FlashGuard: Hardware-Assisted Recovery Against Encryption Ransomware

Jun Xu, Xinyu Xing, Peng Liu
The Pennsylvania State University

Jian Huang, Moinuddin K. Qureshi
Georgia Institute of Technology

jxx13@ist.psu.edu

Abstract

Encryption ransomware is a special kind of malicious software that infects user computers through the same means as other malware, and then quietly scrambles users files, making them unreadable. By the time of discovering the problem, victims are demanded to pay a fee for the decryption key that will make their files usable again. According to an FBI tally, ransomware attacks cost their victims a total of $209 million in the first three months of 2016, a stunning surge upward from $24 million in all of 2015.

To mitigate ransomware attacks, pioneering defense systems mainly focus on ransomware detection which watches for the low-level behavior ransomware engages in reading data from many documents and then overwriting them with encrypted contents. Similar to anti-virus software, these systems are usually vulnerable to evasion. For example, many ransomware variants run with the kernel privilege, which allows them to terminate any defense systems.

In this work, we propose FlashGuard, a firmware-level recovery system that allows victims to offset the damage to their data resulting from encryption ransomware. More specifically, FlashGuard takes advantage of the characteristics of Solid State Drives (SSD), and holds the data potentially encrypted by ransomware. We experimented FlashGuard with a large number of manually labeled ransomware samples. We show FlashGuard can efficiently restore files encrypted by ransomware. In addition, we demonstrate FlashGuard introduces negligible overhead to regular I/O operations, and has trivial impact on SSD lifetime.

Keywords
Encryption ransomware, Recovery system, SSD

RSA Conference Security Scholar

FlashGuard: Hardware-Assisted Recovery Against Encryption Ransomware

Jian Huang*, **Jun Xu****, Xinyu Xing**, Peng Liu**, & Moinuddin K. Qureshi*
*Georgia Tech & **The Pennsylvania State University

Problem Statement and Goals

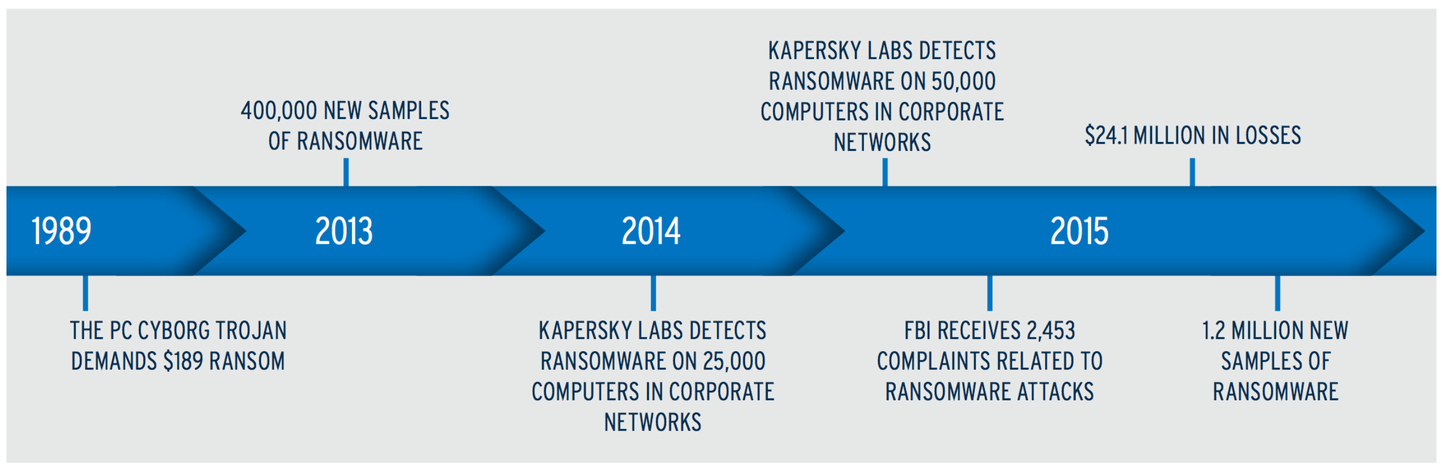


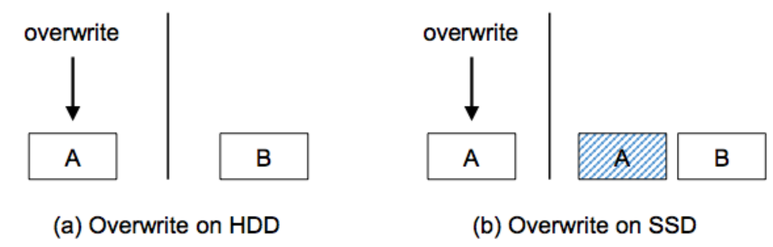
Figure 1. A rapidly growing threat: Ransomware

- **FlashGuard** - A defense against encryption ransomware
- **Goal** - Efficiently and reliably recover the data locked by encryption ransomware

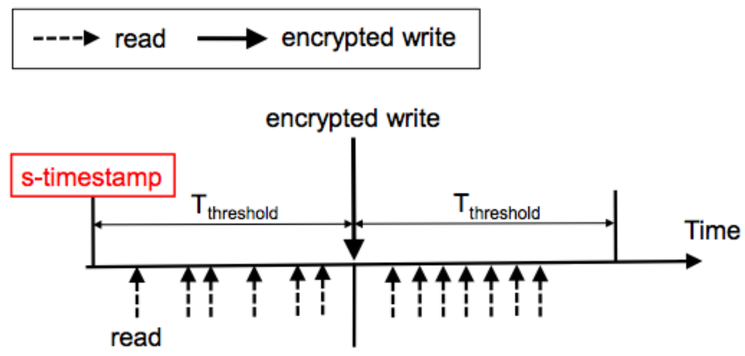
Approach

- SSDs perform out-of-place update and periodic garbage collection to free blocks taken up by stale data
- FlashGuard prevents garbage collection on **blocks potentially encrypted by ransomware** — *Blocks that have been read in a time window during which a write with encrypted data occurs*
- On confirmation of infection, FlashGuard recovers blocks preserved from garbage collection

Out-of-place update on SSD — Place new data in a new block

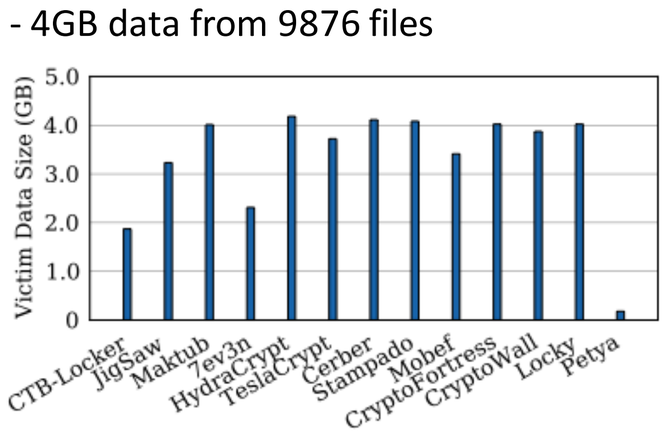


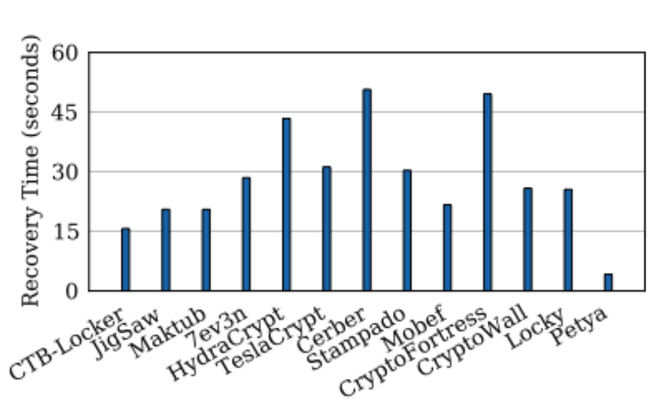
Preserve blocks read in a time window during which a write with encrypted data occurs

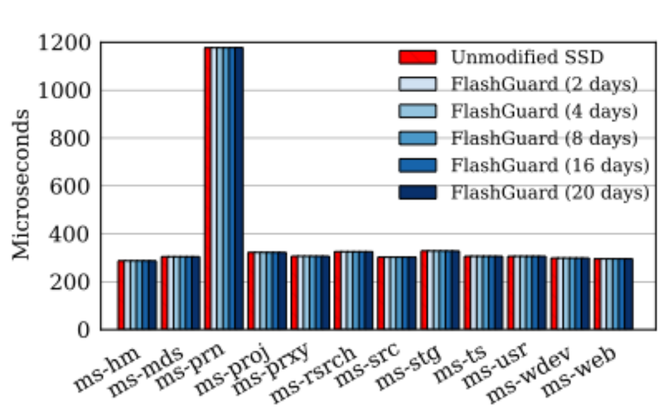


Results

- Evaluation
  - 1,477 samples from 13 families
  - 4GB data from 9876 files







- Future Work
  - Better strategy to select blocks to preserve
  - Reduce performance overhead
- Reference
  - LogRhythm, Inc. (2016). “The Ransomware Threat: A guide to detecting an attack before it’s too late” Retrieved from http://resources.idgenterprise.com/original/AST-0167615_WP_601_Ransomware_Guide_A4_WEB.PDF