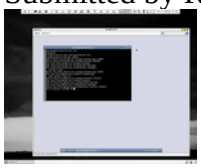
Compartmentalized computing with CLIP OS

By *Roy Schestowitz*
Created *08/11/2018 - 7:22pm*
Submitted by Roy Schestowitz on Thursday 8th of November 2018 07:22:34 PM Filed under OS [1] Gentoo [2]



The design of CLIP OS 5 includes three elements: a bootloader, a core system, and the cages. The system uses secure boot with signed binaries. Only the x86 architecture was supported in the previous versions, and there are no other architectures in the plan for now. The core system is based on Hardened Gentoo. Finally, the cages provide user sessions, with applications and documents.

Processes running in separate cages cannot communicate directly. Instead, they must pass messages using special services on the core system; these services are unprivileged and confined on the cage system, but privileged on the core. These communication paths are shown in this architecture diagram from the documentation. Cages are also isolated from the core system itself ? all interactions (system calls, for example) are checked and go through mediation services. The isolation between applications will be using containers, and the team plans to use the Flatpak format. The

details of the CLIP OS 5 implementation are not available yet, as this feature is planned for the stable release.

A specific Linux security module (LSM) inspired from Linux-VServer will be used to add additional isolation between the cages, and between the cages and the core system. Linux-VServer is a virtual private server implementation designed for web hosting. It implements partitioning of a computer system in terms of CPU time, memory, the filesystem, and network addressing into security contexts. Starting and stopping a new virtual server corresponds to setting up and tearing down a security context.

[3]

OS Gentoo

Source URL: http://www.tuxmachines.org/node/117248

Links:
[1] http://www.tuxmachines.org/taxonomy/term/37
[2] http://www.tuxmachines.org/taxonomy/term/109
[3] https://lwn.net/Articles/768819/