Ransomware Defense via File System Forensics and Flash Data Extraction

Niusen Chen, Josh Dafoe, Bo Chen
CS Department, Michigan Technological University (MTU)
MTU Security and Privacy (SnP) Lab
https://snp.cs.mtu.edu
https://cs.mtu.edu/~bchen

Ransomware

- A piece of special malware that infects a computing device and restricts access to it/its files
- Crypto-ransomware encrypts the data, and ransom needs to be paid to obtain the decryption key

- Ransomware began to rise again by the end of 2022, with Q4's attack volume reaching 154.9 million — the highest since Q3 2021.

https://www.sonicwall.com/2023-cyber-threat-report/?elqCampaignId=13998&sfc=7013h000000MiQZAA0&gclid=CjwKCAiAgbiQBhAHEiwAuQ6BkmbfNdHZWbIdJBPGBn4ut4T3yR5wDxM6JrGQbSMPEUk4O5ClyAmcVxoC7MsQAvD_BwE

Existing Ransomware Defense Strategies

- Ransomware detection
  - Some of the data is still encrypted before the ransomware is detected and blocked
- Data recovery via decryption key
  - Pay for the ransom to obtain the key (costly and no guarantee)
  - Extract the key locally (unreliable)
- Data recovery via remote backups
  - Extra cost (storage, bandwidth) for remote backups
  - Victims may be lazy and may not backup their data remotely
  - Remote backups may not synchronize timely with the local data

Our Ransomware Defense - FFRecovery

Local data recovery

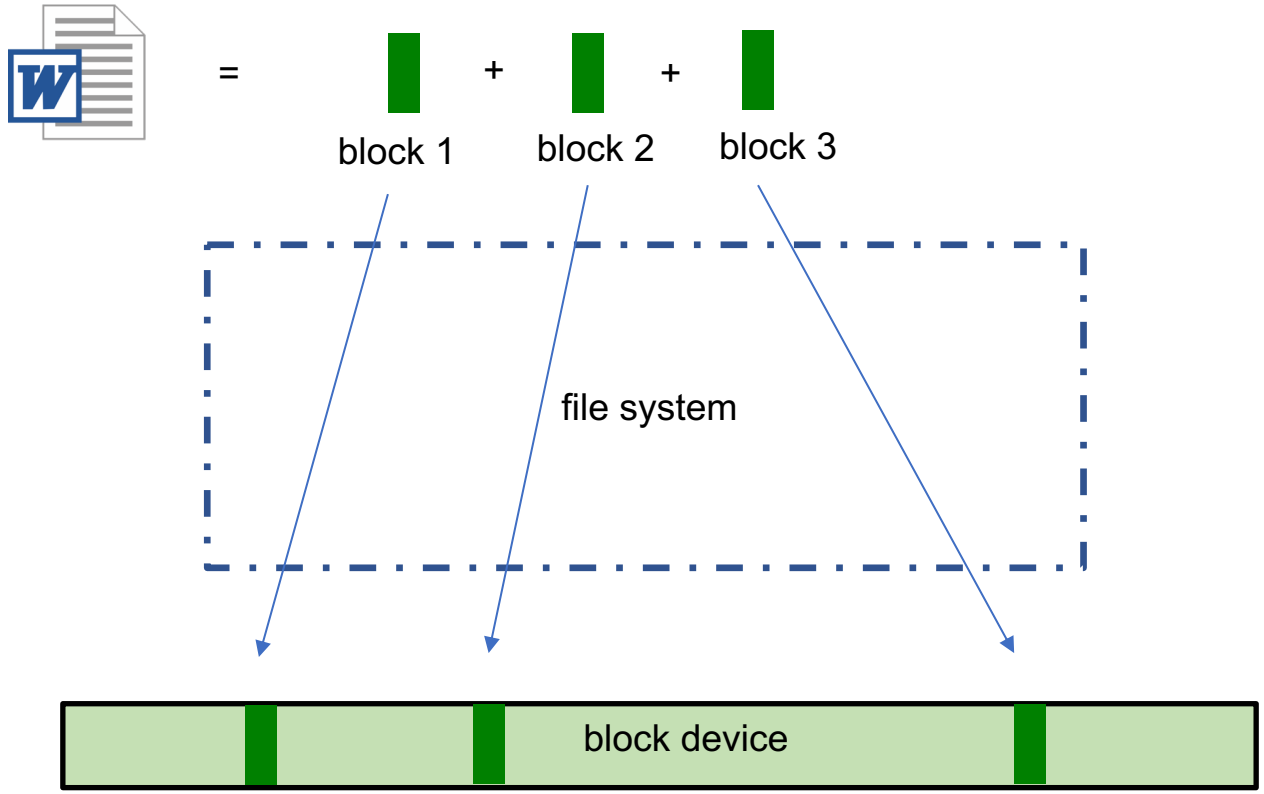
- Do not need to obtain the decryption key
- Do not need to rely on remote backups

Key insights:

- Rely on the special nature of local flash memory storage to preserve the original file data
- Rely on the file system forensics to restore the file system metadata

File System

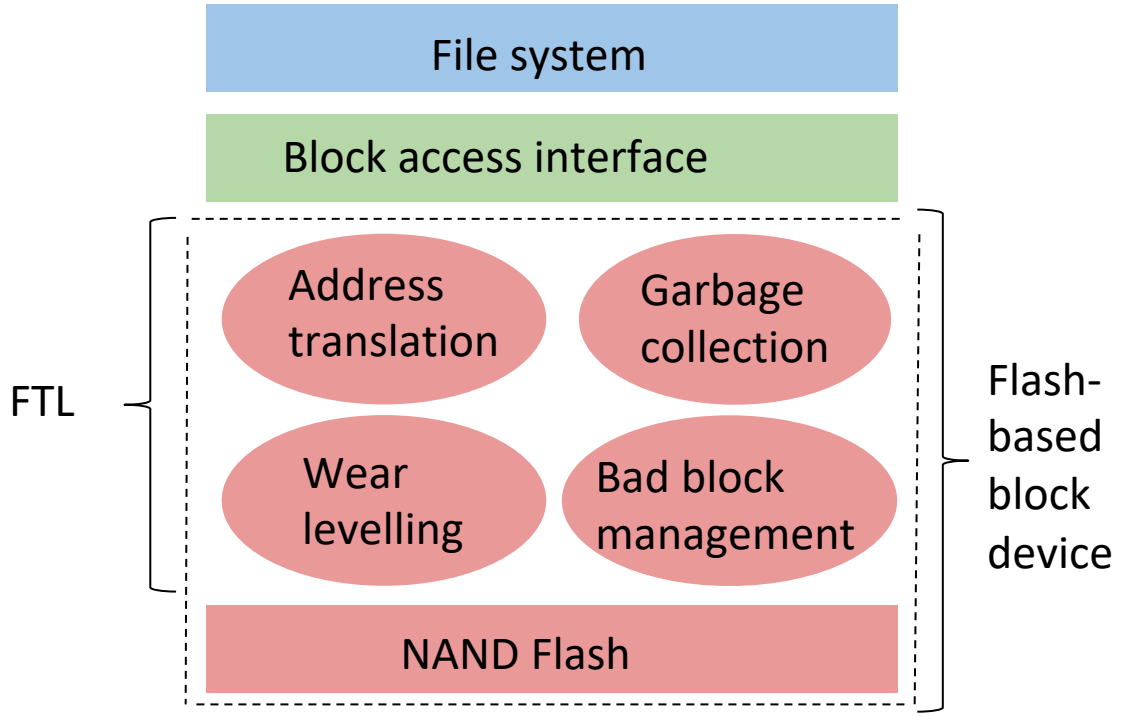
- Provide a mechanism for the OS to organize data
- The user views data as files
- Split into data and metadata sections
  - Metadata provides file location and other information



File system metadata is used to keep track of each file block on the disk

Flash Translation Layer (FTL)

- It is flash firmware embedded into main-stream flash storage devices
- It can handle the special characteristics of NAND flash and emulate the flash storage as a regular block device
- It performs out-of-place updates
- It implements unique functions:
  - Address translation
  - Garbage collection (GC)
  - Wear leveling
  - Bad block management



A flash-based storage system

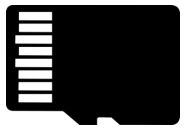
System and Adversarial Model

System Model

- We consider a computing device which is equipped with a flash-based block device
  - Servers, personal computers, mobile devices, etc.

USB sticks

solid state drives (SSD)



SD/miniSD/ microSD cards

Adversarial Model

- Ransomware encrypts user data and demands ransom
- Ransomware can only gain user-level privileges
  - Cannot compromise the OS

Design Overview of FFRecovery

- Step 1: restore file metadata
  - Use file system forensics to restore the file metadata even when the file is deleted/overwritten
- Step 2: restore file content
  - Maintaining original file content and ensuring its recoverability: due to the out of place updates performed in a flash storage medium, the data overwritten at the file system is not immediately deleted by the FTL
- Recover a file after ransomware attacks by combining both its restored file metadata and file content

Forensics-based File Metadata Restoration

Type I: Overwritten Files

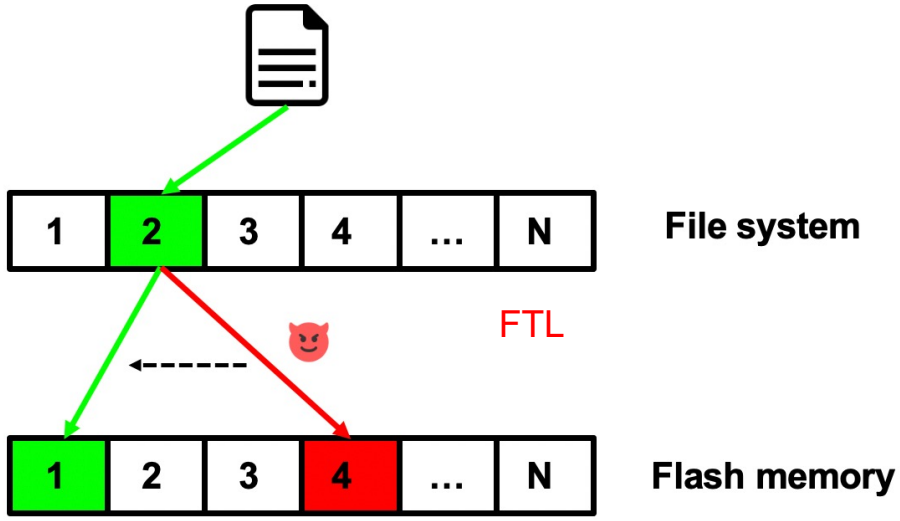
- The logical file location is unchanged
- This location can be found by finding the metadata associated to the file

Type II: Deleted Files

- In non-journaling filesystems, the file location is in the original metadata structure
- In journaling filesystems, the file location is zeroed out, but the changed metadata is maintained in the journal

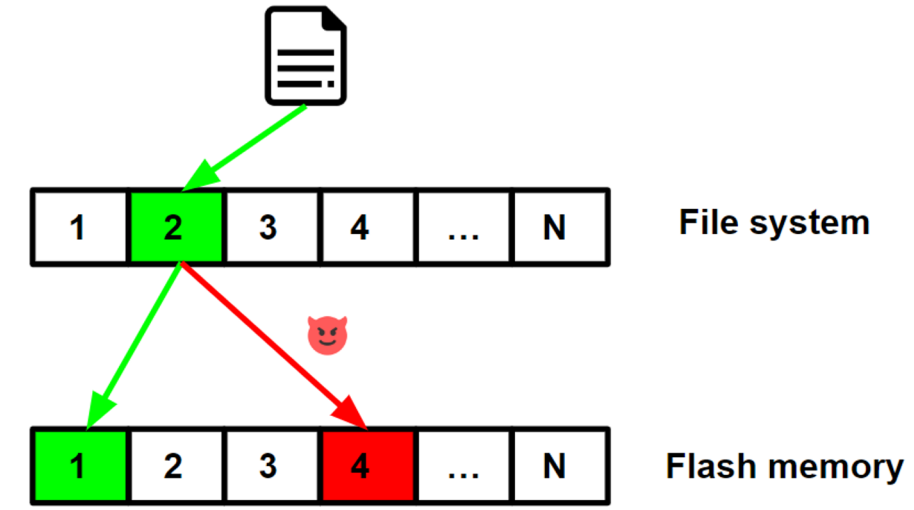
Flash Memory-based File Content Restoration

- FTL performs out-of-place updates
  - After the ransomware corrupts file block 2, the corrupted content will be written to a new flash memory location 4
  - The original content is invalidated but temporarily preserved at flash location 1
- The original content stored at file block 2 can be restored:
  - Maintaining the raw flash data stored at the flash location 1
  - Maintaining the mapping (2->1) between the file system and the flash memory



Ensuring File Content Is Recoverable

- Garbage collection (GC) in the FTL ultimately will reclaim the invalidated content
- We delay the garbage collection on the invalidated content
  - We introduce T_{delay}, a time by which to temporarily freeze GC on the invalid block
  - When a block is invalidated, it waits at least T_{delay} to be reclaimed



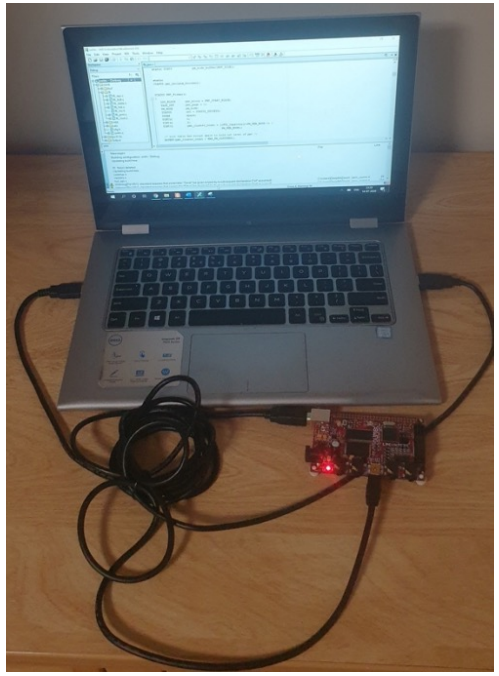
Ensuring Mappings Can Be Rolled Back

- Mappings between the file system and the flash memory are changed during the ransomware corruption
- Unlike the flash memory data, each mapping is much smaller in size, and relying on the out-of-place update and the delayed garbage collection to recover it would be cumbersome
- We reserve a special area in the flash memory to save the affected mappings
  - Upon changing a mapping, its original mapping will be saved to this area
  - The special area hence contains mappings for the latest invalidated data
- Optimization: caching multiple affected mappings and committing them in a batch

Implementation

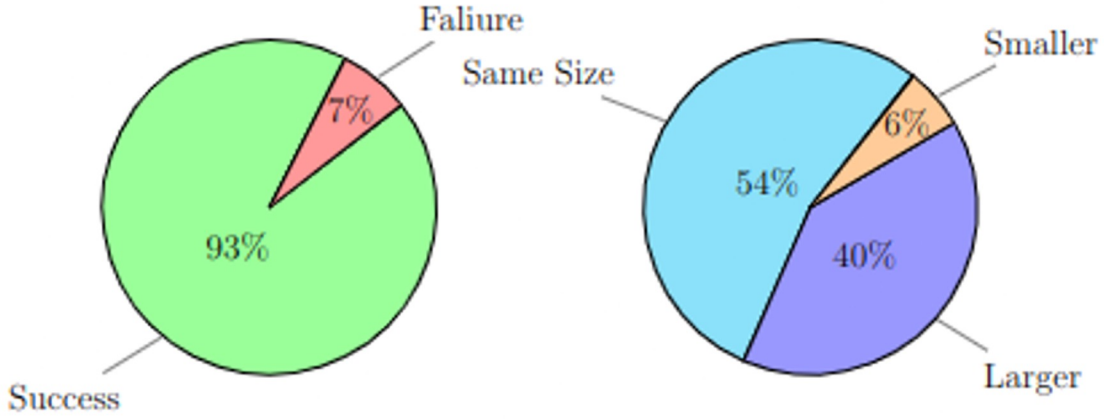
- Windows virtual machine was used in the host computing device
  - FAT16 was used as the file system
- Modified the open-source FTL firmware OpenNFM, and ported the modified firmware to LPC-H3131 development board
  - Used as a flash storage device with our modified FTL firmware

- Developed a filesystem forensics tool using python3



Recovery Rate

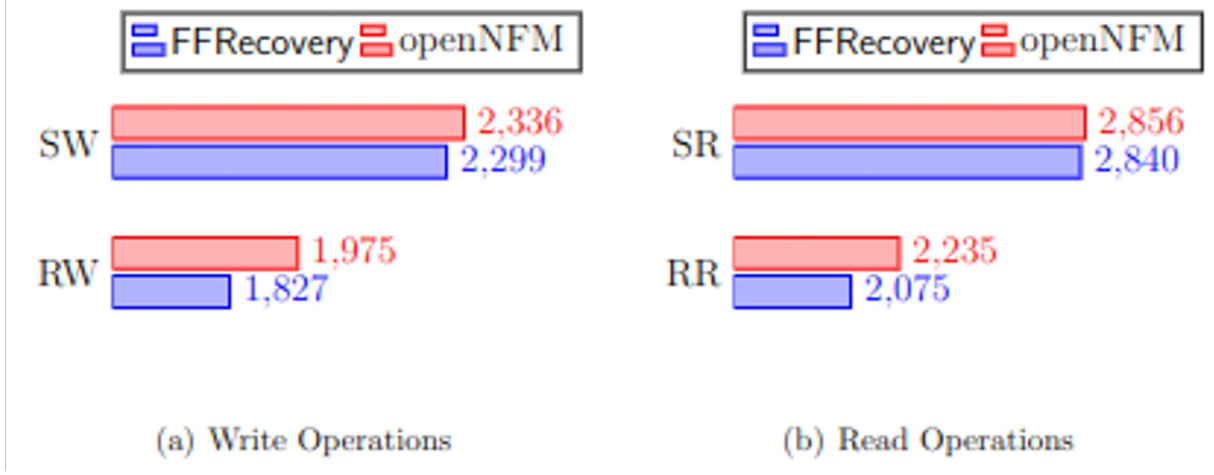
- 100 real ransomware samples were tested
  - The victim file was successfully restored after being attacked by 93 ransomware samples
  - Recovery failed with 7 samples due to blocking prevention, or acting as both locker and crypto ransomware



Throughput Impact

- We used FIO to measure the throughput of FFRecovery and the original flash firmware OpenNFM
  - Sequential write (SW), random write (RW), sequential read (SR), and random read (RR)

- Throughput impact on different I/O patterns is small



(a) Write Operations (b) Read Operations

References

- Chen, Niusen, Josh Dafoe, and Bo Chen. "Poster: Data Recovery from Ransomware Attacks via File System Forensics and Flash Translation Layer Data Extraction." In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp. 3335-3337. 2022.