Chiffrement de disque LUKS sous FreeBSD

Institut Mines-Télécom

Auteurs

Pierre Koebelin

Romain Cherré

Encadrant

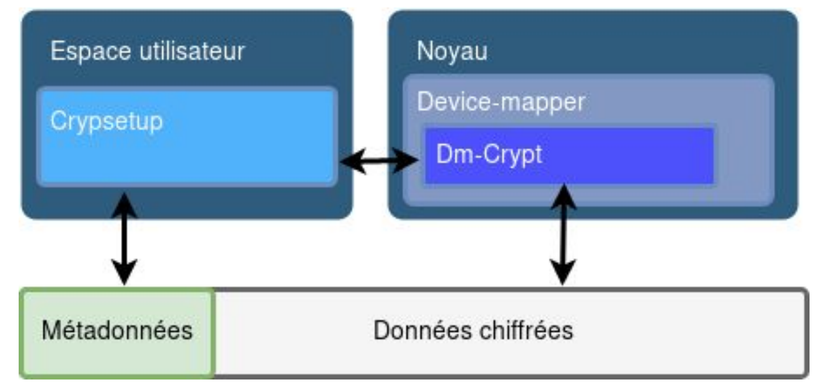
Olivier Paul

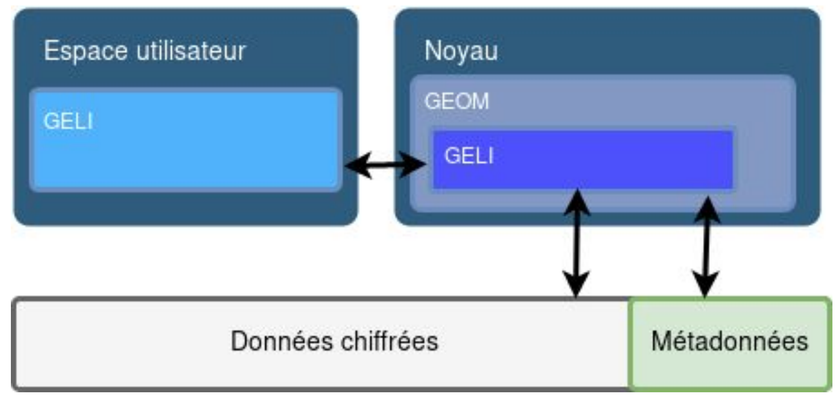
Partenaires

Chiffrement de disque logiciel

Sous linux et FreeBSD

- Chiffrement de disque logiciel grâce à *dm-crypt* et *cryptsetup* sous Linux
- Chiffrement de disque logiciel grâce à *GELI* sous FreeBSD
- LUKS un format sur disque standardisé pour Linux
- Des algorithmes de chiffrement similaires : **AES-XTS**, **AES-CBC**,…
- Des métadonnées de chiffrement au début du disque pour Linux, à la fin du disque pour FreeBSD
- Dm-crypt qui n'a pas connaissance du standard *LUKS* et *GELI* utilise son propre format

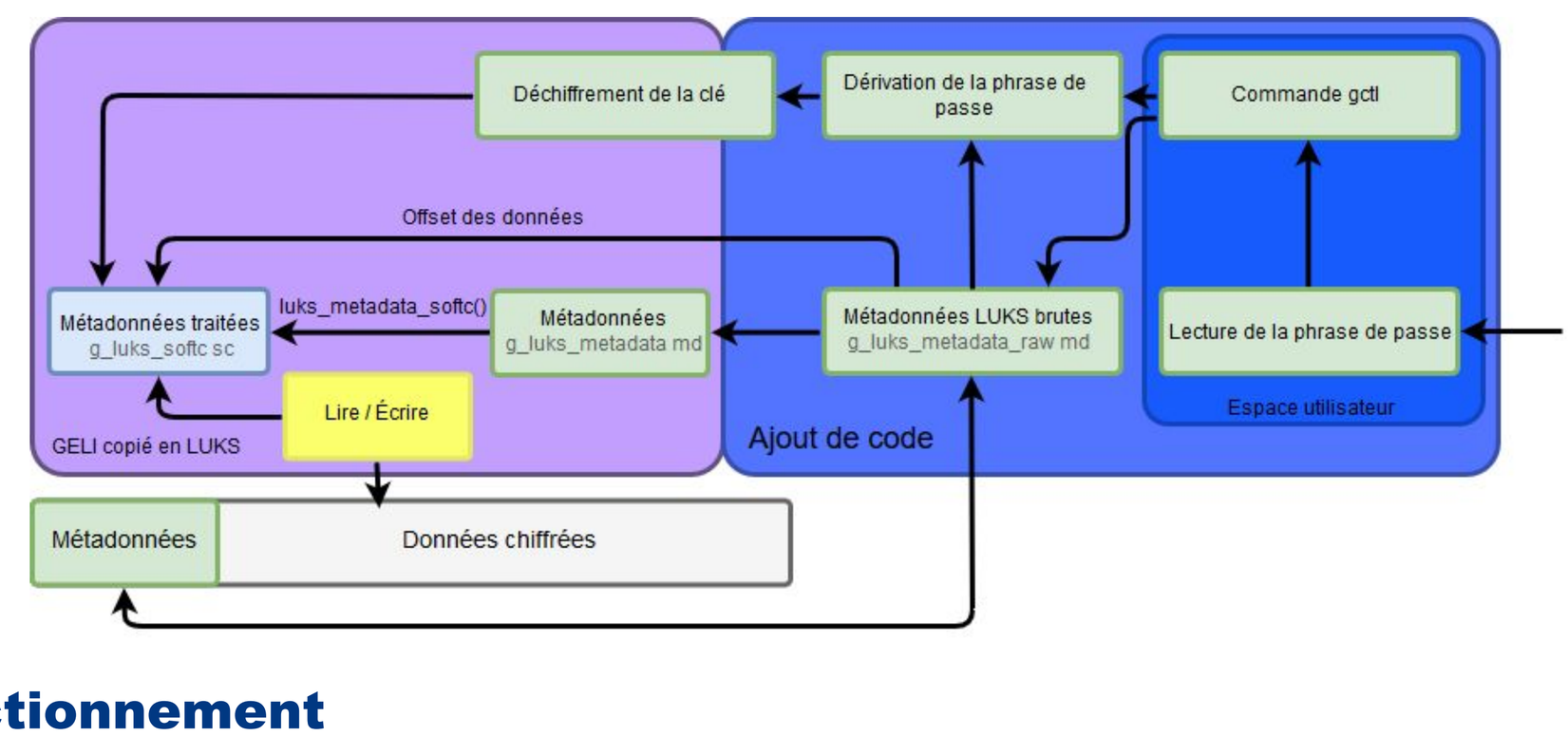




Développement d'un module noyau et de son utilitaire

À partir du code de *GELI*

- Conversion des métadonnées de *LUKS* en métadonnées *GELI*
- Ajout de fonctions pour déchiffrer la clé de chiffrement
- Modification de l'alignement du disque déchiffré avec le disque chiffré dû à l'emplacement des métadonnées
- Utilisation des `flags` de *GELI* pour utiliser la clé maître comme clé de chiffrement, le standard IEEE 1619-2007 prévoit un changement de clé tous les 2^{20} secteurs, ce que ne réalise pas *LUKS*.
- Changement de l'utilisation du champ correspondant à l'algorithme d'authentification en l'algorithme de génération des vecteurs d'initialisation **IV**



Fonctionnement

LUKS sous FreeBSD

- Intégration du module *GLUKS* et de l'utilitaire `geom_luks` dans FreeBSD, grâce à l'API de gestion de disque
- Des systèmes de fichiers compatibles entre Linux et FreeBSD permettent le partage de données chiffrées entre les deux systèmes : **EXT2**, **FAT32**, **NTFS**, **ZFS**, etc
- Support du démarrage sur une partition chiffrée avec LUKS à implémenter
- Intégration à la branche principale de FreeBSD à réaliser avec la revue par les développeurs FreeBSD

Projet de fin d'étude

Janvier 2019

Contact romain.cherre@telecom-sudparis.eu
pierre.koebelin@telecom-sudparis.eu

Site web github.com/PFE-geom-luks