Comparação Entre Dois Sistemas de Arquivos Criptográficos

Jessica Imlau Dagostini <jessicadagostini@gmail.com> [1]
Marisa Richter <marisa@hotmail.com> [1]
Prof. Marcos A. Lucas <mlucas@uricer.edu.br> [2]

CONSIDERAÇÕES INICIAIS

Manter seguros dados em meio digital virou uma das principais preocupações da atualidade. Uma forma de aprimorar a segurança de arquivos é a utilização de um sistema de arquivos criptográfico de qualidade. O presente trabalho realizou um estudo e comparação quanto ao sistema de arquivos *eCryptFS* e o *EncFS*, ambos suportados pela plataforma Linux.

METODOLOGIA

A fim de termos resultados reais para uma boa comparação entre os dois sistemas estudados, utilizamos o *Iozone*, uma ferramenta de *benchmarking* para determinar o *throughput* de ambos. *Benchmarking* é o ato de executar um programa para melhor avaliar o desempenho relativo de um objeto, normalmente executando uma série de testes padrões e ensaios nele.

Somado a isso, leituras de fontes determinaram as demais características levadas em consideração nas comparações realizadas.

REFERENCIAL TEÓRICO

O *eCryptFS* é um sistema de arquivos criptográfico que estende o *CryptFS* e pode ser montado em um diretório ou sob qualquer outro sistema de arquivos, como UFS e NFS, sendo implementado em modo núcleo.

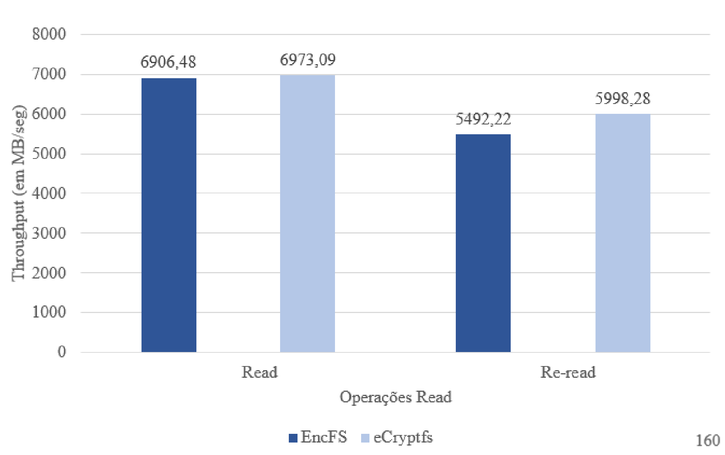
FUSE (*Filesystem in Userspace*), Sistemas de Arquivos em Espaço de Usuário, são aqueles em que os dados e os metadados são produzidos por um processo de usuário.

O *EncFS* é um *FUSE-based* sistema de arquivo criptografado que visa proteger os dados com mínimos problemas.

RESULTADOS E ANÁLISE

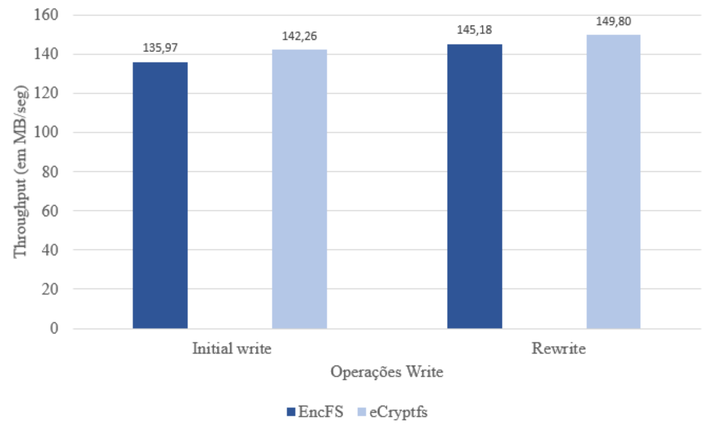
O ambiente onde realizaram-se os testes possui as seguintes configurações:

- Sistema operacional Ubuntu 16.04;
- Processador Intel Core i5 4 núcleos 2.90GHz Cache 6MB;
- Memória RAM de 4GB DDR3;



É possível perceber uma mínima vantagem do *eCryptfs* perante o *EncFS* em operações *read* sendo ela de aproximadamente 1%. Já operações *re-read* o mesmo apresenta uma vantagem maior, de aproximadamente 8,4%.

Em operações *write* e *re-write* as diferenças apresentadas também não foram muito altas. O *eCryptfs* se mostra 4,4% mais eficiente que o *EncFS* em operações *write* e 3% em operações *re-write*.



FileSystem	Principal Vantagem	Principal Desvantagem
eCryptFS	Utilização de *Salting* para proteção de senhas.	Geração de arquivos maiores em *Sparse File*
EncFS	Pode ser criado por *non root users*	Texto de criptografia dá acesso a todo o sistema

Tabela 1 – Principais vantagens e desvantagens dos sistemas.

CONSIDERAÇÕES FINAIS E CONCLUSÃO

A criptografia de arquivos é uma ótima alternativa para manter em segurança os dados de uma organização. Qual ferramenta usar depende muito de especificação, o *eCryptFS* é recomendado pela leve superioridade de desempenho, e por ter maior segurança sobre o *EncFS*. Todavia aos que precisam criptografar arquivos armazenados em nuvem, o *EncFS* é a melhor opção, por ser simples, e ter usabilidade e configuração *user friendly.*

[1] Acadêmicas: discente do curso de Ciência da Computação da URI – Erechim
[2] Orientador: docente do curso de Ciência da Computação da URI – Erechim