CS 5472 - Advanced Topics in Computer Security

Topic 7: Ransomware (2)

Spring 2022 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

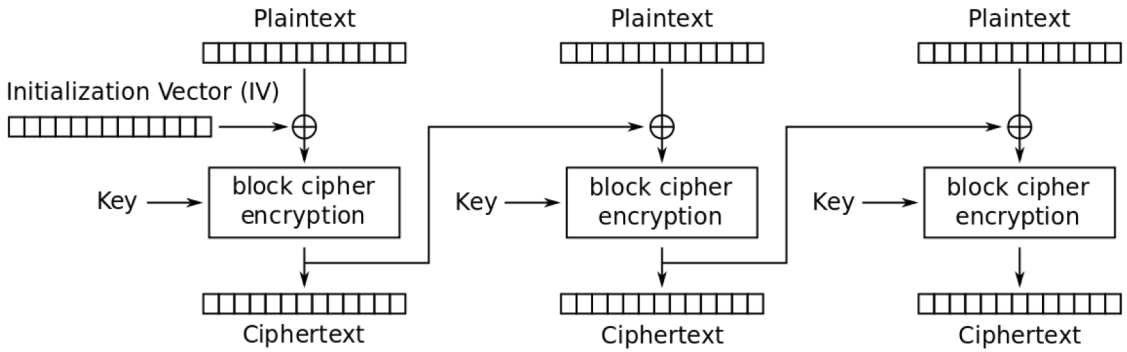
Crypto Ransomware

- Encrypt the data, and ask for ransom
- Defenses:
  - Detection: **need to detect ransomware as soon as possible** to prevent ransomware from corrupting more data (UNVEIL introduced on Tuesday)
    - What if before the ransomware is detected, some of the data have been encrypted by the ransomware
  - A better defense: detection + recovery (today)

A Little More on Detecting Ransomware

- File system access activities
  - File system activities without ransomware are different from that with ransomware

- Cryptographic primitives
  - Block ciphers for encryption



Cipher Block Chaining (CBC) mode encryption

What about Data Recovery? Solution 1

- Back up data online, like using public cloud services
  - iCloud
  - Dropbox
  - Google Drive
  - etc.

- A few limitations for online backup solution
  - What if I don't have Internet connection?
  - What if my Internet connection is low-bandwidth (2G/3G)?
  - Even if I have high-bandwidth Internet connection (4G/LTE), I don't want to pay for the network usage. I will wait until I have free Wi-Fi to back up data
  - Even if I have free Wi-Fi, I cannot do the backup continuously and hence the data in the computer/mobile device are not synchronized with the data of the online backup. Why?

What about Data Recovery? Solution 2

- Manually/ Automatically back up data in the local storage periodically
- Pros: does not rely on network
- Cons:
  - The backup of the entire data will occupy a lot of local storage space
  - The local backup may be also corrupted by the ransomware

Copy-On-Write (COW)

- When the file system reads/ writes files, the data are actually read (by the process) into the memory and written (by the process) back to memory

- Scenarios:
  - 10 processes want to perform I/Os on the same file F, how the OS will handle it?
  - Option 1: each process reads the file F into the memory
    - Pros: easy to manage
    - Cons: a lot of overhead in the memory
  - Option 2: the first process reads the file F into the memory, and the remaining processes directly use this file in the memory
    - Pros: save a lot of overhead
    - Cons: what if one processes wants to modify the file F?

Copy-On-Write (COW)

- Copy-On-Write in the file system:
  - **N** processes read the same file, and only one copy of the file needs to be maintained in the memory (rather than N copies)
  - If one process modifies the file, a modified copy of the file will be created in the memory in a new location, but the original copy of the file is still there

- How can I take advantage of COW for ransomware data recovery (you should be able to find more details in today's paper presentation)?

File System Review

Applications' view:

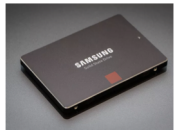
Files (.doc, .pdf, .txt, …)

file systems (FAT, NTFS, EXT4, …), implement system calls like open, read, write, etc

Manage the mappings between the applications' view and the block device's view

block device interface: allow to read/write a block of any size and any alignment.

Physical storage medium (hard disk drive, flash storage, etc.)

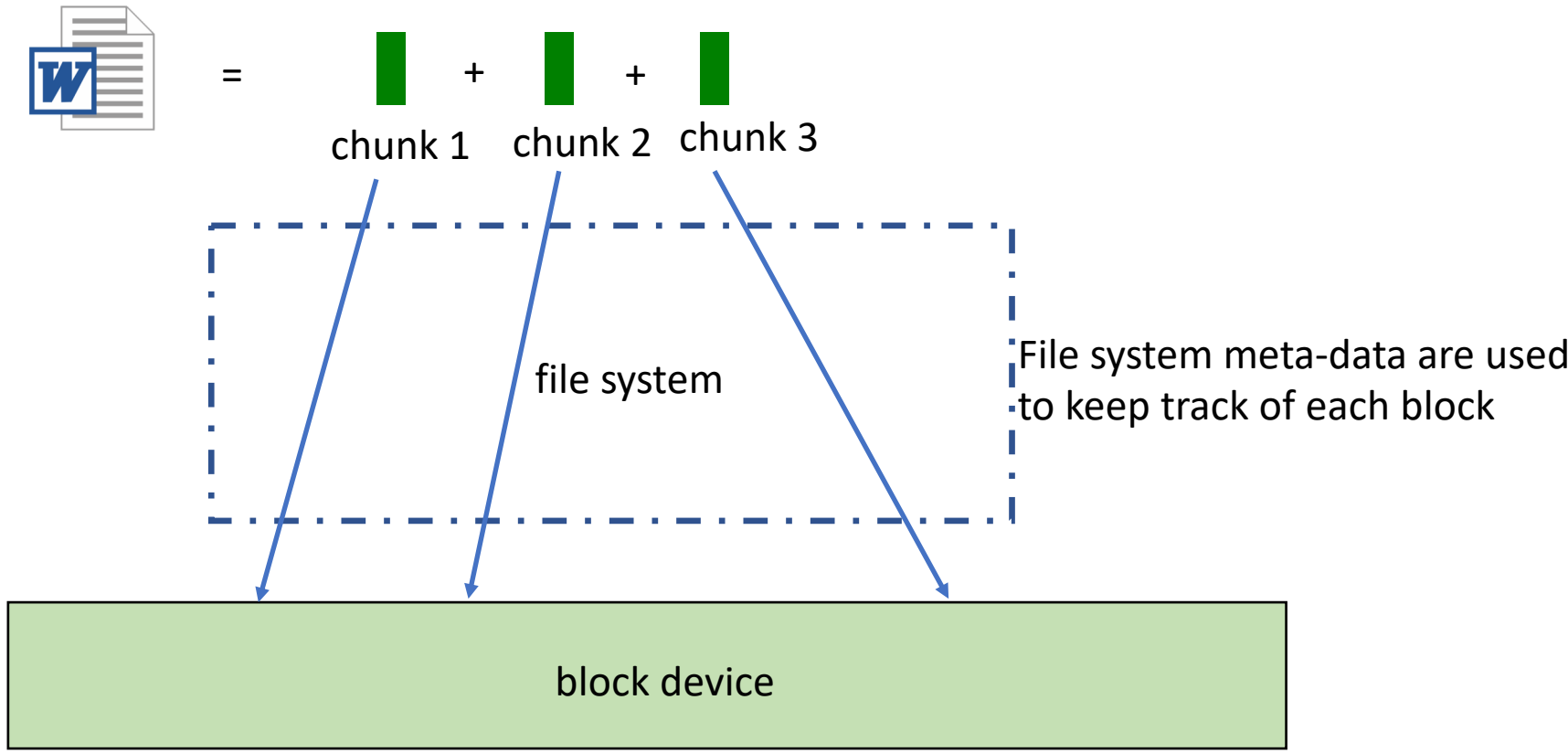


Main Operations of A File System – Write System Call

```
#include <unistd.h>

ssize_t write(int fd, const void *buf, size_t count);
```

Applications' view:



Main Operations of A File System – Read System Call

```
#include <unistd.h>

ssize_t read(int fd, void *buf, size_t count);
```

Applications' view:

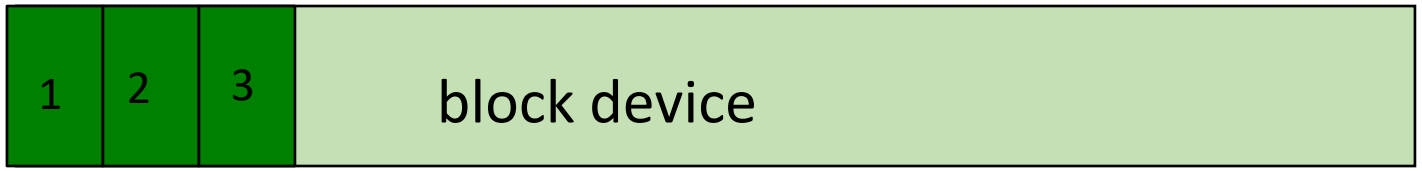
Read the meta-data to find out location of each block

Example: FAT and EXT4

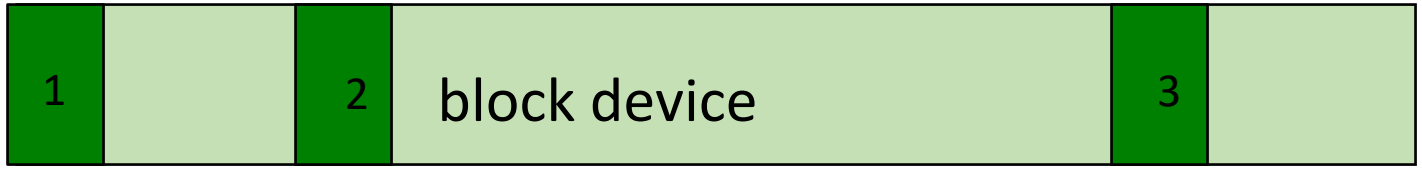
Applications' view:  = chunk 1 + chunk 2 + chunk 3

For different types of file systems, the mappings between the file chunks and the locations in the disk are managed by different strategies

FAT



EXT4



The Efforts of My Research Group on Ransomware/Malware Defenses

- Niusen Chen, Wen Xie, and **Bo Chen**. Combating the OS-level Malware in Mobile Devices by Leveraging Isolation and Steganography. The Second ACNS Workshop on Secure Cryptographic Implementation (SCI '21)(in conjunction with ACNS '21), Kamakura, Japan, June 2021.

- Wen Xie, Niusen Chen, and **Bo Chen**. Incorporating Malware Detection into The Flash Translation Layer. 2020 IEEE Symposium on Security and Privacy (S&P '20), San Francisco, CA, May 2020 (extended abstract).

- Peiying Wang, Shijie Jia, **Bo Chen**, Luning Xia and Peng Liu. MimosaFTL: Adding Secure and Practical Ransomware Defense Strategy to Flash Translation Layer. The Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19), Dallas, TX, USA, March 2019.

- Le Guan, Shijie Jia, **Bo Chen**, Fengwei Zhang, Bo Luo, Jingqiang Lin, Peng Liu, Xinyu Xing, and Luning Xia. Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices. 2017 Annual Computer Security Applications Conference (ACSAC '17), Orlando, Florida, USA, December 2017 (Distinguished Paper Award)

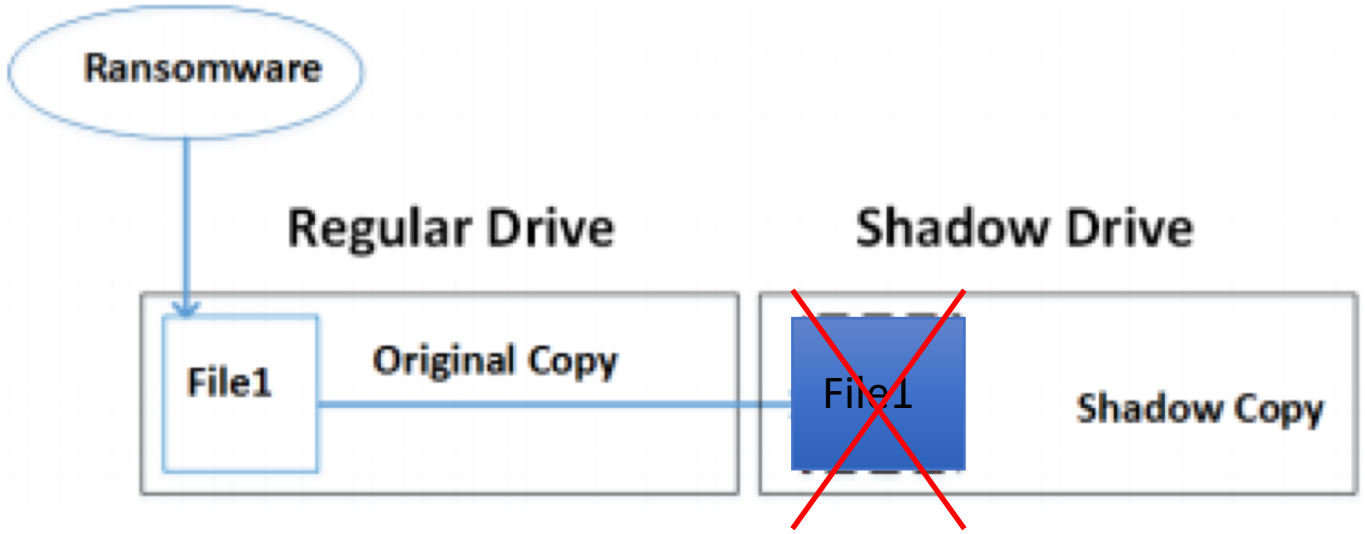
- Kul Prasad Subedi, Daya Ram Budhathoki, **Bo Chen**, and Dipankar Dasgupta. RDS3: Ransomware Defense Strategy by Using Stealthily Spare Space. The 2017 IEEE Symposium Series on Computational Intelligence (SSCI '17), Hawaii, USA, Nov. 27 - Dec. 1, 2017.

Paper Presentation

- ShieldFS: A Self-healing, Ransomware-aware Filesystem

- Presented by Mezbah Islam

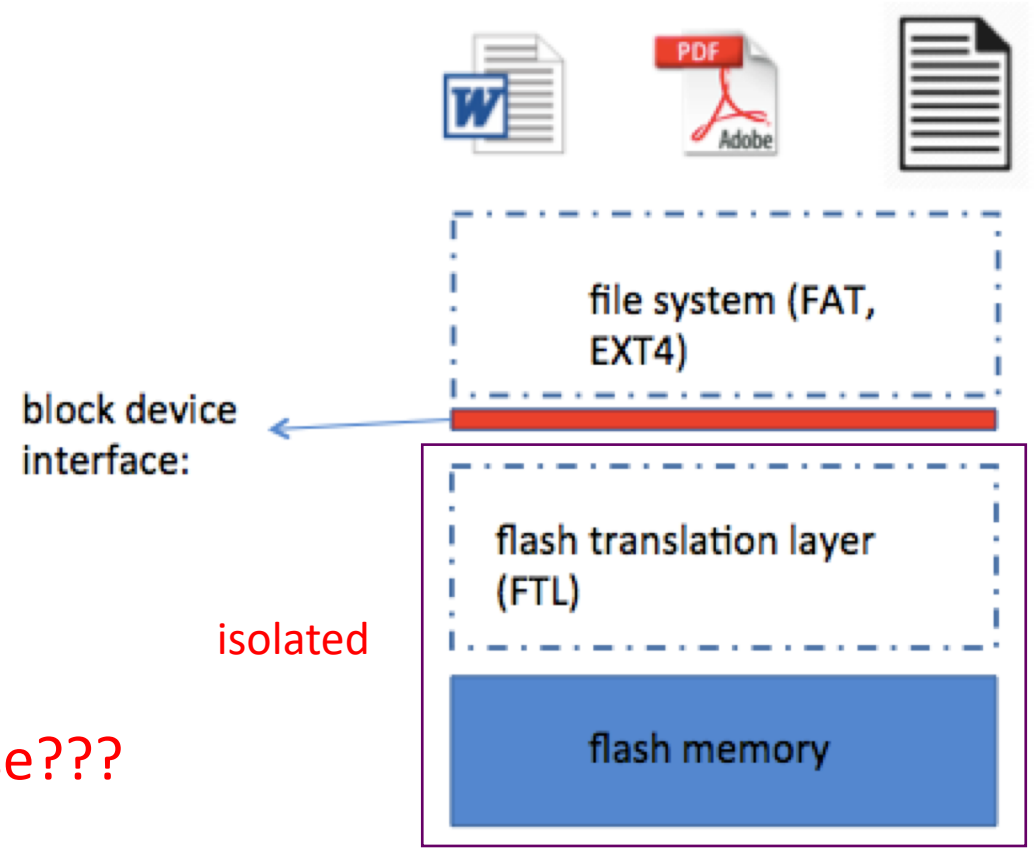
What if The Ransomware can Obtain Root Privilege?



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???



What can We Do? A Better Isolation

- The flash memory uses out-of-place update, which implies that when ransomware tries to overwrite/delete the data, the old data will be still preserved in the flash memory

- Refer to the recommended reading for more technical details if you are interested

Recommended reading:

MimosaFTL: Adding Secure and Practical Ransomware Defense Strategy to Flash Translation Layer