Low-Cost Autonomous Backup Mechanism in SSD against Ransomware

Junghee Lee[1], Donghyun Min[2], Donggyu Park[2], Sungyong Park[2], Youngjae Kim[2]

University of Texas at San Antonio[1], Sogang University[2]

Presenter: Donggyu Park

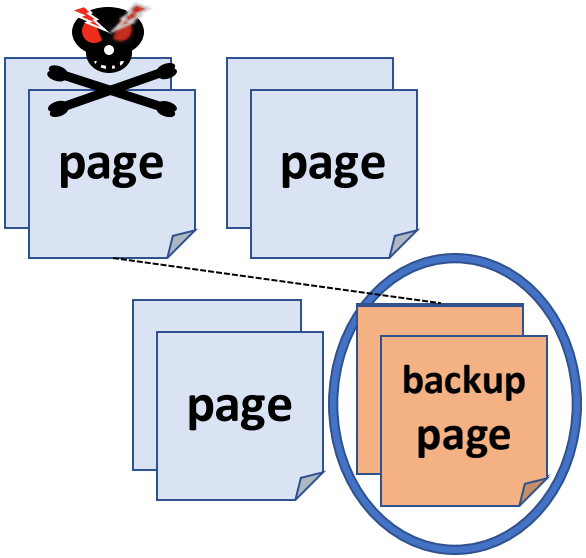




Introduction

- Encryption ransomware attack means that it encrypts files and data and demands owner to pay a ransom to restore the files.
  - It can cause immediate financial damage or loss of important data.

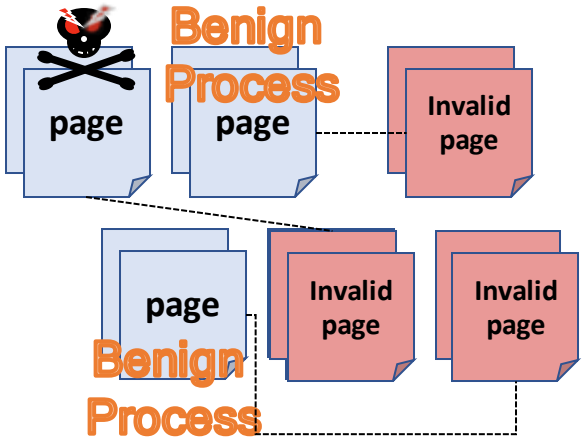
- File backup that is implemented in SSD is intuitive solution.
  - Use invalid page as backup page.



<SSD with File Backup mechanism>

Motivation

- Problem of existing SSD with backup
  - Existing research did not propose backup mechanism applied accurate ransomware detection in SSD.



  - Retention period of backup page depends on workloads.

Family	#Samples	Attack Time (minutes)
Petya	14	2
CTB-Locker	119	14
Jigsaw	5	16
TeslaCrypt	75	44
HydraCrypt	13	70
CryptoFortree	4	75
CrytoWall	799	75

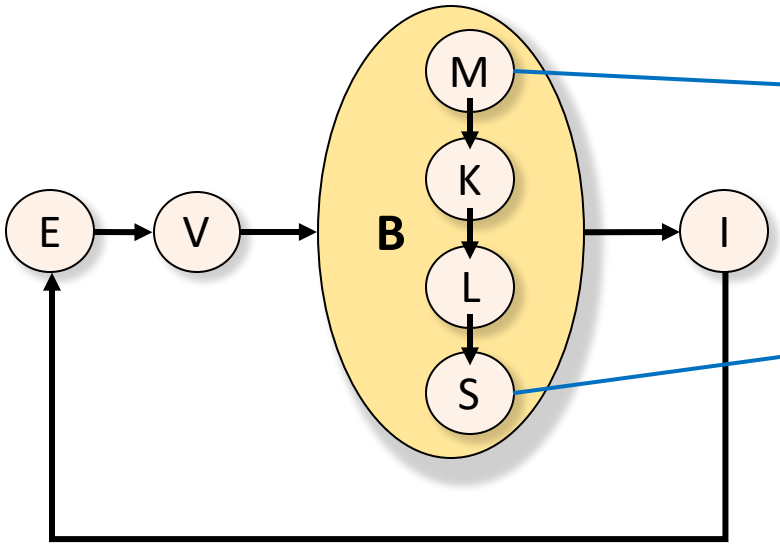
Study of Encryption time[1]

Time can vary depending on workloads

[1] FlashGuard: Leveraing Intrinsic Flash Properties to Defend Against Encryption Ransomware

Autonomous Backup Mechanism

- We apply concrete ransomware detection.
- Managing pages differently to control the backup pages in a concrete way.
  - We use following three indicators to differentiate: Similarity, Entropy, and I/O arrival rate.



<Extended State Transition Diagram of Physical page>

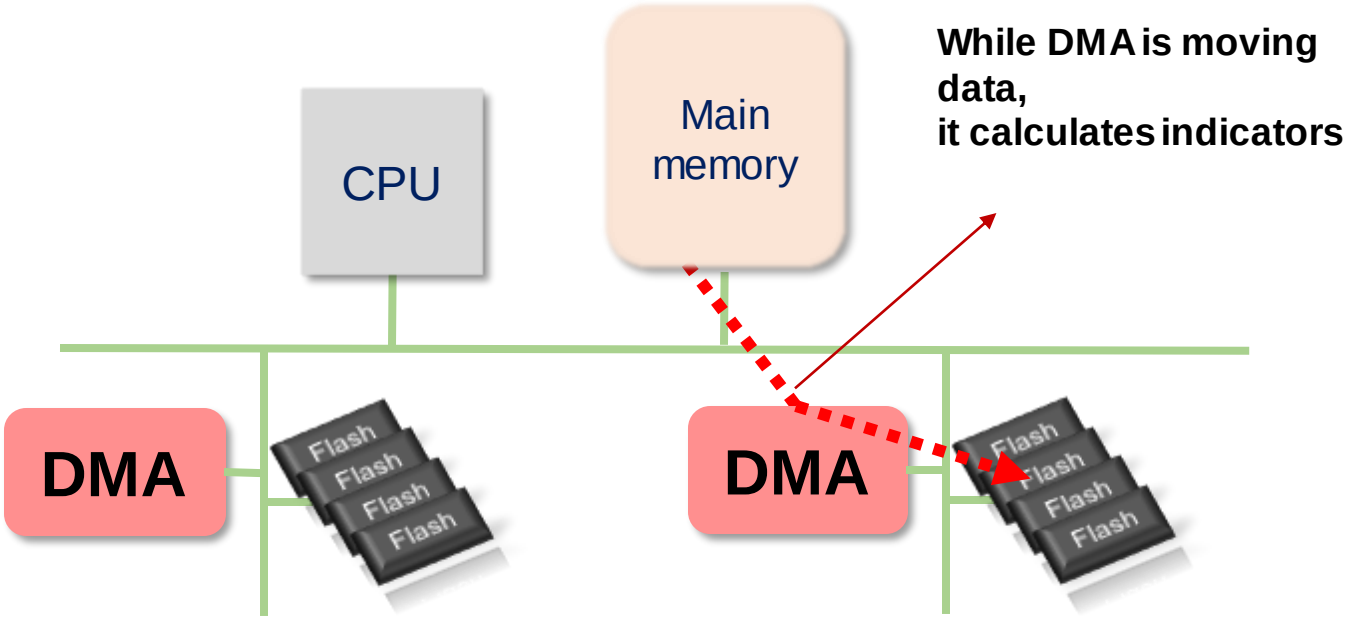
Degree of Ransomware attack
Indication : **Very Strong**

Degree of Ransomware attack
Indication : **Very Weak**

SSD can control the number of backup pages automatically
→ Reduce GC overhead
→ It does not need external study of Ransomware encryption time.

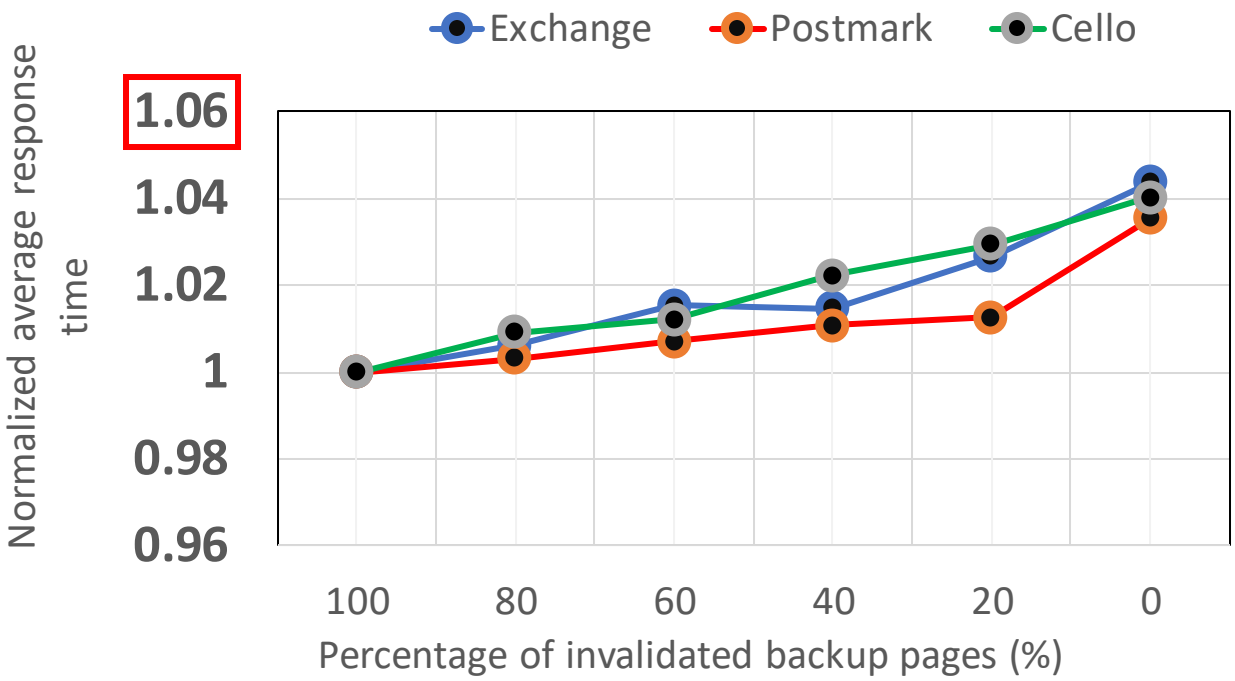
Lightweight Hardware accelerator

- Calculating these indicators using our dedicated hardware accelerator when data is transferred to Flash through DMA.
  - Calculation is very fast because the computation is performed while data being transferred.
  - It is possible to automatically determine which backup stage is proper among these stages.



<Block Diagram of Design of Hardware Accelerator>

Experimental Results



<Normalized Average Response Time>

- We performed experiments varying the percentage of backup pages invalidated by GC.
- The maximum overhead in the average response time is 4.3%, 3.5%, and 4.0% for Exchange, Postmark, and Cello, respectively, which is much less than the existing technique implemented in the OS