LoadPin

LoadPin is a Linux Security Module that ensures all kernel-loaded files (modules, firmware, etc) all originate from the same filesystem, with the expectation that such a filesystem is backed by a read-only device such as dm-verity or CDROM. This allows systems that have a verified and/or unchangeable filesystem to enforce module and firmware loading restrictions without needing to sign the files individually.

The LSM is selectable at build-time with `CONFIG_SECURITY_LOADPIN`, and can be controlled at boot-time with the kernel command line option "`loadpin.enforce`". By default, it is enabled, but can be disabled at boot ("`loadpin.enforce=0`").

LoadPin starts pinning when it sees the first file loaded. If the block device backing the filesystem is not read-only, a sysctl is created to toggle pinning: `/proc/sys/kernel/loadpin/enabled`. (Having a mutable filesystem means pinning is mutable too, but having the sysctl allows for easy testing on systems with a mutable filesystem.)

It's also possible to exclude specific file types from LoadPin using kernel command line option "`loadpin.exclude`". By default, all files are included, but they can be excluded using kernel command line option such as "`loadpin.exclude=kernel-module,kexec-image`". This allows to use different mechanisms such as `CONFIG_MODULE_SIG` and `CONFIG_KEXEC_VERIFY_SIG` to verify kernel module and kernel image while still use LoadPin to protect the integrity of other files kernel loads. The full list of valid file types can be found in `kernel_read_file_str` defined in `include/linux/kernel_read_file.h`.