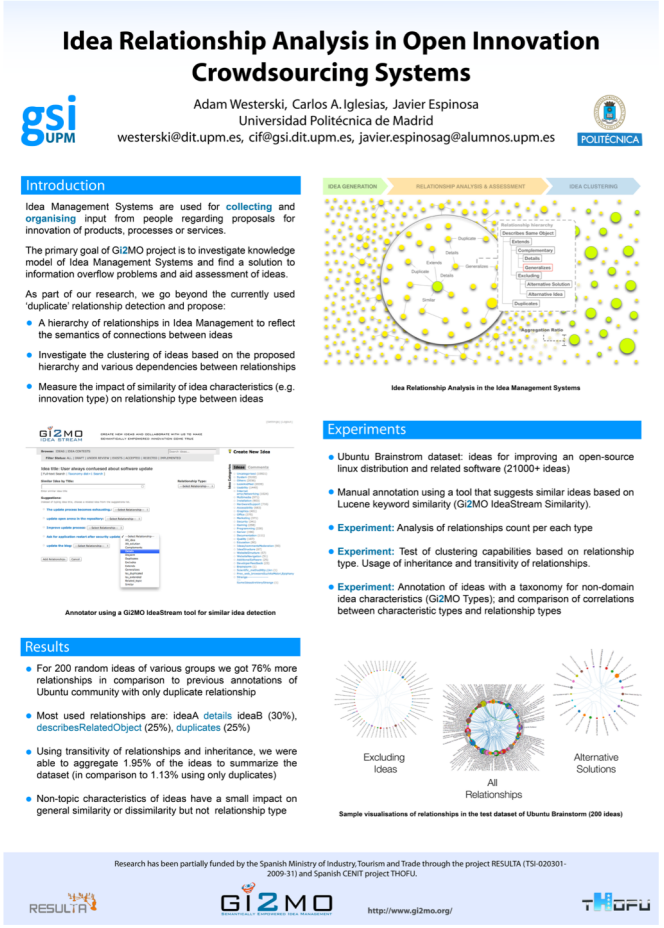
CS 5472 - Advanced Topics in Computer Security

Topic 7: Ransomware (2)

Spring 2019 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

The Explore CSR Workshop April 5 - 7

- The Explore CSR Workshop is a 3-day workshop for undergraduates from underrepresented groups in early April
- Organized by CS department and supported by Google (some engineers from Google are invited)
- There is a poster session (https://explore.cs.mtu.edu/?page_id=60)
  - Time: 5:15-6:30pm **Friday April 5**
  - Location: MUB Alumni Lounge
- You may create a poster on your term project and go there to present your work
  - Great opportunity of training your communication skills
  - Good networking opportunity for other people to know you
  - May be your are lucky to impress engineers from Google
- If you plan do a poster there, let me know and I can pay for the printing of your poster



Crypto Ransomware – A Review

- Encrypt the data, and ask for ransom
- Defenses:
  - Detection: need to detect ransomware as soon as possible to prevent ransomware from corrupting more data
  - Recovery: ensure recoverability of data by preparing backups
  - A hybrid solution: detection + recovery

How to Ensure Data Recovery from Ransomware Attacks?

- Back up data online, like using public cloud services (iCloud, Dropbox, Google Cloud, 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?

Can I Recover My Data without Relying on Online Backups?

- You can back up a copy of data in local storage periodically

- Limitation
  - The backup of the entire data will occupy a lot of local storage space
    - Do I really need to back up the entire data? We will answer this question in today's lecture
  - The local backup may be compromised by the ransomware which can obtain OS-level privilege
    - To solve this problem, we may need to isolate the backup in a lower storage layer (i.e., the flash firmware layer). Checkout the paper "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware" in the recommending reading if you are interested

File System

Applications' view:

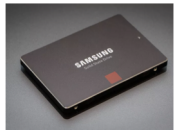
Files (.doc, .pdf, .txt, …)

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

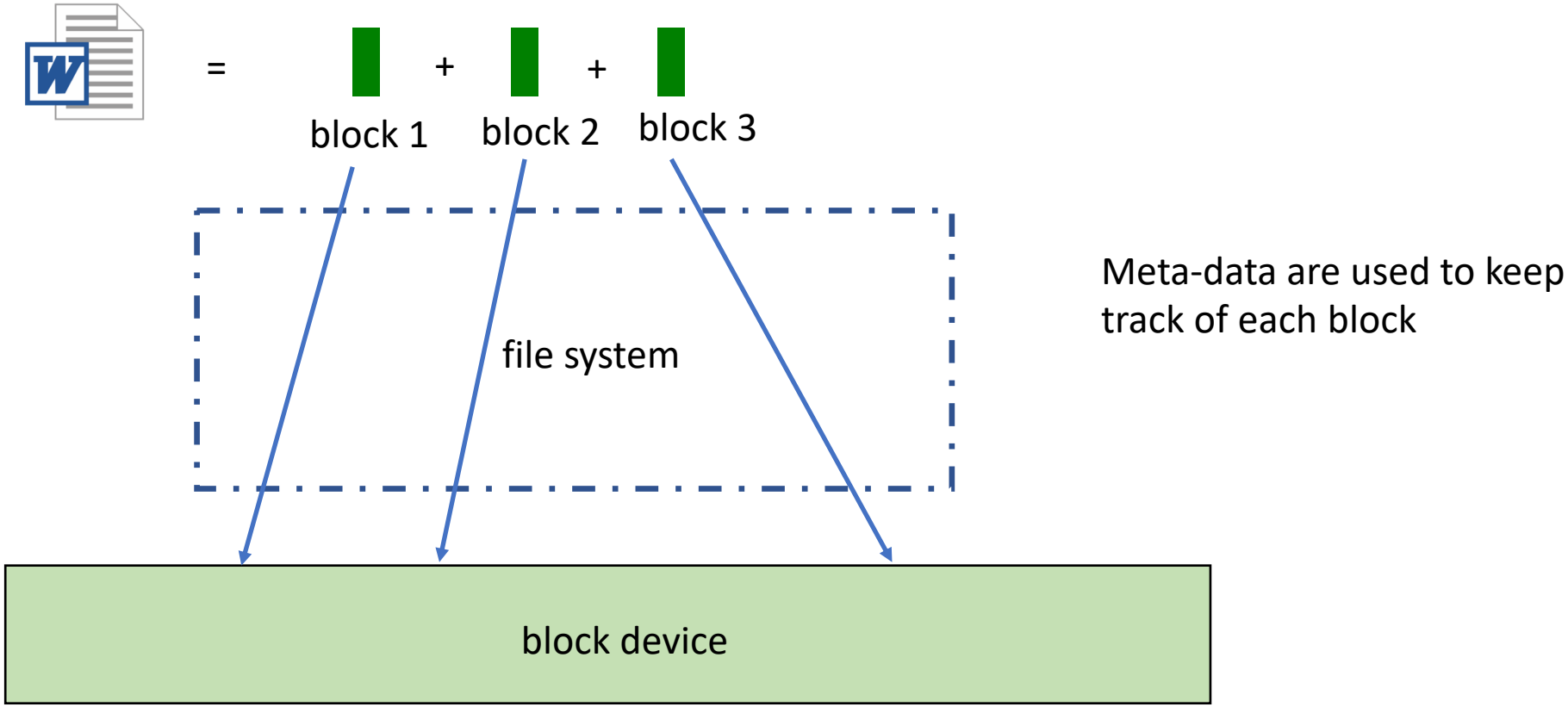
block device interface: allow to read/write a block of any size and any alignment.

Physical storage medium (hard disk, flash, etc)



Main Operations of A File System - Write

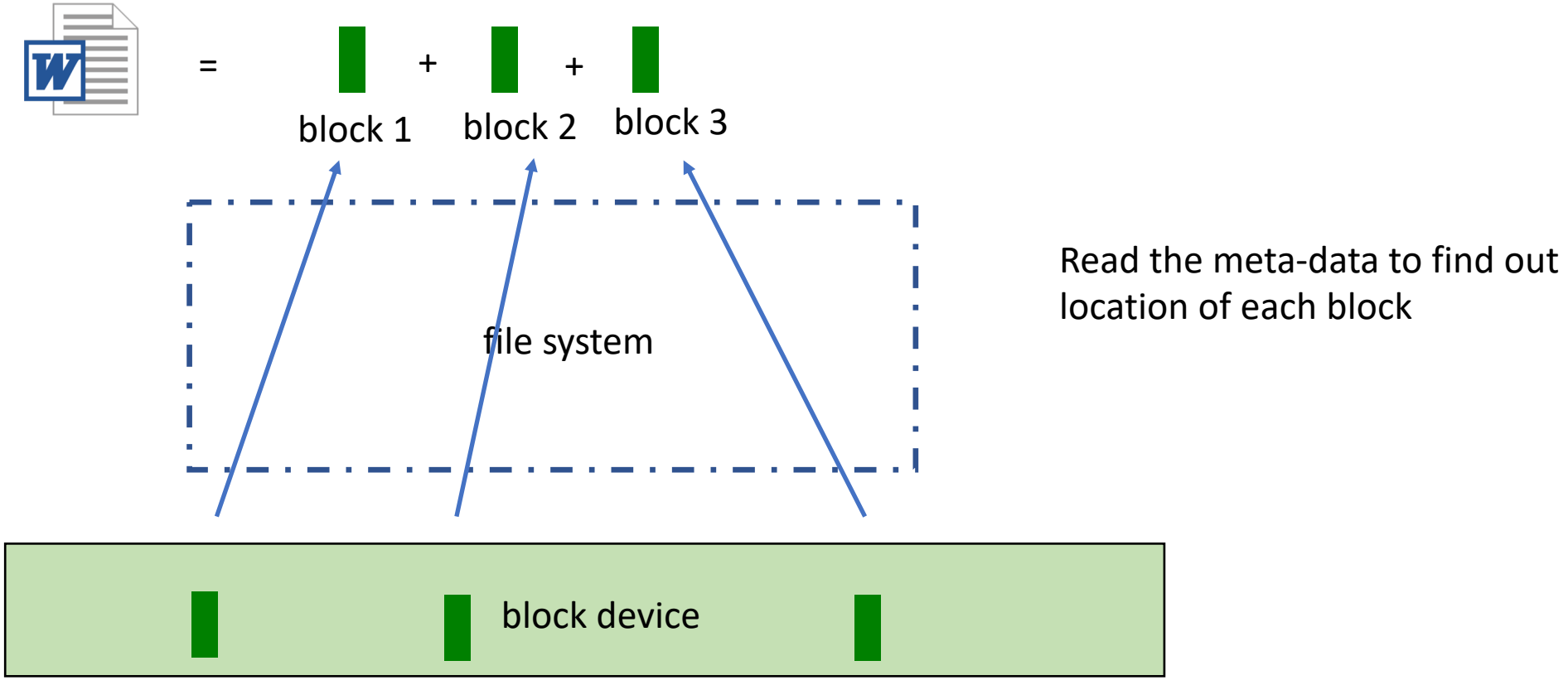
Applications' view:



Meta-data are used to keep track of each block

Main Operations of A File System - Read

Applications' view:



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

Copy-On-Write (COW)

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

- Copy-On-Write in the file system: Multiple processors read the same file, and only one copy of the file needs to be maintained in the memory. Only after 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 this for ransomware data recovery?

The Efforts of My Research Group on Recovery from Ransomware/Malware Attacks

- 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 Andrew Brusso