LOG8415
Advanced Concepts of Cloud Computing

Foutse Khomh
S. Amirhossein Abtahizadeh
Département Génie Informatique et Génie Logiciel
École Polytechnique de Montréal, Québec, Canada
`foutse.khomh[at]polymtl.ca`
`a.abtahizadeh[at]polymtl.ca`

1 Identification

Student's name: Chun-An Bau

Date of the reading note: Oct 28, 2021

Author(s): Zeyu Mi, Haibo Chen, Yinqian Zhang, Shuanghe Peng, Xiaofeng Wang, and Michael Reiter

Title of the article: CPU Elasticity to Mitigate Cross-VM Runtime Monitoring

Publication: 2020 IEEE Transactions on Dependable and Secure Computing

2 Article

Keywords: Cross-VM runtime monitoring, Defense, Cloud environment, CPU resource elasticity

Concepts and definitions:

- Cross-VM runtime monitoring (CRUM): Attack VM continuously collects private information from the target VM that stays in the same physical machine when it is running a program.
- CPU Resource Elasticity as a Service (CREASE): VM running a critical task with a higher clock rate for a short period. Therefore, the amount of information derivable from the side channels goes down quickly, which benefits the VM.

Summary:

Although virtual machines seem to be an isolated environment, it suffers from side-channel attacks. Previously, there were considerable researches regarding preventing the attacks. However, none of them are adequate since they either focus on a specific type of threat or require platform changes.

The authors present a novel solution, CREASE, to deal with the difficulty. When the target VM runs a critical task, it will first increase its clock rate and slow down the suspicious VM's. Doing so reduces the attacker's sampling rate and increases the difficulty of collecting data, which can achieve the goal of protection.

Research contributions:

Present CREASE, a new technique to defend against cross-VM runtime monitoring.

- Reduce the cost of continuously monitoring peers without interfering with their operations.
- Both practical and lightweight, incurring small overheads for both the principal and the peer.

3 Analysis

Quality:

General organization:

□ Very good;

■ Good;

□ Medium;

□ Bad;

□ Very bad.

Language and style:

□ Very good;

■ Good;

□ Medium;

□ Bad;

□ Very bad.

Technique:

■ Very good;

□ Good;

□ Medium;

□ Bad;

□ Very bad;

□ N/A.

Bibliography:

□ Very good;

■ Good;

□ Medium;

□ Bad;

□ Very bad;

Forces of the message:

- Novel solution of CRUM attacks with acceptable overhead.
- Discuss plenty of related works that stand in distinctive layers, like hardware, software, or operating system.

Weaknesses of the message:

- It would be more convincing if the evaluation could involve some real-world scenarios, like reproducing CVE projects and showing CREASE's protection ability.

Future directions:

- Develop more detailed algorithms or procedures to let the industries adopt the solution.
- If more than one (or even a lot) VMs want to run credential tasks, how to handle the starvation of resources?

Other important articles:

- Wait a Minute! A fast, Cross-VM Attack on AES
  RAID 2014: Research in Attacks, Intrusions and Defenses pp 299-319
- One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation
  Proceedings of the 25th USENIX Conference on Security SymposiumAugust 2016 Pages 19–35