CS 5472 - Advanced Topics in Computer Security

Topic 8: Ransomware (2)

Spring 2018 Semester

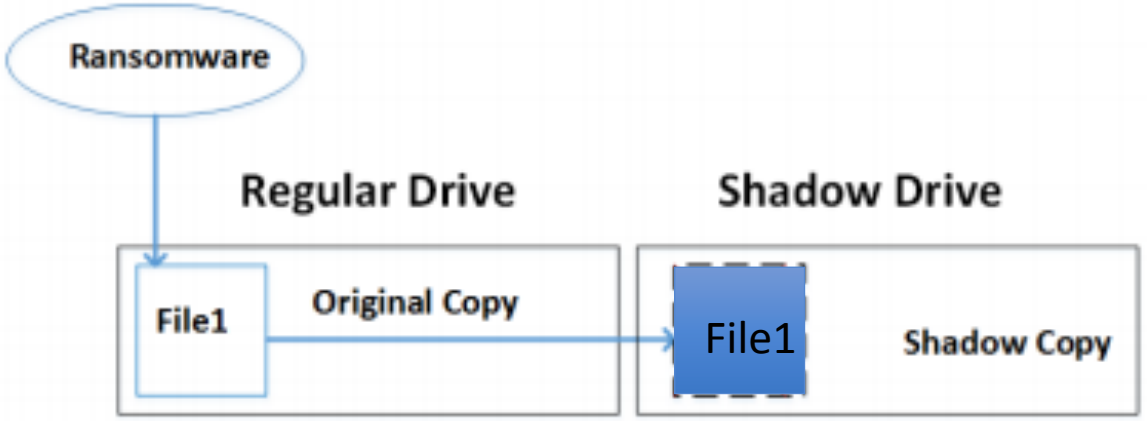
Instructor: Bo Chen

bchen@mtu.edu

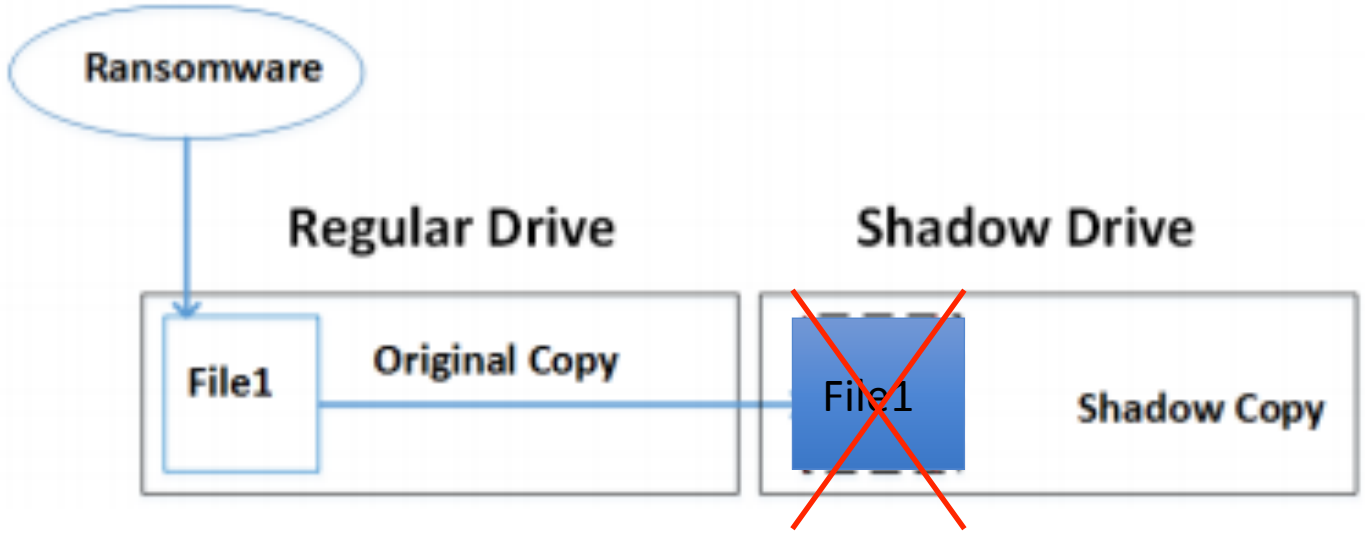
http://cs.mtu.edu/~bchen

How to Defend against Crypto Ransomware?

- Crypto ransomware will encrypt the victim's data
- The encrypted data can be recovered by creating backups
- ShieldFS (*presented by Ryan on Tuesday*) creates a shadow copy, and can allow data recovery based on this shadow copy



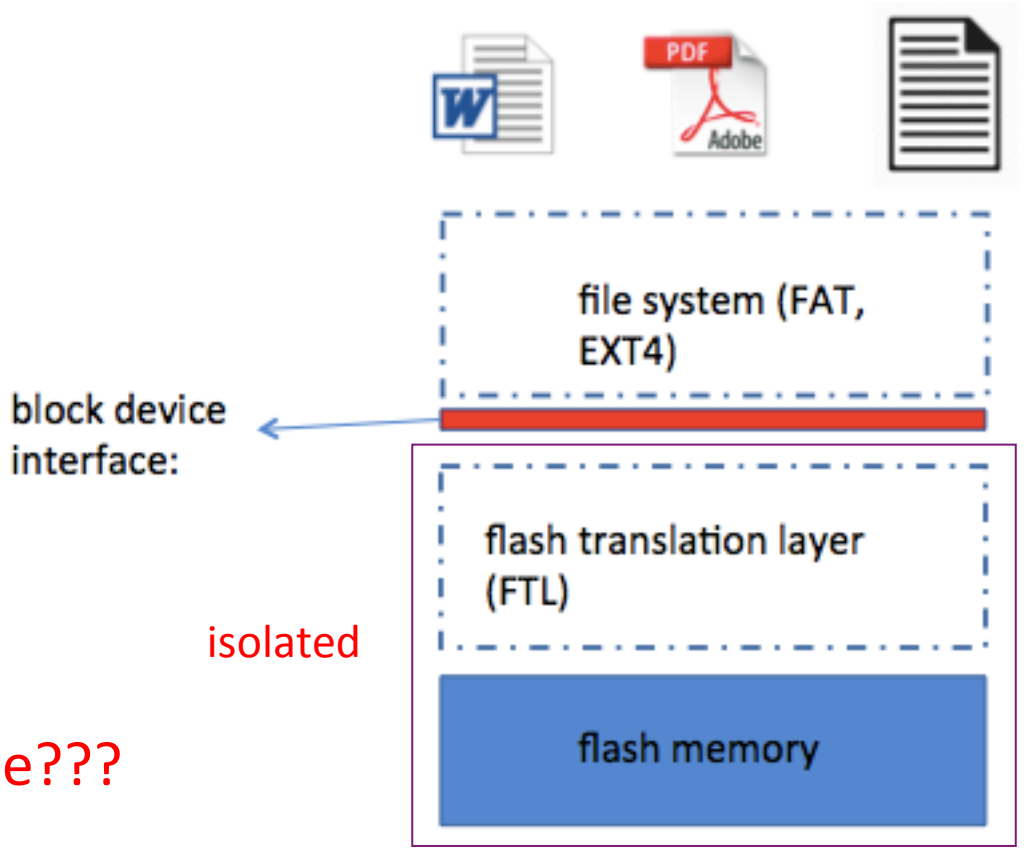
What if The Ransomware can Obtain Root Privilege?



What can We Do? A Better Isolation

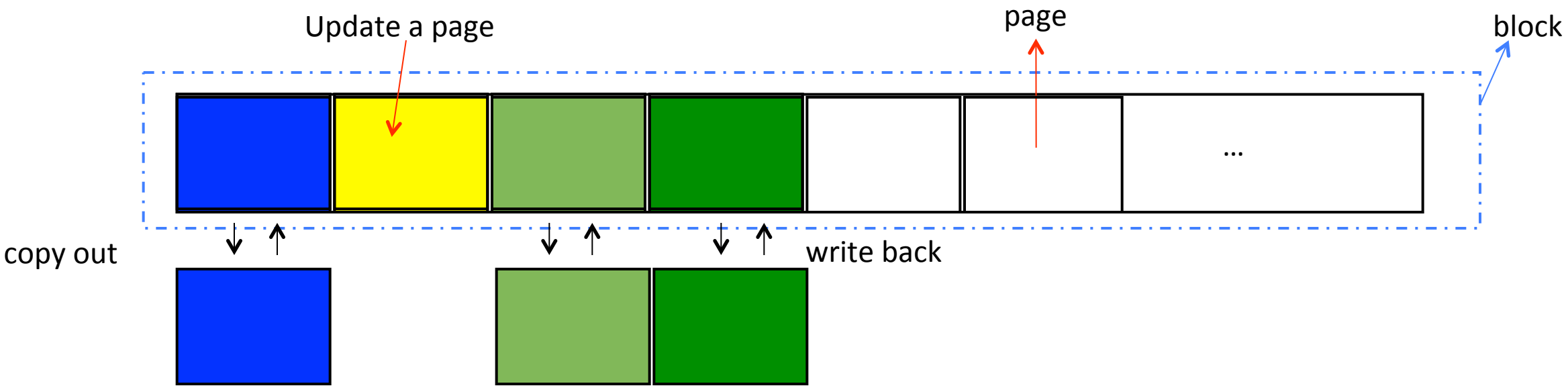
- People today are increasingly turning to flash memory for data storage due to its high throughput and decreasing price
  - Solid state drives (SSD)
  - eMMC cards, miniSD cards
  - USB drives
- A flash device is isolated from the host computer system
  - Independent hardware (processor, RAM)
  - Independent software (flash firmware)
  - Interface: SCSI, ATA, etc

Can we utilize this isolation for ransomware defense???



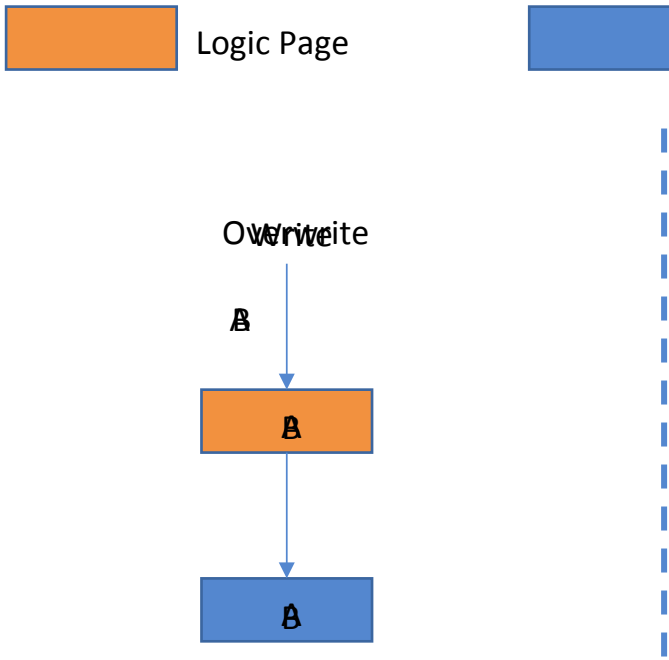
Special Characteristics of Flash Memory

- Update unfriendly
  - Over-writing a page requires first erasing the entire block
  - Write is performed in pages (e.g., 4KB), but erase is performed in blocks (e.g., 128KB)

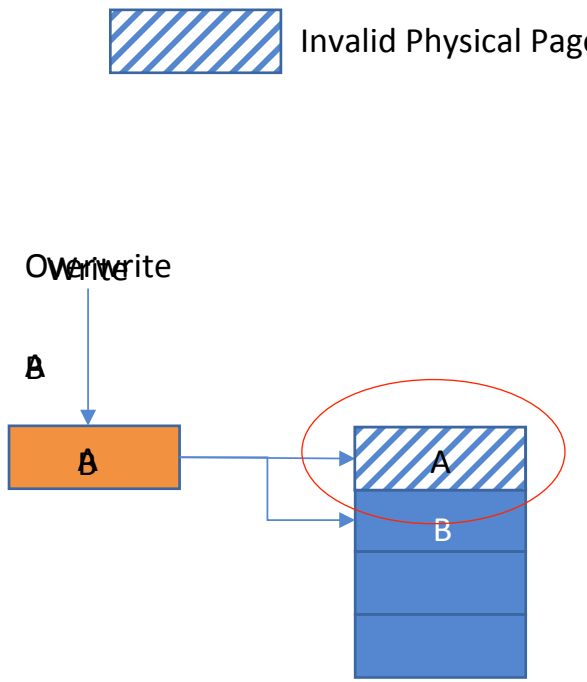


  - Over-write may cause significant write amplification

Flash Memory Feature: Out-of-Place Update



(a) In-place update on mechanical disk drives



(b) Out-of-place update on flash memory

Old data are temporarily preserved before being reclaimed by garbage collection

Research Questions

- Can we take advantage of those old (invalidated) data being preserved in flash memory to recover data being encrypted by crypto ransomware?
  - Crypto ransomware is not able to corrupt those data due to the isolation from flash translation layer
- However, the flash memory is usually equipped with a garbage collection strategy which will periodically reclaim the space occupied by invalid data
  - How to prevent the invalid data from being reclaimed by garbage collection before they are used to recover data corrupted by ransomware

Paper Presentation

- FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware

- Presented by Sophia Farquhar