Advanced Techniques for Container Migration in Moving Target Defense (MTD)

Typ der Arbeit

- Bachelorarbeit
- Projektarbeit

Titel
Advanced Techniques for Container Migration in Moving Target Defense (MTD)

Beschreibung
Advanced Techniques for Container Migration in Moving Target Defense (MTD) Context Microservice Architectures (MSA) using container runtimes have become the de facto standard for agility, scalability, and flexibility in computing domains. However, MSA introduces multiple security risks due to image vulnerabilities, embedded malware, and configuration defects [1]. In multi-tenant environments like public clouds, these vulnerabilities can be exploited when the isolation boundaries are not properly set. Although there is extensive research on improving VMs and containers' isolation, researchers also proved that some attacks, such as side-channel attacks, can bypass them [2]. A preventive security method to avoid such threats is Moving Target Defense (MTD), where the running microservices are migrated to change the attack surface and landscape of the cloud, reducing the time attackers have to target neighboring apps in a public cloud. The main objective of this work is to implement container live migration of MSAs in a Kubernetes environment and optimize them using advanced control policies. Goals The goals of this thesis are as follows: - To have a better understanding of technical challenges regarding container live migration in a Kubernetes environment. - To have a better understanding of the new beta features of Kubernetes for live migration and to use them to successfully live migrate running MSAs. - We optimize the migration based on security and QoS policies of the service environment - We have performance evaluation results from our testbed (e.g., duration, downtime, resource overhead). Tasks To reach those goals, you have to complete the following tasks: - Create, from existing benchmark containers, one microservices (MS) app. - Migrate the containers singularly and then the MS App at once, using the newly implemented beta features of Kubernetes: Checkpoint/restore [3] and StatefulSet [4]. - Compare results between the 2 methods and the nature of the container microservice. - Use KubeVirt live-migration method [5], which consists of migrating the whole VM node hosting the containers rather than moving the containers or pods in the VM node (interesting but probably slower). - Optimize and control the migration based on dynamic security policies and performance requirements References [1] M. Souppaya, J. Morello, and K. Scarfone, "Application container security guide", 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-190. [2] Zhang Yinqian, Juels Ari, K. Reiter Michael and Thomas Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys", Proceedings of the ACM Conference on Computer and Communications Security (CCS '12), pp. 305-316, 2012. [3] "KubeVirt [Official site]. https://kubernetes.io/blog/2023/04/28/statefulset-start-ordinal/," accessed: 30-August-2023. [4] "KubeVirt [Official site]. https://kubernetes.io/blog/2022/12/05/forensic-container-checkpointing-alpha/," accessed: 30-August-2023. [5] "KubeVirt [Official site]. https://kubevirt.io/user-guide/operations/live_migration/," accessed: 30-August-2023.

Voraussetzungen

- Prior experience with containers and Kubernetes - Prior experience with container migration - Good programming skills - Good understanding of cybersecurity concepts - Basic understanding of computer networks, security functions and network protocols - Love for algorithms!

Themen Betreuer
Gür Gürkan
gueu@zhaw.ch

Hauptbetreuer
Gür Gürkan
gueu@zhaw.ch

Labor
Kein Labor

Primäres Fachgebiet
Information Security

Weitere Fachgebiete

- Kommunikation

Studiengang

Institut / Zentren

- Institut für Informatik (InIT)

Interne Partner

- Keine

Englisch
Ja