DISKSHIELD: A Data Tamper-Resistant Storage for Intel SGX

Jinwoo Ahn†, Junghee Lee‡, Yungwoo Ko†, Donghyun Min†,
Jihyun Park†, Sungyong Park†, Youngjae Kim†

†Sogang University, Republic of Korea,
‡Korea University, Republic of Korea

SOGANG UNIVERSITY

KOREA UNIVERSITY

AsiaCCS 2020

Motivation: The dangers of ransomware

Motivation: Two characteristics of powerful ransomware

1. Ring-0 level rootkit malware

- Disabling the system (OS) using the latest exploits.

2. Backup data attack

- Deleting all local or remote backup files of infected computer.

Motivation: Two characteristics of powerful ransomware

1. Ring-0 level rootkit malware

- Disabling the system (OS) using the latest exploits.

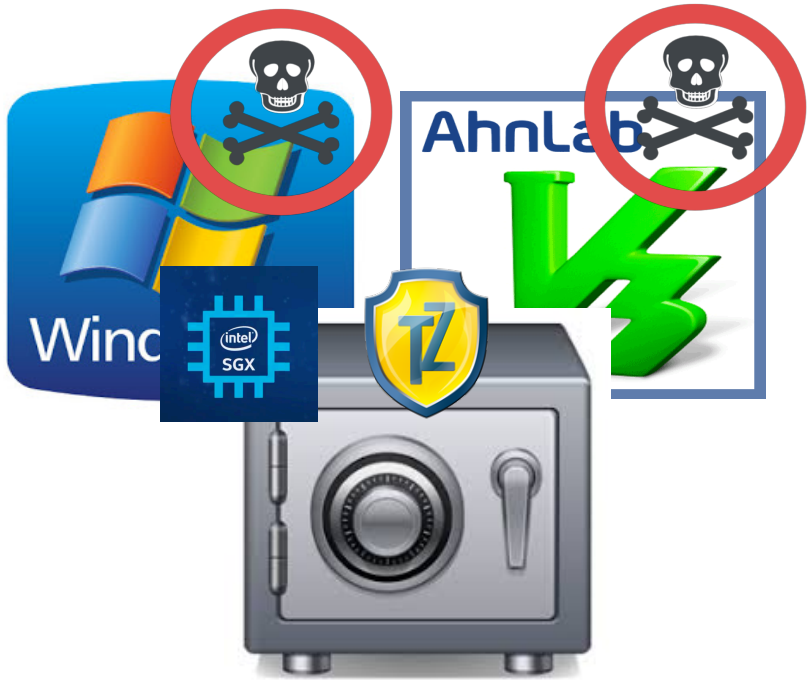
Defense against data tampering attack:
Isolation from OS + Safe Disk Partition from Malware

- Deleting all local or remote backup files of infected computer.

Opportunity: TEE and Storage devices

Trusted Execution Environment(TEE)

TEE provides code and data areas isolated from the OS.

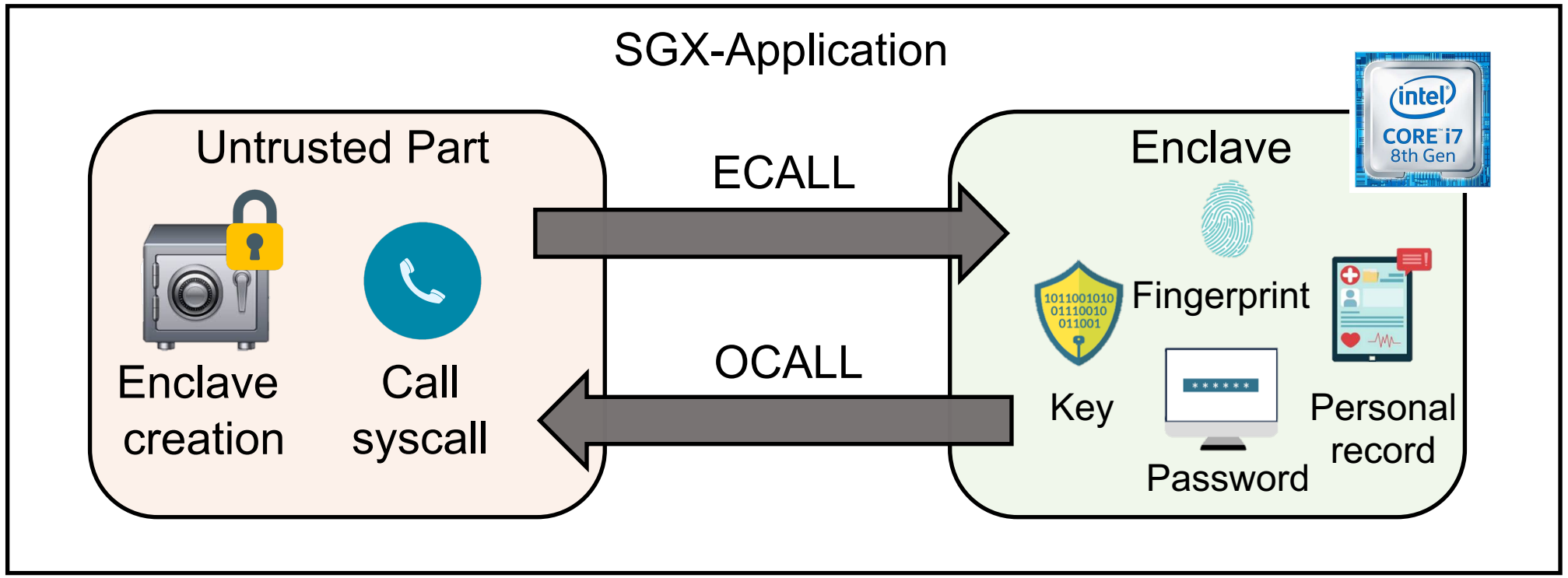


Defense on storage devices

Storage is the last barrier to storing data

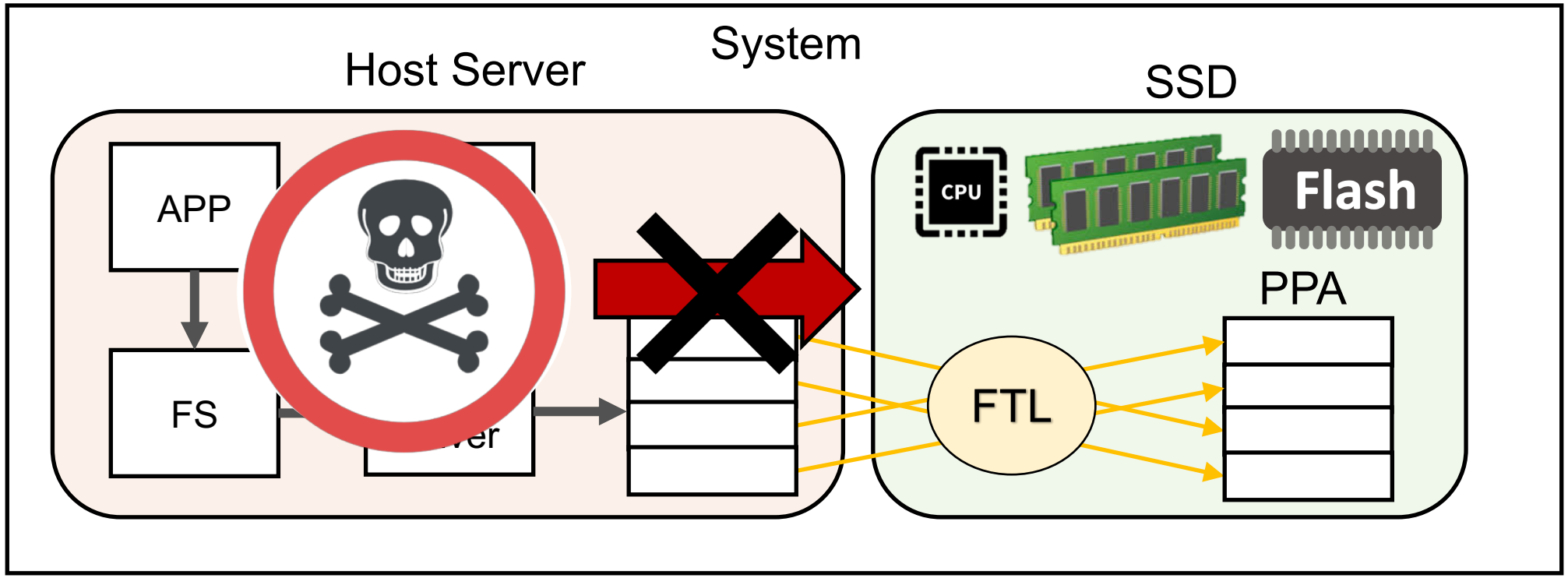
Background: Intel SGX

- Intel SGX guarantees the **confidentiality** and **integrity** of applications even if system components such as OS are damaged.



Background: Solid State Drive

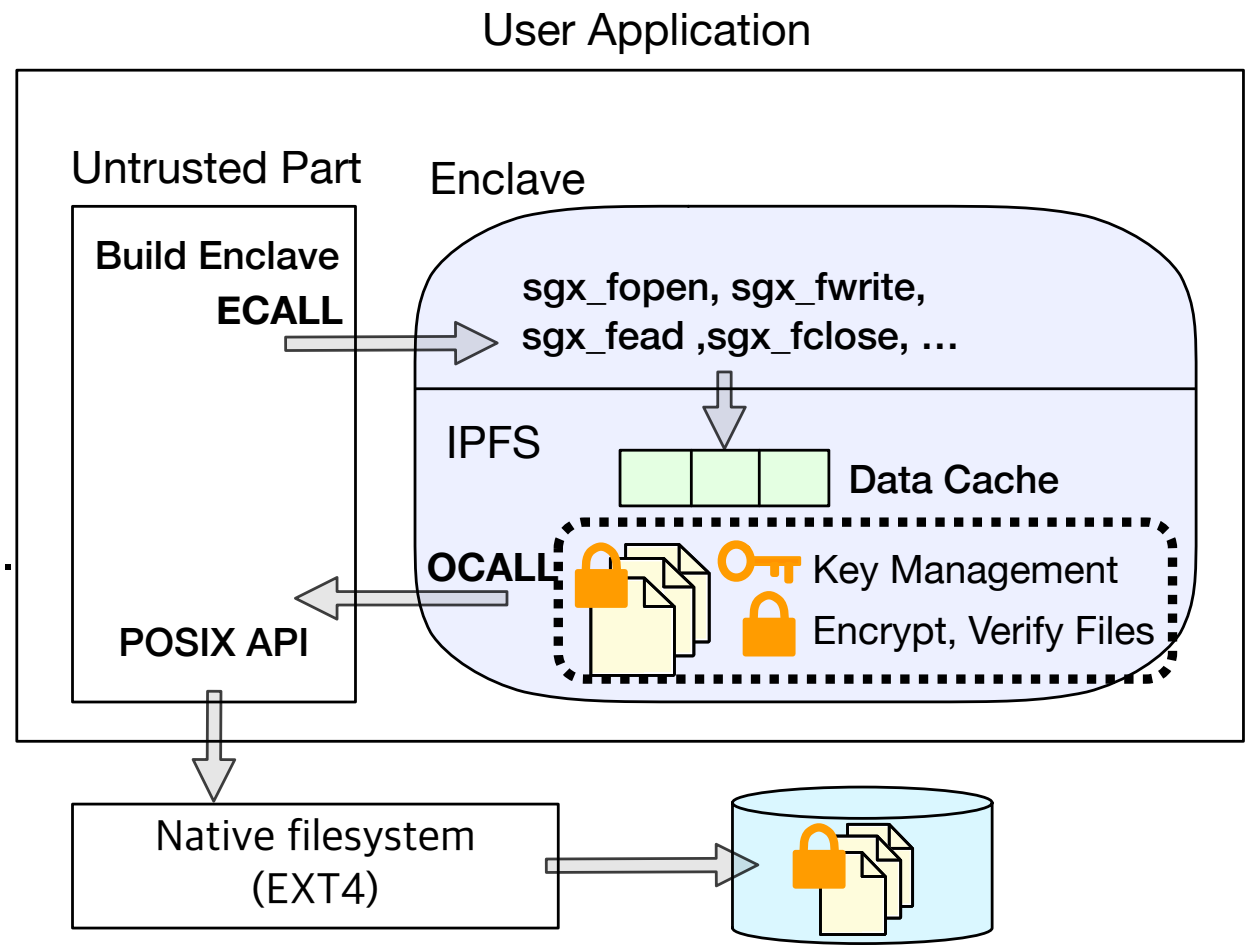
1. In-device computation capability
2. Isolated space from host server



Related work: Intel Protected File System(IPFS)

1. TEE-based solution: IPFS
   - IPFS guarantees the confidentiality and integrity of files created by SGX application.
   - IPFS is a user-level file system dependent on native filesystem(EXT4).

- **WRITE : Encrypt & Sign Data**
- **READ : Decrypt & Verify Data**

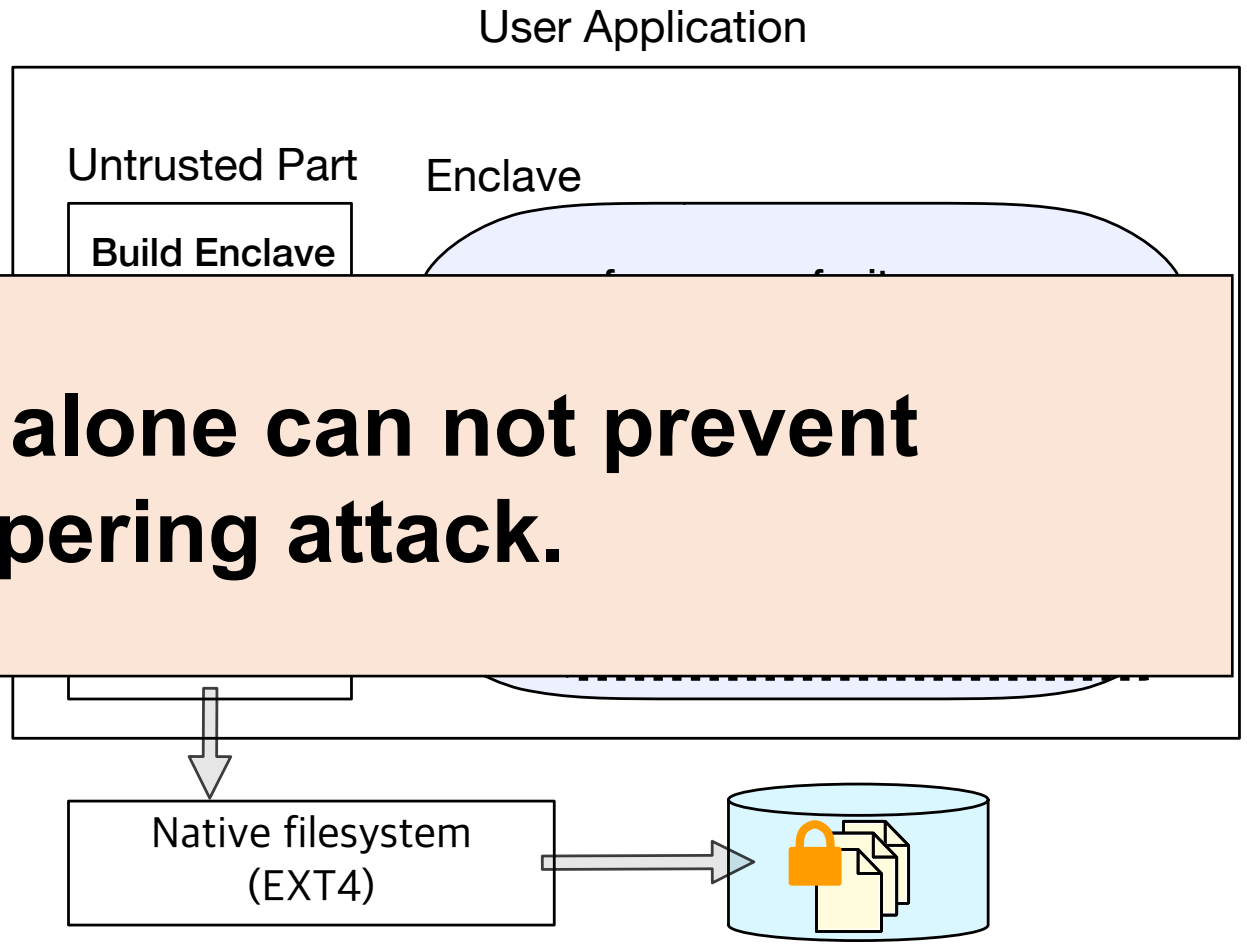


Related work: Intel Protected File System(IPFS)

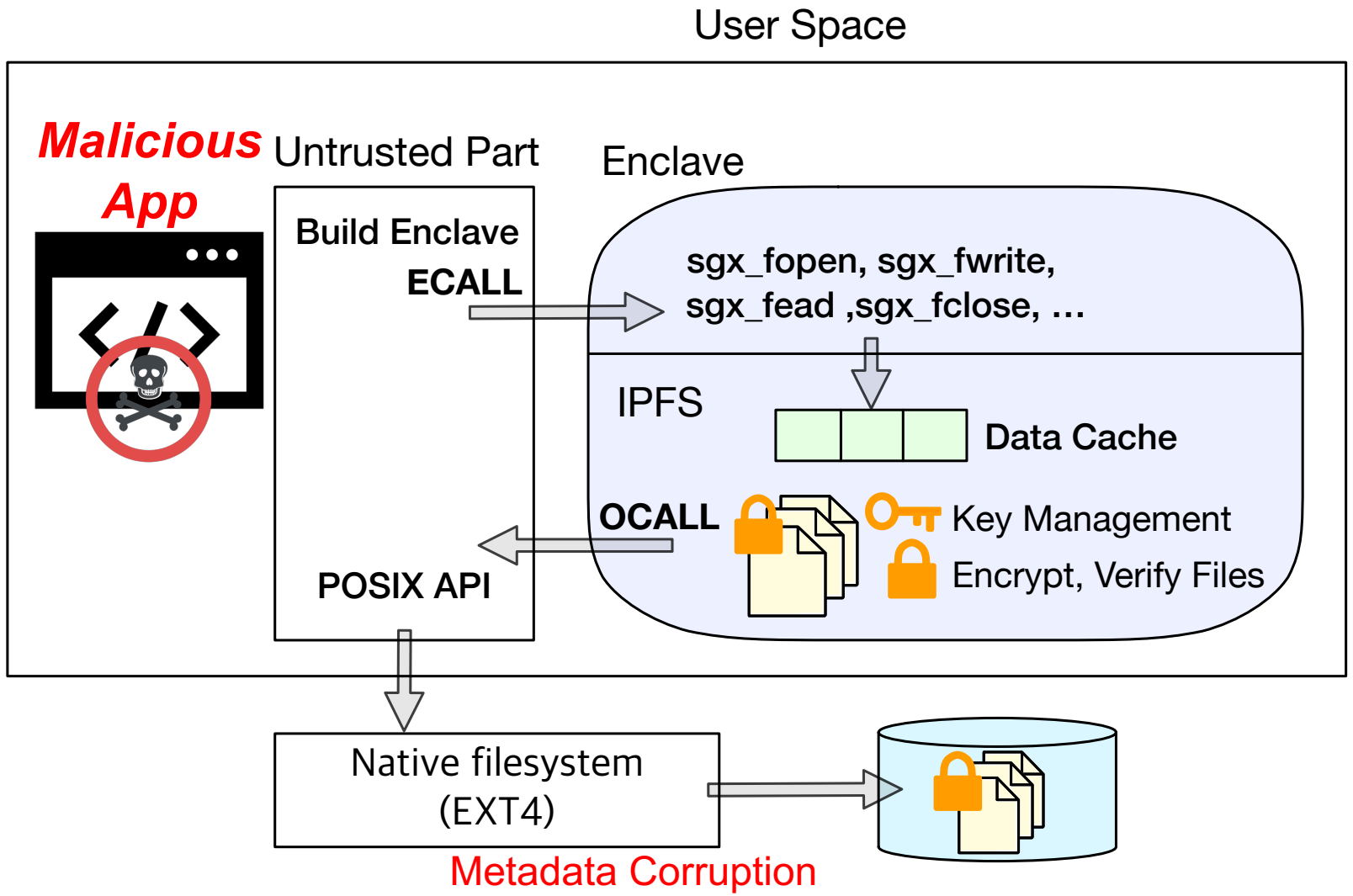
1. TEE-based solution: IPFS
   - IPFS guarantees the confidentiality and integrity of files created by SGX

Read verification alone can not prevent data tampering attack.

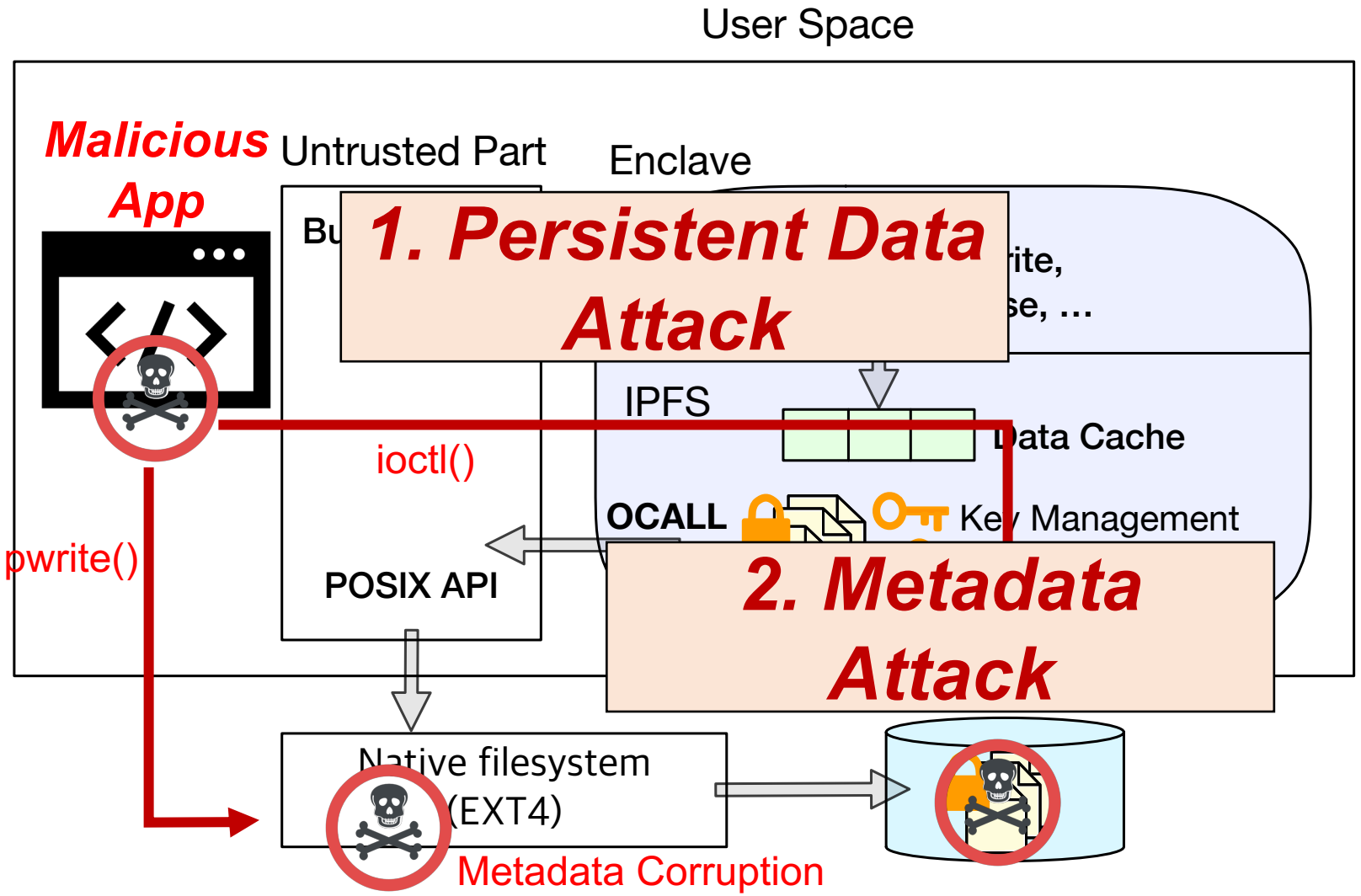
- **WRITE : Encrypt & Sign Data**
- **READ : Decrypt & Verify Data**



Related work: limitation of IPFS

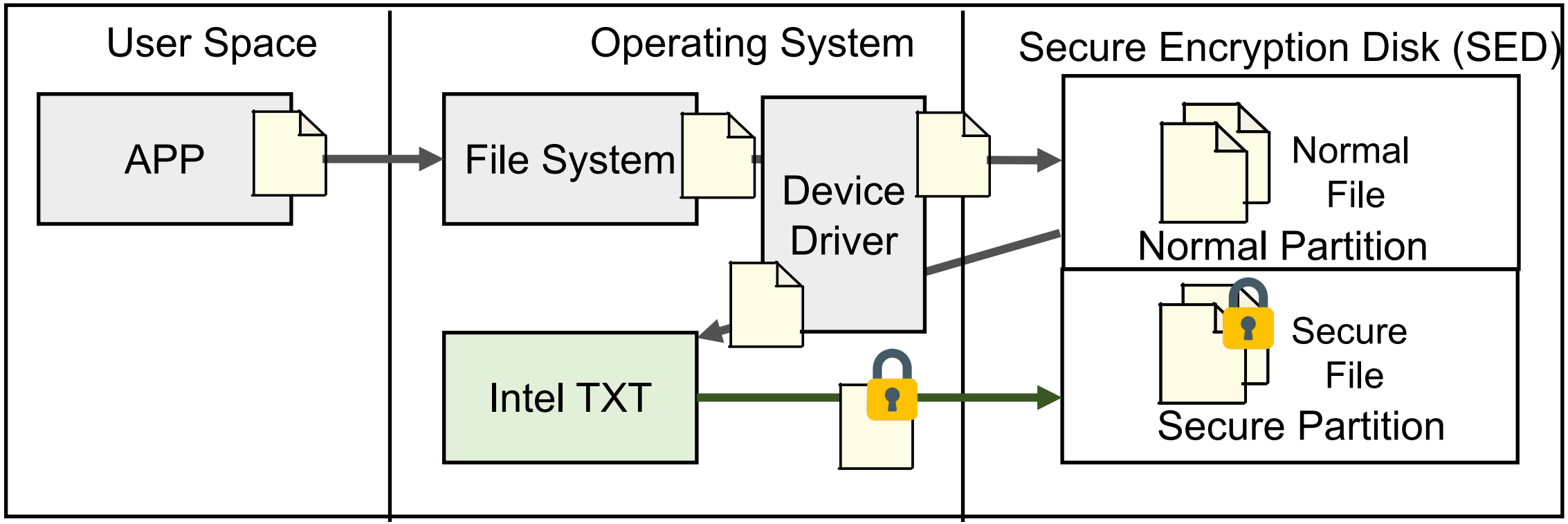


Related work: limitation of IPFS



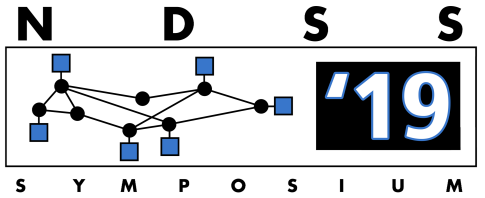
Related work: Inuksuk

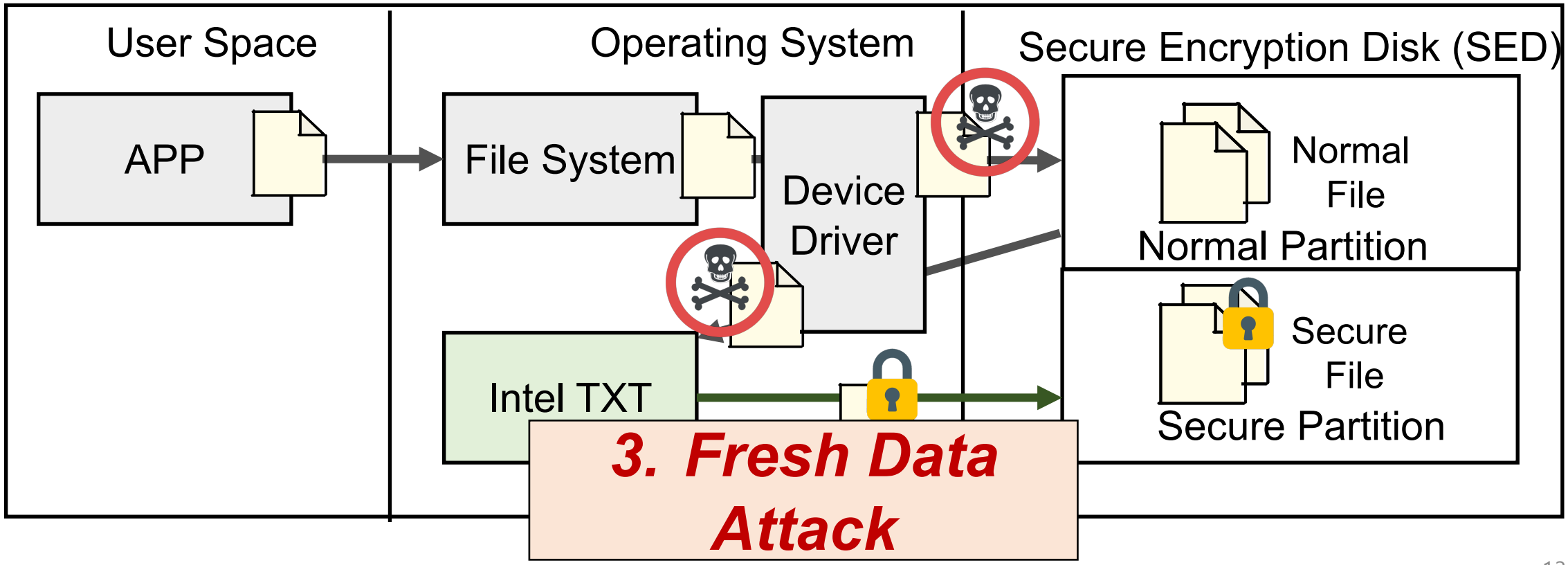
2. TEE + Disk based solution: 2. Inuksuk



Related work: Inuksuk

2. TEE + Disk based solution: 2. Inuksuk

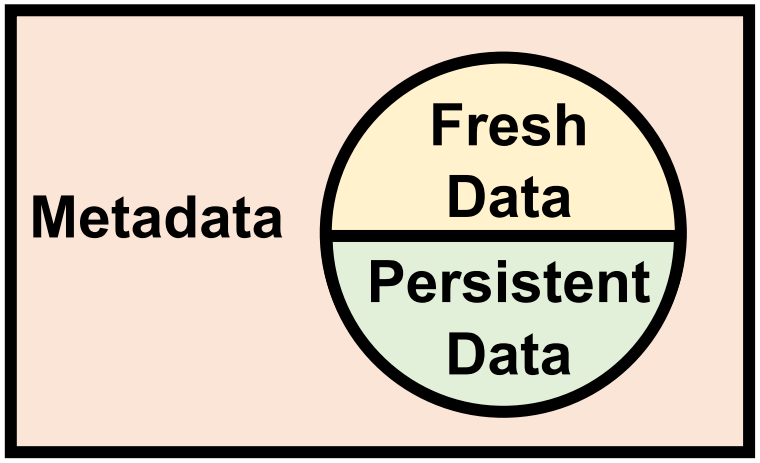




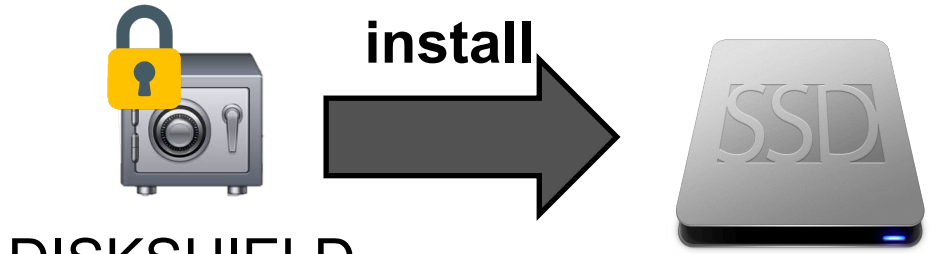
System proposal: DISKSHIELD

- Robust data-tampering resistant storage system from privileged malware.
  - Protect all kinds of data: persistent data, fresh data, metadata.
- It runs without additional disks in local environment.
  - No additional cost is required for purchasing external disk.

File attack surface:



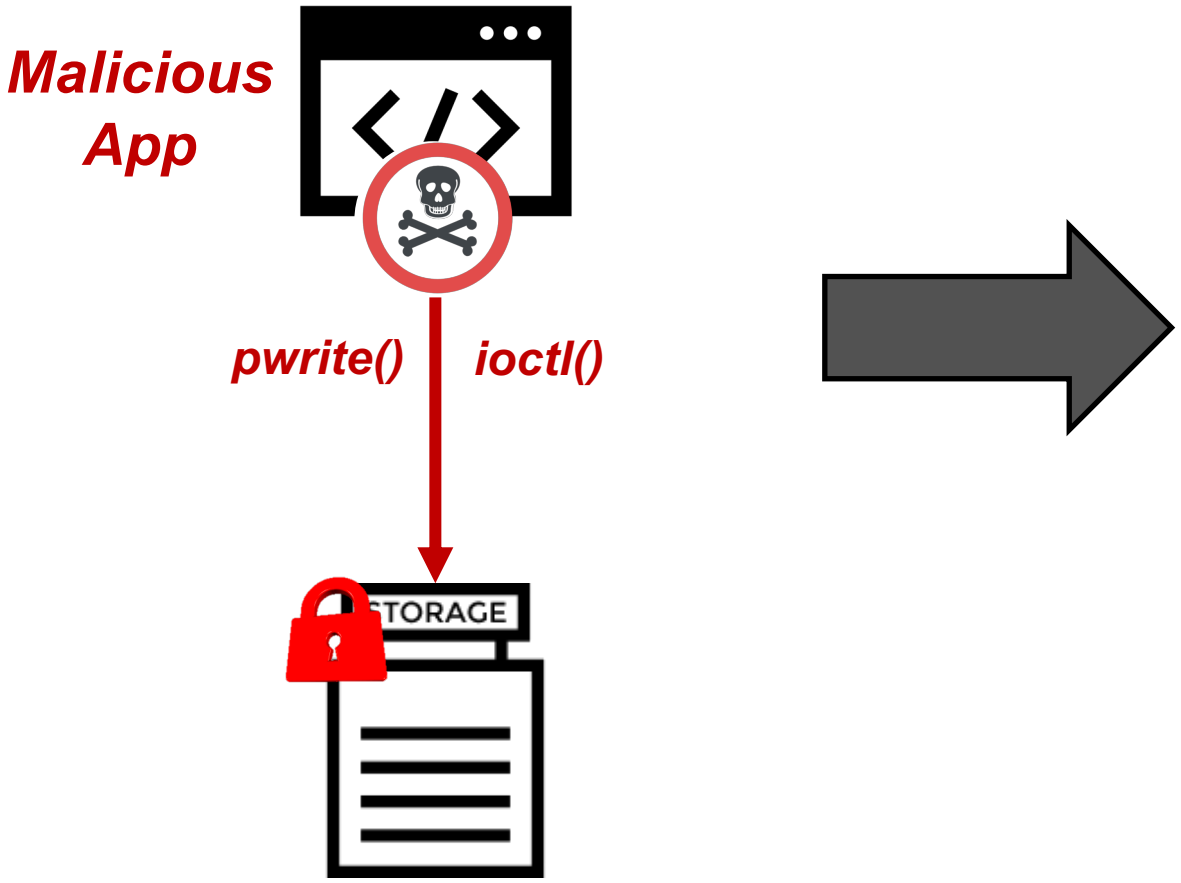
Firmware update to existing SSD!



DISKSHIELD

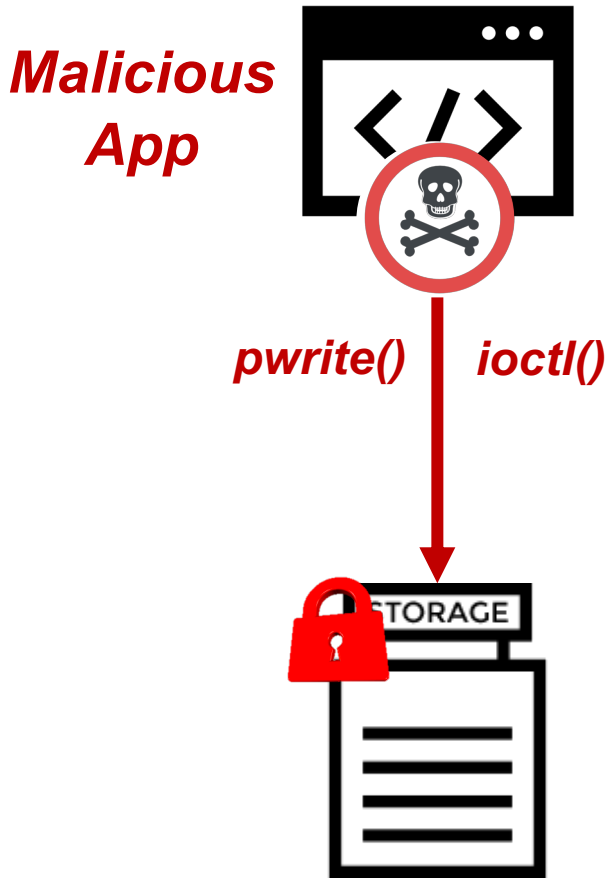
System proposal: Data protection from any attack surface

Persistent data attack

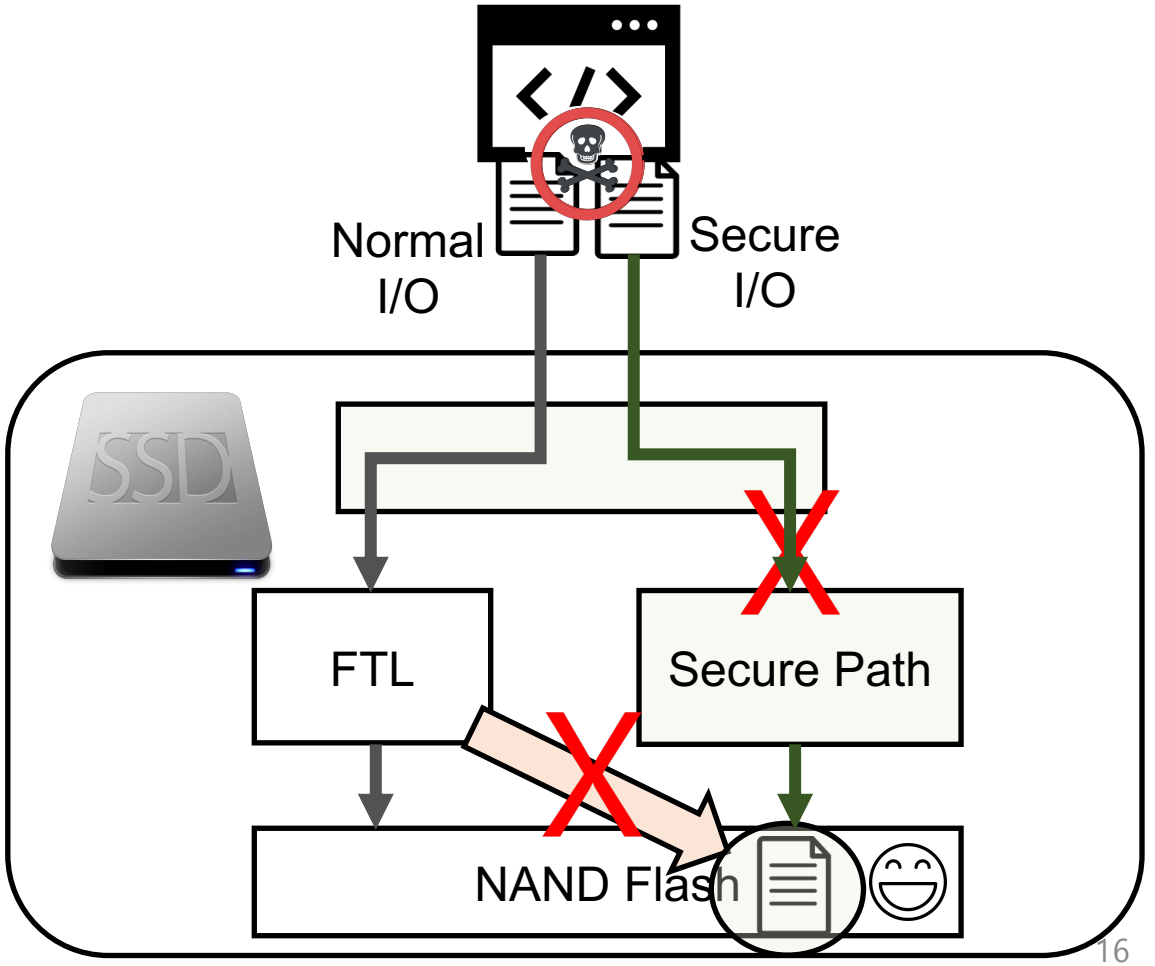


System proposal: Data protection from any attack surface

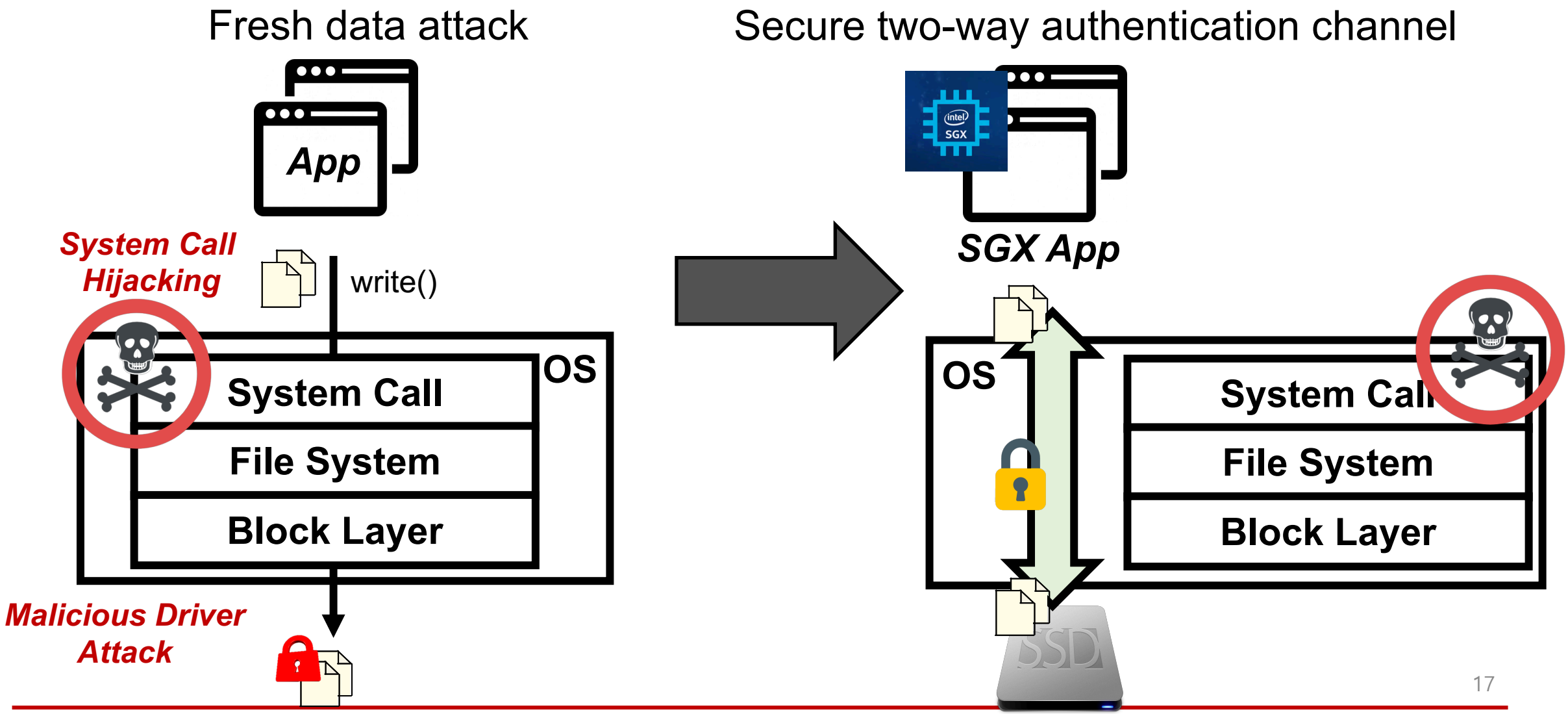
Persistent data attack



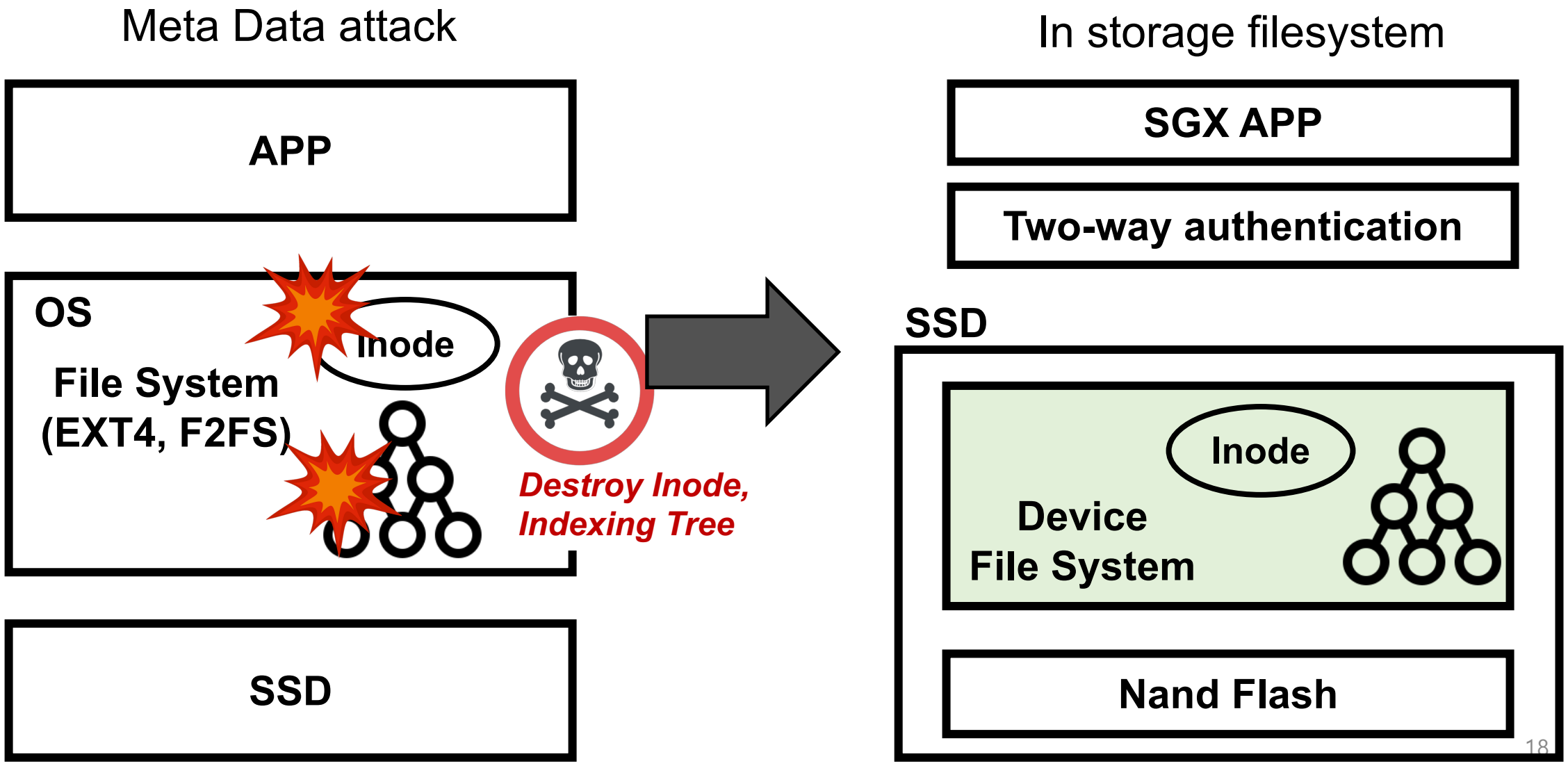
Access control in device



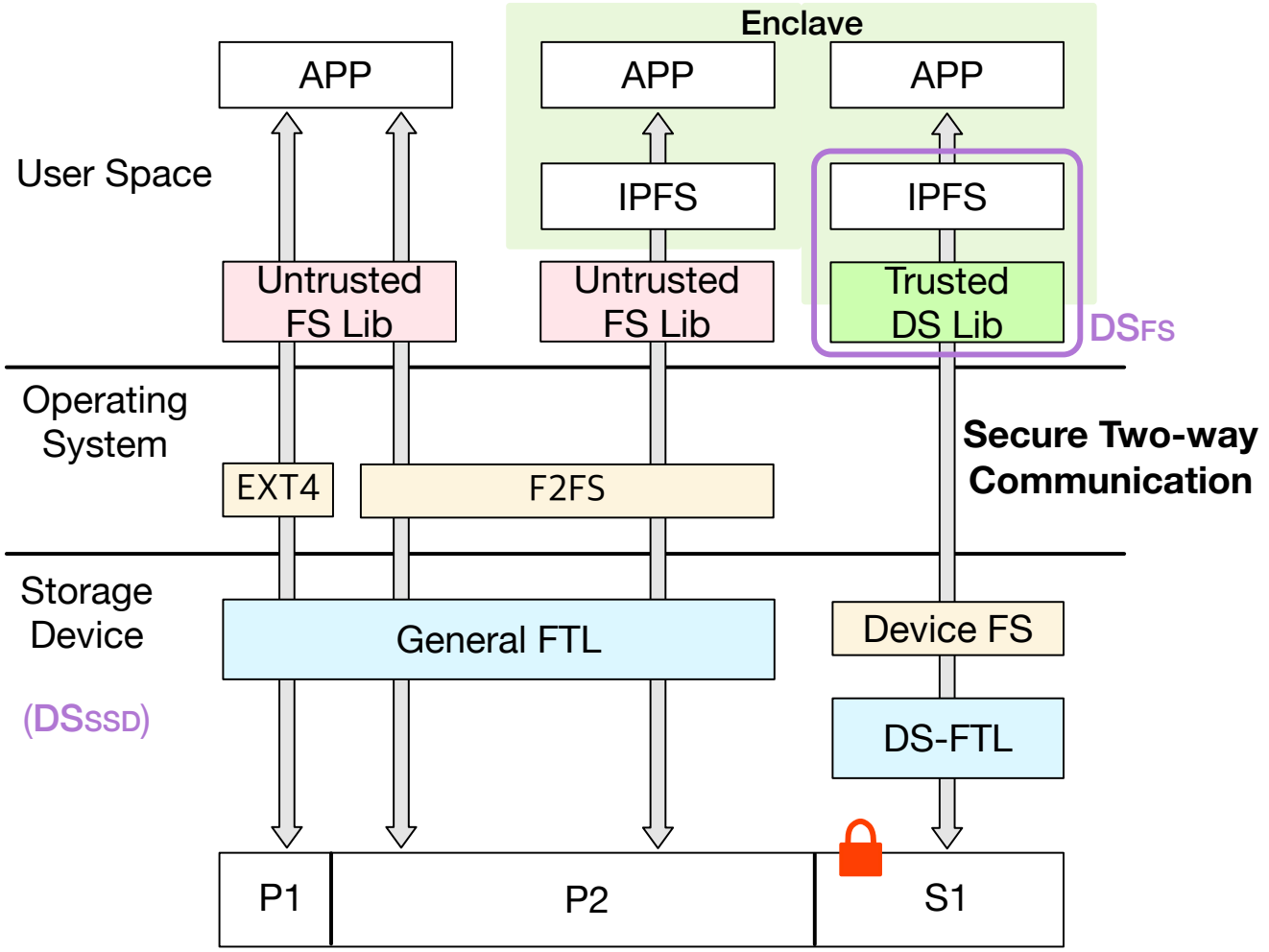
System proposal: Data protection from any attack surface



System proposal: Data protection from any attack surface



Design & Implementation: system components



DSFS :
-Extension of IPFS in SGX
-Two-way authentication module

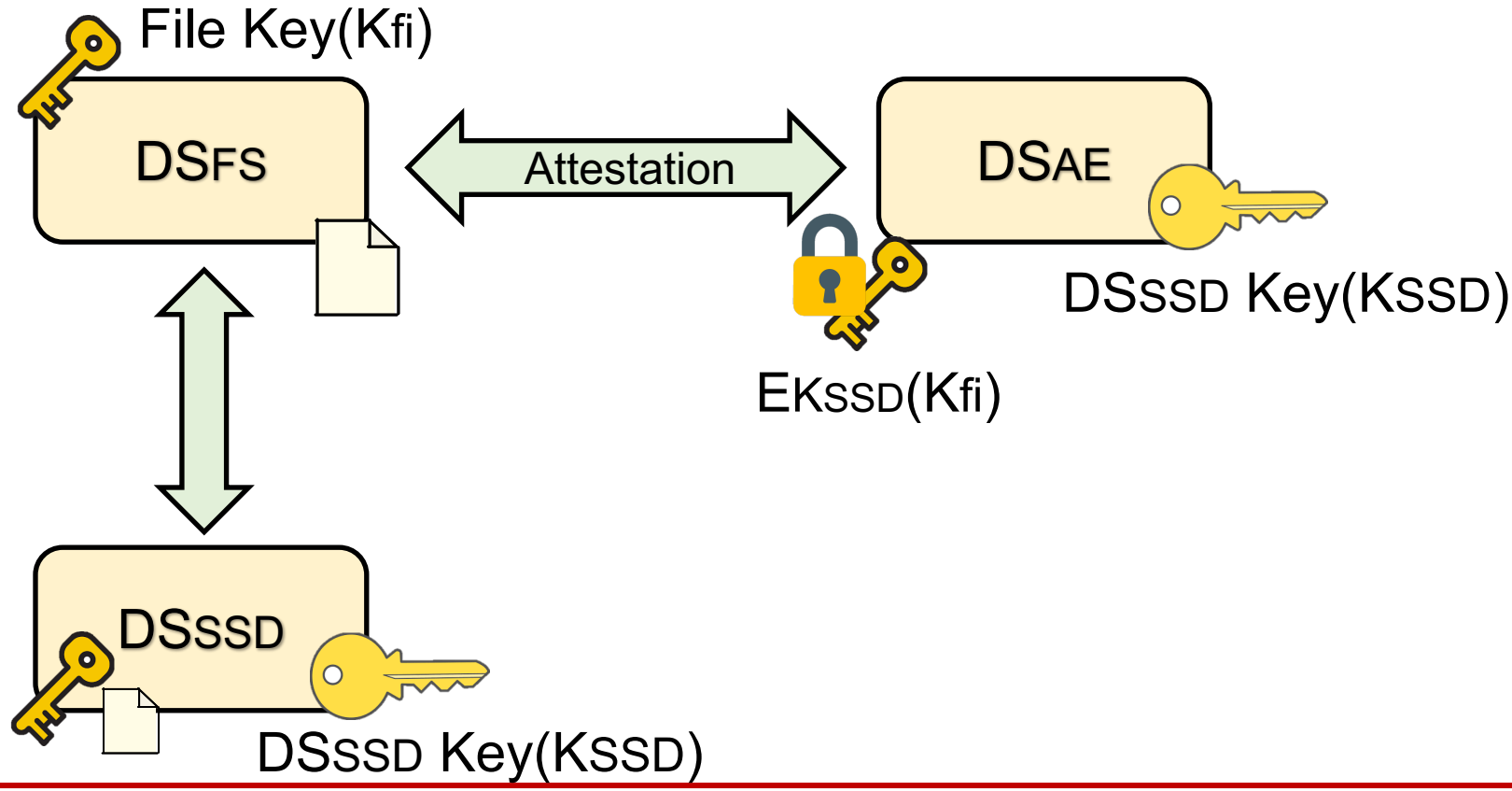
DSSSD :
-SSD Firmware implmentation
-Device filesystem
-Device level authentication system

DSAE :
-Key manager between DSFS and DSSSD

Design & Implementation: ***DSAE***

DSAE enables two-way authentication by sharing a file key between DSFS and DSSSD.

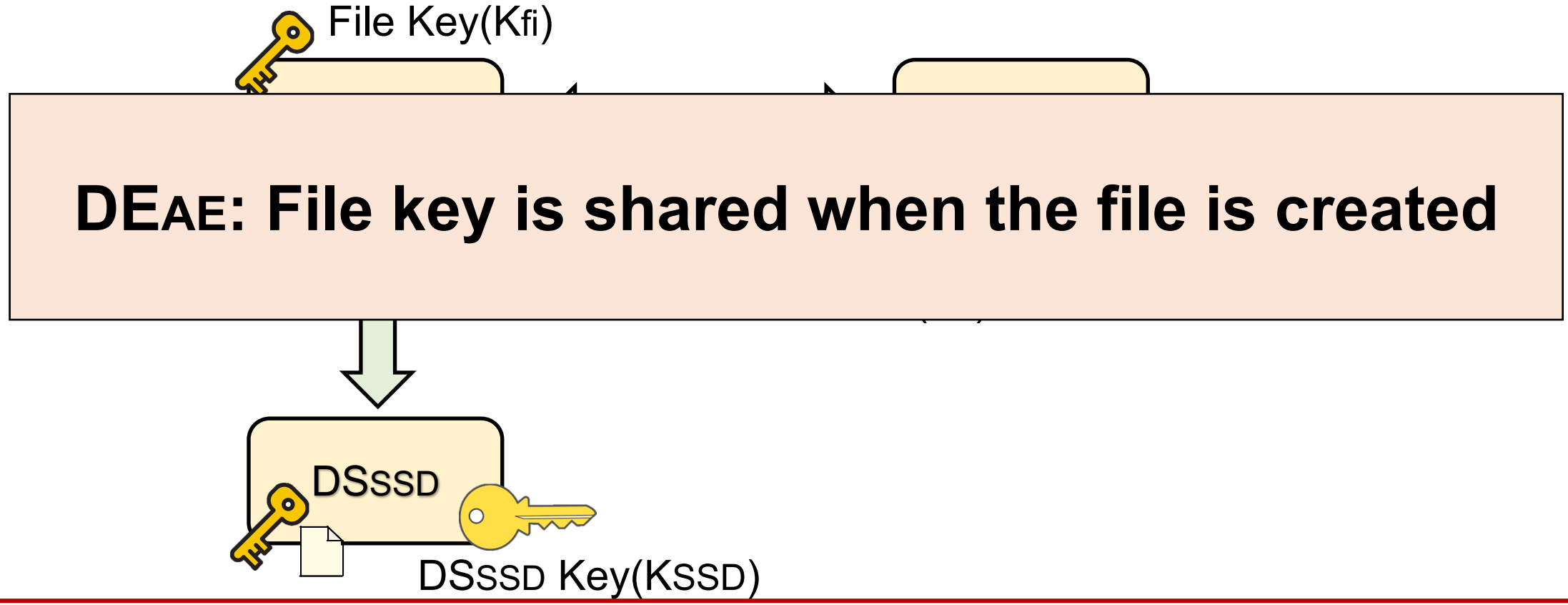
When creating a file, the key generated by DSFS is securely shared with DSSSD.



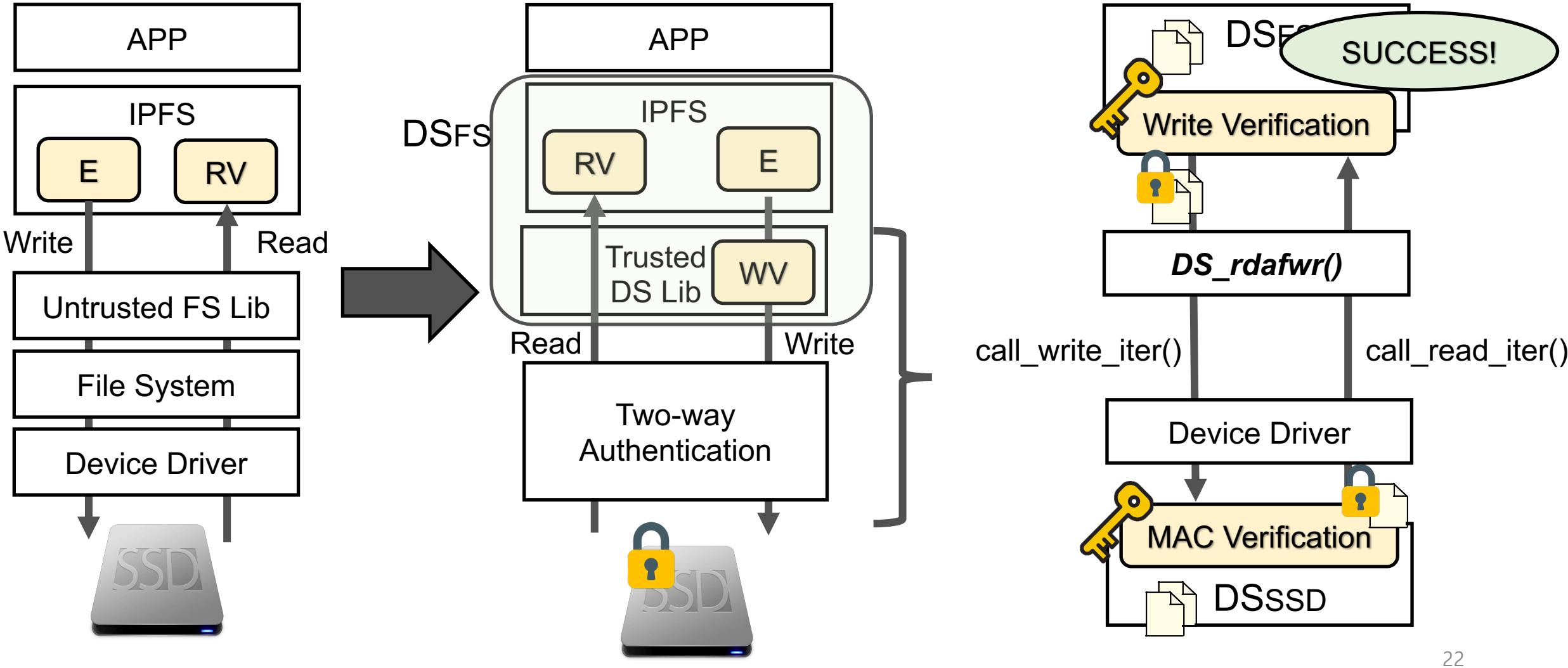
Design & Implementation: *DSAE*

DSAE enables two-way authentication by sharing a file key between DSFS and DSSSD.

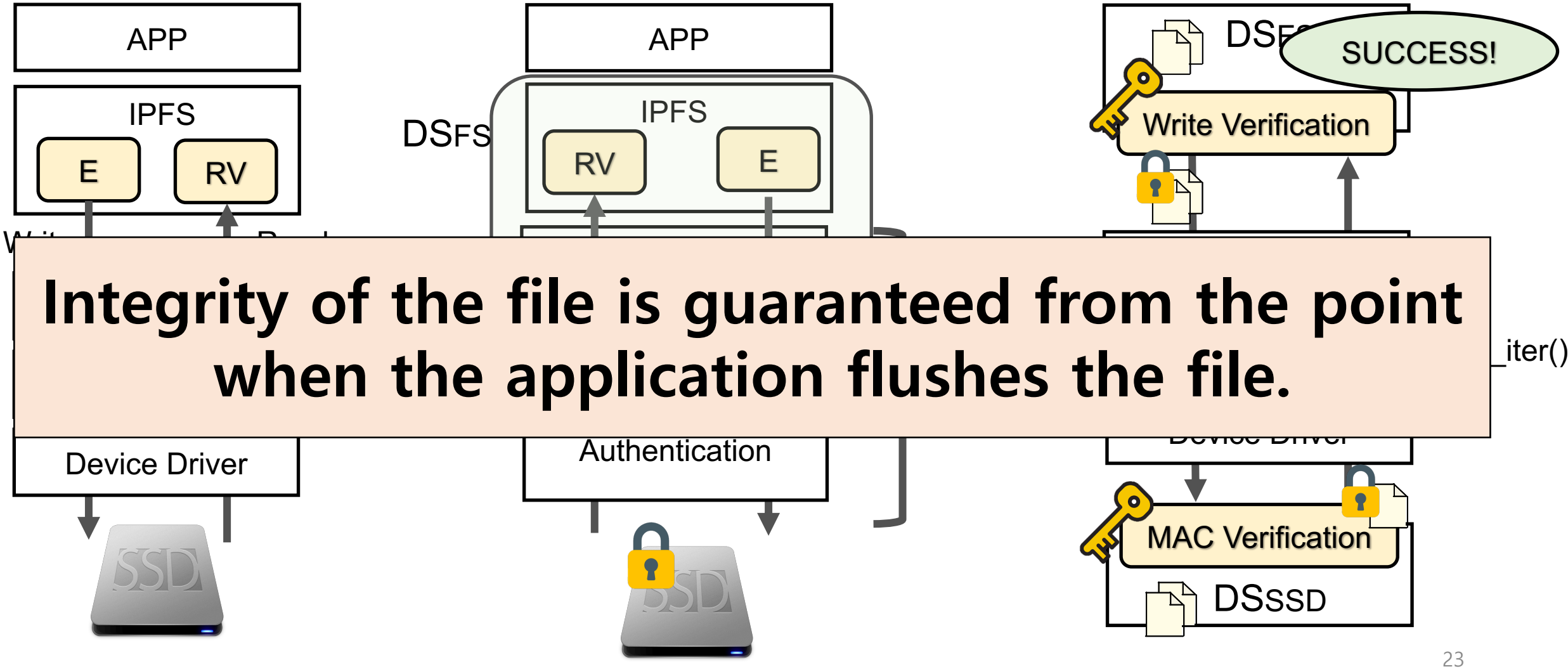
When creating a file, the key generated by DSFS is securely shared with DSSSD.



Design & Implementation: ***DSFS***

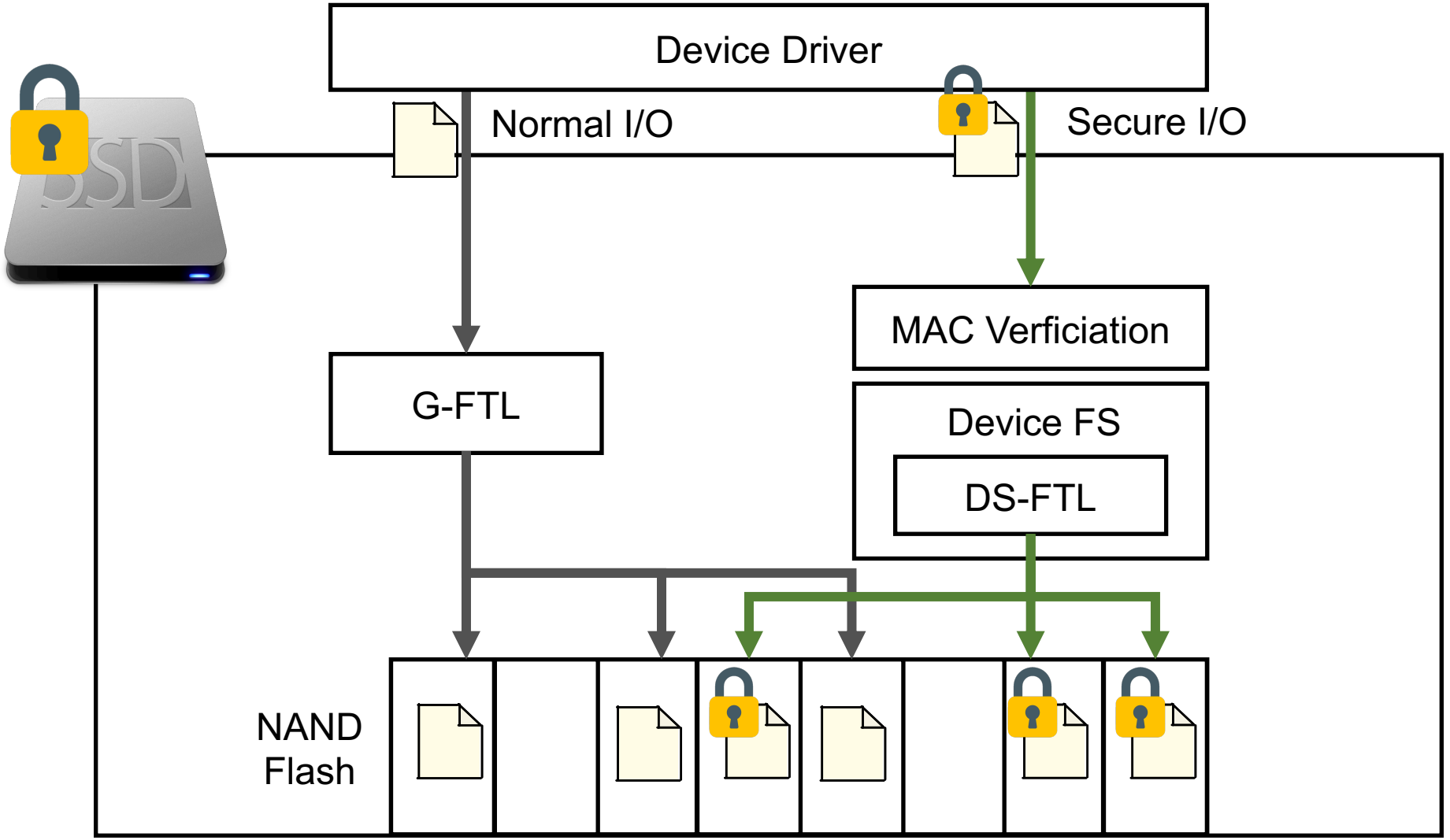


Design & Implementation: ***DSFS***

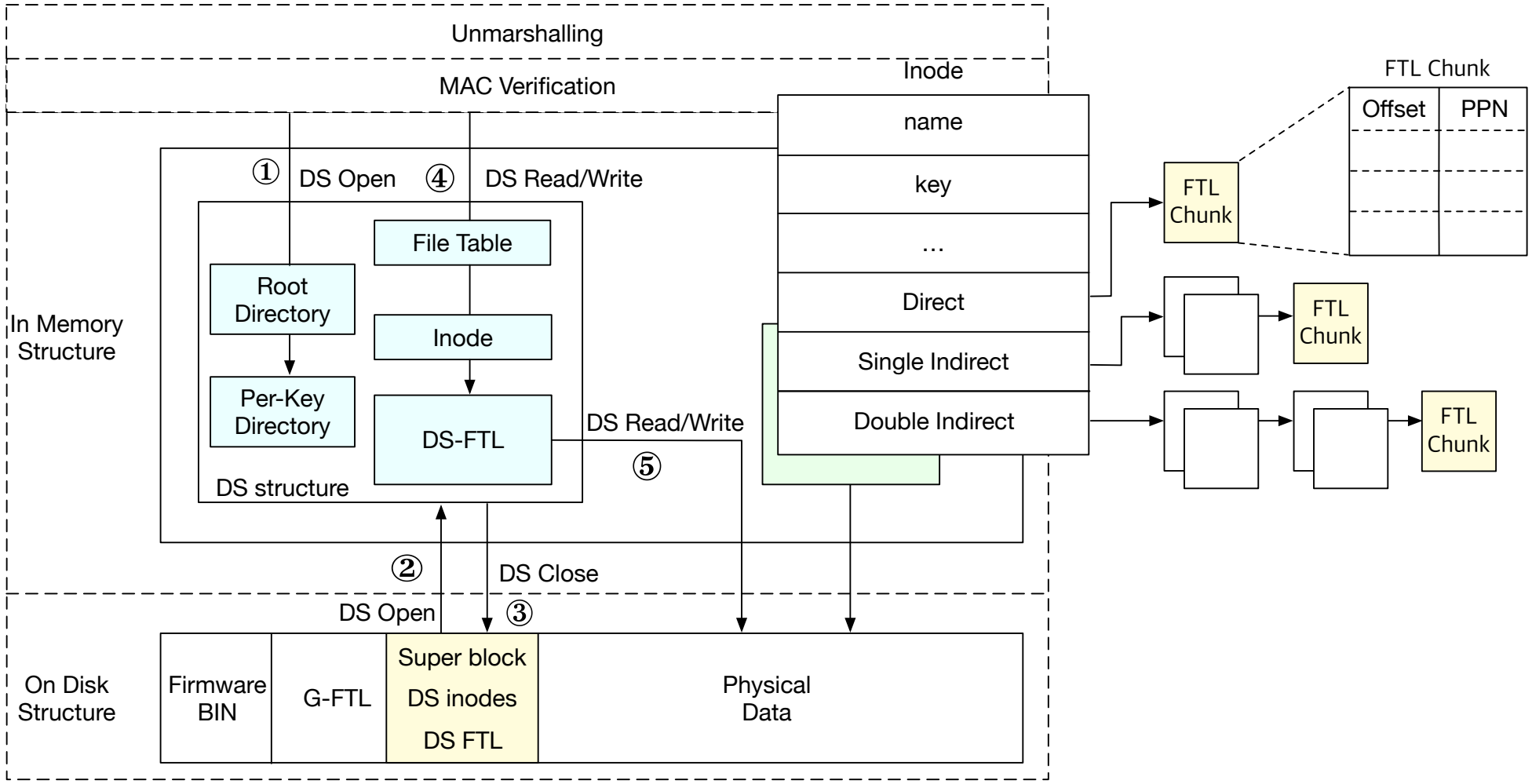


Integrity of the file is guaranteed from the point when the application flushes the file.

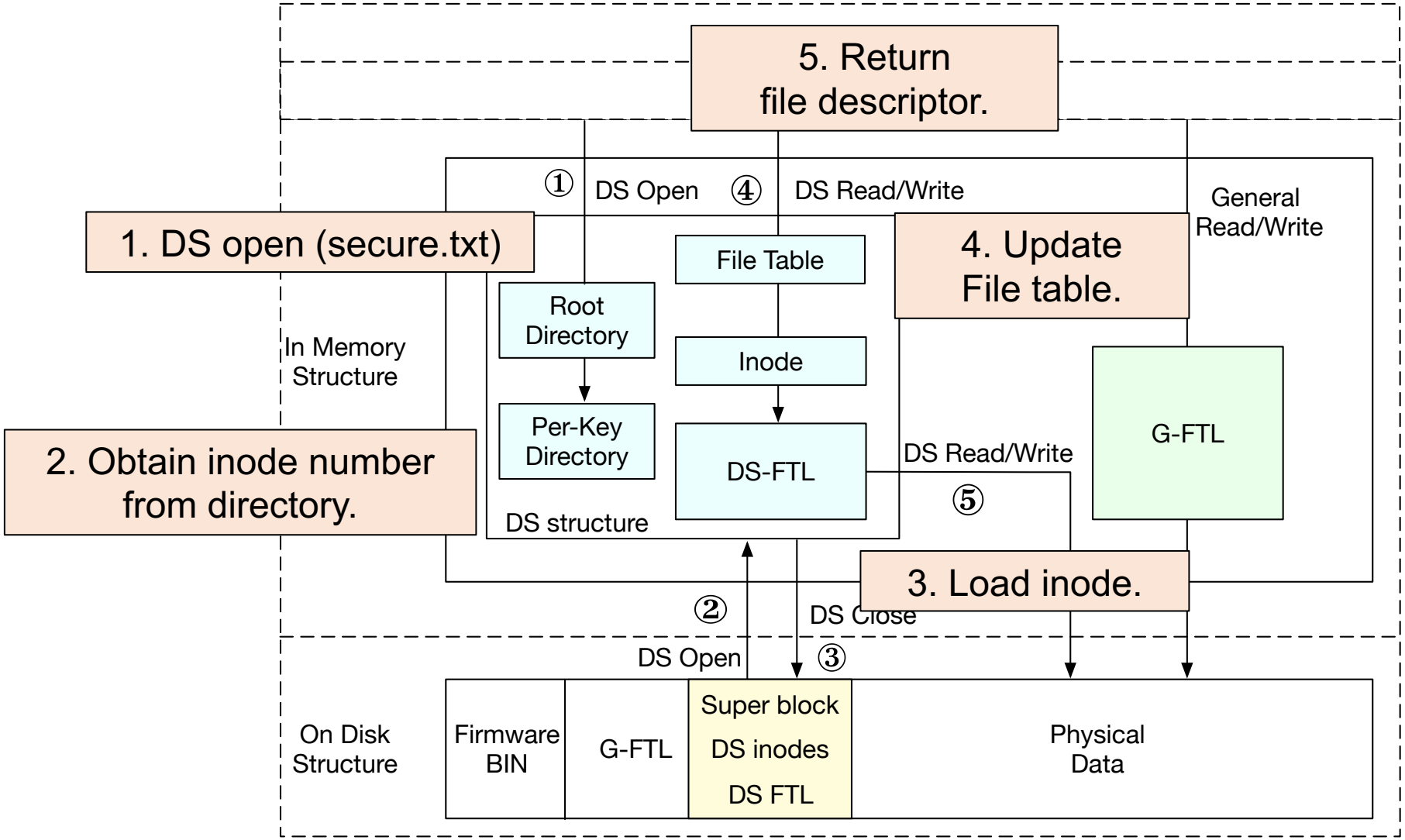
Design & Implementation: ***DSSSD***



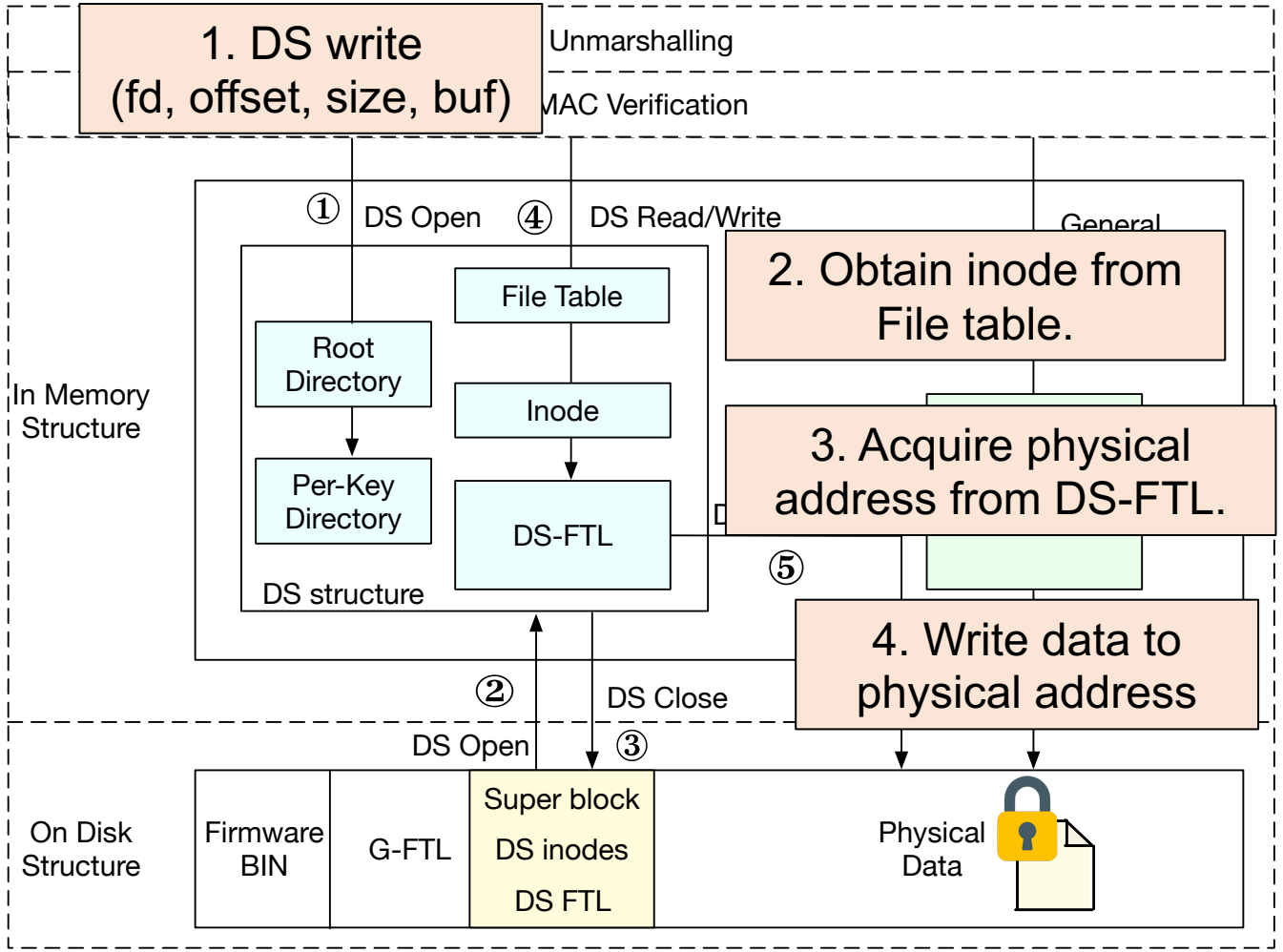
Design & Implementation: ***DSSSD***



DSSSD : secure file open flow



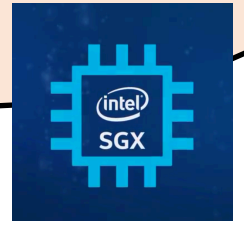
DSSSD : secure file write flow



Evaluation: Prototype implementation

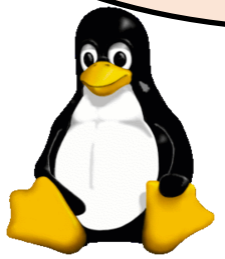
SSD: 2661 Loc
Kernel: 243 Loc
SGX SDK: 791 Loc

DSFS, DSAE

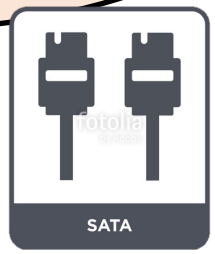


Intel SGX

Two-way Authentication Module

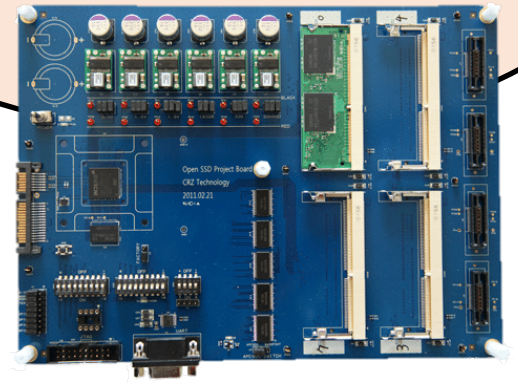


Linux 4.10.16



SATA Interface

DSSSD



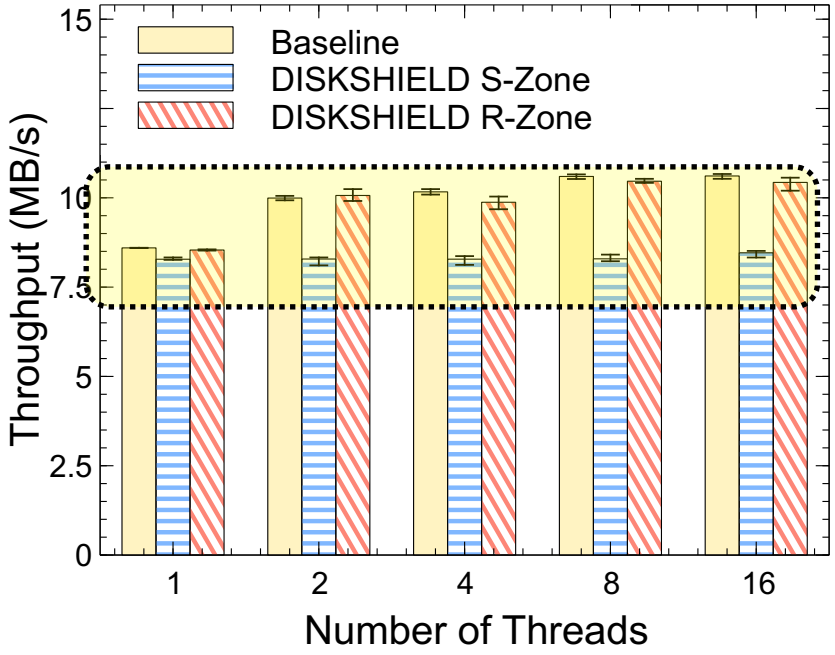
Open SSD Jasmine

Evaluation

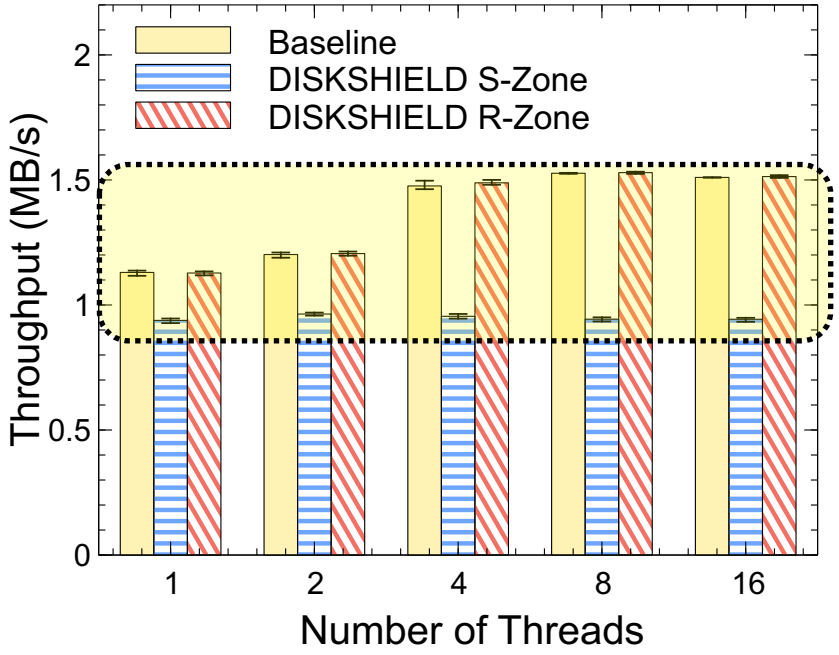
Baseline, R-zone: Normal I/O
S-zone: Secure I/O

Baseline : IPFS + EXT4 + Normal SSD
R-zone : IPFS + EXT4 + DSSSD (normal)
S-zone : DSFS + DSSSD (secure)

1. Baseline and R-zone throughput are the same
- **There is no normal I/O overhead of DSSSD.**



Big file Read

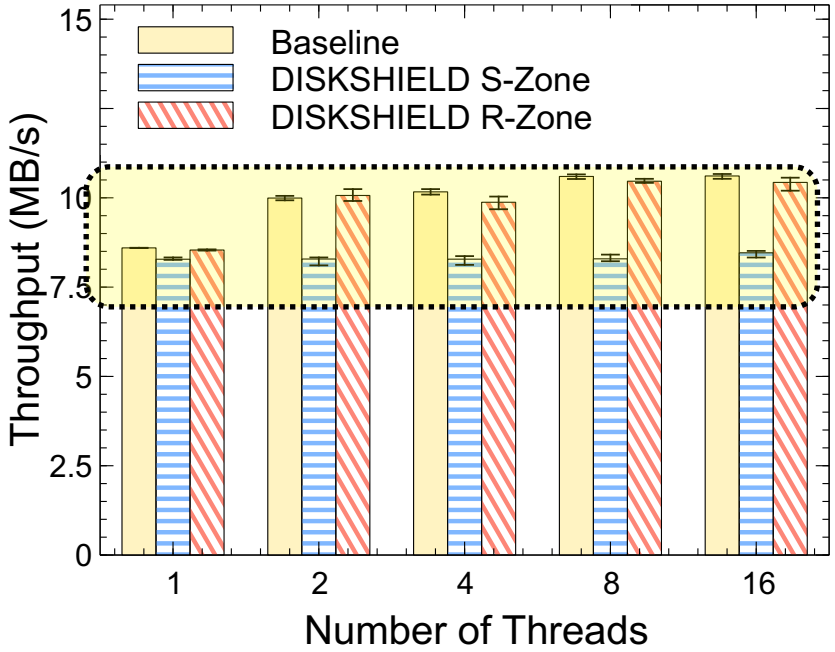


Big file Write

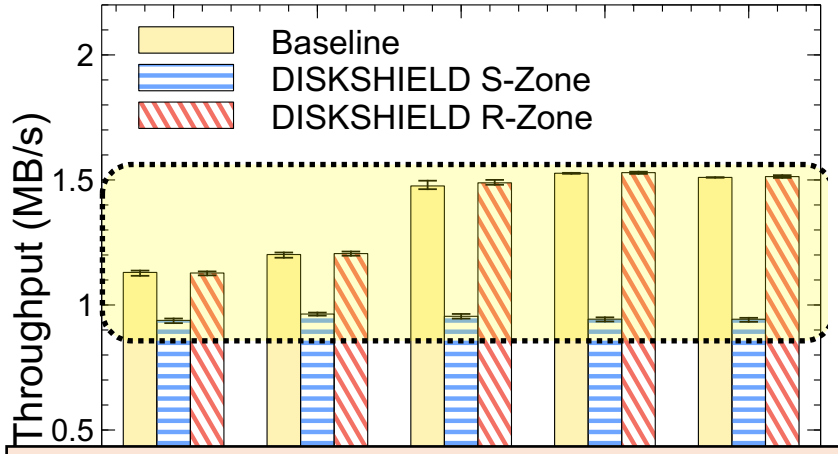
Evaluation

Baseline, R-zone: Normal I/O
S-zone: Secure I/O

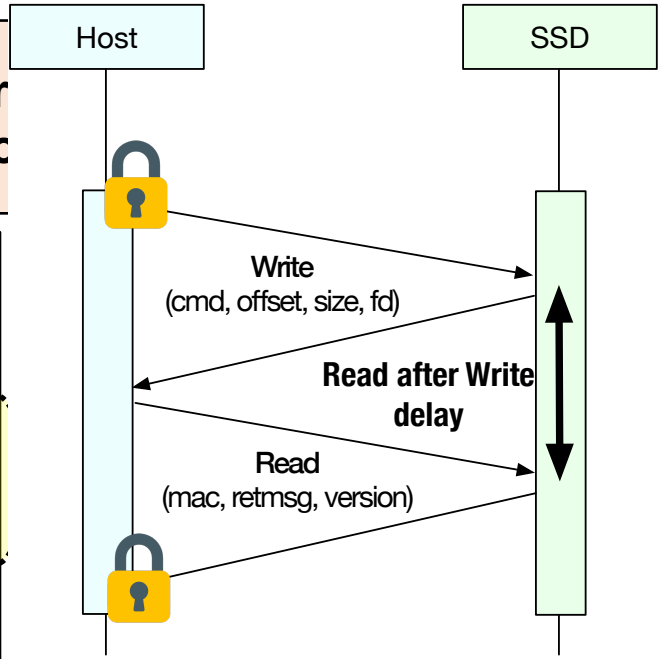
Baseline : IPFS + EXT4 + Normal SSD
R-zone : IPFS + EXT4 + DSSSD (normal)
S-zone : DSFS + DSSSD (secure)



Big file Read



1. Baseline and R-zone thr
- **There is no normal I/O c**

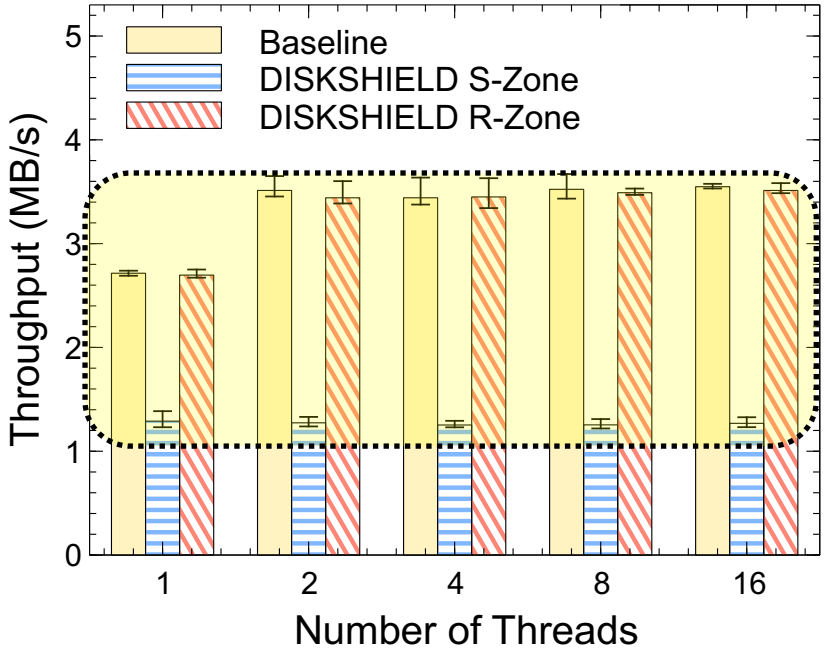


2. In S-zone, throughput was 17% lower than baseline.
- **Two-way authentication module overhead**

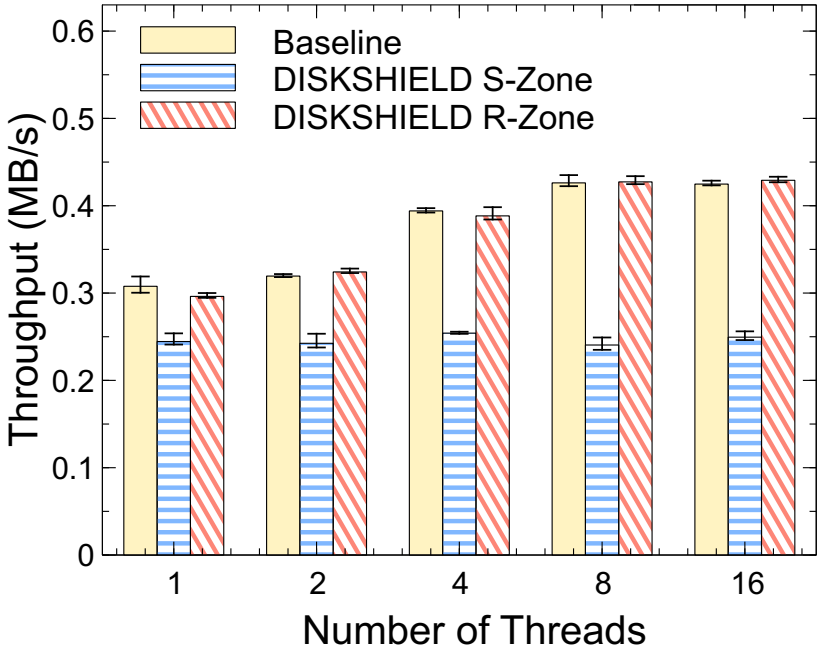
3. S-zone is not scalable even if the number of threads increases.
- **Corase-grained lock of two-way authentication module**

Evaluation

1. S-Zone's read throughput drops by more than 50%.
- Overhead to load/store multiple inodes in DSSSD
  - DSSSD loads only one inode. -> No cache effect!
  - It should prefetch multiple inodes at once like EXT4 filesystem.



Small file Read



Small file Write

Conclusion

- DISKSHIELD guarantees file integrity from privileged data tampering attacks.
  - Defense of all attack surfaces: Persistent data attack, Fresh data attack, metadata attack
- DISKSHILED runs in local environment without additional disk.
  - It can be implemented only by firmware update to existing SSD without hardware cost.

DISKSHIELD: A Data Tamper-Resistant Storage for Intel SGX

Jinwoo Ahn

jinu37@sogang.ac.kr