SGX-SSD: A Policy-based Versioning SSD with Intel SGX

Jinwoo Ahn†, Seungjin Lee†, Jinhoon Lee†, Yungwoo Ko†,
Donghyun Min†, Junghee Lee‡, Youngjae Kim†

†Sogang University, Republic of Korea,
‡Korea University, Republic of Korea

SOGANG UNIVERSITY

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

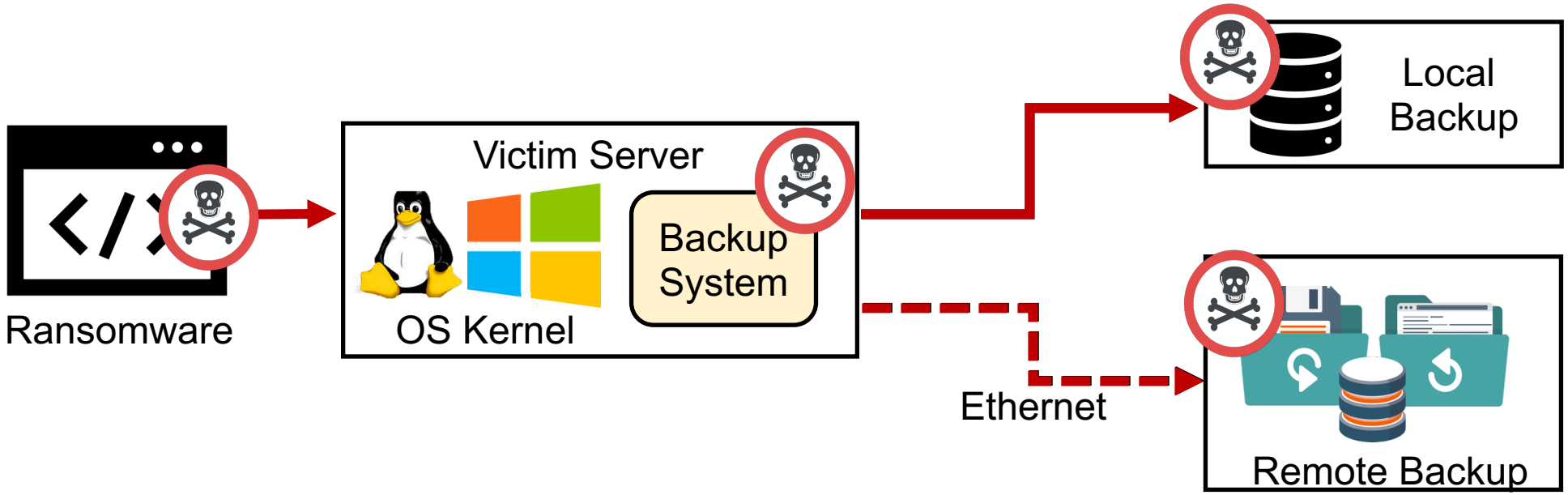
HotStorage '20

서강대학교
SOGANG UNIVERSITY

Motivation: Malware's Data Tampering Attack

Problem: Ring-0 level rootkit malware's data tampering attack

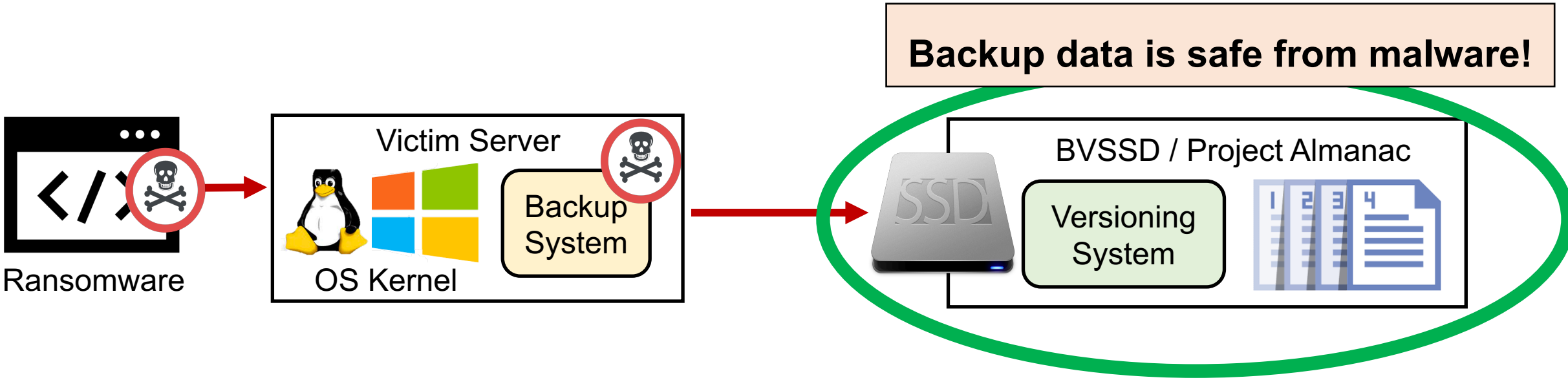
- It enhances the privilege of victim, and compromises software-based backup system.
- It finds and destroys victim's local or remote backup data.



Motivation: Malware's Data Tampering Attack

Existing Solution: Versioning SSD **[BVSSD, Systor 12], [Project Almanac, Eurosys 19]**

- Versioning SSD implements versioning system in SSD firmware.
- SSD firmware is isolated from host server.
- Even if OS is compromised, it is impossible to destroy backup data.



Motivation: Integrity vulnerability of Versioning SSD

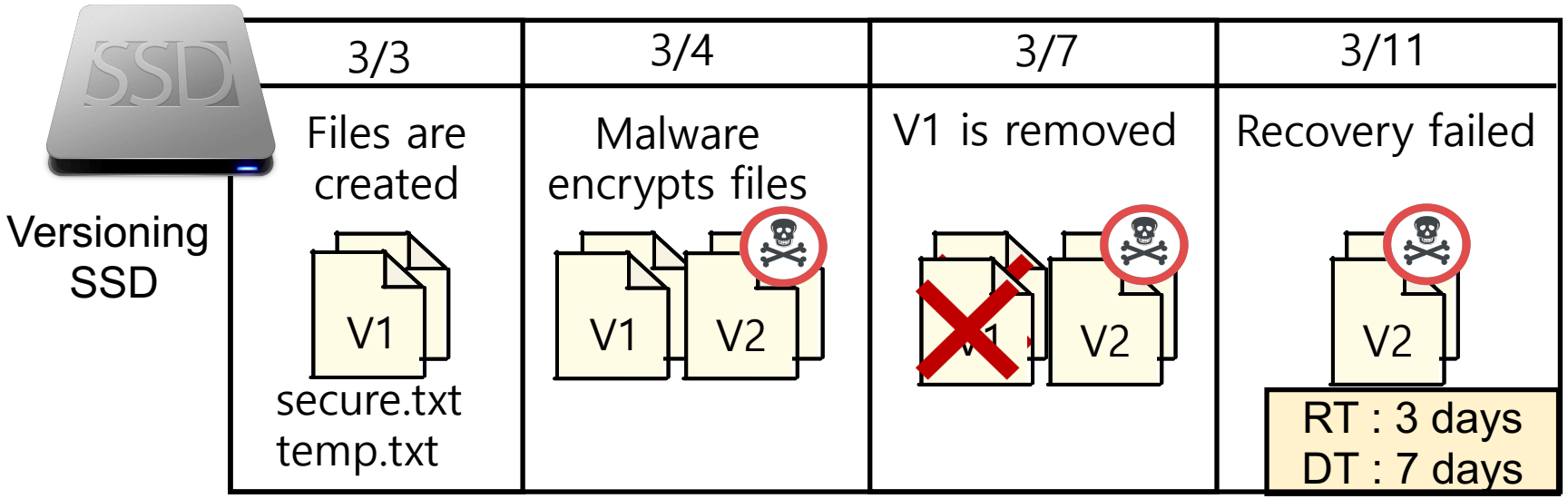
Versioning SSD preserves all file data for a ***fixed retention time(RT).***

- Space overhead extremely increases as all files are backed up regardless of the importance.
- To free up space, Versioning SSD aggressively erases old backup data in a way that limits RT.

Dwell Time: A period that the malware stays undetected in victim system

Integrity vulnerability occurs when:

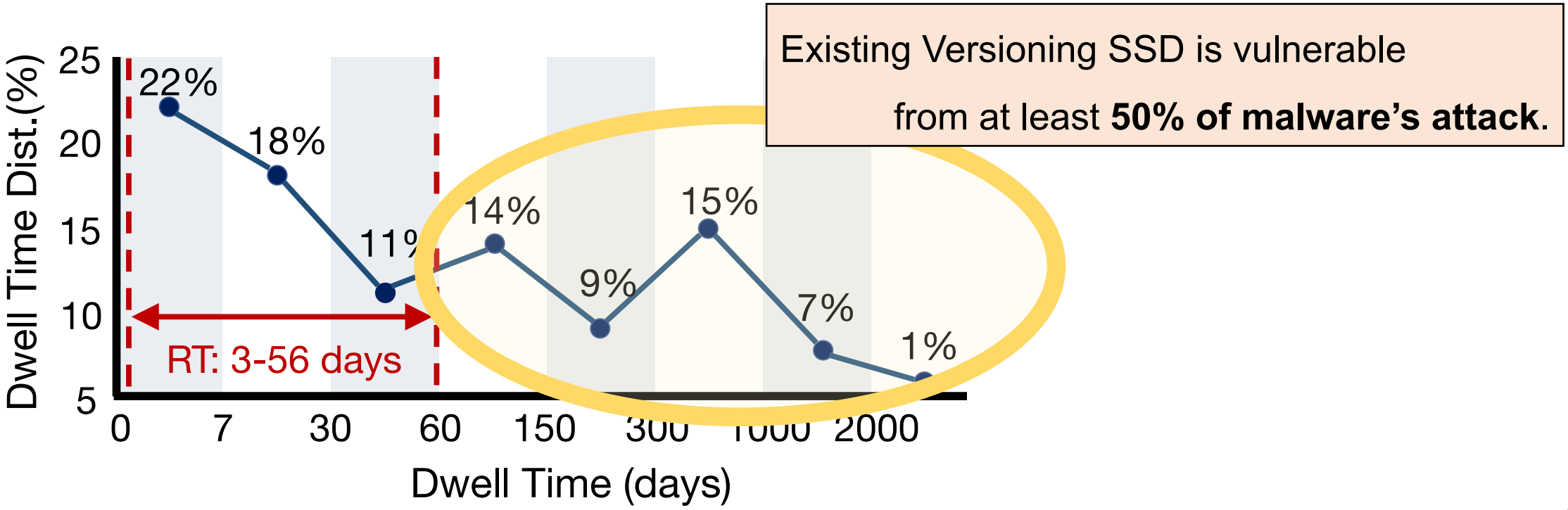
Malware Dwell Time (DT) > Versioning SSD Retention Time (RT)



Motivation: Integrity vulnerability of Versioning SSD

Malware's average DT is longer than the RT of Versioning SSDs.

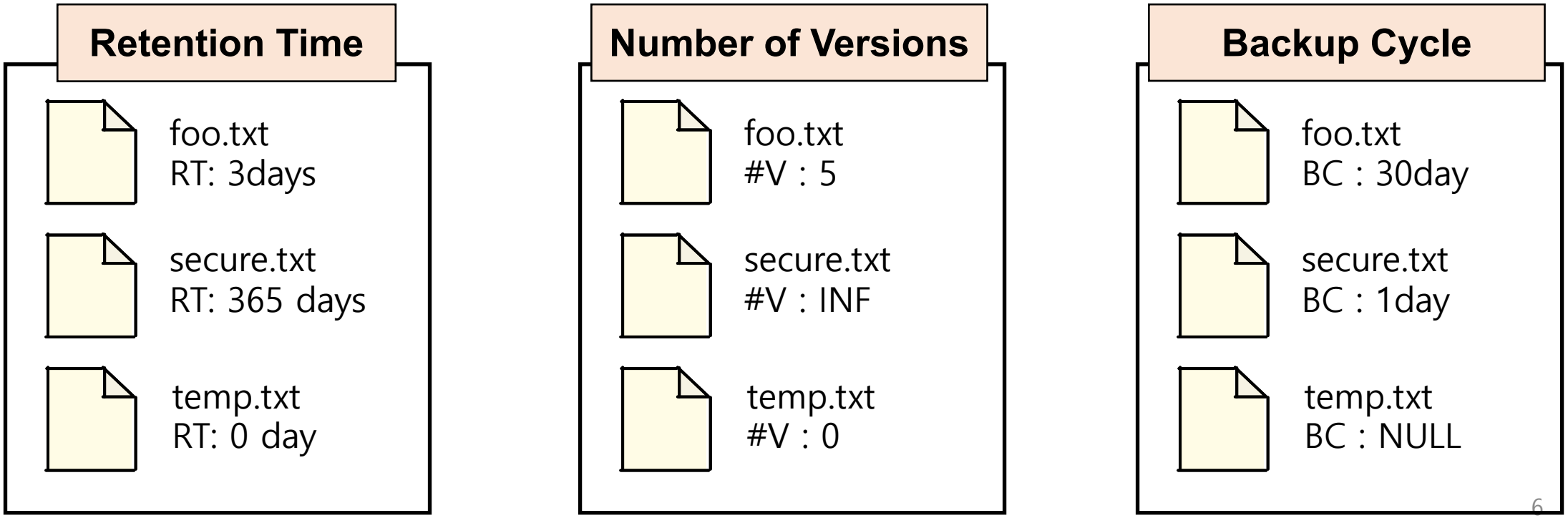
- Project Almanac provides 3-56 days of RT depending on the workload's write intensity.
- However, more than 50% of malware has a DT of 60 days or more.



Motivation: Keeping deeper history for important files

SGX-SSD: Policy-based per-file versioning SSD

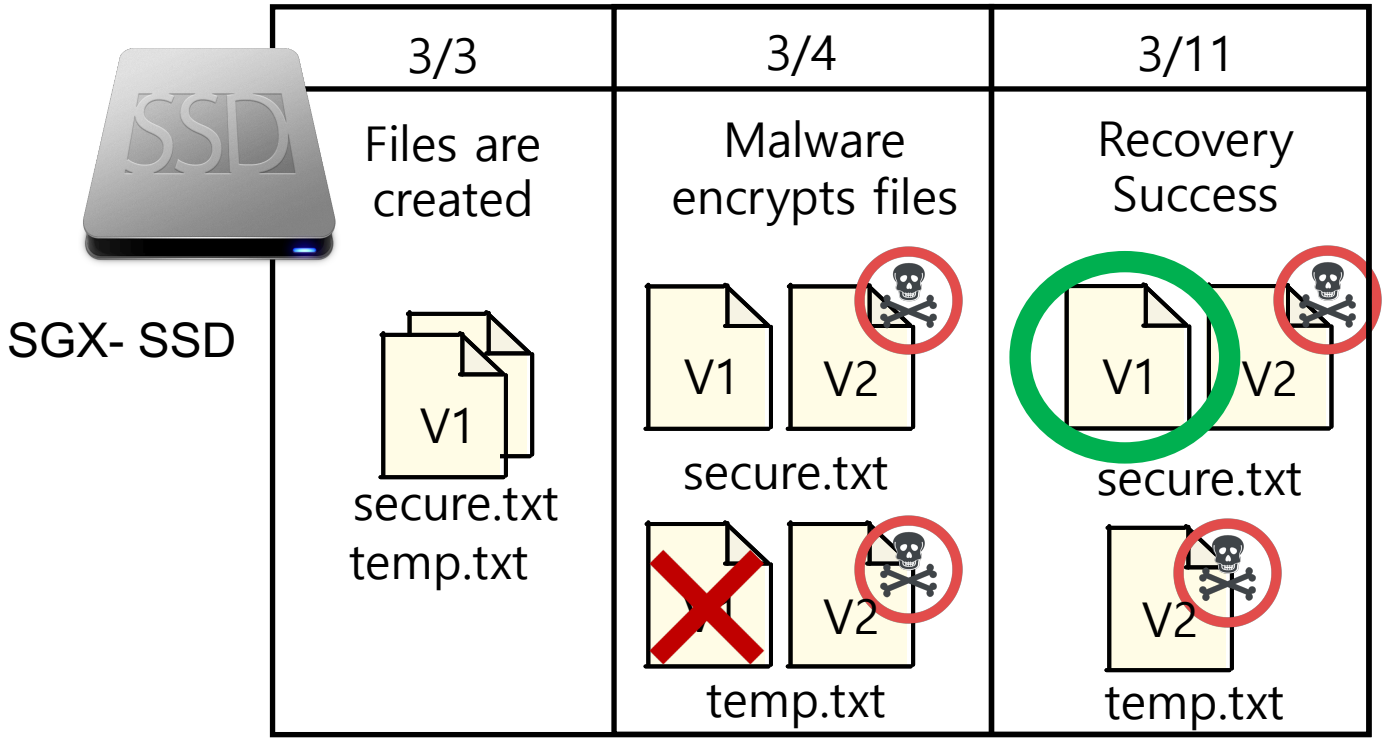
- Each file version is maintained according to policy set by users.
- We defined 3 types of policy a user can set.
- SGX-SSD minimizes the space consumption for versions to keep deeper history for important files.



Motivation: Keeping deeper history for important files

SGX-SSD guarantees integrity from malware with long DT.

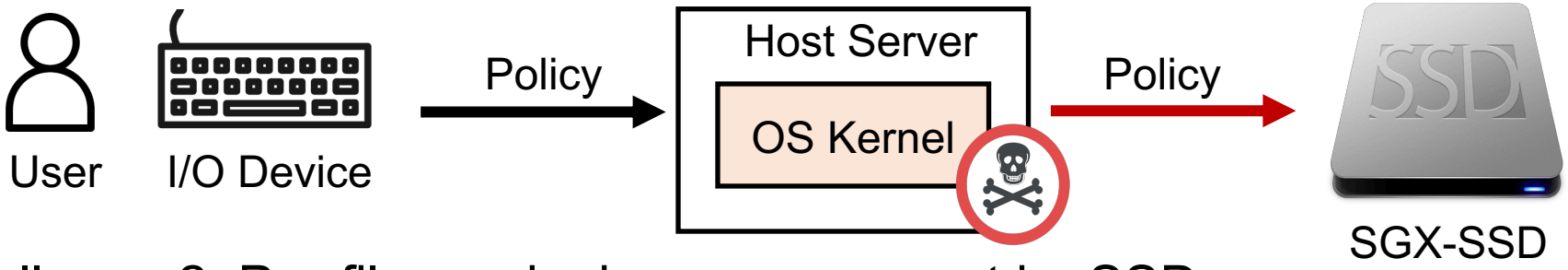
- Malware DT: 7days, RT of secure.txt: 30days, RT of temp.txt: 0day



Design Challenge: SGX-SSD

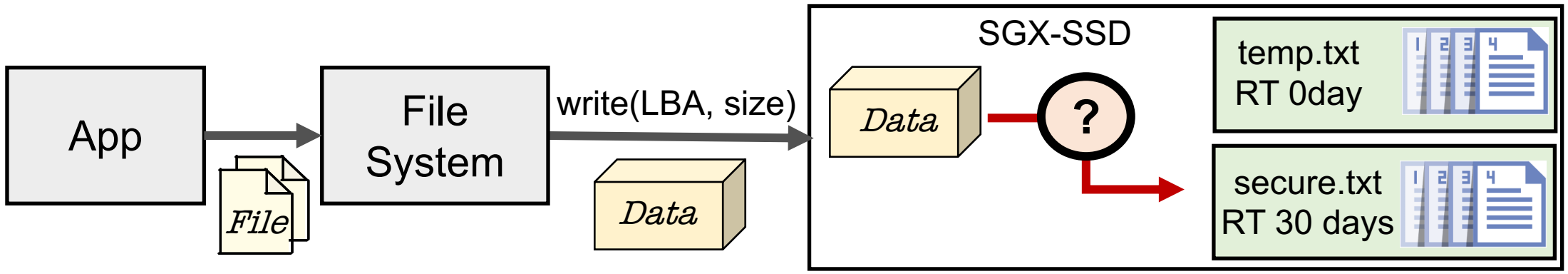
Challenge 1: Secure Host Interface on Compromised OS

- How can the policy request entered by a user be safely delivered to the SSD?



Challenge 2: Per-file versioning management by SSD

- How can SSD recognize the file semantics corresponding to each block?



Summary

- We defined the integrity vulnerability of the existing Versioning SSD.
- To solve this, we proposed a per-file versioning implementation in SSD firmware.
- By solving the aforementioned two challenges, the integrity of the file can be selectively guaranteed even if the OS is compromised.
- Detail of SGX-SSD can be found at [https://arxiv.org/abs/2004.13354].

SGX-SSD: A Policy-based Versioning SSD with Intel SGX

Jinwoo Ahn

jinu37@sogang.ac.kr

SOGANG UNIVERSITY

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

HotStorage '20

서강대학교
SOGANG UNIVERSITY