DEFY: A Deniable, Encrypted File System for Log Structured Storage

WRITTEN BY:

TIMOTHY PETERS

MARK GONDREE

ZACHARY PETERSON

PRESENTED BY:

NICHOLAS BURTON

What is encryption?

Why hide encryption?

Previous Work on the Matter

- Anderson and others…

Previous Work on the Matter

- Anderson and others…
- StegFS, McDonald and Kuhn

Previous Work on the Matter

- Anderson and others…
- StegFS, McDonald and Kuhn
- StegFS, Pang, Tan, and Zhou

Previous Work on the Matter

- Anderson and others…
- StegFS, McDonald and Kuhn
- StegFS, Pang, Tan, and Zhou
- DenFS, Gasti and others

Previous Work on the Matter

- Anderson and others…
- StegFS, McDonald and Kuhn
- StegFS, Pang, Tan, and Zhou
- DenFS, Gasti and others
- Mobiflage, Skillen and Mannan

Previous Work on the Matter

- Anderson and others…
- StegFS, McDonald and Kuhn
- StegFS, Pang, Tan, and Zhou
- DenFS, Gasti and others
- Mobiflage, Skillen and Mannan
- WhisperYAFFS

Why is DEFY different?

Main component of DEFY?

Main component of DEFY?

YAFFS

YAFFS (Yet Another Flash File System)

YAFFS (Yet Another Flash File System)

- Read and Write at Page level, delete at Block level (NAND Flash Architecture)

YAFFS (Yet Another Flash File System)

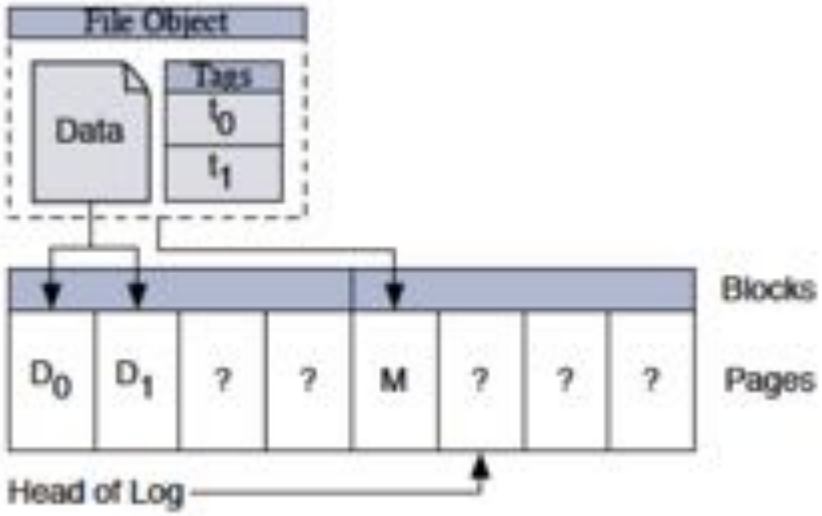
- Read and Write at Page level, delete at Block level (NAND Flash Architecture)
- Per-page Out Of Bounds (OOB) Area for MetaData (NAND Flash Architecture)

YAFFS (Yet Another Flash File System)

- Read and Write at Page level, delete at Block level (NAND Flash Architecture)
- Per-page Out Of Bounds (OOB) Area for MetaData (NAND Flash Architecture)
- Dynamic Wear Leveling (NAND Flash Architecture)

YAFFS (Yet Another Flash File System)

- Read and Write at Page level, delete at Block level (NAND Flash Architecture)
- Per-page Out Of Bounds (OOB) Area for MetaData (NAND Flash Architecture)
- Dynamic Wear Leveling (NAND Flash Architecture)
- Log Structured File System



Design Requirements

Design Requirements

- Deniability Levels

Design Requirements

- Deniability Levels
- Secure Deletion

Design Requirements

- Deniability Levels
- Secure Deletion
- Authentication Encryption

Design Requirements

- Deniability Levels
- Secure Deletion
- Authentication Encryption
- Minimizing Data Loss

Design Requirements

- Deniability Levels
- Secure Deletion
- Authentication Encryption
- Minimizing Data Loss
- Wear Leveling

Design Requirements

- Deniability Levels
- Secure Deletion
- Authentication Encryption
- Minimizing Data Loss
- Wear Leveling
- Easy Deployment

Design Overview

Design Overview – Deniability Levels

- Each level is associated with a Level Directory, which exists under the root directory.
- All files in each level are within its given directory.
- Each level has its own name and key, derived from user password

Design Overview – Authentication Encryption

Input: Data Page $\langle d_1, \ldots, d_m \rangle$ with page ID id, OOB data d_{oob}, counter x, and per-level keys K_ℓ, M_ℓ

1: $ctr_1 \leftarrow$ PAD-128$(id||x||1)$
2: $c_1, \ldots, c_m, c_{oob} \leftarrow$ AES-CTR$^{ctr_1}_{K_\ell}(d_1, \ldots, d_m, d_{oob})$
3: $\sigma \leftarrow$ HMAC-SHA256$_{M_\ell}(c_1, \ldots, c_m, c_{oob})$
4: $ctr_2 \leftarrow$ PAD-128$(id||x||0)$
5: $x_1, \ldots, x_m, x_{oob} \leftarrow$ AES-CTR$^{ctr_2}_{\sigma}(c_1, \ldots, c_m, c_{oob})$
6: $t \leftarrow \sigma \oplus x_1 \ldots \oplus x_m \oplus x_{oob}$

Output: Tag t, Page $\langle x_1, \ldots, x_m \rangle$ and OOB x_{oob}

(a) AON Encryption.

Input: Encrypted Page $\langle x_1, \ldots, x_m \rangle$ with page ID id, OOB data x_{oob}, counter x, tag t, per-level keys K_ℓ, M_ℓ

1: $ctr_2 \leftarrow$ PAD-128$(id||x||0)$
2: $\sigma \leftarrow t \oplus x_1 \oplus \ldots \oplus x_m \oplus x_{oob}$
3: $c_1, \ldots, c_m, c_{oob} \leftarrow$ AES-CTR$^{ctr_2}_{\sigma}(x_1, \ldots, x_m, x_{oob})$
4: $\sigma' \leftarrow$ HMAC-SHA256$_{M_\ell}(c_1, \ldots, c_m, c_{oob})$
5: if $\sigma' \neq \sigma$ return $\perp$
6: $ctr_1 \leftarrow$ PAD-128$(id||x||1)$
7: $d_1, \ldots, d_m, d_{oob} \leftarrow$ AES-CTR$^{ctr_1}_{K_\ell}(c_1, \ldots, c_m, c_{oob})$

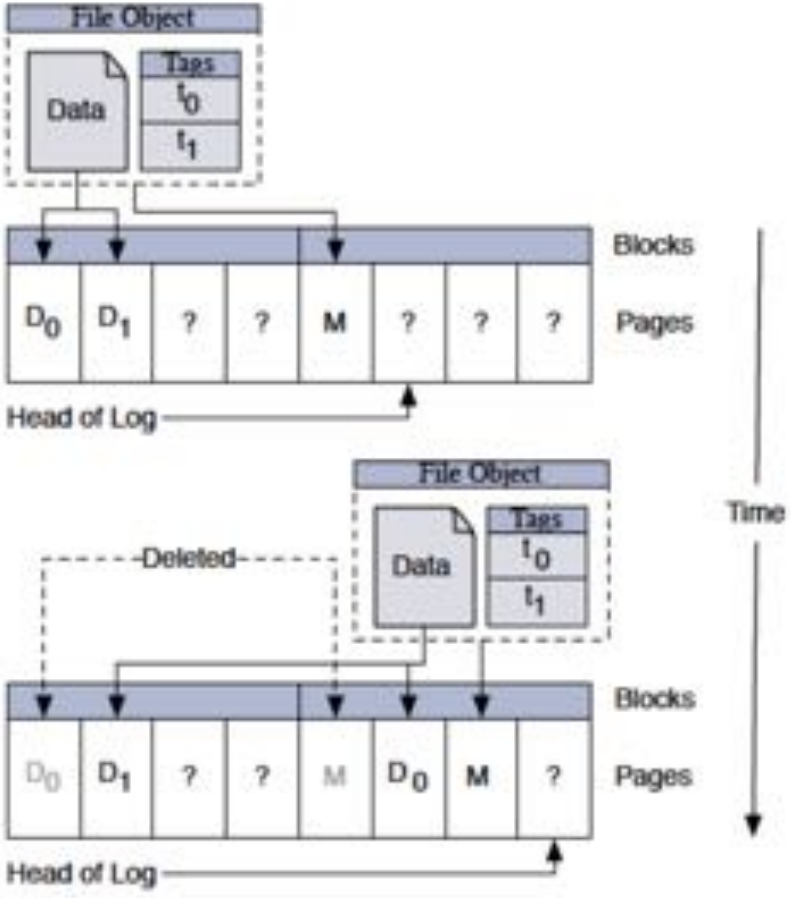
Output: Page $(d_1, \ldots, d_m)$, OOB d_{oob}

(b) AON Decryption.

Design Overview – Secure Deletion

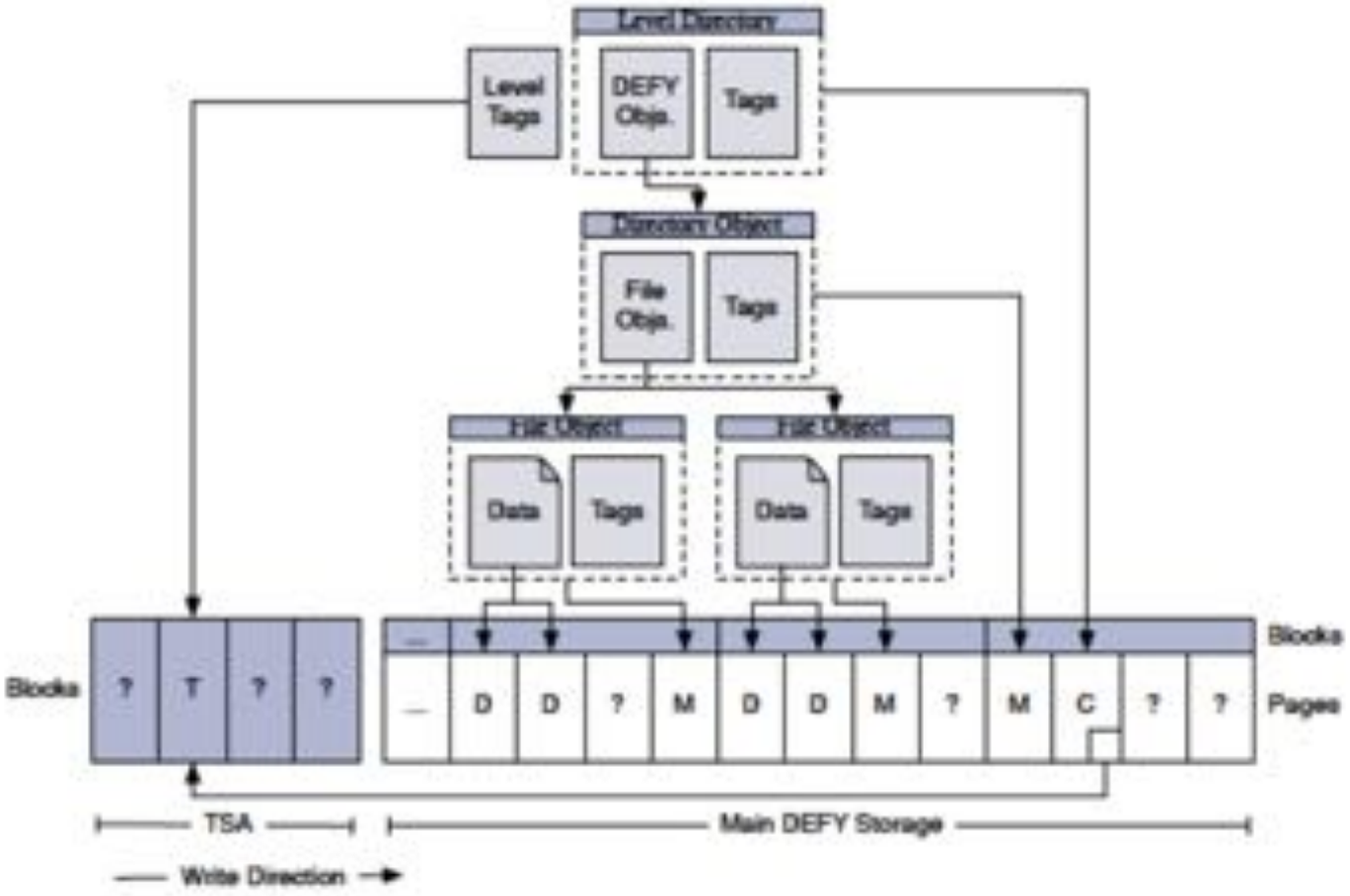
- All or Nothing transform
- Single parts of ciphertext cannot be decrypted
- Only the entire cyphertext can be decrypted
- To achieve secure deletion, part of the ciphertext is deleted, making it impossible to get back the original data.

Design Overview – Secure Deletion & Authentication Encryption



OOD Area and MetaData

OOD Area and MetaData

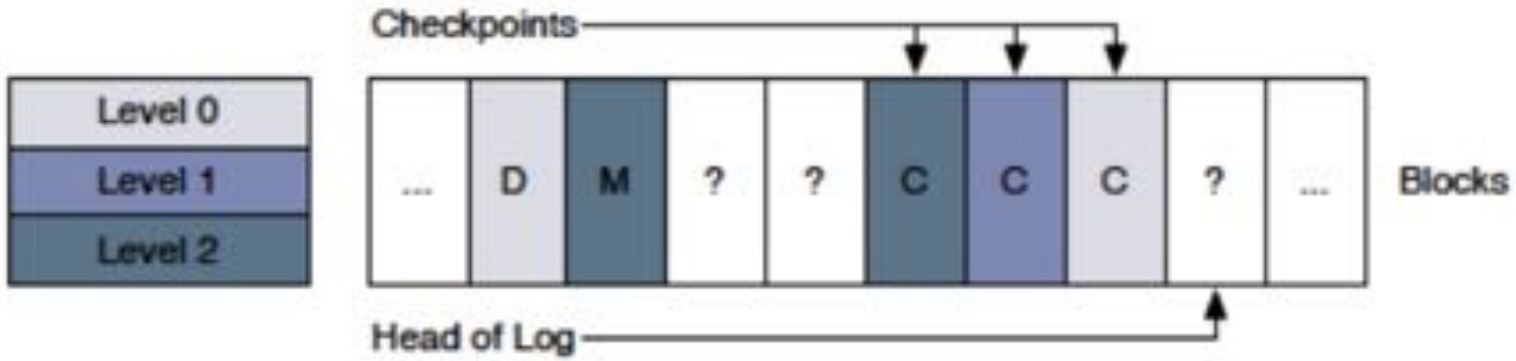


Design Overview – Minimized Data Loss

- Any encrypted page will be viewed as free by the page allocator
- DENY uses 3 methods to mitigate this problem

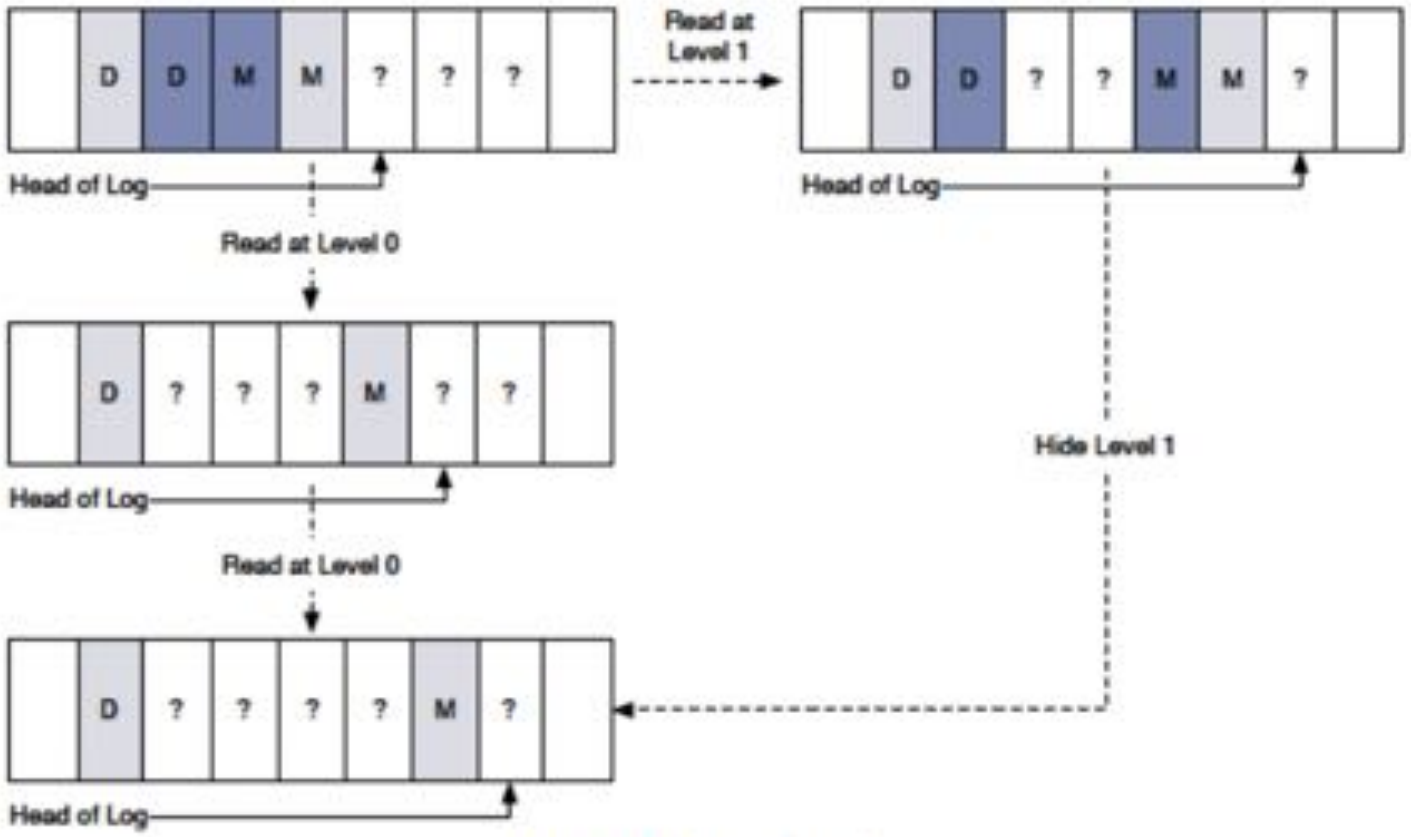
1. When higher levels are revealed, all lower levels are as well
2. One level per block policy
3. DEFY writes checkpoints in a way the prevents overwriting of higher levels

Design Overview – Minimized Data Loss



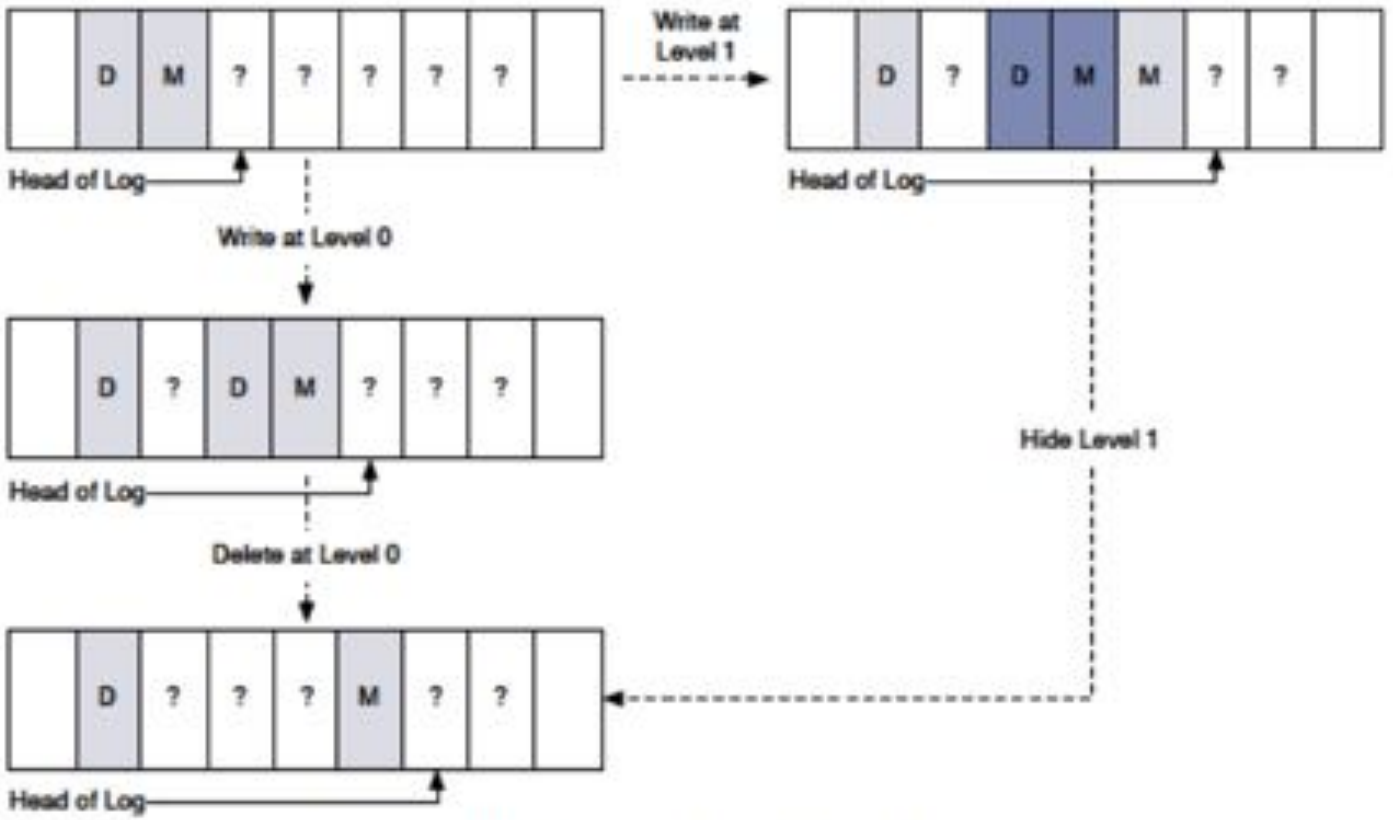
Security Analysis

Security Analysis



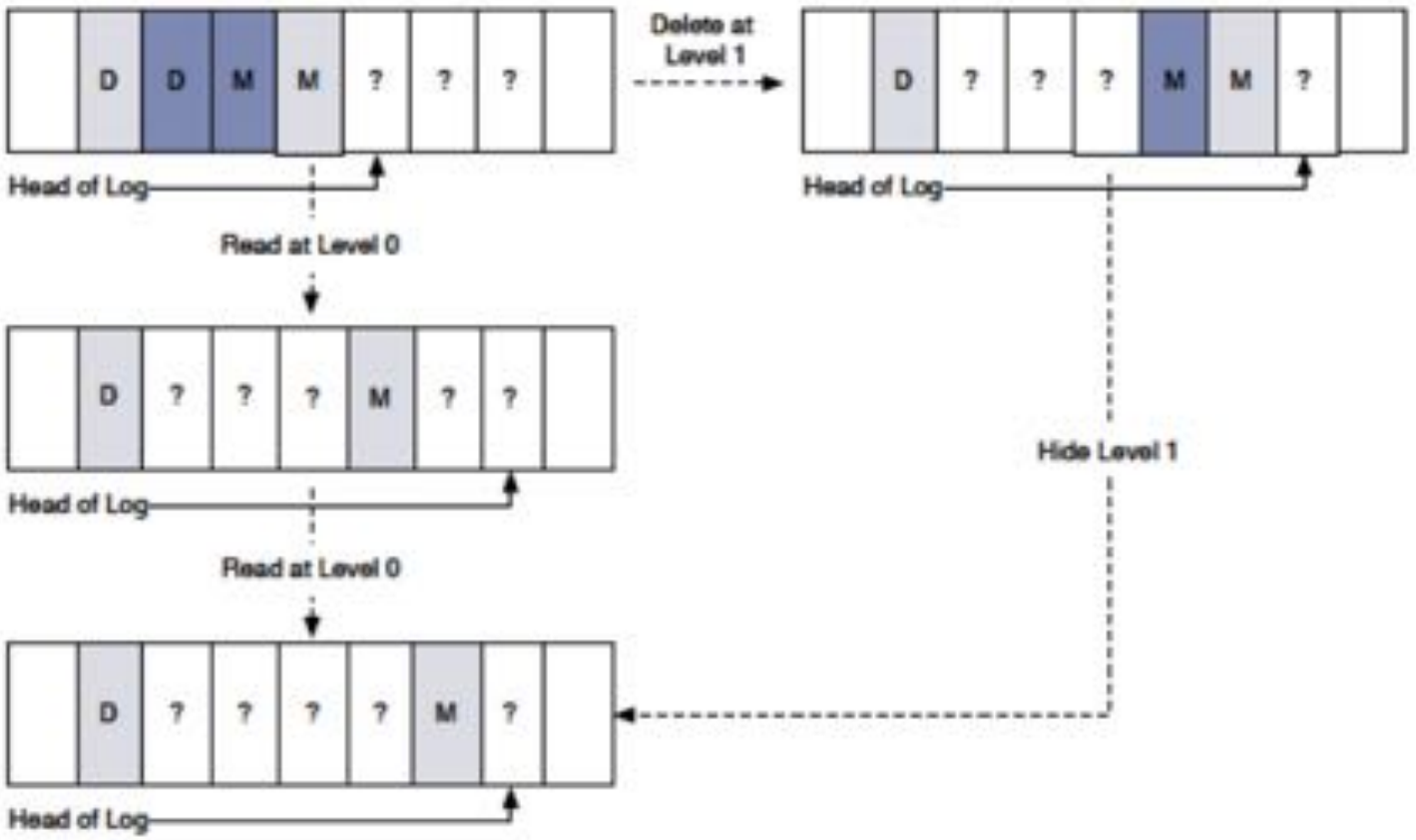
(a) Reading a block.

Security Analysis



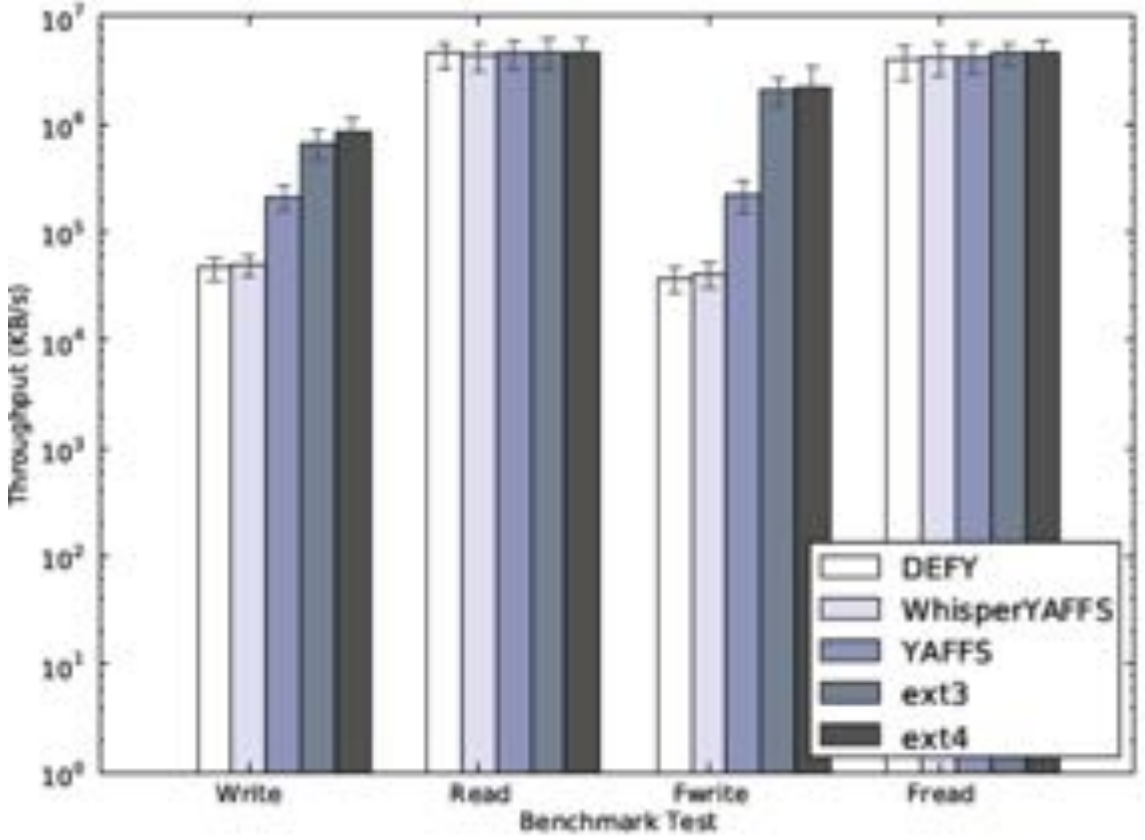
(b) Writing a new block.

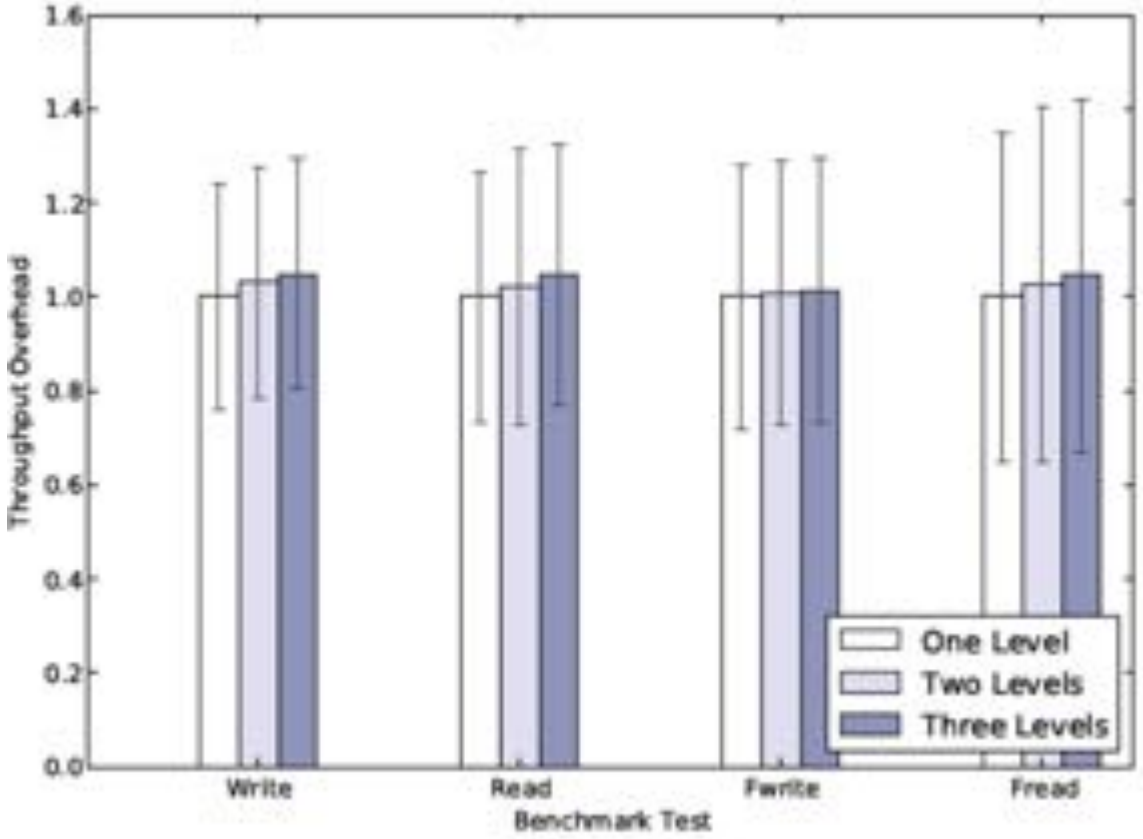
Security Analysis



(c) Deleting a block.

Overhead


Throughput (KB/s)
Write
Read
Fwrite
Fread
Benchmark Test
DEFY
WhisperYAFFS
YAFFS
ext3
ext4


Throughput Overhead
Write
Read
Fwrite
Fread
Benchmark Test
One Level
Two Levels
Three Levels

Questions ?