CERIAS

The Center for Education and Research in Information Assurance and Security

An MTD-based Self-Adaptive Resilience Approach for Cloud Systems

Miguel Villarreal-Vasquez,, Pelin Angin, Norman Ahmed and Bharat Bhargava
Department of Computer Science, Purdue University, West Lafayette, IN, USA

INTRODUCTION

- Our proposed Moving Target Defense (MTD) [1, 2] narrows the exposure window of a node to attacks, which increases the cost of attacks on a system and lowers the likelihood of success and the perceived benefit of compromising it.
- ***Virtual Reincarnation***: Virtual machines running a distributed application vanish and completely new virtual machines take their place.

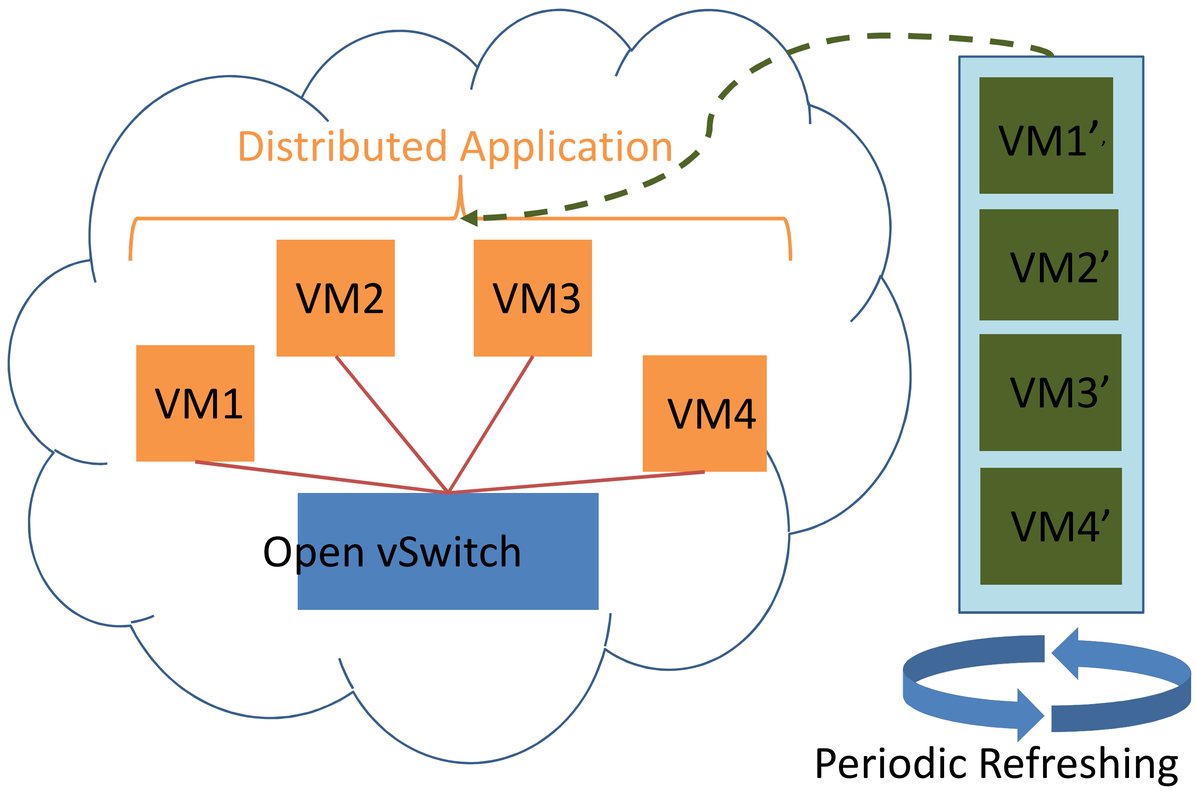

Fig. 1 An MTD-based Self-Adaptive Resilience Approach for Cloud Systems. The target is continuously replaced by a new component with an entire new configuration.

BACKGROUND

- Partition of runtime execution in time intervals.
- VMs run only for a predefined lifespan.
- Proactive monitoring their runtime below the OS

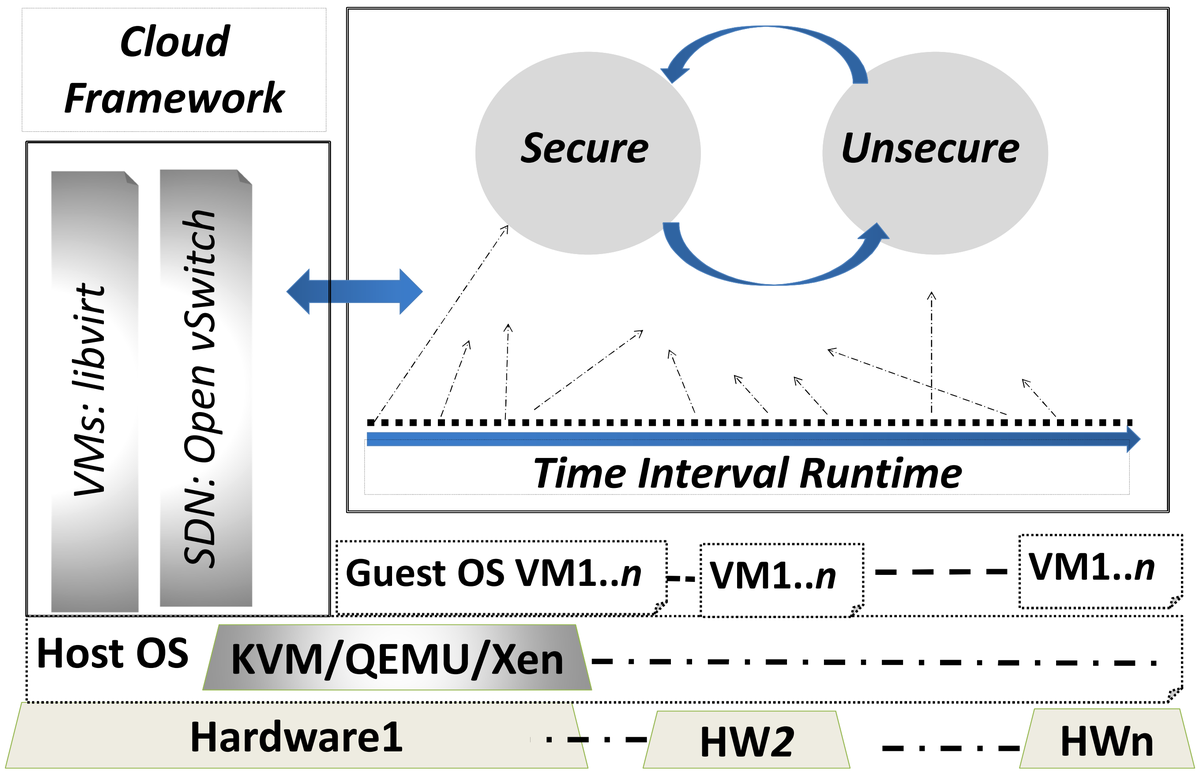

Fig. 2 Moving Target Defense Infrastructure. Vertical bars are the Host OS components: libvirt and Open vSwitch.

HYPOTHESIS AND APPROACHES

- Taking into account the main components of the state of a virtual machine (i.e. memory and network), is it possible to build a generic resilient platform without service interruptions in the reincarnation process?
- Two approaches: Stateful and Stateless replacement

PRELIMINARY RESULTS (STATELESS REPLACEMENT)

1. Reincarnation time of one minute: VMs are created on the fly.
2. Reincarnation time of 20 seconds: VMs are created in advance.
3. Trade off between security and performance.

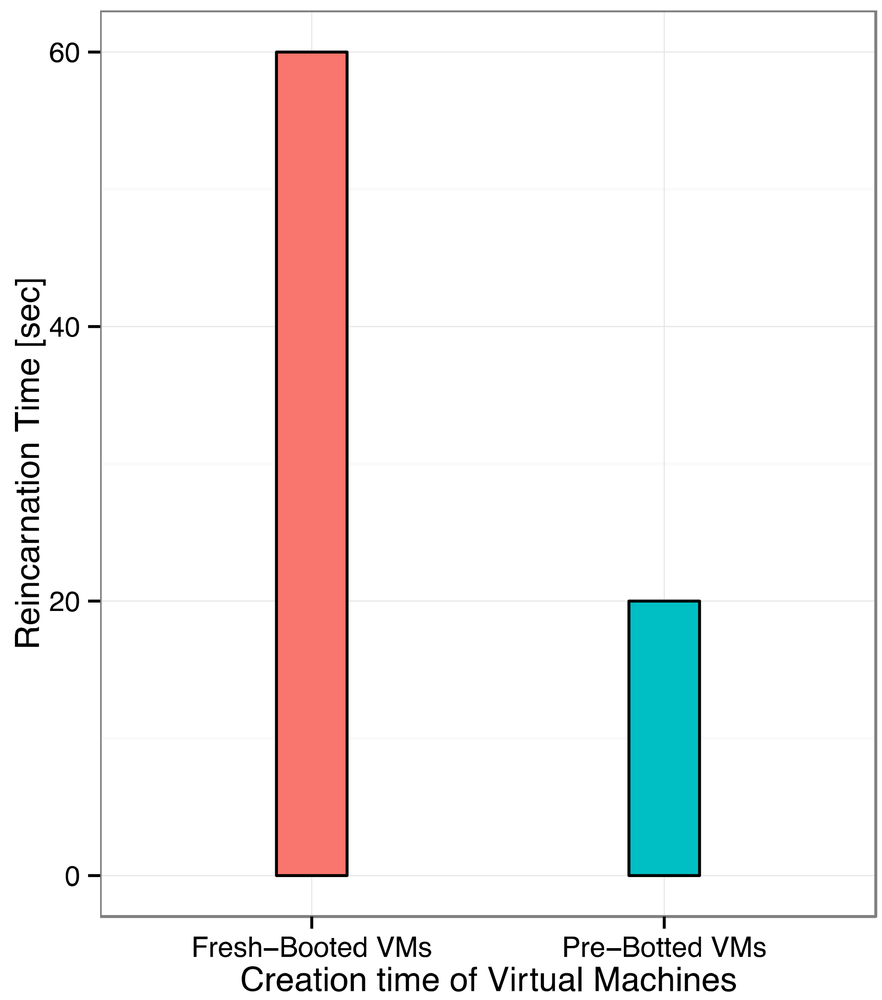

Fig. 3 Reincarnation times with current implementation: VMs are created either in advance or on the fly.

FUTURE WORK (STATEFUL APPLICATIONS)

1. Stateless application such as BFT applications allow the replacement of VMs without keeping their states due to their failure-resistant design.
2. Certain applications require to keep the state of VMs: The new VM is created running a different version of the executable binary and it is synchronized with the old machine.

REFERENCES

[1] N. Ahmed and B. Bhargava. "Mayflies: A moving target defense framework for distributed systems," in Proceedings of the 2016 ACM Workshop on Moving Target Defense, 2016, pp. 59–64.

[2] M. Villarreal-Vasquez, B. Bhargava, P. Angin, N. Ahmed, D. Goodwin, K. Brin and J. Kobes. An MTD-based Self-Adaptive Resilience Approach for Cloud Systems. In Submission to IEEE CLOUD 2017

Acknowledgement: This research is supported by NGC Research Consortium. We collaborated with Daniel Goodwin, Kory Brin and Carlos Otero.

CERIAS

PURDUE UNIVERSITY