Encriptação de disco

Natã Santana de morais

Problema

- Dados são matéria-prima para a informação
- Dados interessam a empresas
- Como evitar que ataques cibernéticos ou roubos interfiram em nossos dados ?
- Criptografia de disco

Objetivo

- O que é criptografia de disco?
- Como funciona?
- Softwares que realizam a função

Criptografia de disco

- Dados ilegíveis - bits
- Criptografia do disco inteiro
- Área de inicialização não é criptografada

Criptografia transparente

- Automática
- Dados são acessíveis mediante senha ou chave de decriptação.

TPM

- Chip processador de criptografia seguro incorporado a placa mãe
- Autenticação
- Vantagens e desvantagens

TrueCrypt

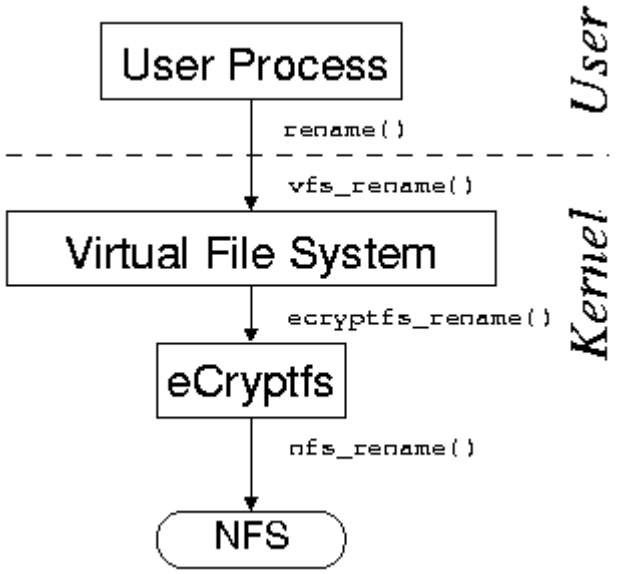
- Código aberto e multiplataforma
- Discos virtuais
- Encriptação transparente
- Descontinuado
- Utiliza vários algoritmos, entre eles: AES e SHA-512

Criptografia para Sistemas Operacionais

- Linux
- Windows

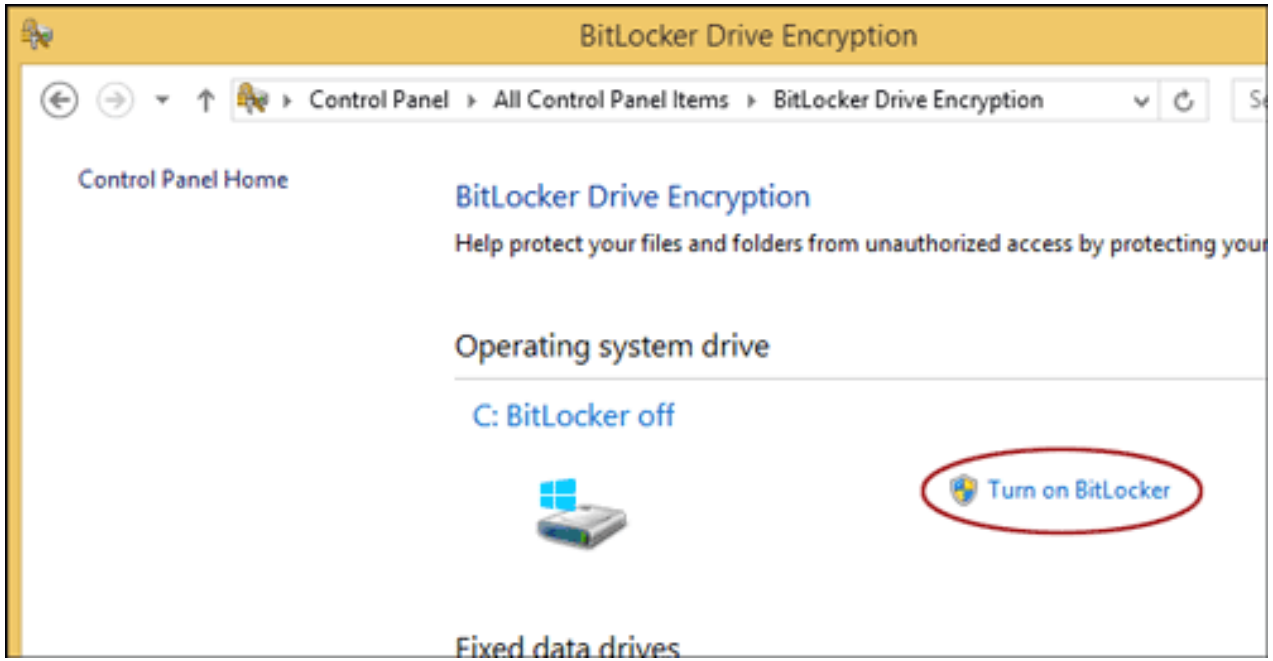
Criptografia para Linux

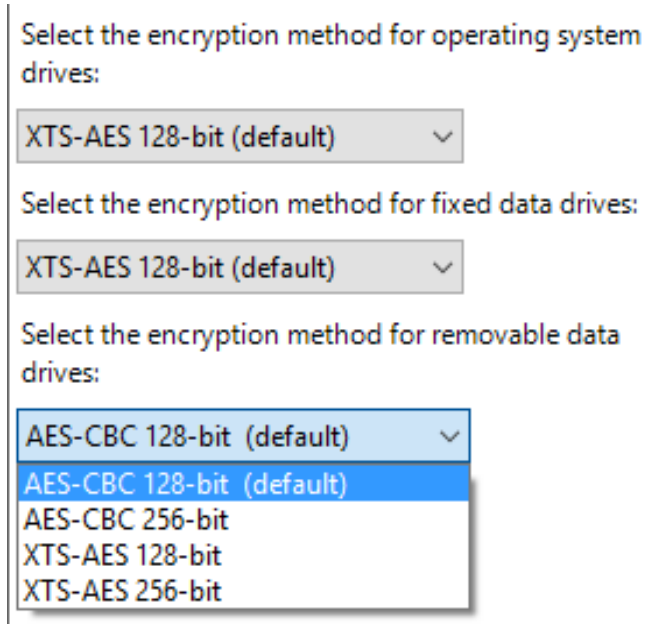
- eCryptfs – pacote de software de criptografia de disco
- Baseado no GnuPG – base completa para criptografia e assinatura de dados
- Suporta vários algoritmos criptográficos, mas por padrão utiliza o AES.



Criptografia para Windows

- BitLocker – criptografia de disco inteiro
- Solução integrada
- Só pode ser habilitado em computadores com TPM
- BitLocker usa a criptografia AES, de 128 ou 256 bits.


BitLocker Drive Encryption
Control Panel
All Control Panel Items
BitLocker Drive Encryption
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives


Select the encryption method for operating system drives:
XTS-AES 128-bit (default)
Select the encryption method for fixed data drives:
XTS-AES 128-bit (default)
Select the encryption method for removable data drives:
AES-CBC 128-bit (default)
AES-CBC 128-bit (default)
AES-CBC 256-bit
XTS-AES 128-bit
XTS-AES 256-bit


BitLocker Drive Encryption
Encrypting...
Drive C: 15.4% Completed
Close
Manage BitLocker