

Sistemele criptate de fisiere sub Linux

Dragos Acostachioaie

Universitatea “A.I.Cuza” Iasi,

Facultatea de Informatica

dragos@adt.ro

Introducere

- Tipuri de sisteme de criptare a fișierelor
 - *Criptarea la nivel de volum* – criptează întreg conținutul unei partiții sau disc (nivel de driver)
Exemple: PGPDisk, SFS, Linux CryptoAPI
 - *Criptarea la nivel de fișier* – criptează fișiere (nivel de aplicație)
Exemple: PGP, GPG
 - *Criptarea la nivel de sistem de fișiere* – criptează un sistem de fișiere (nivel de nucleu)
Exemple: CFS, TCFS, CryptFS

Sistemul *CryptFS*

- Implementat la nivelul nucleului
- Sistemul de fisiere criptat poate fi montat “deasupra” unui alt sistem de fisiere
- Datele sunt criptate inainte de a fi scrise pe disc si sunt decriptate dupa ce au fost citite
- Este utilizat un sistem de chei publice si private
- Pentru criptare este utilizat algoritmul Blowfish
- www.filesystems.org

Sistemul *CryptFS*

- In loc ca un sistem de fisiere sa fie montat intr-un punct de montare, acesta va fi montat ca dispozitiv de tip *loop*
- Operatiile de intrare/iesire cu dispozitivul *loop* trec prin sistemul *CryptFS*, criptand datele
- Un fisier ordinar poate fi utilizat ca dispozitiv de tip bloc, care poate contine un sistem de fisiere = dispozitivul de tip *loop* (*loopback*)
- Nu ofera suficienta siguranta pentru sistemele de fisiere jurnalizate (*ext3*, *reiserfs*)

Dm-crypt si cryptoapi

- Nucleele Linux din seria 2.6.x implementeaza o infrastruktura generica, numita *device-mapper*, care ofera posibilitatea de a crea niveluri virtuale de dispozitive de tip bloc, putand “suprapune” diferite mecanisme peste sisteme de fisiere reale (concatenare, criptare, oglindire etc.)
- Unul dintre dispozitivele de tip *device-mapper* este *dm-crypt*, care ofera criptarea transparenta a dispozitivelor de tip bloc, utilizand *cryptoapi*

Dm-crypt si cryptoapi

- *Cryptoapi* este o interfata de programare pentru aplicatii (API), care ofera algoritmi de criptare, in cadrul nucleului Linux
- Pe viitor, nucleul Linux va oferi suport pentru dispozitive de criptare hardware
- Pentru a crea un sistem de fisiere criptat trebuie urmati pasii:
 - Partitia sau discul care va stoca sistemul de fisiere criptat trebuie populat cu date aleatorii, pentru a reduce posibilitatea decriptarii datelor

Dm-crypt si cryptoapi

- Se initializeaza sistemul de fisiere criptat cu *cryptsetup* (*cryptsetup create hda3 /dev/hda3*)
- Este necesara introducerea unei parole (*passphrase*); aceasta va fi procesata printr-o functie de dispersie (*hash*), iar rezultatul va constitui cheia de criptare
- In urma initializarii este creat un dispozitiv special (*/dev/mapper/hda3*)
- Dispozitivul nou creat poate fi utilizat ca un disc obisnuit (montat, demontat etc.)
- La fiecare pornire a sistemului trebuie initializat dispozitivul (va fi solicitata parola folosita la prima initializare)