Abstract

In today's internet world, Malicious and malfunctioning contents from the internet are regular problems for host systems such as Smartphones, Desktops, Clouds etc. Almost all underlying operating systems provide security from most of the threats. However, we need to add some extra defense to our system. Sandboxing is an important security technique that lets programs run in its isolated environment. A sandbox is a tightly controlled environment where programs run. It provides access to a tightly controlled set of resources for programs, such as memory, scratch space on the disk, network access, and input devices. A program running in the sandbox has just as many permissions as it needs without having additional permissions that could be misused. Sandbox restricts a program to access resources outside the sandbox. Sandbox prevents malicious or malfunctioning programs from accessing rest of the system. Nowadays, most of the mobile operating systems, desktop applications like web browsers, browser plugins, document viewers and cloud computing systems are using sandboxing mechanism to run applications. For the implementation of the sandboxing mechanism, software vendors rely on underlying operating system security features. There are different ways and
Sandboxing in Linux: From Smartphone to Cloud

approaches that can be used to implement sandbox mechanisms. This paper highlights the Linux security features such as Chroot, Cgroups, Capabilities, SCI, Namespaces, Seccomp, Resource Limit, LSMs such as SELinux, Virtualization and grsecurity that can be used in the implementation of the sandboxing mechanism.

References


31. Oracle. Linux containers (lxc), consolidate with oracle linux containers.


40. DON REVELLE. Hypervisors and virtual machines.


43. Paul Sabanal and Mark Vincent Yason. Digging deep into the flash sandboxes.  

Index Terms

Computer Science

Information Sciences
Keywords

Chroot, Namespace, Cgroups, Seccomp, Capabilities