Table ronde
Impact du chiffrement

Plan de l'atelier

- Introduction
- Mise en pratique du chiffrement
  - Chiffrement matériel (Paulo Mora de Freitas)
  - Chiffrement Windows Truecrypt (Paulo Mora de Freitas)
  - Chiffrement Windows Bitlocker (Paulo Mora de Freitas)
  - Chiffrement MacOS Filevault (Paulo Mora de Freitas)
  - Chiffrement Linux Dm-crypt (Jacques Beigbeder)
  - Chiffrement de conteneurs (Ludovic Billard)
- Table ronde impact du chiffrement (Pierre Vincens)
- Conclusion

Beaucoup de questions autour du chiffrement ?

- Comment le faire accepter aux utilisateurs?
- Comment choisir les mots de passe et/ou 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 organiser les espaces chiffrés ?
- Comment « traiter » le problème de la sauvegarde ?
- Comment « gérer » une panne sur un équipement chiffré?
- Quel est l'impact du chiffrement sur les performances ?
- …

Impact du chiffrement

Données chiffrées :
comment s'organiser ?

Données chiffrées : comment s'organiser ?

- Chiffrement complet du disque
  - Accès complet via une opération de déverrouillage

    → protection limitée à une machine éteinte
- Chiffrement par conteneur
  - Conteneur global dédié aux données à sécuriser

    → risque de données oubliées hors zone chiffrée
  - Conteneurs dédiés « projets »

    → accès restreint au projet ouvert

    → conteneur de taille plus petite pouvant être traité globalement comme un seul fichier (sauvegarde).

    → autant de clés à gérer que de containers (séquestre ?).

Cas de la 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

Impact du chiffrement

Mot de passe

Séquestre

Quelques remarques ?

- 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

Mots de passe ?

- Des possibilités dépendantes de la solution
  - Truecrypt → Une seule clé (et un CD de recouvrement si boot)
  - Dm-crypt → huit clés équivalentes
  - Filevault → mot de passe de l'utilisateur
- Des stratégies différentes :
  - Mots de passe spécifiques à chaque équipement
  - Mots de passe commun à tout le parc, à un groupe
  - Ordinateurs à usage individuel, partagé.

  → Ex : une stratégie mixte proposée par Ludovic Billard

=> Les situations de recouvrement sont variables :

→ personne en déplacement qui a oublié son mot de passe

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

Stockage des clés de recouvrement

- Mise sous enveloppe
  - écrit sur papier, gravé sur CD
  - disponibilité d'un coffre fort (minimiser les ouvertures)
- Stockage dans un fichier chiffré (coffre fort logiciel)
  - ex : Applicatif type KeePass
- Quelques remarques
  - Se protéger d'une défaillance ou perte de support
    - stockage en plusieurs lieux
    - duplication des « images » de recouvrement Truecrypt

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

Impact du chiffrement

Sauvegarde
des
données

Sauvegardes de données chiffrées

- Une obligation de sauvegarde renforcée
- Des adaptations éventuellement nécessaires
  - Sauvegarde du conteneur sous sa forme chiffrée
    - Vu comme un fichier, la modification d'un bit implique une nouvelle sauvegarde complète du fichier

      → peu adaptée à une sauvegarde incrémentale si modifications récurrentes du contenu

      → la restitution de données se fait globalement (pas d'indexation par fichier)

      → les données restent chiffrées sur le support de sauvegarde
  - Sauvegarde du contenu déchiffré
    - La clé doit être fournie (ou le conteneur ouvert)

      → implique un mécanisme complexe pour maintenir le niveau de sécurité.

      → est-il pertinent de chiffrer des données sur le disque et non sur le support de sauvegarde

Scénari de sauvegarde

- Sauvegarde par simple copie sur un disque externe
  - Un portable linux chiffré (dm-crypt)
  - Un disque externe pour la sauvegarde chiffré par dm-crypt

  → sauvegarde : un script simple
  - Phase 1 : montage du disque externe
  - Phase 2 : rsync des espaces à sauvegarder
  - Phase 3 : démontage du disque

  → Nombreuses adaptations possibles
- Sauvegarde incrémentale
  - Nombreux logiciels de sauvegarde supportent le chiffrement du support d'écriture et des transferts de données

    → la clé est globale à l'ensemble des données sauvegardées

Script de synchronisation

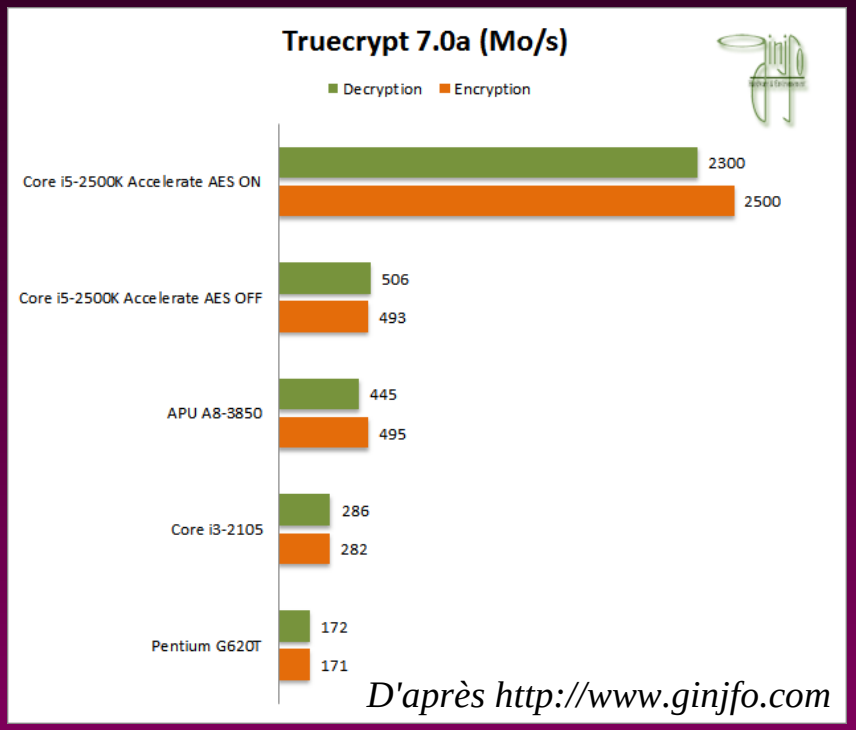
```
#/bin/bash

UUID_Encrypted=a6b...
UUID_decrypted=545...
PARTID=ub1
PARTMOUNT=/mnt
SRC=.../mondir/
DEST=$PARTMOUNT}/mondir/

cryptsetup luksOpen /dev/disk/by-uuid/$UUID_Encrypted $PARTID
mount luksOpen /dev/disk/by-uuid/$UUID_Decrypted $PARTMOUNT
rsync -avzH --delete ${SRC} ${DST}
umount /mnt/usb1
cryptsetup luksClose $PARTID
```

Impact du chiffrement

Performances

Support accélération matérielle pour AES

- Support sur certains processeurs core-i5 et core-i7
- Facteur x4 à x5 (2,3Go/s)
- Logiciel supporté
  - Truecrypt depuis 7.0
  - Linux Crypto-API (dm-crypt,...)
  - Filevault (Mac OS X Lion)
  - ...



D'après http://www.ginjfo.com

Dm-crypt (Linux)

- Truecrypt
  - Test fait par Ludovic Billard
    - Temps de boot allongé : 1mn34 (non chiffré) → 2mn29 (chiffré)
      Machine de test : Intel Core i5-480M (2.66 GHz / 2.93 GHz Turbo - Cache L3 3Mo), 4 Go de RAM, HDD 500 Go 5400 rpm
  - Support de l'accélération matérielle AES-NI depuis la version 7.0
- Dm-crypt
  - Support de l'accélération matérielle AES-NI
  - Sur test locaux, pas de dégradation observée sauf si usage intensif du swap

Impact du chiffrement

Du côté des utilisateurs...

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...

Ce que le chiffrement ne fait pas...

- 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

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 ?

Impact du chiffrement

Du côté des administrateurs...

Stratégie de déploiement

- Cas de nouveau matériel :
  - Étape supplémentaire lors de l'installation
    → implique un temps de mise en service plus long dans le cas de Truecrypt.
- Cas de matériel ancien :
  - Linux (dm-crypt) : nécessite une réinstallation pour chiffrer le système
  - Windows avec Truecrypt : pas de réinstallation mais temps de chiffrage «long»
    → implique de disposer de l'équipement pendant quelques heures (planification,...)

Ce qui pourrait ne pas être chiffré...

- Ordinateurs « industriels »
  - Pilote d'expériences
- Ordinateurs sans données
  - ATTENTION au swap, données temporaires
- Ordinateurs avec des OS anciens
  - Pas de support d'outils de chiffrement
  - Performance incompatible avec l'usage

MAIS

- Prendre des précautions contre le risque de vol (protection des locaux, équipement attaché,...)
  → de l'ordinateur
  → des disques

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

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 conteneurs

  → 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

Quelques liens...

- Information DSI CNRS
  - https://aresu.dsi.cnrs.fr/spip.php?rubrique99
  - http://www.dsi.cnrs.fr/services/securite/Documents/manuel.pdf
- 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