HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Analyse des protections et mécanismes de chiffrement fournis par BitLocker

Romain Coltel
<Romain.Coltel@hsc.fr>
3/04/2012

Sommaire

- Contexte
  - Objectif
- Fonctionnement général de BitLocker
  - Protection des données et moyens d'accès
- Le cœur de BitLocker : les méta-données
  - Comment les trouver
  - Comment les interpréter
- Implémentation et démonstration
  - FUSE
  - Exemple d'utilisation

Contexte

- Contexte général
  - Études post-mortem ou post-intrusion de partitions
  - Partitions chiffrées avec BitLocker
  - Outils d'analyse sous Linux

- Objectif
  - Être capable de lire des partitions chiffrées avec BitLocker, sous Linux

Fonctionnement général de BitLocker

Fonctionnement général

- Qu'est-ce qu'il fait ?
  - Chiffre des volumes en entiers

    → Bas niveau

  - Fournit des clés de chiffrement sûres

    → Générées par le système

  - Assure la sécurité de la chaine de démarrage

    → Après démarrage, (dé)chiffrement de manière transparente

Fonctionnement général

- Qu'est-ce qu'il ne fait pas ?
  - Ce que fait Encrypting File System (EFS)

    → Chiffrement fichier par fichier impossible
  - Chiffrement sur réseau

    → Chiffrement des accès disque, pas des interfaces réseau

Le cœur de BitLocker : Les méta-données

Accès aux données

- Trusted Platform Module (TPM)
- TPM et code PIN
- TPM, code PIN et clé USB
- TPM et clé USB
- Carte à puce
- ...

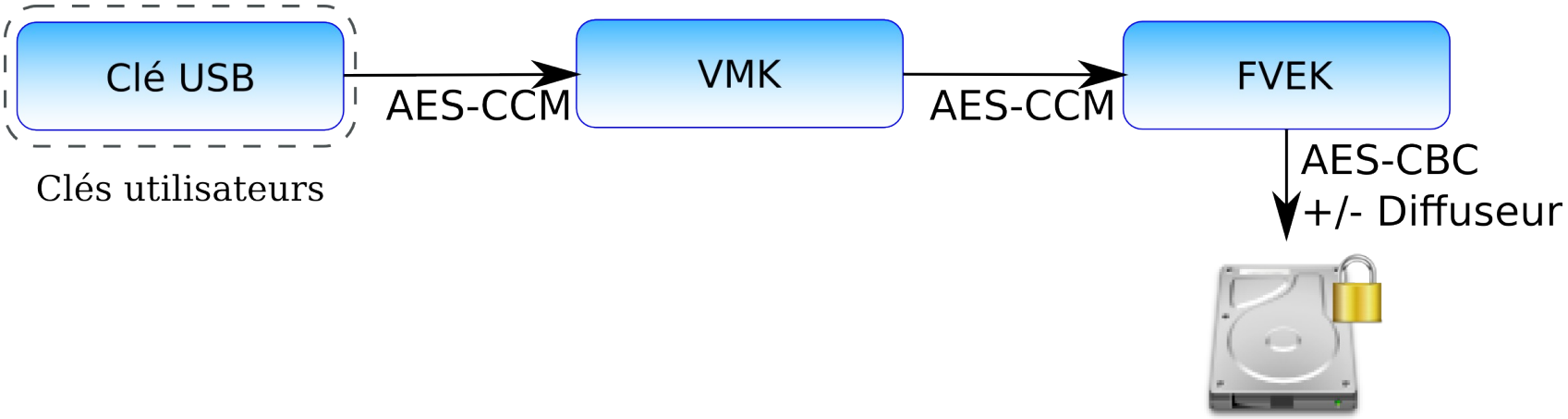
→ Grande panoplie de moyens d'accès

Algorithmes de chiffrement

- Chiffrement des données basé sur AES (AES-CBC)
- 4 possibilités :
  - AES-128 + Diffuseur (par défaut)
  - AES-256 + Diffuseur
  - AES-128
  - AES-256

Cœur de BitLocker

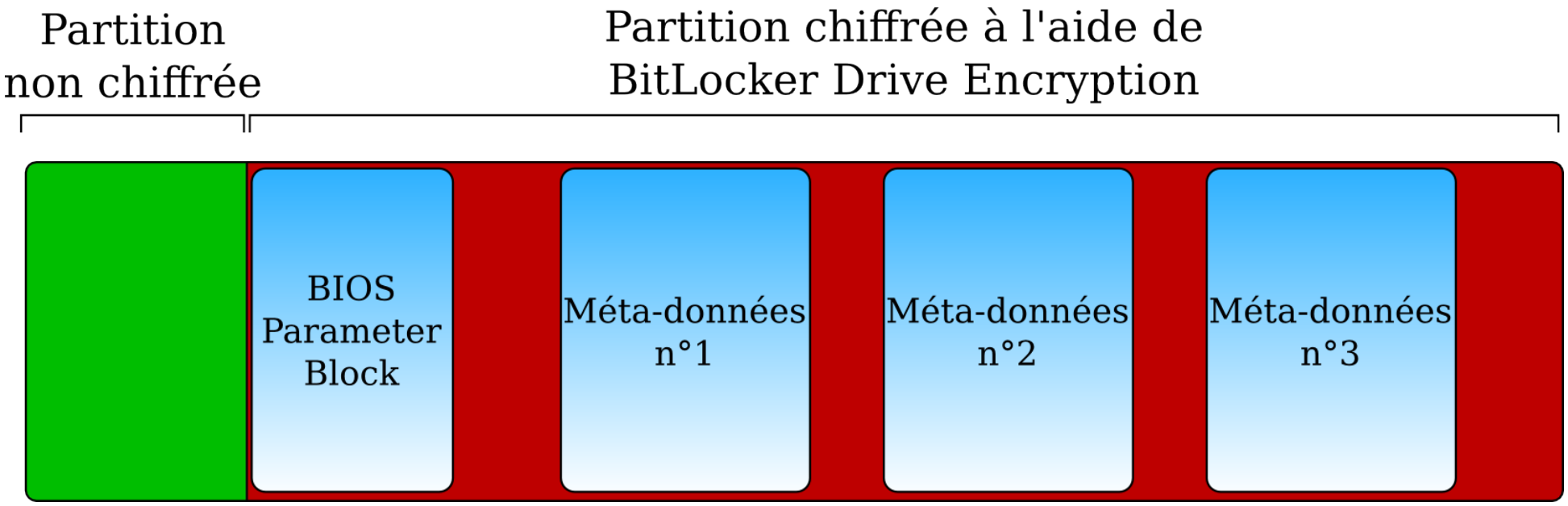
- Différentes clés entrent en jeu



→ Problème : comment et où trouver ces clés ?

Disposition des données

- Exemple : disque type chiffré avec BitLocker



Bios Parameter Block (BPB)

- Intérêt :
  - Signature (-FVE-FS-)
  - Nombre d'octets par secteur
  - ...

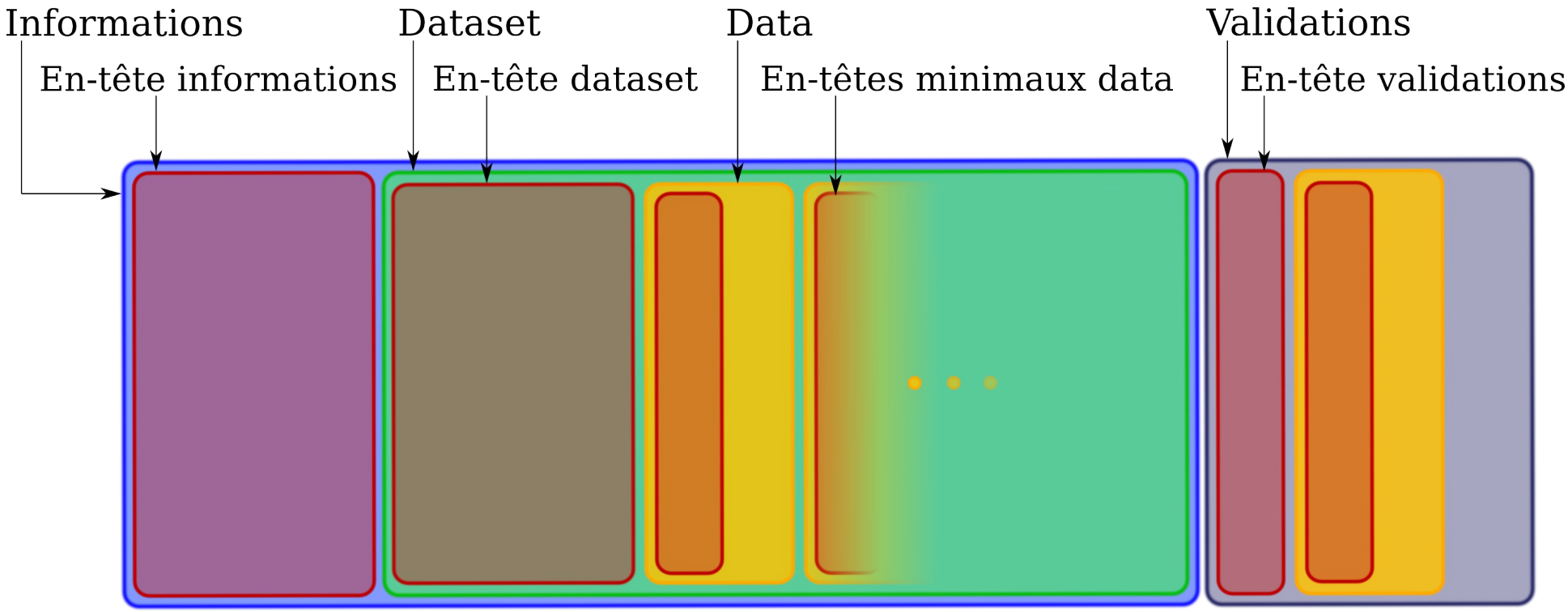
- Récupération des adresses des méta-données
  - Sous Windows Vista :

    bytePerSector * sectorPerCluster * MetadataLcn = premiereAdresse
  - Sous Windows 7 :

    adresses indiquées en dur

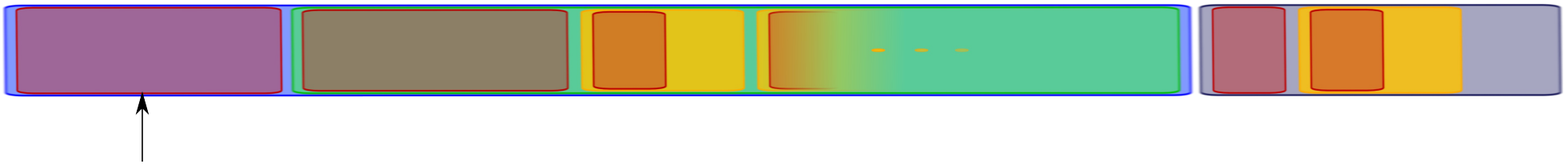
Méta-données

- Constitution globale



Partie Informations

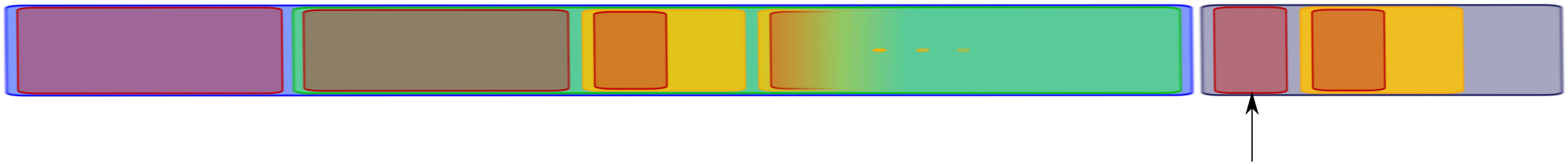
- En-tête Informations



Adresse relative	Taille	Champ	Contenu
0x00	8	Signature	-FVE-FS-
0x08	2	Taille	Taille Informations
0x0a	2	Version	1 = Vista | 2 = Windows 7
...			
0x20	8	Metadata1	Adresse 1er bloc
0x28	8	Metadata2	Adresse 2è bloc
0x30	8	Metadata3	Adresse 3è bloc
0x38	8	BootSectorBackup	Adresse pour le BPB

Partie Validations

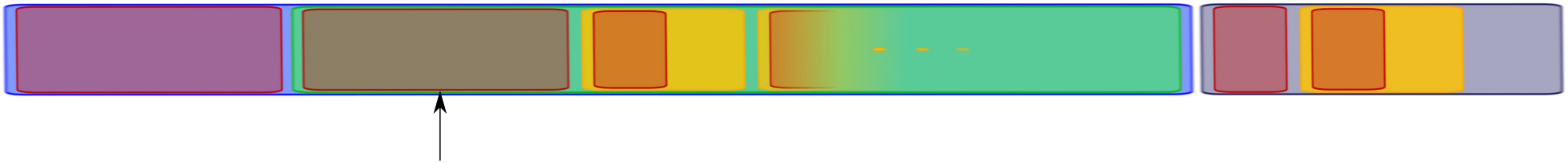
- En-tête Validations



Adresse relative	Taille	Champ	Contenu
0x00	2	Taille	Taille Validations
0x02	2	Version	1 = Vista | 2 = Windows 7
0x04	4	Checksum	CRC32 des Informations

Dataset

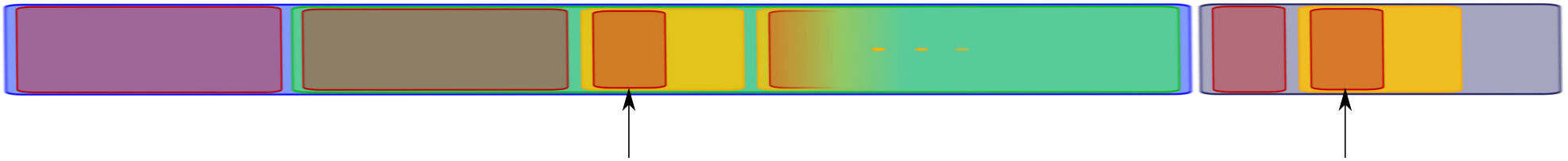
- En-tête Dataset



Adresse relative à Informations	Taille	Champ	Contenu
0x40	4	Taille	Taille de Dataset
0x44	4	Inconnu	
0x48	4	Taille	Taille de cet en-tête
0x4c	4	Taille	Taille de Dataset
0x50	16	GUID	Identifiant de Dataset
0x60	4	NextCounter	Nombre de Data générés + 1
0x64	4	Algorithme	Chiffrement des données
0x68	8	Timestamp	Date de chiffrement

Data

- Partagent en-tête commun



Adresse relative	Taille	Champ	Contenu
0x00	2	Taille	Taille de cette Data
0x02	2	Type spécifique	Type spécifique au type global
0x04	2	Type Data	Type global de la donnée
0x06	2	Statut	Égal à 1

- Type spécifique : renseigne sur le contenu de Data
- Type de donnée : format de Data

Data des Informations

- Un Data pour nom du volume et date de chiffrement
- Un Data par moyen d'accès au disque
  - VMK est chiffrée par chaque clé d'accès
  - Dans chacun de ces Data, au moins deux Data :
    - → VMK chiffrée par clé d'accès (clé utilisateur)
    - → Clé d'accès chiffrée par VMK
- Un Data pour FVEK
  - Chiffrée par VMK
- Pour Windows 7 : une Data Virtualization
  - Adresse du « boot sectors backup »
  - Nombre d'octets sauvegardés

Data des Validations

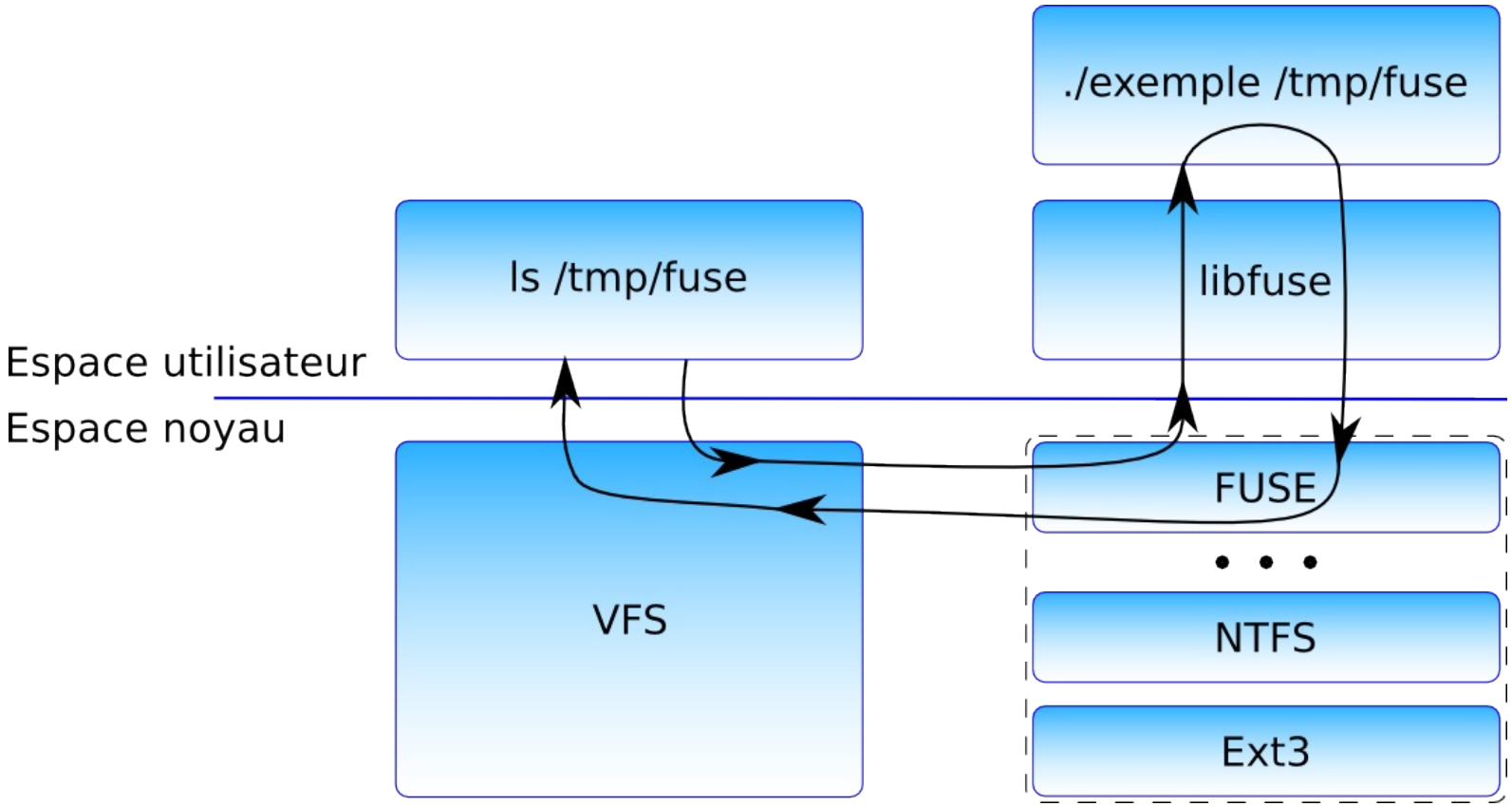
- Un et un seul Data

- Mais deux possibilités :
  - Type KEY : empreinte SHA256 des Informations
  - Type AES-CCM : contient Data de type KEY chiffré avec VMK

L'implémentation : FUSE & Dislocker

Implémentation

- Principe de FUSE



Démonstration

Vidéo...

http://www.hsc.fr/ressources/outils/dislocker/

Conclusion

- Avant
  - Structures explicitées mais introuvables
  - Pilote de lecture de partition BitLocker Vista (version alpha)
- Maintenant
  - Lecture de partitions BitLocker possible sous Linux et MacOSX
  - Support du déchiffrement BitLocker de Windows Vista ou 7
- Après
  - Lecture de partition chiffrées sous Windows 8 ?
  - Utilisation du TPM ?
  - Écriture sur une partition chiffrée ?

Questions ?

<Romain.Coltel@hsc.fr>

Références

- AES-CBC+Diffuser, a Disk Encryption Algorithm for Windows Vista – Niels Ferguson, Microsoft (2006)
- Detecting BitLocker – Jamie Hunter, Microsoft System Integrity Team (2006)
- Nvbit: Accessing Bitlocker volumes from linux – nvlabs (2006)
- Implementing BitLocker Drive Encryption for Forensic Analysis – Jesse D. Kronblum, ManTech International Corporation (2009)
- Windows Internals 5th Edition – Mark E. Russinovich et David A. Solomon (2009)
- BitLocker SSTIC – Aurélien Bordes (2011)

Hervé Schauer Consultants

- Société de conseil en sécurité des systèmes d'information depuis 1989
- Prestations intellectuelles d'expertise en toute indépendance
  - Pas de distribution, ni intégration, ni infogérance, ni investisseurs, ni délégation de personnel
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
  - Sécurité Windows / Unix et linux / embarqué / informatique industrielle / applications
  - Enquêtes inforensiques / Expertise judiciaire
  - Sécurité des réseaux : TCP/IP, téléphonie, réseaux opérateurs, réseaux industriels...
  - Organisation de la sécurité, droit des systèmes d'information
- Certifications
  - D'entreprise : ISO 9001 (formations certifiantes), OPQF, OPQCM, ARJEL, PCI-DSS
  - Individuelles : CISSP (ISC)², LSTI, EXIN, QSA, GIAC, OSCP, etc.