FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware

Jian Huang
Georgia Institute of Technology
Atlanta, GA
jian.huang@gatech.edu

Jun Xu
Pennsylvania State University
University Park, PA
jxx13@ist.psu.edu

Xinyu Xing
Pennsylvania State University
University Park, PA
xxing@ist.psu.edu

Peng Liu
Pennsylvania State University
University Park, PA
pliu@ist.psu.edu

Moinuddin K. Qureshi
Georgia Institute of Technology
Atlanta, GA
moin@ece.gatech.edu

ACM SIGSAC Conference on Computer and Communications Security
2017

Presented by Lara Lazier

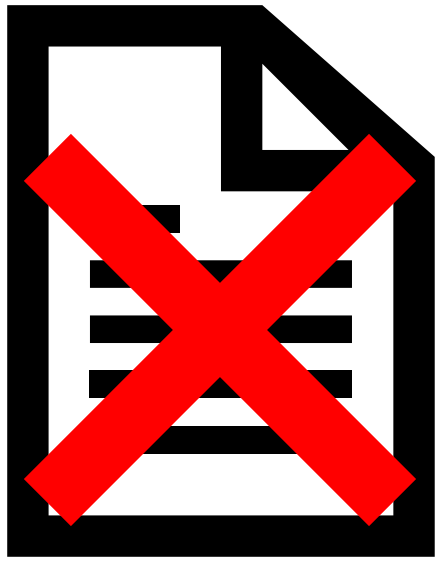
Idea

A Firmware solution FlashGuard:

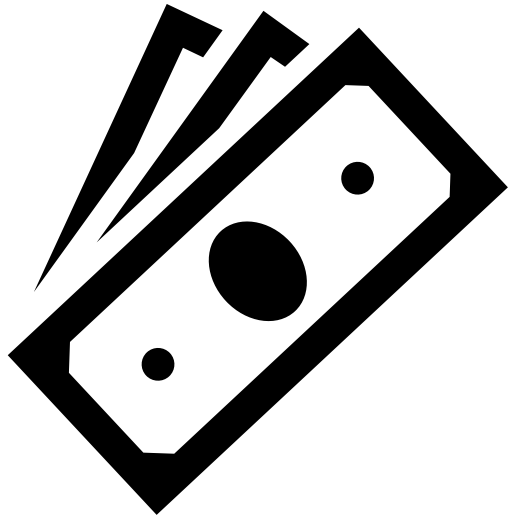
- Defends data stored on SSD from Encryption Ransomware
- Leverages intrinsic Flash Properties
- Works also when Ransomware has kernel privileges

What is a Ransomware?

Files are encrypted



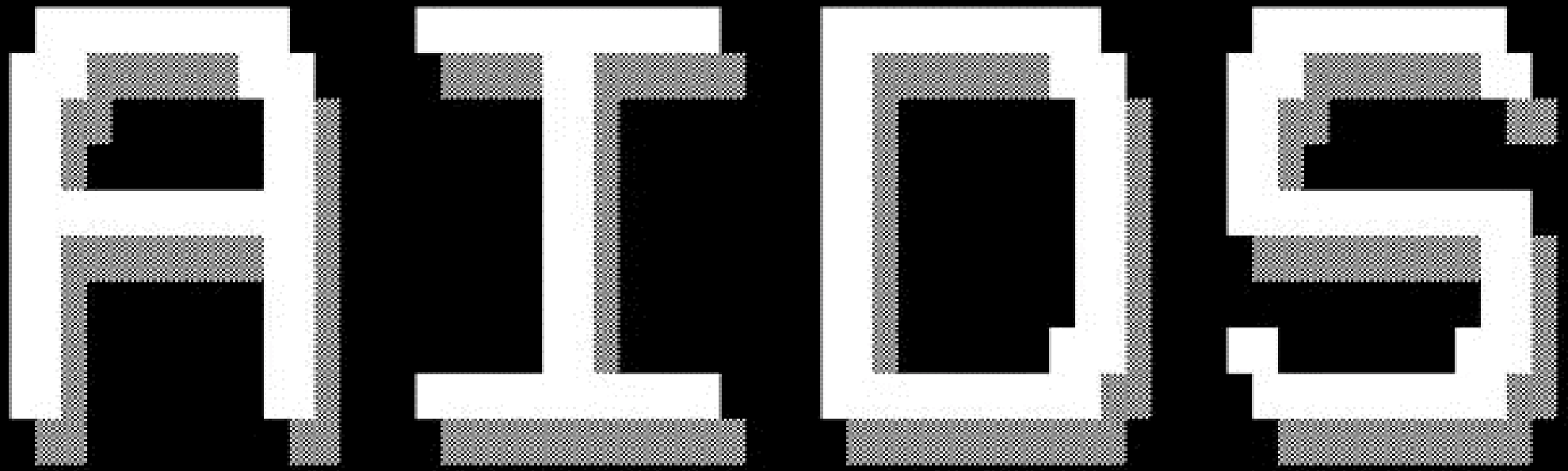
Files are deleted



Ransom is asked for the key to decrypt files

ATTENTION:

I have been elected to inform you that throughout your process of collecting and executing files, you have accdientally ¶HÜ¢KΣ► yourself over: again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a Ĵĭтûs has infected your system. Now what do you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and rememember, there is NO cure for



From 2014 the number of ransomware in circulation increases significantly

Ransomware remains the key malware threat in both law enforcement and industry reporting.

Wannacry attacks in mid-2017 affected more than 200 000 victims in 150 countries, with losses over **USD 4 Billion**

Internet Organized Crime Threat Assessment 2018 - Europol

Ransomware Countermeasures

Ransomware Detection Programs:

- Dynamic analysis that detects ransomware footprints by tracking how ransomware interacts with user data

- Does not provide proper cure for the damage that has already been caused
- Program can be stopped by a Ransomware with kernel privileges

Ransomware Countermeasures

Backup:

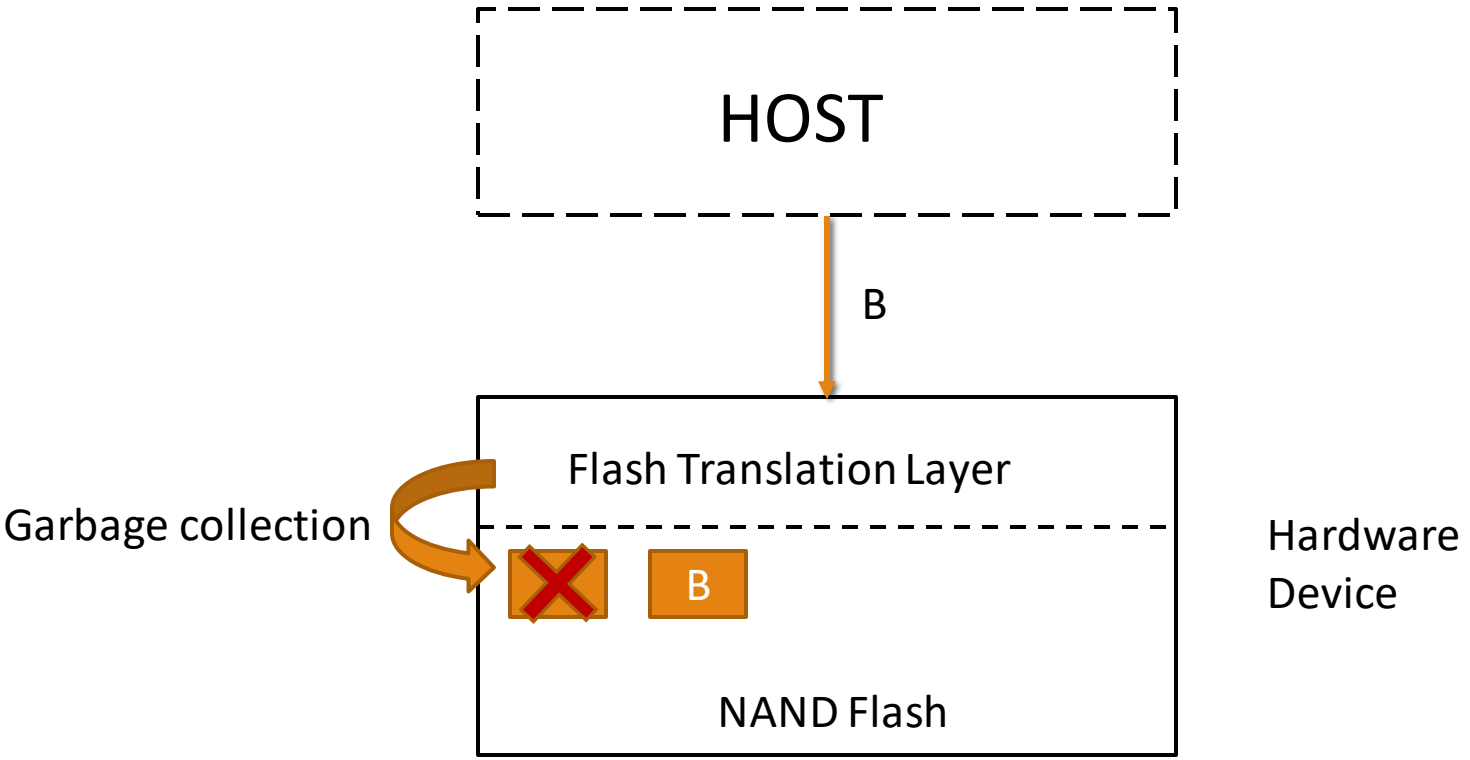
Both mechanism do not work when Ransomware obtains kernel privileges

SSD Layout

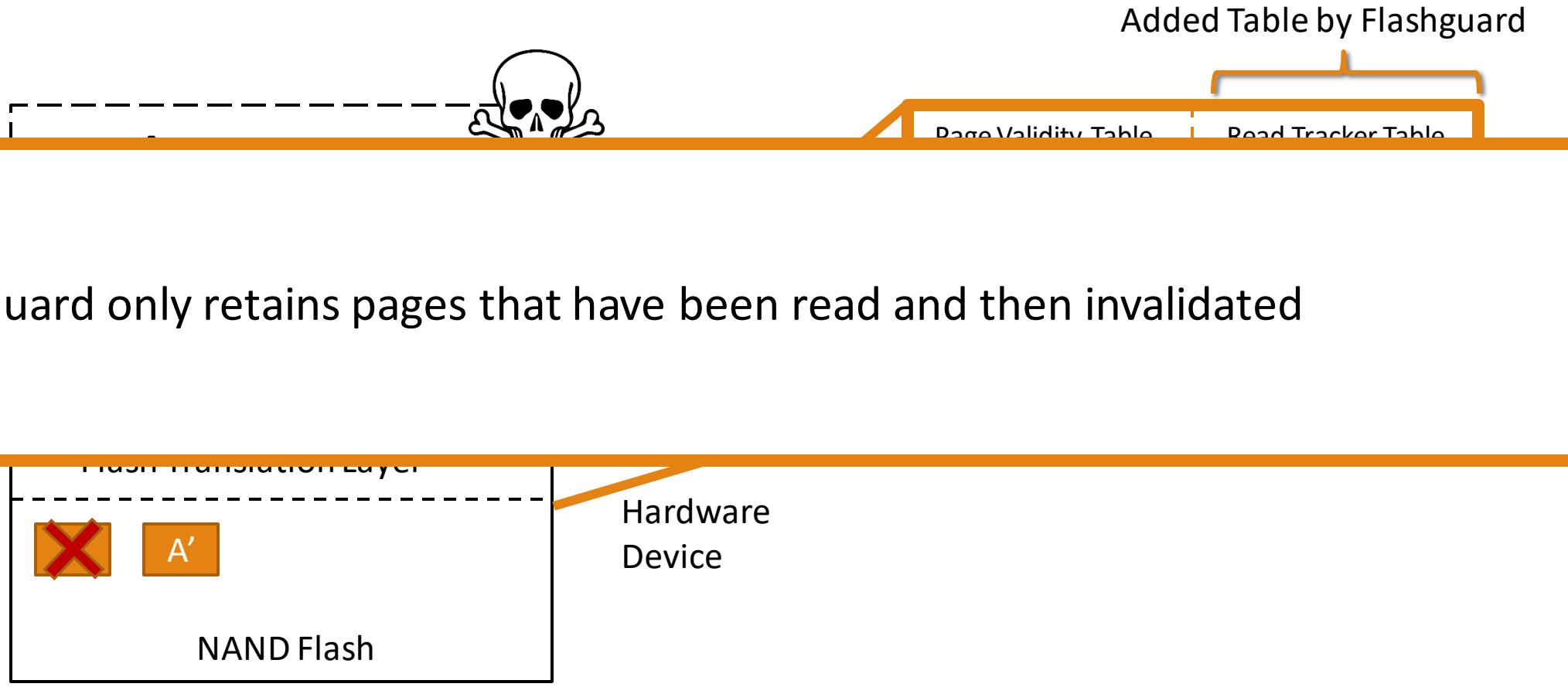
The Flash Translation Layer can only write to free pages

Erase operation can only be performed on block granularity

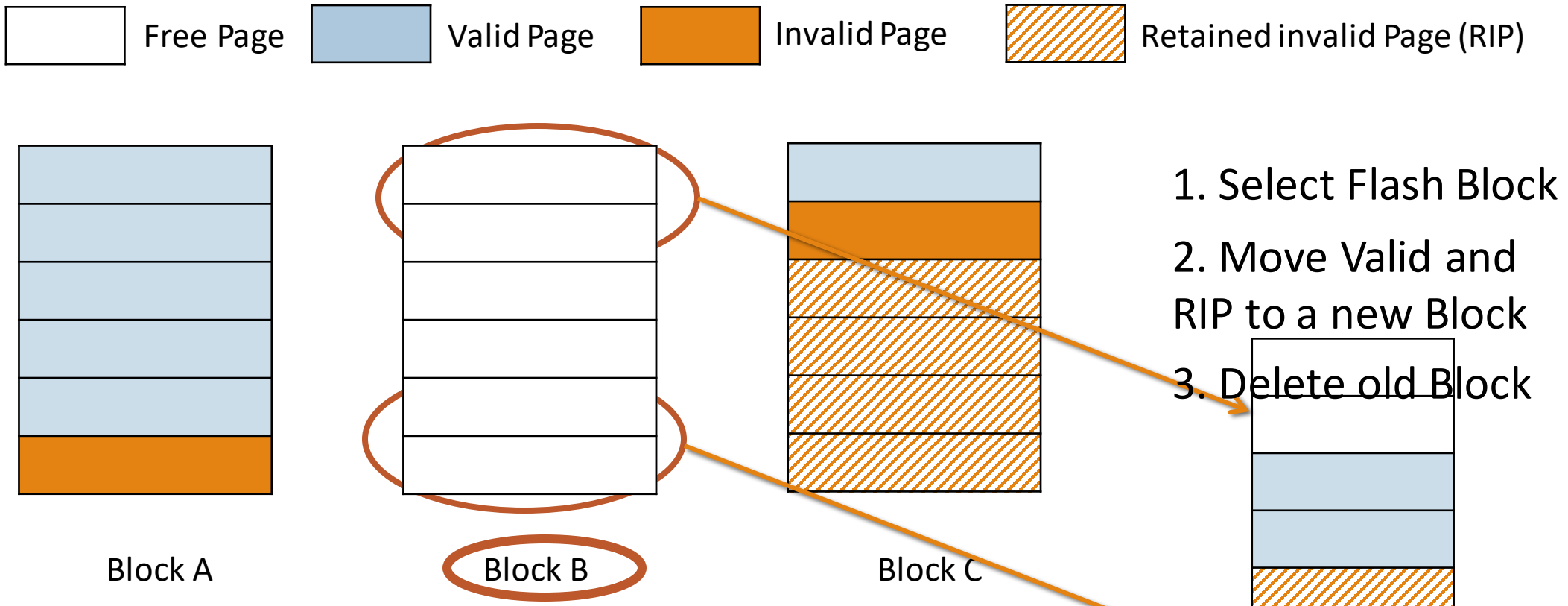
Out-of-place update



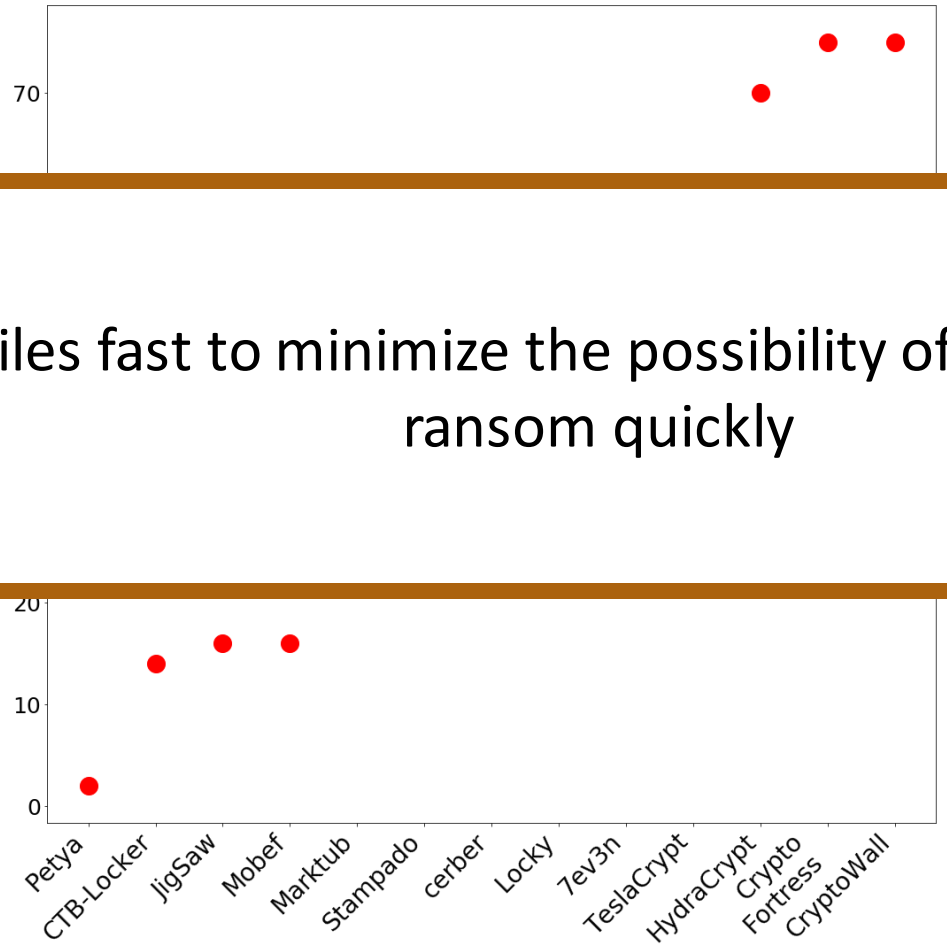
Which data should be retained?



Garbage Collection



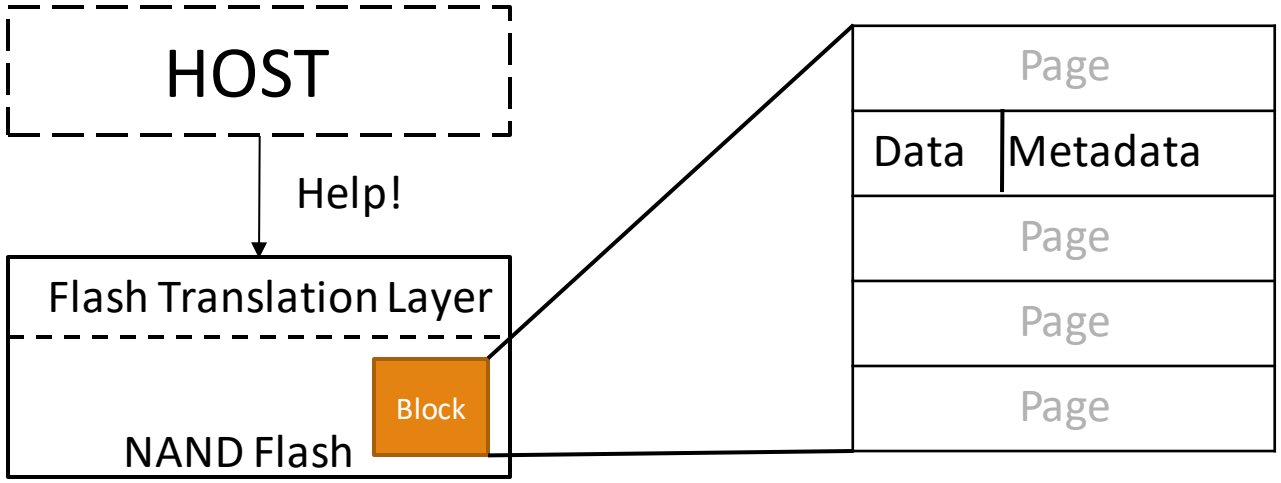
Ransomware Study



Ransomware encrypts files fast to minimize the possibility of getting caught and to collect the ransom quickly

Recovery Model

- After a threshold (20 days) the retained invalid pages are invalidated and can then be collected by the garbage collector.
- FlashGuard retains all the versions of a file, even if read and overwritten multiple times, and is able to restore all these versions



- When Ransomware is detected the SSD has to be inserted in a clean host and then Flashguard can start with the recovery
- By using the Metadata (Timestamp, RIP flag, LPA…) we can easily restore the data.
- Any existing Data recovery tool can be used

Evaluation & Key Results

Evaluation

- Implemented on a real SSD
- 1477 Ransomware samples tested
- Real World Workloads (from Florida International University and Microsoft Servers) and some I/O intensive Benchmarks

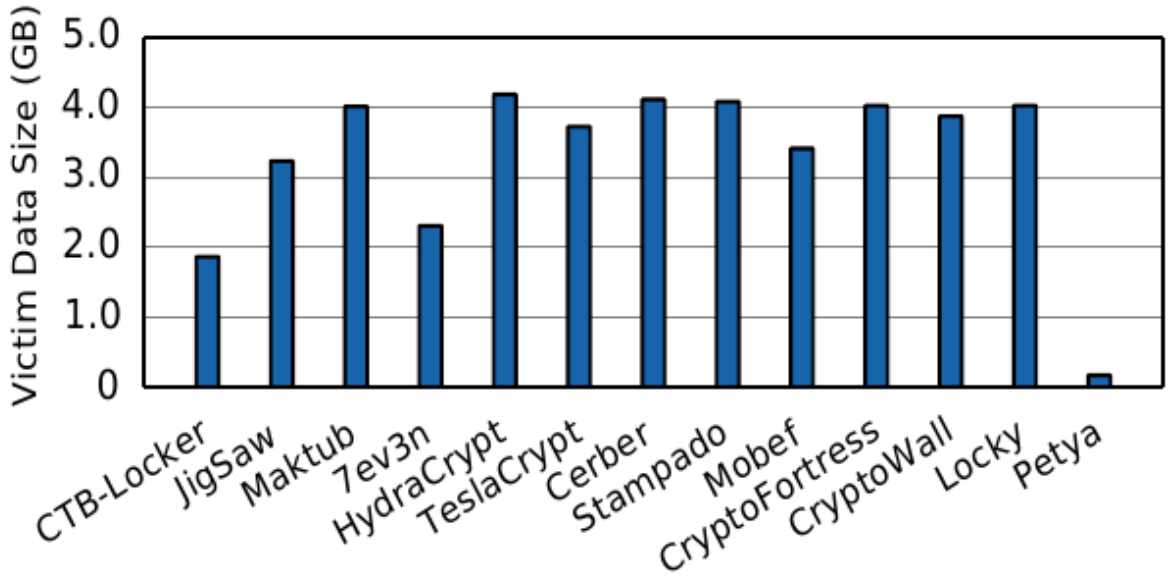
Key Results

- Impact on Storage Performance
  - For most of the workloads **latency** and **throughput** is almost the same.
  - For **I/O intensive** workloads, FlashGuard increases average latency up to 6.1% and the throughput drops by 0.6%
- Impact on SSD Lifetime
  - Impact on SSD Lifetime is negligible
  - Write Amplification (WAF) increases up to 4% (reduction of ca. **2 Weeks** of lifetime) in Microsoft/FIU workloads because of additional page movement

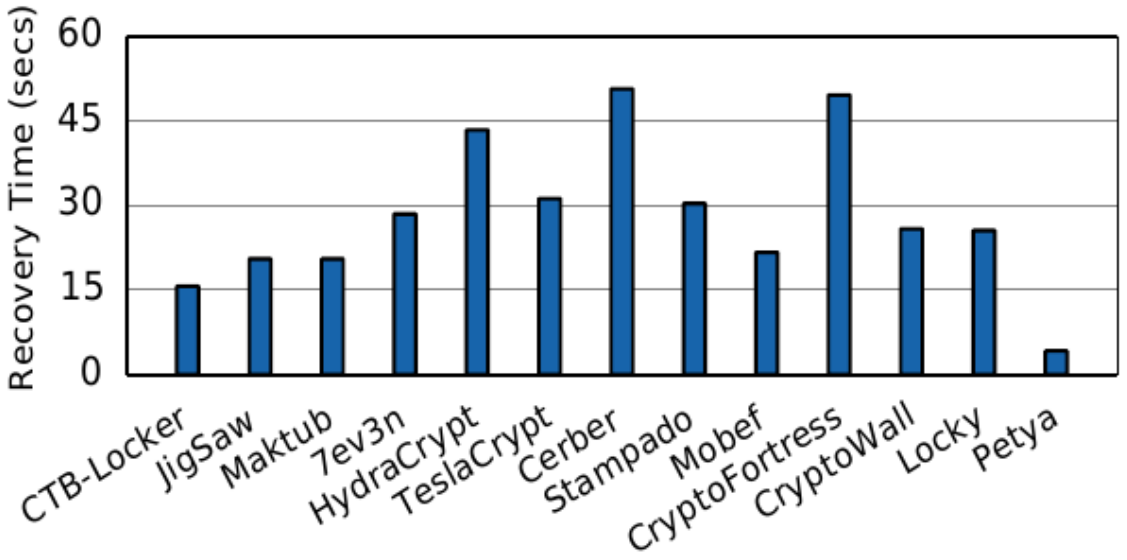
Results

- Efficiency on Data Recovery

Victim Data Size



Recovery Time



When scanning the entire Flash device Recovery takes **707.7 seconds**

Summary

The number of Ransomware is increasing and the solution available to not guarantee reliable recovery of data

The goal is to find a mechanism to reliably recover all data encrypted by ransomware

A Firmware solution FlashGuard:

- Defends data stored on SSD from Encryption Ransomware
- Leverages intrinsic Flash Properties
- Works also when Ransomware has kernel privileges

Strengths, weaknesses & key take-aways

Strengths

- No false negatives
- FlashGuard is able to recover all encrypted data from major families of Ransomware
- It is resistant to Ransomware with kernel privilege, because isolated from host
- Little to no overhead in storage operations and SSD lifetime
- Takes advantage of the intrinsic flash properties
- Intuitive and easy to understand

Weaknesses

- High False Positive rate
- Design contradicts secure deletion
- Only in Flash Memory
- Some explanation are very superficial
- Manual investigation for recovery
- 5718 lines of code

Key Take-aways

- FlashGuard is the first firmware-level defense system against encryption Ransomware
- It can efficiently reinstate the damaged files
- FlashGuard is naturally resistant to the ransomware with kernel privileges
- Negligible performance overhead (up to 6%)
- Trivial impact (less than 4%) on SSD lifetime

Follow-up works

- **"SSD-Insider: Internal Defense of Solid-State Drive against Ransomware with Perfect Data Recovery",** SungHa Baek, Youndon Jung, Aziz Mohaisen, Sungjin Lee, DaeHun Nyang
- **"RansomBlocker: a Low-Overhead Ransomware-Proof SSD",** Jisung Park, Youngdon Jung, Jonghoom Won, Minji Kang, Sungjin Lee, Jihong Kim
- **"Amoeba: An Autononomous Backup and recovery SSD for Ransomware Attack Defense"**,Donghyun Min, Donggyu Park, Jinwoo Ahn, Ryan Walker, Junghee Lee, Sungyong Park, Youngjae Kim
- **"MimosaFTL: adding Secure and Practical Ransomware Defense Strategy to Flash Translation Layer"**, Peiying Wang, Shijie Jia, Bo Chen, Luning Xia, Peng Liu

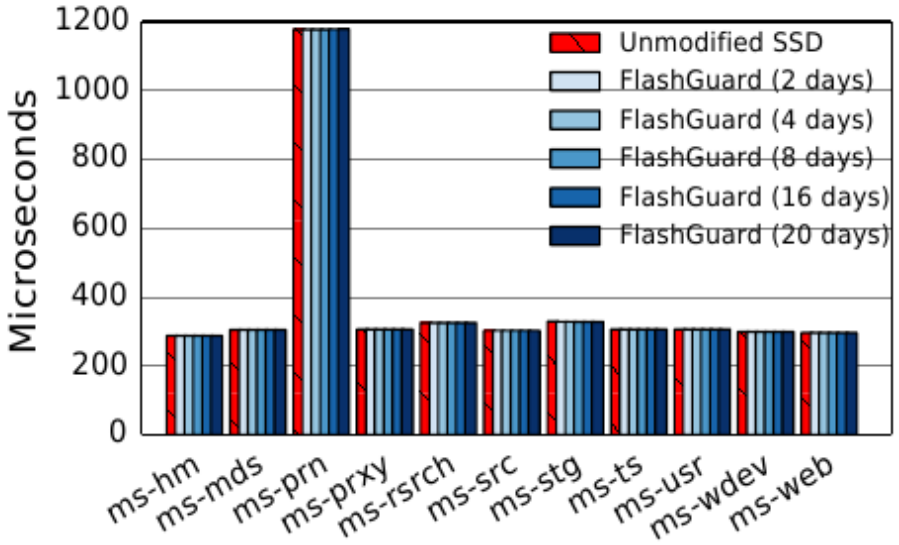
Questions?

Discussion Starter

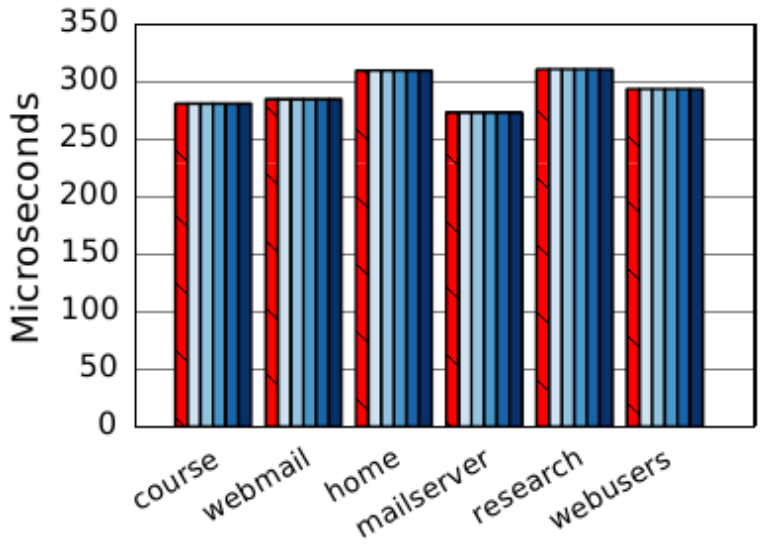
- Can you think of a way to trick FlashGuard?
- Do you have any idea how one could decrease the number false positives?
- Would you buy a SSD with FlashGuard?
- What could be done for secure deletion?
- For what else could out-of-place update be used for?
- What are your main take away?

Backup Slides

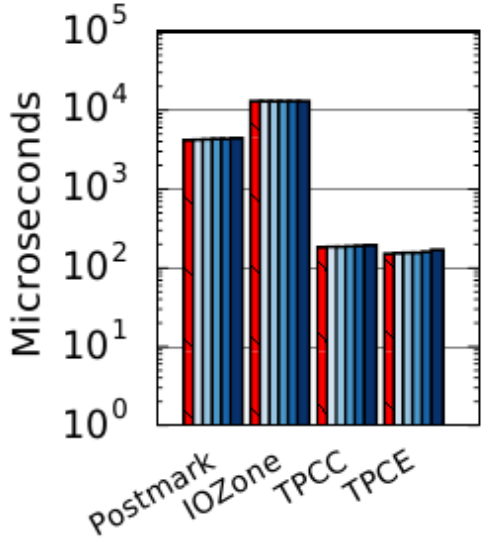
Average Latency



(a) Server Storage in Enterprise

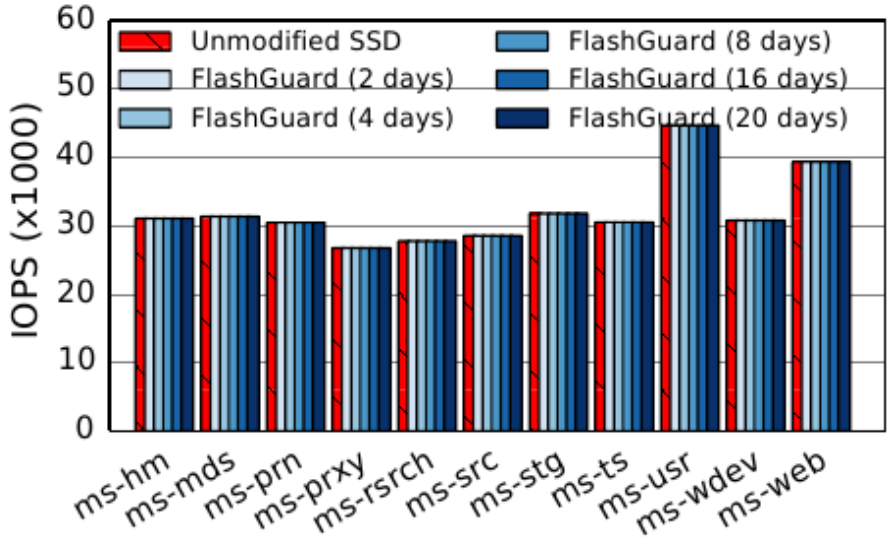


(b) Server Storage in University

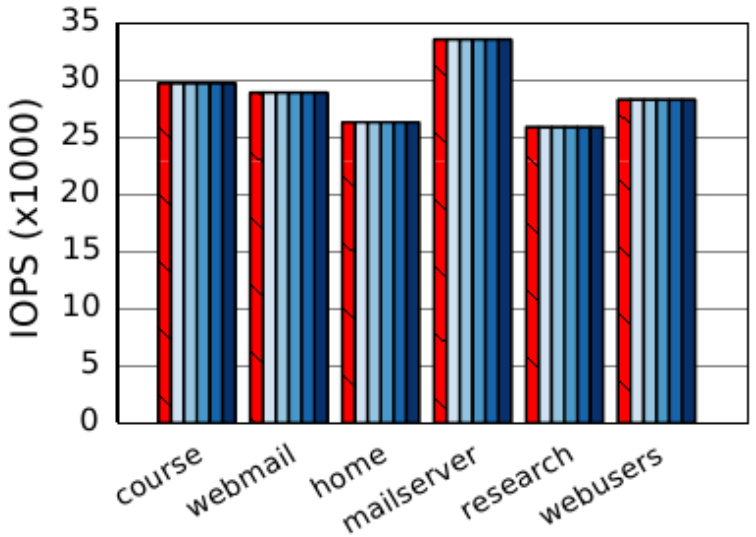


(c) Misc I/O Workloads

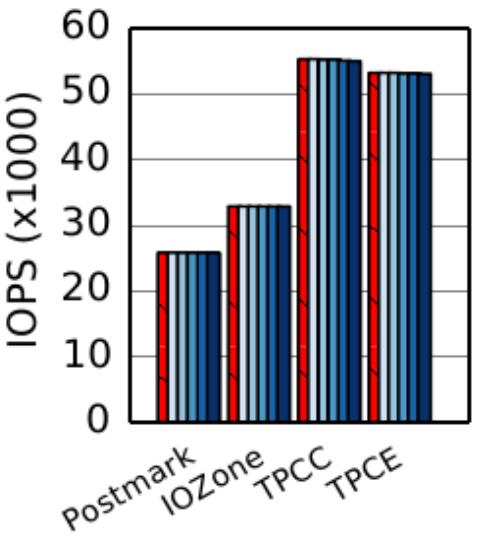
Average Throughput



(a) Server Storage in Enterprise

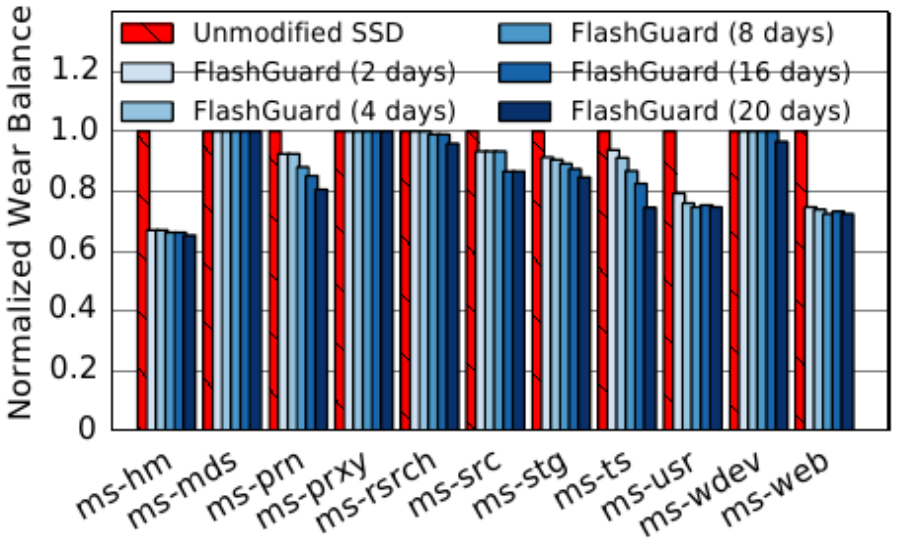


(b) Server Storage in University

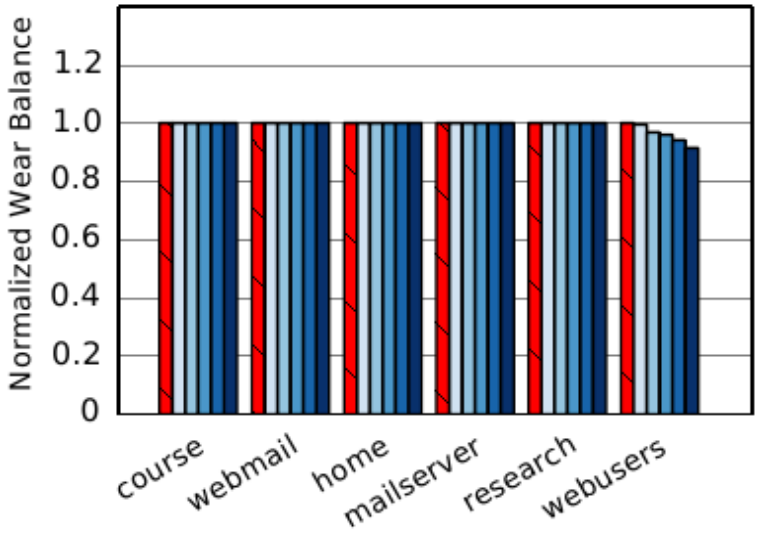


(c) Misc I/O Workloads

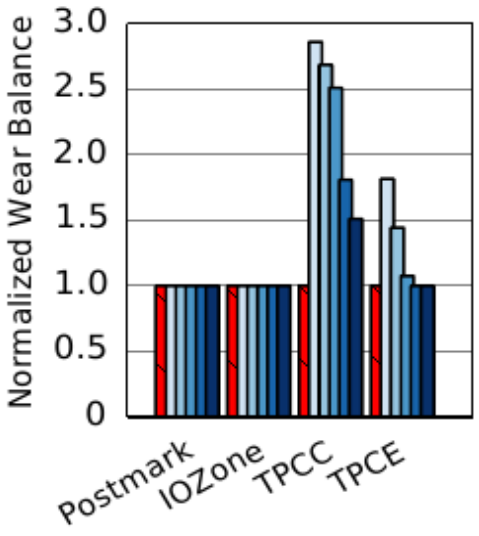
Normalized Wear Balance



(a) Server Storage in Enterprise

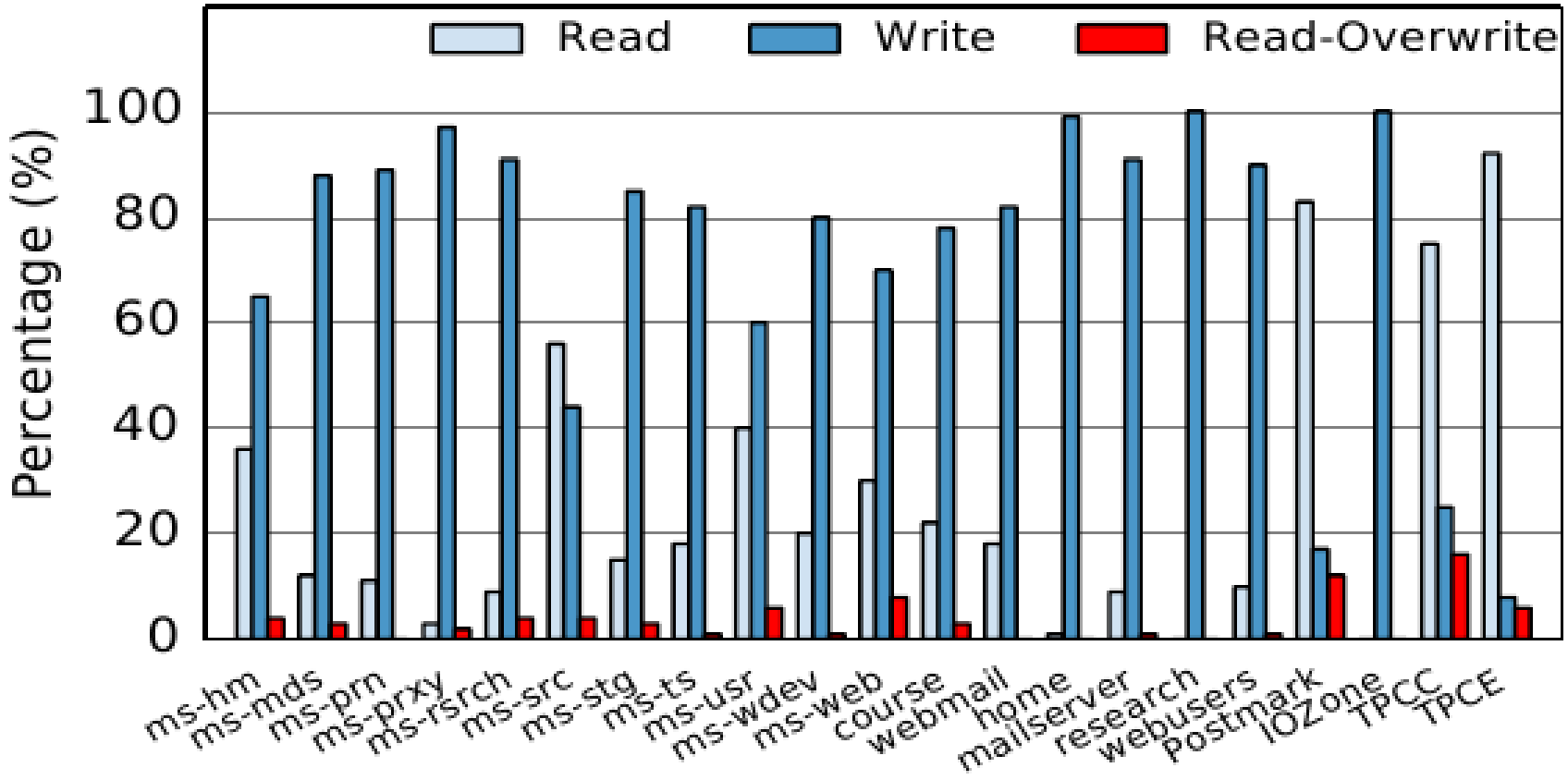


(b) Server Storage in University



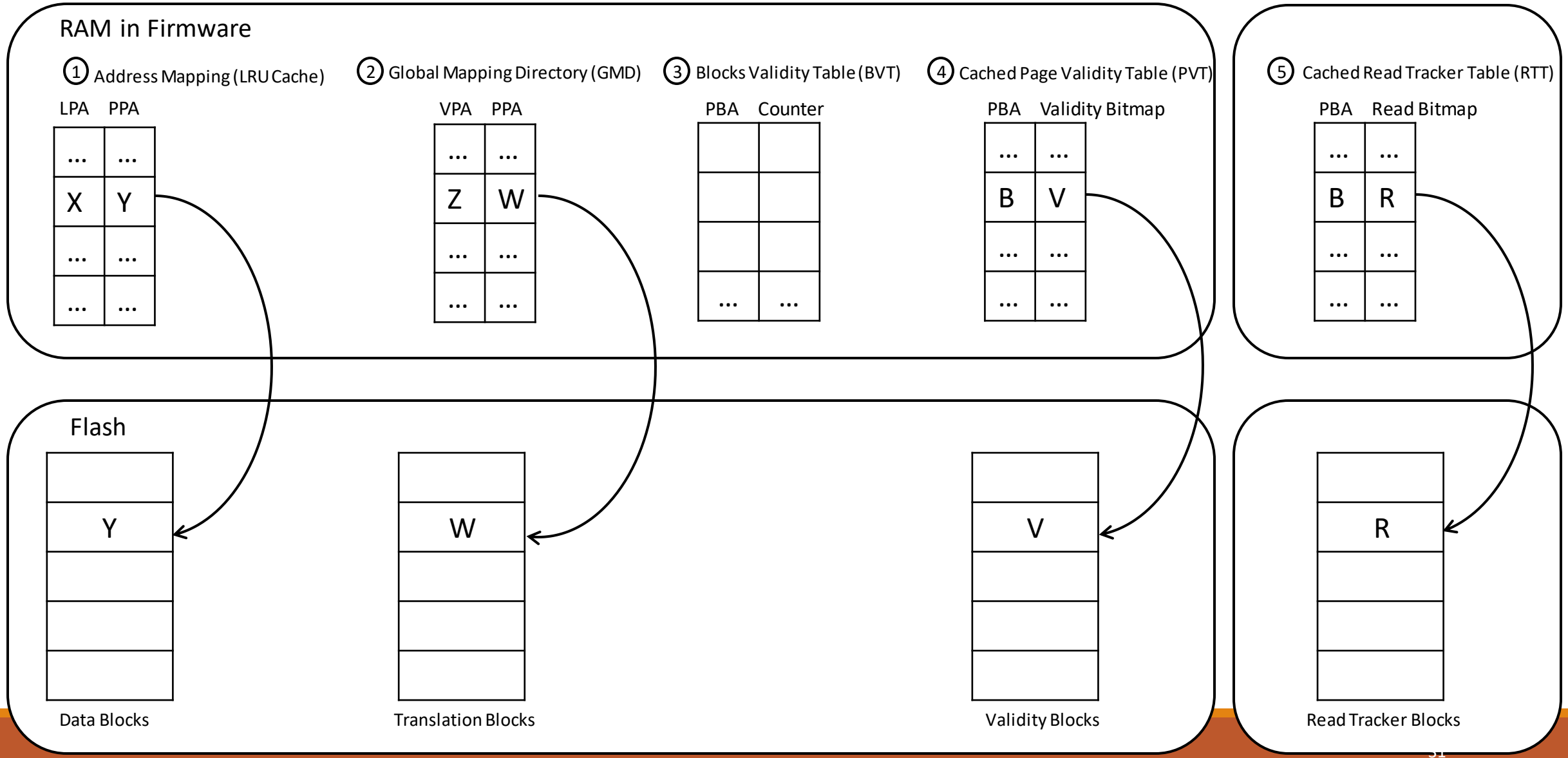
(c) Misc I/O Workloads

I/O Pattern


Read
Write
Read-Overwrite
Percentage (%)
100
80
60
40
20
0
ms-hm
ms-mds
ms-prn
ms-prxy
ms-rsrch
ms-src
ms-stg
ms-ts
ms-usr
ms-wdev
ms-web
course
webmail
home
mailserver
research
webusers
Postmark
IOZone
TPCC
TPCE

Ransom-Aware FTL

Table for RFTL



Tracking Invalid Data