LOG8415
Concepts avancés en infonuagique

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

October 27, 2021

1 Identification

Student's name: Yanis Toubal

Date of the reading note: n.d.

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: Z. Mi, H. Chen, Y. Zhang, S. Peng, X. Wang and M. K. Reiter, "CPU Elasticity to Mitigate Cross-VM Runtime Monitoring," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 1094-1108, 1 Sept.-Oct. 2020, doi: 10.1109/TDSC.2018.2846742.

2 Article

Keywords: Virtual Machine, Cross-VM runtime monitoring, CPU elasticity, Cloud service, Cloud security

Concepts and definitions:

- Virtual Machine (VM): Virtualization of a computer system that provide the same functionalities as a physical computers by using software. It runs it's own operation system independently of the host machine or other virtual machines.
- CPU elasticity: Ability to supply CPU power on demand based on the workload.

- Cross-VM runtime monitoring: Type of attack where a malicious VM continuously collect data from a target VM when it's performing an operation.
- Cloud security: Practice of protecting the data, the application and the infrastructure of a cloud-based environment from attacks.
- CREASE: It stands for CPU Resource Elasticity as a Service. It's the security solution agaisnt Cross-VM runtime monitoring that this paper puts forward. It consists of attributing a higher frequency to a VM that performs a security-critical operation for the duration of the operation at the cost of other VMs frequency.

Summary: This article present a new security technique that provides a protection agaisnt Crum type of attacks. It expands on the research that lead to this technique, it explains how it works and why its efficient and it talks about its limits.

With the increasing popularity of cloud services, security is getting more and more important for cloud providers. One of the most important service namely virtual machines have been found to be vulnerable to certain attacks. One of those attacks is the Cross-VM Runtime Monitoring (Crum). The goal of this paper is to provide a practical security mechanism agaisnt this type of attack. In the past many other solutions have been put forward, but lacked practical usability.

When designing this solution, they wanted something that was general, elastic and lightweight. The researchers took into account the elastic cloud business model, a broad set of Crum attacks and the most important informations to protect in a VM when designing their solution. CREASE is the name of the solution that they came up with which is an increase in CPU allocation given to the VM that is performing a security-critical operation that is taken from other VMs.

The proposed solution was subject of a security analysis by the researchers. They modeled the Crum attacks and analyzed some metrics. They concluded that their solution wasn't eliminating the threat completely but made these type of attacks harder to pull. Since their solution requires changes to VM hypervisors, they couldn't test it in a public cloud and instead they ran all the tests locally. They ran numerous tests on this environnement to see the effectiveness and the performance which showed promising results.

Research contributions: This paper gave a new promising solution CREASE to secure VMs agaisnt Crums attacks. The proposed solution is efficient, practical and lightweight.

The solution is elastic which gives a lot of flexibility to the cloud provider aswell as the user. The solution is based on clock-rate (CPU) and use a detection technique for suspicous activity from other VMs to see if a protection is necessary. These approaches haven't been used together before this paper.

The authors of the papper also provided an in-depth evaluation of an implementation of the solution. They coded the solution and setup an environment where they extensively tested it.

3 Analysis

Quality:

General organization:	Language and style:	Technique:	Bibliography:
☐ Very good;	☐ Very good;	☐ Very good;	☐ Very good;
☒ Good;	☒ Good;	☒ Good;	☒ Good;
☐ Medium;	☐ Medium;	☐ Medium;	☐ Medium;
☐ Bad;	☐ Bad;	☐ Bad;	☐ Bad;
☐ Very bad.	☐ Very bad.	☐ Very bad;	☐ Very bad;
		☐ N/A.	

Forces of the message:

- The language used was very appropriate and most of the technical terms were precisely defined by the authors which made the text easier to comprehend.
- The authors explained in-depth their solution along with it's limitations which shows a great understanding of the topic.
- The evaluation of the solution is very detailed and illustrated with many graphs which show the efforts they made to evaluate their solution.
- The authors talked many times about other related solutions and refer to many other research papers related to their topic which shows a good variety of point of views that added to the quality of the text.

Weaknesses of the message:

- Very few visual supports have been used which made the text less interesting and harder to understand.
- Some sections, namely section 2 and 4, are really short and lack details compared to the other sections which made the reading less fluid and less detailed.
- The solution wasn't tested in a public cloud which makes it less credible and less complete.

Future directions: This article provides a new potential solution to protect VMs agaisnt Crums attacks that could be used by cloud providers.

This new technique could be very helpful for renforcing the cloud security of cloud providers.

Trying it in a public cloud setting could be helpful to see better see it's potential and possible flaws. Studying more possible attacks could also be helpful to see it's effectiveness.

This study shows a very promising solution which could have important financial impacts for both cloud providers and clients. A good point to explore would be the economical aspect of it in a cloud service setting.

Other important articles:

- Fine grain cross-VM attacks on Xen and VMware are possible!
  Technical Report 2014/248, IACR Cryptology ePrint Archive
  Apr. 2014

- Seriously, get off my cloud! cross-vm rsa key recovery in a public cloud.
  Cryptology ePrint Archive, Report 2015/898
  2015

- Wait a minute! A fast, cross-VM attack on AES.
  In Research in Attacks, Intrusions and Defenses – RAID 2014, volume 8688 of LNCS, pp. 299–319, 2014

- Cross-vm side channels and their use to extract private keys.
  In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 305–316, 2012.