XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg 2017

Eliminação Segura de Arquivos em Memória Não-Volátil

Julia S. Weber, Avelino F. Zorzo

Faculdade de Informática –PUCRS – Porto Alegre – RS – Brasil

Alunos: Darley Krefta, Osni Dorini.

UTFPR UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MINISTÉRIO DA EDUCAÇÃO

BRASIL GOVERNO FEDERAL

Introdução

- A quantidade de dispositivos móveis em circulação é muito grande, e com isso vem a necessidade de tornar os dados mais seguro.
- Com o uso crescente de memória flash em dispositivos, cresce também a necessidade de garantir a proteção dos dados armazenados.
- Dados pessoais e sigilosos estão armazenados e estes dados não podem ser recuperados por terceiros, principalmente quando forem apagados.
- Apagamentos em dispositivos na maioria das vezes é somente logico e não físico, permitindo o acesso por meio de ferramentas a estes dados.

Proposta

- A eliminação segura dos dados consistem em apagar permanentemente os dados nos dispositivos, de modo que os dados se tornem irrecuperáveis.
- Remoção segura de arquivos em memórias não-voláteis emprega operações de sobrescrita com zeros e de apagamento de blocos.
- O método proposto é híbrido combinando as operações;
  - Sobrescrita com zeros;
  - Apagamento;
- Evitando o desgaste prematuro da memória.

Memoria Flash

- Sistemas de arquivo são normalmente implementados em memória *flash* com tecnologia NAND.
- Trabalha em alta velocidade;
- Dividido em blocos de células, cada bloco consiste em um determinado numero de paginas, as paginas variam entre 512, 2048 ou 4096 bytes em tamanho.
- Uma unidade de apagamento, é a região mínima de apagamento.
- Não é possível gravar dados em um bloco de memoria flash, a menos que o mesmo, tenha sido apagado anteriormente.
- Quando é executada uma operação de apagamento em uma unidade, todos os seus blocos são preparados para uma escrita futura.

Característica da Memoria Flash

- A memória flash permite dois estados, apagado e não apagado e apagar memória flash causa desgaste físico.
- Para diminuir o desgaste é utilizado duas

camadas de controle:

  - FTL (FlashTranslation Layer) Redirecionar endereços lógicos do sistema de arquivos do sistema operacional para endereços físicos em *flash* NAND. Utiliza uma tabela de mapeamento.
  - MTD (Memory Technology Device) executar as funções primitivas na memória flash(ler e apagar)

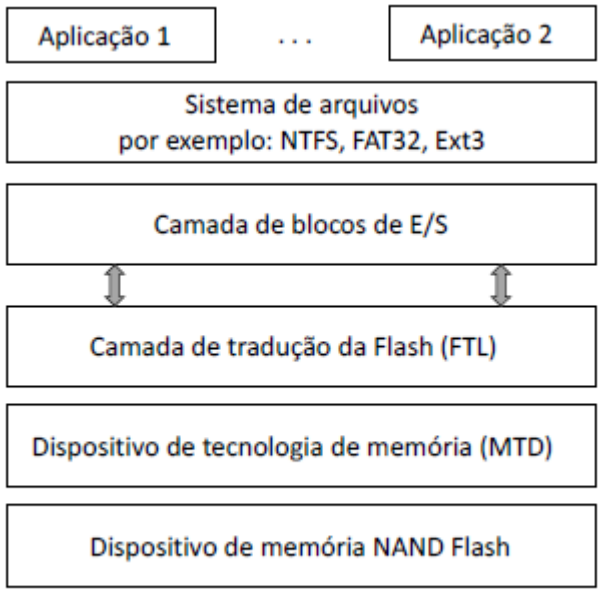


Figura 1 – Arquitetura de uma memória *flash* do tipo NAND

Velocidades

- Operações de apagar, levam muito mais tempo que escrita e leitura.
- SLC NAND Flash: Single-level cell(1 bit célula)
- MLC NAND Flash: Multi-level cell(2 bits célula)

Tabela 1 – Especificações de Memória flash NAND [15]

Características	SLC NAND Flash	MLC NAND Flash
Leitura	30 μs	250 μs
Escrita	250 μs	2700 μs
Apagamento	3ms	4ms
Tamanho de bloco	4.328 Bytes	8.568 Bytes
Tamanho de unidade	270,5 KBytes	1.606,5 KBytes

Métodos de Remoção Segura

Como um sistema operacional faz a remoção de um arquivo simplesmente liberando os blocos que o arquivo ocupava em disco (*deletion by unlinking*), a sua recuperação com ferramentas forenses é possível, desde que os blocos ainda não tenham sido alocados e sobrescritos por outro arquivo.

- Uso de criptografia para realizar a eliminação, onde um arquivo é armazenado de forma criptografada e a sua remoção é realizada eliminando-se a chave de criptografia.
- Uso de sobrescrita para realizar a eliminação, onde os blocos pertencentes a um arquivo que deve ser removido são sobrescritos com padrões binários..

Método de SUN

- O método de SUN é híbrido, pois combina sobrescrita com zeros, e apagamento de blocos:
- Procura um bloco a ser deletado.
- Verifica se o custo da substituição por zeros (*zero-overwriting*) nos blocos é menos custoso do que apagar a unidade de apagamento (*erase blocks*) que contém os blocos excluídos. Se o custo de substituir é menos custoso do que apagar a unidade de apagamento, a substituição com zeros é executada.
- Caso contrário, os blocos válidos são copiados para outra unidade de apagamento e o apagamento da unidade é aplicado para excluir dados.

Método de Huang

- Huang propõe um método que utiliza duas passagens:
- Na primeira passagem, os blocos do arquivo são sobrescritos com zero (*zero overwriting*).
- Na segunda passagem, realiza-se o apagamento da unidade de apagamento que contém os blocos, após copiar os blocos válidos (de outros arquivos) para uma nova posição. Huang realiza estas duas passagens para ficar em conformidade com os principais padrões sugeridos para limpeza de dados.

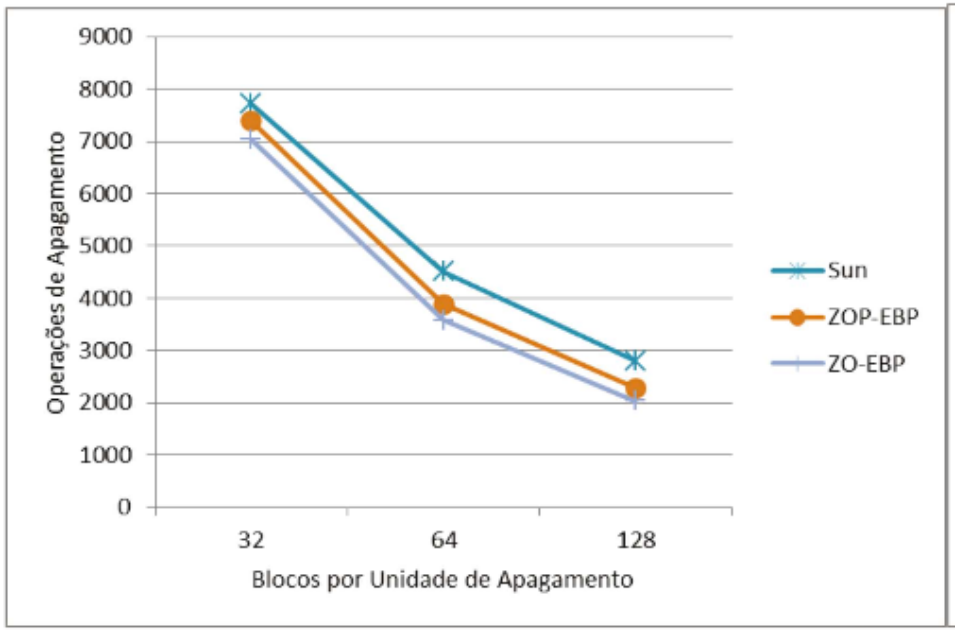
Método proposto

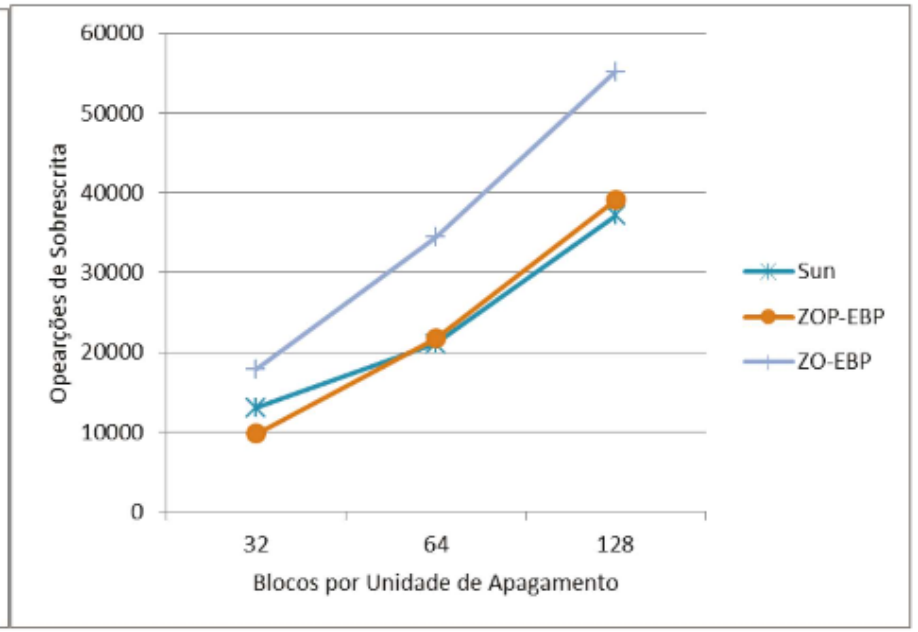
- O método proposto é calcular a penalidade entre apagar e substituir por zeros. No método Sun, ele somente considera os blocos a serem removidos e blocos válidos, causando problemas no calculo se não existem blocos válidos e somente blocos a serem removidos e livres.
- O método proposto é um hibrido de Sobrescrita e apagamento assim como o Sun, porém o calculo considera a penalidade para realizar processo.
- Custo = Tempo – Beneficio + Penalidade

Experimentos

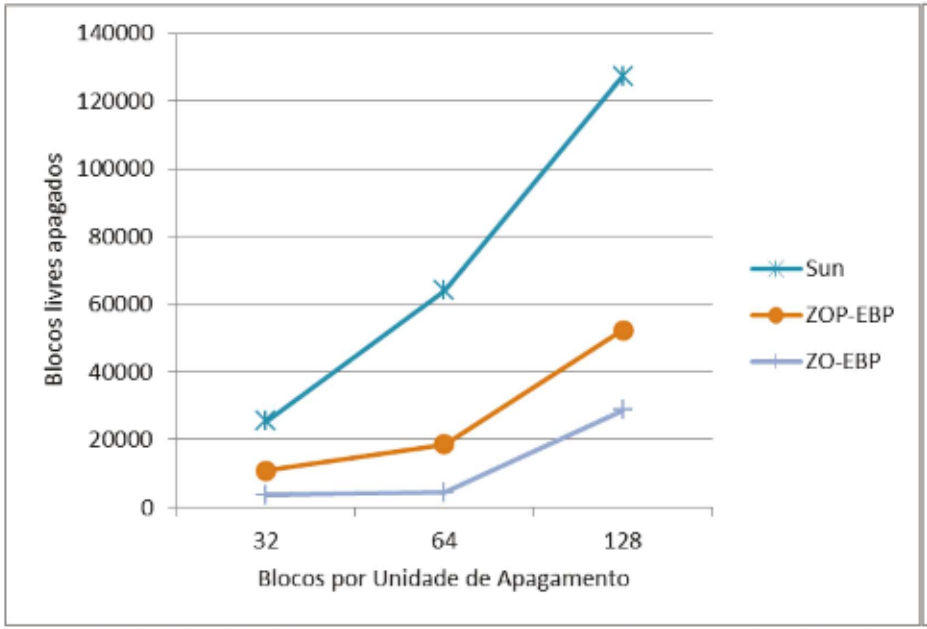
Método	Apagamentos		Sobrescritas com zeros		Livres apagados		Blocos operados	
Zero-over	1271	20,89%	220260	100%	0	0%	301604	37,86%
Erase	6083	100%	0	0%	75563	100%	576290	72,35%
Sun	4510	74,14%	21067	9,56%	64111	84,84%	318857	40,03%
ZOP-EBP	3889	63,93%	21701	9,85%	18712	24,78%	291371	36,58%
ZO-EBP	3575	58,77%	34380	15,61%	4449	5,89%	272262	34,18%
Huang	6083	100%	220260	100%	75563	100%	796550	100%

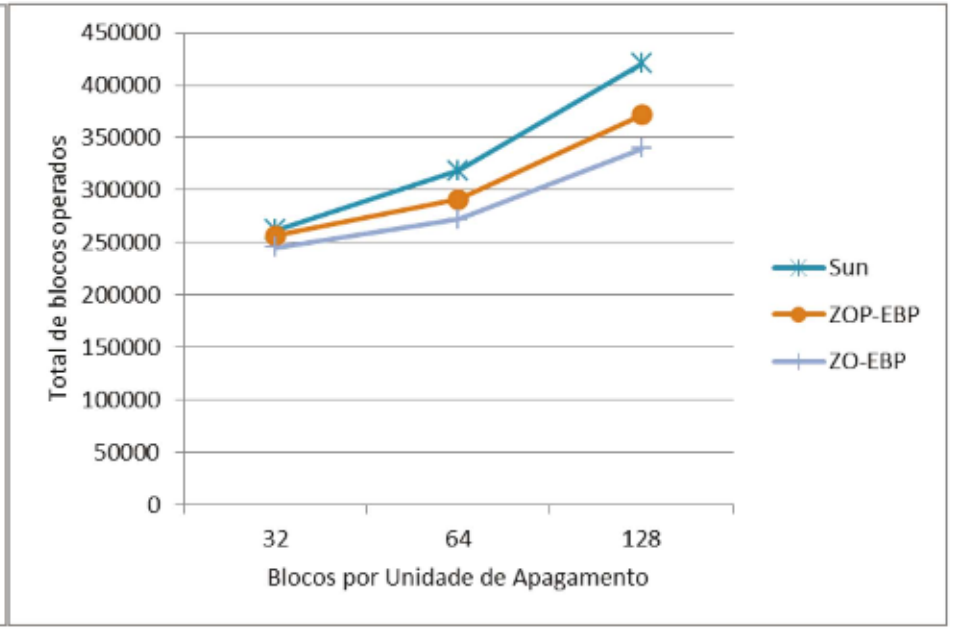
Conclusão





Conclusão





Conclusão

- Pelas análises realizadas, um método é considerado como tendo bom desempenho se apresenta um equilíbrio entre Sobrescritas e Apagamentos, realiza uma quantidade relativamente pequena de operações sobre blocos e minimiza a quantidade de blocos livres que são prematuramente apagados.