Contribution ID : **67** Type : **not specified**

Exploring New Frontiers in Container Technology

Wednesday, 14 November 2018 09:00 (45)

Containers (or Operating System based Virtualization) are an old technology; however, the current excitement (and consequent investment) around containers provides interesting avenues for research on updating the way we build and manage container technology. The most active area of research today, thanks to concerns raised by groups supporting other types of virtualization, is in improving the security properties of containers.

The first step in improving security is actually being able to measure it in the first place, so the initial goal of a research programme for container security involves finding that measure. In this talk I'll outline one such measure (attack profiles) developed by IBM research, the useful results that can be derived from it, the problems it has and the avenues that can be explored to refine future measurements of containment.

Contrary to popular belief, a "container" doesn't describe one fixed thing, but instead is a collective noun for a group of isolation and resource control primitives (in Linux terminology called namespaces and cgroups) the composition of which can be independently varied. In the second half of this talk, we'll explore how containment can be improved by replacing some of the isolation primitives with local system call emulation sandboxes, a promising technique used by both the Google gVisor and the IBM Nabla secure container systems. We'll also explore the question of whether sandboxes are the end point of container security research or merely point the way to the next Frontier for container abstraction.

I agree to abide by the anti-harassment policy

Yes

Primary author(s) : BOTTOMLEY, James (IBM)

Presenter(s) : BOTTOMLEY, James (IBM)

Session Classification : LPC Main Track

Track Classification : Refereed talk