Bilan du groupe Sécurité

- Etat des lieux, alertes, etc.
- Retour de l'enquête
- Rapport d'activité
- Chiffrement

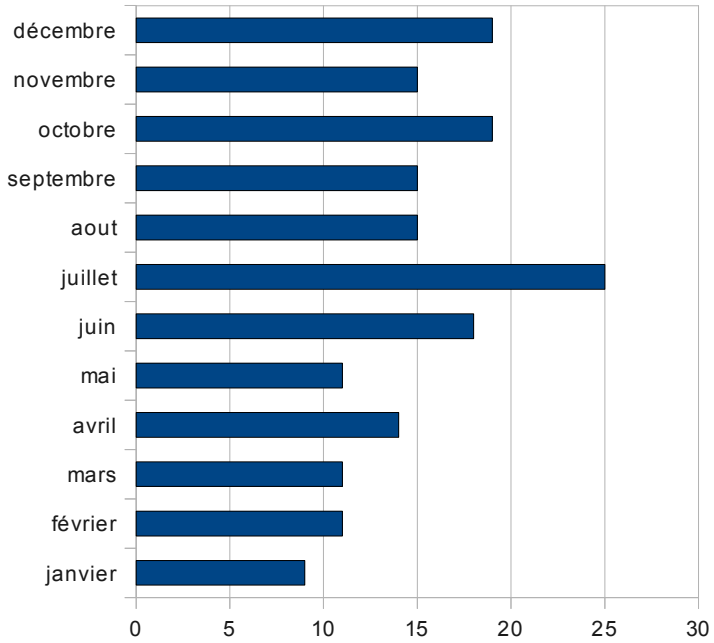
Th.Mouthuy

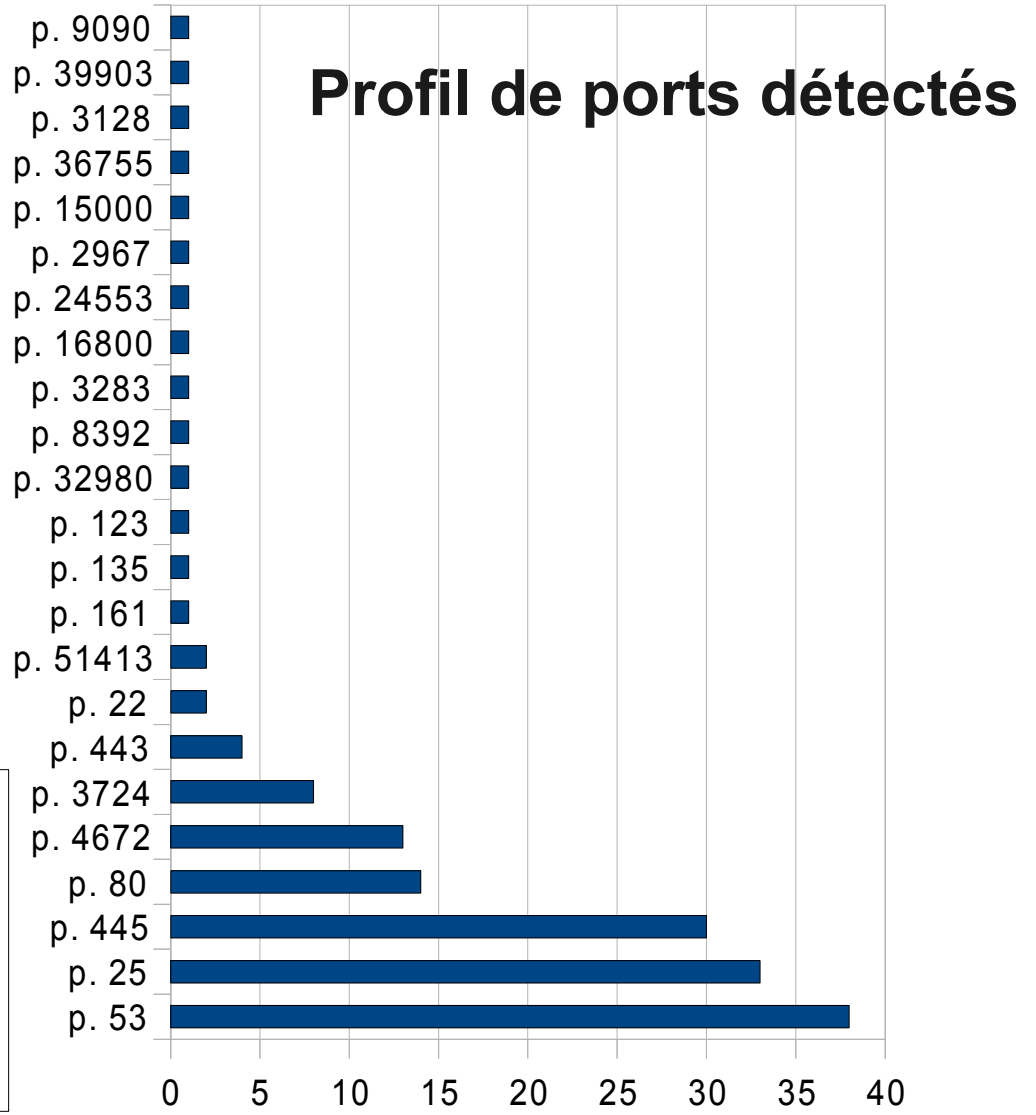
Alertes Extra en 2010/2009/2008

Problème	½ 2010	2009	2008	Commentaire
Virus	40	69	16	Faiblesse AV local ? Portables ?
P2P	19	21	17	**!! Augmentation continuelle**
Erreur	0	13	2	Config ou 192.168 ou ...
DNS changer	6	4	4	
Site défacé	3	8	4	**!! MAJ logiciels, anciens sites, hébergements**
Jeu en réseau	0	6	1	Jeu en réseau
Relais NAT ou Skype ?	4	6	5	
VOL de portables	4	5	5	Au CNRS [500,2000]/an 150 déclarés
PLAINTES	6 =1+3+2	10 =5+3+2	3	**Majors +** AOL + CERT (hors virus)...
Compromission SSH + root	0	2	0	**MAJ système !**

Histogrammes

182 alertes en 2009 (87 en 2010)





25, 53, 445	: Virus
4762, 5041	: P2P
16800	: TvAnts
3724	: World of Warcraft
80 et 53	: parfois NAT
443	: P2P, erreur, ?

Exemple d'un courrier SONY

I am writing this letter on behalf of SPE Acquisitions, Inc., ("SPEA") a **Sony Pictures Entertainment company**.

...

The unauthorized distribution or public performance of copyrighted works constitutes copyright infringement under the Copyright Act, Title 17 U.S Code Section 106(3)-(4). This conduct may also violate the Berne Convention for the Protection of Literary and Artistic Works, The Universal Copyright Convention as well as bilateral treaties with other countries that allow for protection of our copyrighted works even beyond U.S borders.

We have received information that an individual has utilized the below-**referenced IP** address at the noted date and time to offer downloads of the above-mentioned work through a "**peer-to-peer**" service.

Since **you own this IP address**, I request that you immediately do the following:

1) **Disable access to the individual** who has engaged in the conduct described above; and
2) **Terminate any and all accounts** that this individual has through you.

…

Et un autre de Columbia...

We are writing this letter on behalf of Columbia Pictures Industries Inc., ("**Columbia Pictures**") who owns certain rights under copyright law in the title 2012.

You are receiving this notice because your Internet account was identified as having been used recently to copy and/or distribute illegally the copyrighted motion pictures and/or television shows listed at the bottom of this notice. This notice provides you with the information you need in order to take immediate action that can prevent serious legal and other consequences. These actions include:

1. **Stop downloading or uploading** without authorization any motion pictures or TV shows owned or distributed by Columbia Pictures; and

2. **Permanently delete** from your computer(s) all unauthorized copies you may have already made of these movies and TV shows.

Avec un peu d'humour ?

On behalf of the rights holder for the content listed below, we are writing this letter to state that we have a good faith belief that the unauthorized sharing (distribution) and downloading of this content has occurred by an individual making use of the IP address below at the date and time referenced at the end of this notice.

Harry Potter and the Philosopher's Stone (Document)
WWW.XXX.YYY.ZZZ

Unauthorized file sharing is illegal. However, **we truly appreciate your interest in Harry Potter and the Philosopher's Stone (Document)**. We are making every attempt to provide this wonderful content to you in a host of legitimate ways, one of which is through the following website:

http://www.apple.com/itunes

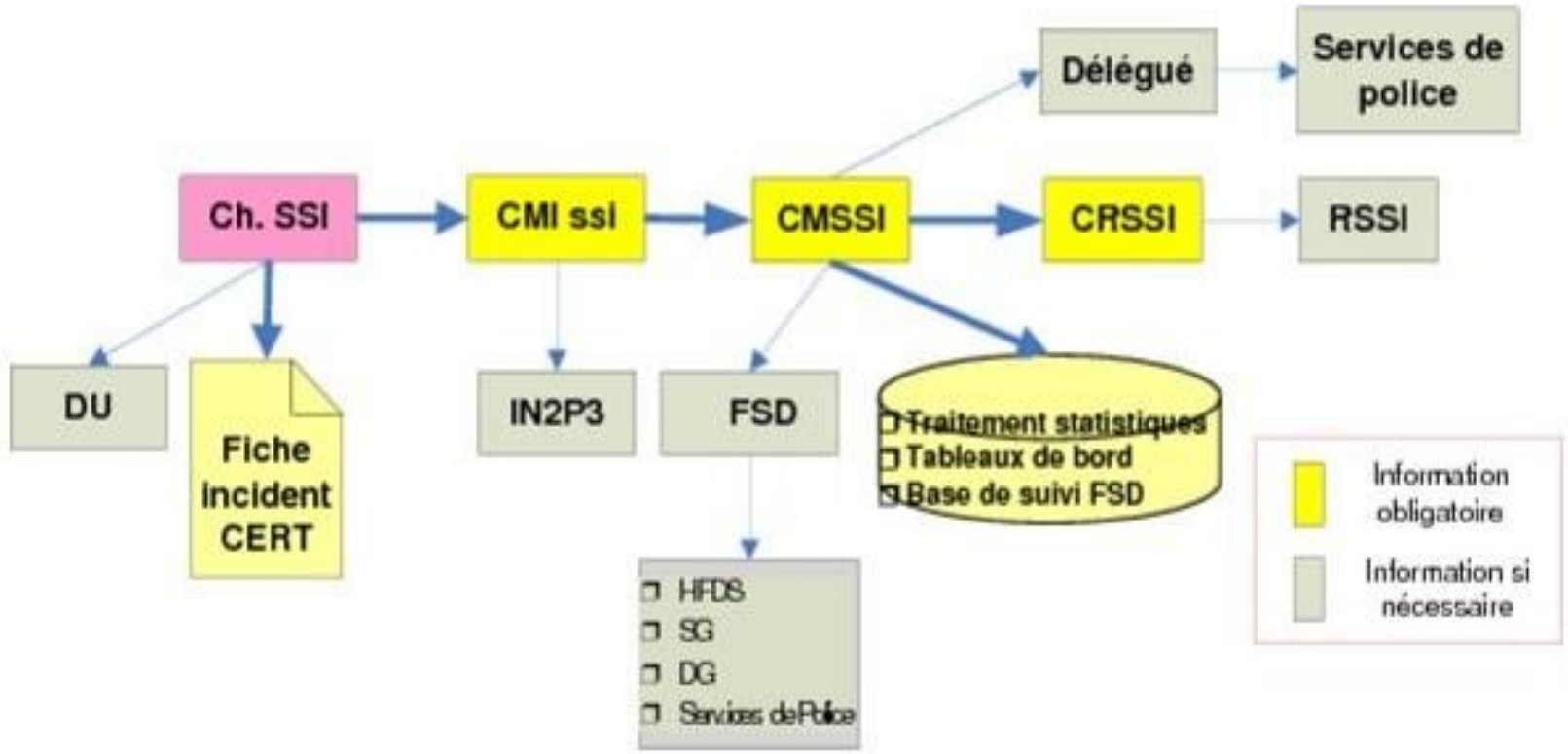
Et Hadopi alors ?

Sanctions pour «négligence caractérisée» : La nouvelle loi prévoit de sanctionner un abonné qui n'a pas sécurisé correctement sa connexion (attention au WiFi !)

- Une contravention pouvant aller jusqu'à 3.750 euros
- Une suspension de l'accès au Net pendant un mois.

En cas d'incident....

- Avertir la chaine fonctionnelle



Analyse enquête

Serveurs: 1875 → 1981
Serveurs grille : 2193 → 2406 → Augmentation 10 %
Fixe Linux : 1155 → 1195
Fixe Windows : 1664 → 1736 → Augmentation 3-4 % sauf MAC
Fixe Mac : 99 → 114
Portables Linux : 247 → 284
Portables Windows : 1109 → 1200 → Augmentation ~10 %
Portables Mac : 308 → 339
Arrivée des PDA : 6 → 33 Augmentation facteur 5
Tripwire PEU répandu (3 serveurs, 2 grille)

MAJ portables : Windows 100 %, Linux 50%

AV Mail : 3 NON (Ganil *prévu*,LAL *migr 2010*, Caen *étude*)

En conclusion partielle...

- Forte augmentation de PC vérolés...
- Souvent reliés aux visiteurs (mauvaise utilisation)

- **Améliorer l'information** aux visiteurs
- **Attention au P2P** – Problèmes en vue !

- Encore quelques éléments non sécurisés sur le réseau

- Nouvelles technologies et **nouveaux dangers** !

- Réunion sécurité à Lyon le 19 janvier 2010 (combiné avec sécurité grille)

En conclusion partielle...

Rapport d'activité envoyé à la direction le 8 mars 2010

	Référence	état	Explication
Relations IN2P3/CNRS	2.1		
Charte informatique	2.2		A remettre à jour dans certaines unités
Accueil utilisateur	2.3		Politique de fermeture des comptes manquante dans certains laboratoires
CSSI	2.4		Terminer les nominations
PSSI	2.4		Gros chantier à mettre en oeuvre
Connexion Renater	3.1		
Connexions dans les labos	3.2		1 laboratoire avec des HUBS ! Attention aux nouveaux équipements « mobiles connectés »
Contrôle d'accès au réseau	3.3		Inciter le dernier laboratoire
Cloisonnement	3.4		
VPN	3.4		Promouvoir cette technique de connexion externe. Attention à la porte ouverte sur le monde extérieur.
Wifi	3.5		Essayer d'augmenter le niveau de sécurité, mais pas trop grave si le cloisonnement est actif
FTP	3.6		Encore 1 laboratoire « ouvert »
Email sécurisé	3.7		Encore trop de ports POP, IMAP ouverts
Intranet	3.8		4 laboratoires avec des mot de passe circulant en clair

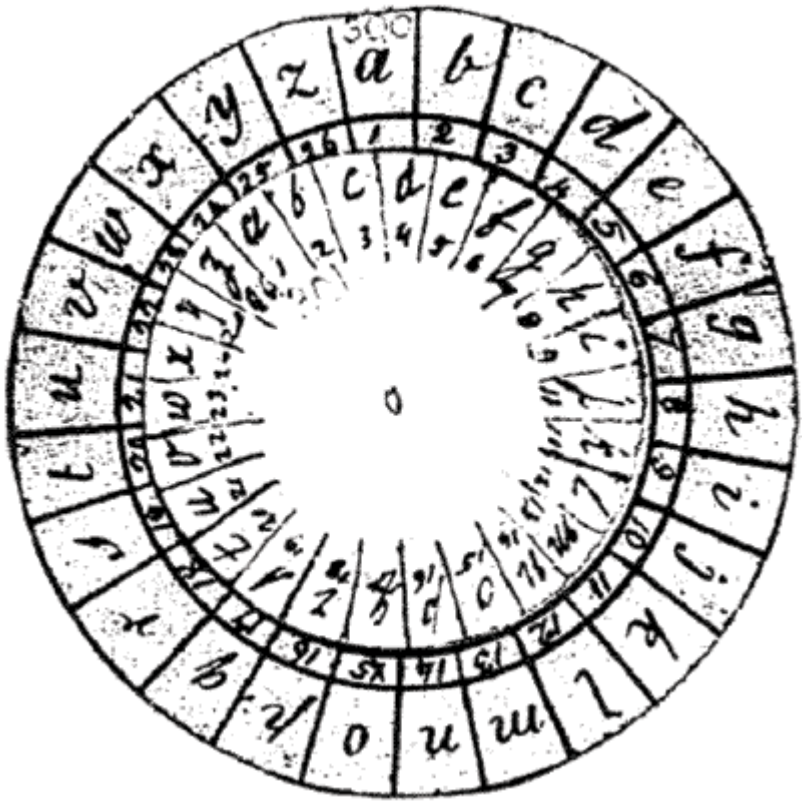
Th. Mouthuy, B. Delaunay, 2009 bilan sécurité IN2P3 15

Filtrage en entrée	3.9		Fermer les services du 3.7, nettoyer les ACL
Alertes et incidents	4.1		Quelques problèmes de configuration Problèmes d'information des visiteurs
Virus de messagerie	4.3		Même s'il faut rester vigilant
Authentification	5.1		On devrait pouvoir améliorer
Administration des serveurs	6.1		L'enregistrement des LOGS est OK, mais peu d'alerte de compromission ou d'attaque
Administration des serveurs grille	6.2		Même constat qu'en 6.1, Mais les serveurs sont moins administrés
Administration des postes fixes	6.3		Attention aux Mac Os
Administration des portables	6.4		Attention aux Linux+Mac Os Les utilisateurs ont les droits d'administration !
Mise à jour des systèmes	6.5		Problème intrinsèque des postes nomades
Antivirus sur les postes	6.6		Peu de retour sur les mises à jour.
Pare-feu	6.7		Peu utilisé sur les fixes. OK sur les nomades Il faudrait essayer de systématiser cet emploi sur l'ensemble des postes (fixe, serveur et nomade).
Chiffrement des portables	7.0		La phase de tests est terminée (hormis les disques chiffrants). La phase systématique peut démarrer.

Th. Mouthuy, B. Delaunay, 2009 bilan sécurité IN2P3 16

Ce n'est pas fini....

Et maintenant le sujet tant attendu...



Chiffrement et enjeux

Beaucoup de portables volés...

Entre 500 et 2000 / an au CNRS (estimation)
150/an déclarés CNRS, 5 déclarés IN2P3 en 2009.

Données « sensibles » ou à caractère personnel

Données dont la divulgation, la perte ou l'altération peut porter préjudice à l'organisme.

- Données sensibles (contrats, résultats)
- Courriels
- Mots de passe, clefs SSH, certificats
- Données dans les caches

Utilisables en cas de vol...

→ Chiffrer les disques des portables

Historique

- *Déc 2008* : Problématique Windows, Linux, Mac
- *Avril 2009* : Recensement options matérielles et logicielles
- ☹ pas de budget → choix des gratuits :
  ⇒ truecrypt, dm-crypt, Filevault
- *Juin 2009* : Chiffrement tous portables au CPPM
  → problèmes : clavier AZERTY, dual boot
- *Sept 2009* : Guide de chiffrement
- *Nov 2009* : Possibilité des disques chiffrant chez Dell
- *Avril 2010* : Tests des disques chiffrant
- *Mai 2010* : Maintenant, il faut le faire....

Solutions possibles

- **Matérielles**

  Disques chiffrant : Seagate et Samsung (SSD)
  - Utilisation du logiciel Wave...
  - Directement ou sous AD

- **Logicielles**
- Truecrypt sous Windows
- dm-crypt sous Linux
- FileVault sous Mac

Le disque dur chiffré

La solution contre la perte et le vol des portables

Société Wave Systems – partenaire Dell

Un disque de stockage performant

- 80, 120,160, 320, 500… GB
- 5400 et 7200 tpm
- Format 1,8 ”, 2.5 ”
- SATA
- Mécanique ou SSD

+

La technologie SED (Self-Encrypted Drive)

- Chiffrement matériel – AES 128 bit
- Contrôles d’accès intégrés
- Protection de toutes les partitions
- Basée sur des spécifications internationales (Opal)

=

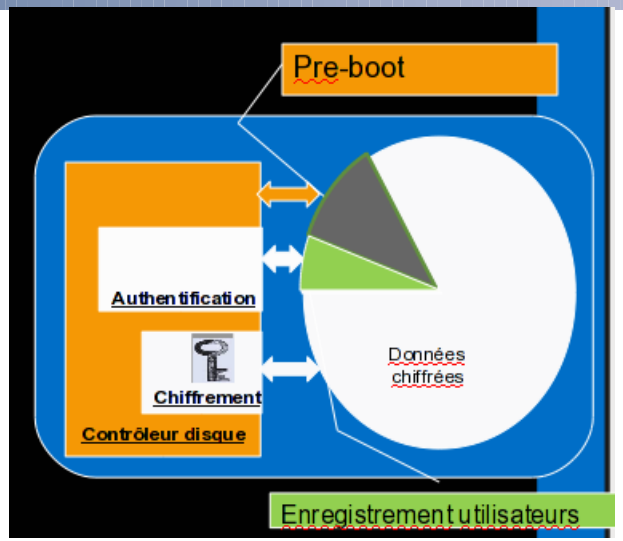
Le disque SED

- Chiffrement toujours actif

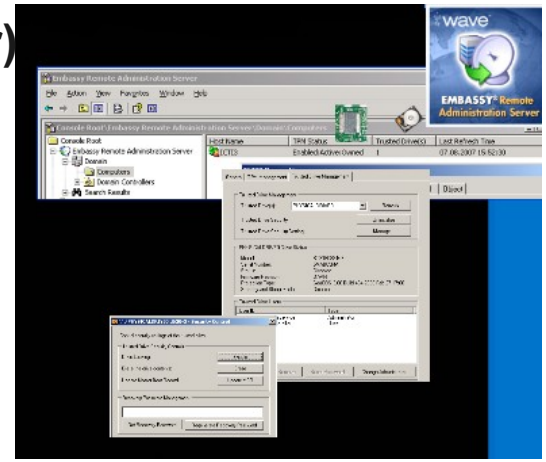
•Haute performance de chiffrement

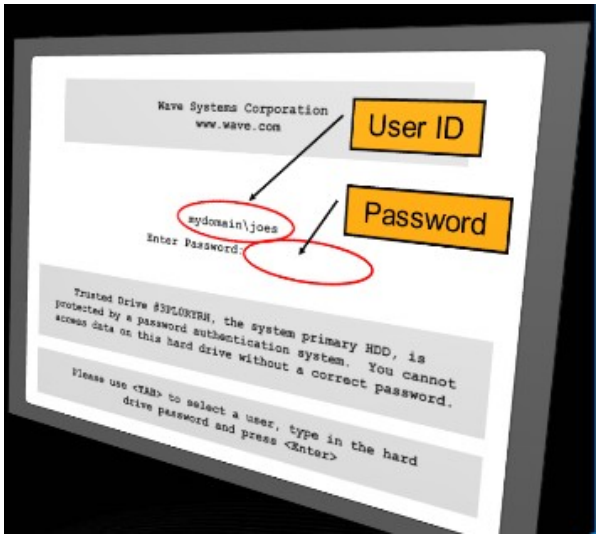
- Sécurité matérielle
- Effacement instantané du disque
- Constructeurs déjà engagés : Seagate, Samsung, Toshiba, Western Digital, Fujitsu…

Wave Systems (Direct ou sous AD)



ERAS (Embassy Remote Administration Server)
- identifie le PC
- initialise le disque
- active la protection
- gère mdp de secours
- enregistre historique





Disque chiffrant

- Le premier utilisateur enregistré est l'administrateur ! Il a les pouvoirs !
  → Sauvegarde automatique de son mdp sur clef, disque, montage réseau...

- On peut enregistrer 5 utilisateurs différents

- C'est plus automatique sous AD avec ERAS
- Il y a un mdp de secours installé par défaut

Problème Linux avec disque chiffrant

Pas de logiciel avant 1 an (si jamais !)

- Utiliser le dual boot ? Alors, c'est simple

- Utiliser une machine Windows pour mettre le mdp sur un second disque... puis l'utiliser sur un portable sous Linux
  ⇨ Pas trop complexe !

Solutions logicielles : linux avec dm-crypt

Cas simple : Il y a une option dans l'installation
ex. SL5, Fedora, autres ?

Une partition boot qui demande le mdp puis démarre le système – ensuite transparent !

Plusieurs mdp possibles (Admin, utilisateur..)

Sur MacOs

Security
Show All
General
FileVault
Firewall
Require password to wake this computer from sleep or screen saver
For all accounts on this computer:
Disable automatic login
Require password to unlock each System Preferences pane
Log out after
60
minutes of inactivity
Use secure virtual memory
Disable remote control infrared receiver
This computer will work with any available remote.
Pair...
Click the lock to prevent further changes.

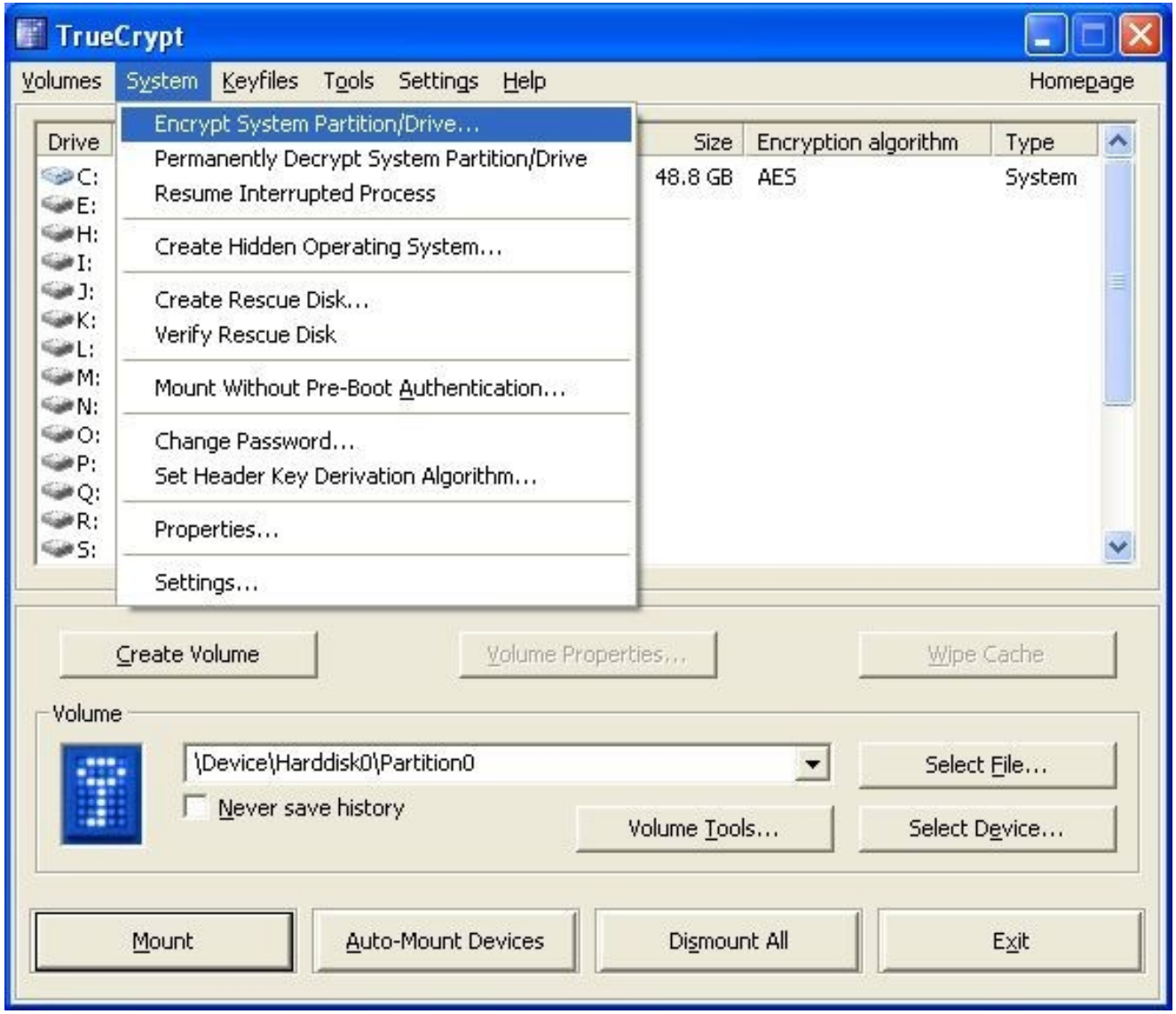
MacOS FileVault

Truecrypt pour Windows...

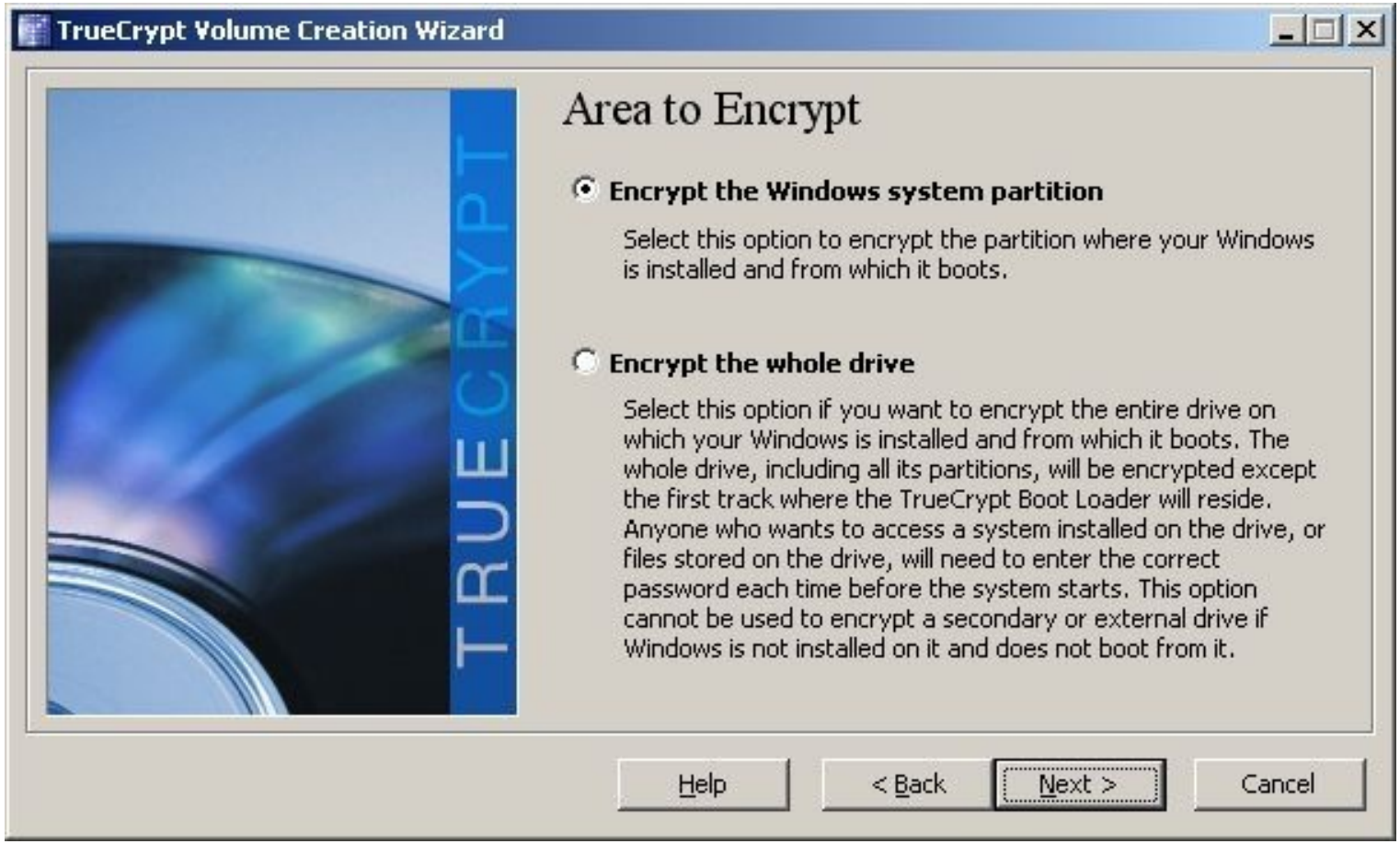
- Installer truecrypt : www.truecrypt.org
- Actuellement 6.3a (essais avec 6.1a)

- Attention à faire un backup des données si le portable est ancien !

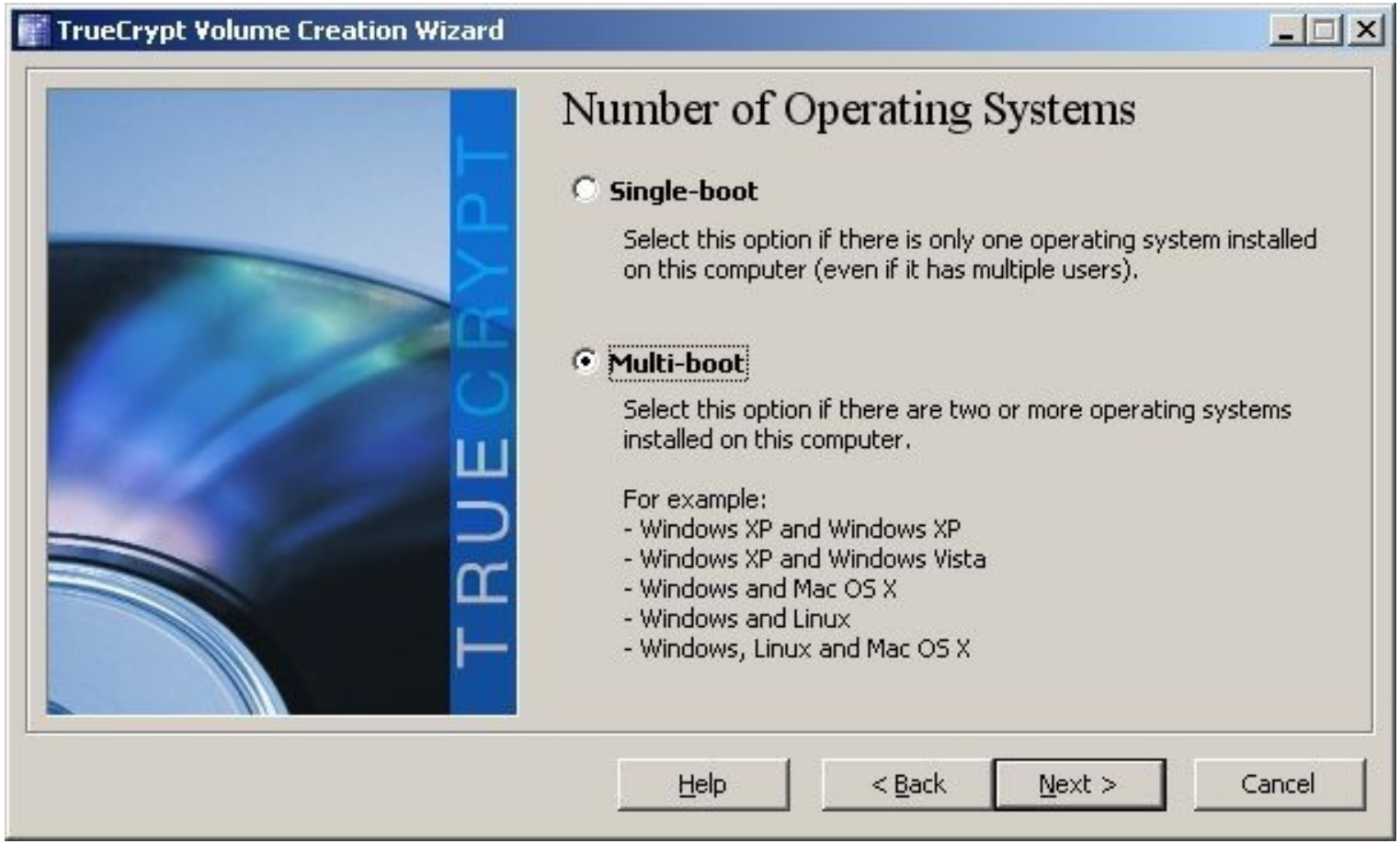
Démarrage...


TrueCrypt
Volumes
System
Keyfiles
Tools
Settings
Help
Homepage
Encrypt System Partition/Drive...
Permanently Decrypt System Partition/Drive
Resume Interrupted Process
Create Hidden Operating System...
Create Rescue Disk...
Verify Rescue Disk
Mount Without Pre-Boot Authentication...
Change Password...
Set Header Key Derivation Algorithm...
Properties...
Settings...
Drive
Size
Encryption algorithm
Type
C:
48.8 GB
AES
System
E:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
S:
Create Volume
Volume Properties...
Wipe Cache
Volume
\Device\Harddisk0\Partition0
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Sélection d'une partition ou du disque



Cas du multi-boot !



Mot de passe – Attention clavier FR

CD de secours... Vérification

Truecrypt... suite et fin

Pas du dual boot natif!!!

Le BOOT est TRUECRYPT

- Partitionner comme souhaité
- Installer Linux avant le chiffrement
- Chiffrer en mentionnant le « Multi-boot »

- Démarrage avec « ESC »

Partage de partitions

Problème du partage des partitions...

- Truecrypt tourne sous Linux.. On pourrait monter la partition Windows
- dm-crypt est spécifique. Le contraire ne marche donc pas !
- Sinon, il faut utiliser truecrypt sous Linux.. à la main !

C'est donc une galère avec les solutions logicielles !

Et en cas de problème sur le disque ?

Problème général !

- Si le portable est volé ?
- Si le disque a un problème ?

- **Il faut mettre en place un système de sauvegarde...**
- **Il faut mettre en place le séquestre des clefs !**

Conclusions sur le chiffrement des portables

- **La solution matérielle est préconisée** ! Simplicité !

- Si c'est impossible (ancien matériel), utiliser la solution logicielle (truecrypt, dm-crypt, filevault)

- **Le séquestre des clefs est essentiel !**
- **Un service de sauvegarde est essentiel !**
- Le choix d'un mdp administrateur/utilisateur est crucial aussi

- Un guide de chiffrement logiciel est prêt...

- Yapluka !!!

Et quid des autres supports ?

P.ex. les clefs USB, facilement égarables...

Solutions logicielles

Avec Truecrypt
20-30 € (8 Go)
Compatibilité ?

Logiciel inclus
Mil. grade ?
160 € (8 Go)

Solutions matérielles

Empreintes digitales
Prob de fiabilité ?
60 € (8 Go)

Code à clef (+ admin)
50 € (8 Go)

En fin !

Nos «données» ont de la valeur ...

Protégeons-les !

C'est simple ! C'est efficace !