PhD Topic
Defense mechanisms against attacks within virtualized infrastructures

Place of work: Orange Labs, Caen, Normandie, France

Advisors: Sylvie Laniepce (Orange) and Jean-Marc Menaud (Ecole des Mines de Nantes)

Start date: October 2017

Funding: CDD Orange 3 years + CIFRE contract between Orange and Ecole des Mines de Nantes

Requirements:

- Master of Computer Science degree or equivalent diploma

- Strong skills both in low layer computer (OS, virtualization, hardware architecture) and in security (intrusion detection technics),

- Fluent in English

- Strong team-working abilities

Application to be sent through Orange.jobs : https://orange.jobs/jobs/offer.do?joid=61241&lang=FR

Context and state of the art:

Current defense technics against attacks strongly inherit from the host-based monitoring model of traditional siloed infrastructures which enables the monitoring of the entire stack from the application layer down to the hardware / software interface.

With clouds, virtualized infrastructures are largely widespread. Virtualized infrastructures draw a virtualization boundary between the virtualizing part (infrastructure part, usually under the control of a cloud operator) and the virtualized part (user domain). Two dominant virtualization approaches currently co-exist: the hardware-level approach for which the virtualization boundary is at the machine hardware interface (hypervisor) and, the operating system-level (OS-level) approach for which the virtualization boundary is high in the stack at the OS / application interface (container). Some research works examine other virtualization boundary alternatives such as i) “mid-level” virtualization boundary based on new object-based storage abstractions [1] or, ii) minimalist virtualization boundary (unikernel monitor) [2].

These last years, research efforts on virtualization have primary concentrated on improving execution performances.

Few efforts have been devoted to exploring the impact and the possible benefits of the placement of the virtualization boundary, on defense technics. This is of importance because the security

monitoring capabilities of both the virtualizing part and the virtualized part strongly depend on the placement of the virtualization boundary, especially for low level operations (system level) monitoring.

For example, for the container-based virtualization approach for which the user domain consists of application processes and the operating system becomes the virtualizing part - i.e. the OS is part of the infrastructure - defense technics based on control-flow integrity in kernel space are no more usable within the user domain but are leveragable at infrastructure level [3]. Similarly, an anomaly detection system based on the analysis of syscalls sequences monitored at the OS level (that is, at infrastructure level) has been proposed [4].

For hypervisor-based virtualization, the user domain stack remains relatively unchanged (compared to non-virtualized infrastructure's one) with full visibility from application layer down to the 'now virtualized' hardware / software interface. One could believe that traditional defense technics operating solely at user domain level fit all the needs. However, introspection technics become more and more promising for offering powerful monitoring capabilities at hypervisor level with valuable advantages in terms of security (isolation, high privilege) [5].

In a world where several possible placements of virtualization boundary exist (virtual machine, container, unikernel) and where others may appear, is it possible to conceive generic infrastructure-delivered defense technics against attacks?

Challenges:

The objective of the thesis is to characterize, for different types of infrastructure virtualization technics, the software abstractions monitorable on each side of the virtualization boundary in order to propose defense mechanisms of the user domains, at infrastructure level and as much generic as possible (in regards to the employed virtualization technic).

This thesis will particularly consider the new opportunities offered at infrastructure level to defense against attacks: isolation, high privilege, user domain cross-view, virtualization-related services such as dynamic resource allocation, etc.

In this thesis, the main challenge to be solved is to conceive defense technics based on observations at low layer (system) of the behavior of the user domains, and as much generic as possible.

Expected results:

- Analysis of the state of the art of virtualization technics and existing defense technics at low layer
- Proposition and specification of intrusion detection and reaction technics at virtualization layer
- Implementation of these technics in prototypes for both hardware (KVM hypervisor) and OS-level (docker) virtualization, to demonstrate their genericity
- Evaluation (detection rate, reaction, genericity)

References:

[1] Van Moolenbroek, D. C., Appuswamy, R., & Tanenbaum, A. S. (2014, June). Towards a flexible, lightweight virtualization alternative. In Proceedings of International Conference on Systems and Storage (pp. 1-7). ACM.

[2] Williams, D., & Koller, R., Unikernel Monitors: Extending Minimalism Outside of the Box. In 8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 16)

[3] Díez-Franco, I., & Santos, I. (2016, October). Feel Me Flow: A Review of Control-Flow Integrity Methods for User and Kernel Space. In International Conference on EUropean Transnational Education (pp. 477-486). Springer International Publishing.

[4] Amr S Abed, Charles Clancy, David S Levy,Intrusion detection system for applications using linux containers, Security and Trust Management, Lecture Notes in Computer Science, vol. 9331, 2015, pp. 123-135

[5] Hebbal, Y., Laniepce, S., & Menaud, J. M. Virtual Machine Introspection: Techniques and Applications. In 10th IEEE International Conference on Availability, Reliability and Security (ARES), 2015