Escape Games: Overview of Container Runtime Security

Master's Thesis

Computing in the Humanities Degree Program
Bamberg University

Author: Edith Förster
July 2024

Supervisor: Prof. Dr. Dominik Herrmann
Privacy and Security in Information Systems Group

Abstract

Containerization technology has become increasingly popular as corporations adopt cloud architecture solutions. Containers streamline the development, testing, and deployment of applications by bundling them with necessary components, including the operating system environment. However, security concerns remain the primary obstacle to widespread adoption. In multi-tenant environments, such as those offered by Container as a Service (CaaS) providers, the risk of container breakouts is a critical concern. This thesis focuses on identifying the technical features essential for selecting a container runtime software to mitigate the threat of container breakouts. These criteria are developed by gaining a sufficient background understanding of the Linux kernel technolo- gies underlying containerization. We evaluate four popular runtimes – LXC, Apptainer, runC, and gVisor – by examining their static features, architecture, rootless operation capabilities, and publicly known vulnerabilities. Our findings suggest that runC is the least suitable option due to its weak configurations, as well as a history of flaws and lax patching policy. Apptainer stands out for its use in high-performance computing (HPC) due to its immutability guarantees and design-centric integration of rootless containers. LXC presents a reliable choice due to its maturity, while gVisor is worth considering for those seeking the latest innovations. However, to effectively mitigate the threat of container breakouts, it is essential to investigate why they occur empirically – possibly due to leaked credentials or phishing rather than flaws in runtime software.

Keywords: container escape, docker, security