Poster: Userland Containers for Mobile Systems

Isaac Ahlgren  
*Loyola University Chicago*, iahlgren@luc.edu

Victor Rakotondranoro  
*Loyola University Chicago*, vrakotondranoro@luc.edu

Yasin N. Silva  
*Loyola University Chicago*, ysilva1@luc.edu

Eric Chan-Tin  
*Loyola University Chicago*, chantin@cs.luc.edu

George K. Thiruvathukal  
*Loyola University Chicago*, gkt@cs.luc.edu

Recommended Citation
Authors
Isaac Ahlgren, Victor Rakotondranoro, Yasin N. Silva, Eric Chan-Tin, George K. Thiruvathukal, and Neil Klingensmith

This conference proceeding is available at Loyola eCommons: https://ecommons.luc.edu/cs_facpubs/343
EXTENDED ABSTRACT

Mobile platforms are not rising to their potential as ubiquitous computers, in large part because of the constraints we impose on their apps in the name of security. Mobile operating systems have long struggled with the challenge of isolating untrusted apps. In pursuit of a secure runtime environment, Android and iOS isolate apps inside a gauze of platform-imposed programming languages and runtime libraries, leaving few design decisions to the application developers. These thick layers of custom software eschew app portability and maintainability, as development teams must continually tweak their apps to support modifications to the OS’s runtime libraries. Nonstandard and ever-changing interfaces to those APIs invite bugs in the operating system and apps alike.

Mobile-only APIs have bifurcated the population of software running on our devices. On one side sits the conventional PC and server programs: compilers, shells, servers, daemons, and many others that use the standard libraries and programming models to interface with the computer and the outside world. On the other side lives the apps: mobile-only and purpose-built, they often serve as user interfaces to some larger cloud-based system. Under the weight of the numerous OS-imposed constraints, it is difficult for app developers to innovate: large classes of applications are simply impossible to port to mobile devices because the required APIs are unsupported. To deal with these crossplatform dependencies, it is necessary to maintain multiple code bases. In the past, dependency issues have typically been solved through the use of containers. However, deploying containers on mobile systems present unique challenges. To maintain security, mobile operating systems do not give users permission to launch Docker containers [2].

To solve this issue, we consider an older idea known as userland containerization. Userland containerization allows users to launch non-root containers on mobile devices. Userland containerization works by inserting a modified operating system kernel between the host kernel and the guest processes (see Figure 1).

We have done an in depth study on the performance of usermode containers like the user mode linux (UML) kernel [1], repurposing it as a userland hypervisor between the host kernel and the guest processes. We prototype a proof-of-concept usermode kernel with an implementation that is guided by the findings of our empirical study. Our kernel introduces a new technique—similar to paravirtualization—to optimize the syscall interface between the guest process and the usermode kernel to improve its I/O performance. The redesigned syscall interface provides I/O performance comparable to VMWare Workstation. Furthermore, we achieve 3.5×-5× more network throughput and equal disk write speed compared to VMWare Workstation.

Figure 1: Components of a userland container (privileged shaded gray). All components of the guests, including the guest kernel and roofs are owned by an unprivileged user.

Figure 2: Throughput for each of the virtualization platforms running on desktop. Our paravirtualized userland containers (bars outlined in black) achieve nearly the same performance as VMWare Workstation.

REFERENCES


Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

HotMobile ’23, February 22–23, 2023, Newport Beach, CA, USA
© 2023 Association for Computing Machinery.
https://doi.org/10.1145/3572664.3581588