypt

- Logiciel gratuit
- Version actuelle: 7.1a (février 2012)
- Par défaut: AES 256, RIPEMD-160
- Produit qualifié par l'ANSSI

http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/

Windows : TrueCrypt




Version système requise	Kernel 2.4 & 2.6 32 ou 64 bits	Snow Leopard 32bits Tigre, leopard, Lion 32 ou 64 bits Lion des montagnes 32 et 64 bits	XP, Vista, 7, 2003, 2008 32 ou 64 bits	Windows 8, 2012 (non officiel)
Chiffrement de surface	✗	✗	✓	✗
Chiffrement de partition système	✗	✗	✓	✗
Chiffrement d'un volume	✓	✓	✓	✗
Chiffrement d'un conteneur	✓	✓	✓	✓
Internationalisation de l'interface	✗	✗	✓	✓
Démontage automatique	✗	✓	✓	✗

DualBoot : Windows chiffré + Linux chiffré
http://www.artiflo.net/2009/05/dualboot-os-fde-windows-chiffre-linux-chiffre/

Création de clé USB Linux bootable
http://www.linuxliveusb.com/

Partir en mission > Réglementation relative au contrôle des données électroniques à l'étranger
http://www.securite-informatique.gouv.fr/gp_article714.html