

Title: Lic-Sec: an enhanced AppArmor Docker security profile generator

Author: Hui Zhu, Christian Gehrman

Affiliation: Lund University

Abstract: Along with the rapid development of cloud computing technology, containerization technology has drawn much attention from both industry and academia. In this paper, we perform a comparative measurement analysis of Docker-sec, which is a Linux Security Module proposed in 2018, and a new AppArmor profile generator called Lic-Sec, which combines Docker-sec with a modified version of LiCShield, which is also a Linux Security Module proposed in 2015. Docker-sec and LiCShield can be used to enhance Docker container security based on mandatory access control and allows protection of the container without manually configurations. Lic-Sec brings together their strengths and provides stronger protection. We evaluate the effectiveness and performance of Docker-sec and Lic-Sec by testing them with real-world attacks. We generate an exploit database with 42 exploits effective on Docker containers selected from the latest 400 exploits on Exploit-db. We launch these exploits on containers spawned with Docker-sec and Lic-Sec separately. Our evaluations show that for demanding images, Lic-Sec gives protection for all privilege escalation attacks for which Docker-sec failed to give protection.