Universidade Federal do Ceará – UFC

Aluno: Natã Santana de Morais

Número: 383808

Curso: Ciência da Computação

Disciplina: Criptografia

Encriptação de disco

Crateús – CE

04/12/2017

Introdução

Tudo gera em torno dos dados. Mas, não basta ter dados é preciso interpretá-los e transformá-los em informações. Hoje, principalmente para empresas, dados são a matéria-prima para seus negócios. Dado isso, informações como essas precisam estar disponíveis e principalmente seguras.

A encriptação de disco possibilita a criptografia de dados que são armazenados em conjunto de discos básicos ou de discos independentes. Esse tipo de criptografia protege as informações utilizando a encriptação, ou seja, tornando os dados ilegíveis.

Esta mesma criptografia é usada a fim de impossibilitar o acesso não autorizado de dados. Em meio a competitividade e ataques cibernéticos, proteger seus dados é a primeira coisa a se pensar.

Objetivos

O objetivo desse trabalho é apresentar e mostrar o que é criptografia de disco. Apesar não ser um assunto complexo é importante que alcancemos o conhecimento necessário nesse assunto. No mercado, os dados são tão importantes como o dinheiro. Saber lidar com eles é imprescindível.

O alvo desse projeto é não só conhecer esse tipo de criptografia, mas também saber diferenciar os vários tipos, suas vantagens e desvantagens, funcionalidade e aplicabilidade.

Desenvolvimento

Há vários modos de encriptar discos e também estão disponíveis muitas ferramentas para a realização do mesmo. Nesse ramo existe a criptografia de disco inteiro, ou seja, a prática de criptografar tudo no disco, menos a gravação mestre de inicialização ou a área similar de um disco inicializável. A criptografia de disco criptografa metadados do sistema de arquivos, como estrutura de diretório, nomes de arquivos e etc.

Também existe um conceito bastante importante, a encriptação transparente. O nome “transparente” vem do fato de que os dados são automaticamente criptografados ou descriptografados quando carregados ou salvos. Com esse tipo de criptografia, os arquivos são acessíveis imediatamente após a chave ser fornecida. A partir disso, nenhum dado armazenado em um volume criptografado pode ser lido sem usar a senha ou chave de criptografia correta.

Existe também, a criptografia a nível de sistemas de arquivo. O EFS (Sistemas de Arquivos com criptografia) criptografa arquivos individuais em qualquer unidade. O EFS criptografa arquivos com base na conta de usuário associada a ele. Se um computador tiver vários usuários ou grupos, cada um poderá criptografar seus próprios arquivos independentemente.

Concluído isso, vem a questão, qual a melhor escolha: criptografia de disco ou criptografia a nível de sistemas de arquivo? A criptografia de disco às vezes é usada em conjunto com a criptografia de nível de sistemas de arquivos. A diferença é que em nível de sistemas de arquivos, os metadados não são criptografados.

Temos também, nesse ramo, o conceito de TPM. O mesmo, é um processador de criptografia seguro incorporado na placa-mãe que pode ser usado para autenticar um dispositivo de hardware. Porém, se algo acontecer com a placa-mãe ou o TPM, o usuário não poderá acessar os dados em outro computador. A não ser, que esse usuário tenha uma chave de recuperação separada.

Um dos softwares para criptografia de disco era o TrueCrypt. O mesmo era de código aberto e multiplataforma (Windows, Mac, Linux). O algoritmo funcionava criando discos criptografados que podiam ser montados como unidades virtuais. Esse algoritmo utilizava a encriptação transparente. Infelizmente, por motivos de brechas de segurança não resolvidas, o TrueCrypt foi descontinuado. O mesmo utilizava algoritmos como AES e SHA-512.

Atualmente para sistemas LINUX, temos o pacote de software de criptografia de disco chamado eCryptfs. O eCryptfs suporta vários algoritmos criptográficos, mas por padrão ele utiliza o AES. O eCryptfs é baseado no GnuPG. O GnuPG é uma base completa para criptografar e assinar dados, mas para cada sistema operacional existe uma ferramenta complementar dentro da suíte GnuPG. A criptografia do eCryptfs é baseada na manipulação dos dados em sistemas de arquivos virtuais, na qual passam pela criptografia eCryptfs e logo após são inseridos nos discos reais.

Já no Windows, é possível encriptar o disco utilizando a ferramenta BitLocker. O mesmo criptografa toda a unidade. Essa ferramenta é uma solução integrada no Sistema Operacional Windows. O BitLocker, por padrão, só pode ser habilitado em computadores com TPM – um chip integrado à placa-mãe que armazena as chaves de criptografia de forma segura, não permitindo que o disco seja descriptografado em outro computador. Se o seu computador não possui esse dispositivo, será apresentado um erro.

O BitLocker usa AES (Criptografia AES) como algoritmo de criptografia com comprimentos de chaves configuráveis de 128 ou 256 bits. A configuração de criptografia padrão é AES-128, mas as opções são configuráveis usando a Política de Grupo.

Conclusão

Criptografar dados é a prática crucial para a segurança da informação. Há várias ferramentas para isso, basta somente usá-las. Atualmente, se faz necessário criptografar dados. Pois, hoje em dia, tudo gira em torno de dados.

Portanto, se deseja segurança, faça já criptografia.