NAME

ld-elf-cap.so.1, **rtld-elf-cap** — capability-mode run-time link editor

DESCRIPTION

The **ld-elf-cap.so.1** is a version of ld-elf.so.1(1) specific to the sandbox environment created using libcapsicum(3), which provides certain extended or modified linker services for that environment:

- Will not attempt to use global file system namespaces that are not available when running under cap_enter(2).
- Expects to be directly executed using fexecve(2), with the desired binary to run passed as file descriptor 3.
- Recognizes the addition symbol cap_main, which will be used instead of the normal ELF entry point for a binary when in sandbox mode. This makes it easy a single binary to select different behavior when run in the different environments.
- Interprets the LD_LIBCACHE environmental variable set by sandbox start routines, and implements **ld_libcache_lookup**(), allowing file descriptors for binaries and libraries passed across fexecve(2) to be used by libcapsicum(3), as well as applications.
- Implements a version of **ld_insandbox**() that returns true, overriding the libc function that returns false.

Applications using cap_main will need to export it as a dynamic symbol, perhaps using gcc(1) 's -rdynamic command line flag.

Most capability-mode applications will be started using the APIs defined in libcapsicum(3), which properly set up the run-time environment for **ld-elf-cap.so.1**.

SEE ALSO

gcc(1), ld-elf.so.1(1), cap_enter(2), fexecve(2), libcapsicum(3)

HISTORY

Support for capabilities and capabilities mode was developed as part of the TrustedBSD Project.

BUGS

WARNING: THIS IS EXPERIMENTAL SECURITY SOFTWARE THAT MUST NOT BE RELIED ON IN PRODUCTION SYSTEMS. IT WILL BREAK YOUR SOFTWARE IN NEW AND UNEXPECTED WAYS.

The format of LD_LIBCACHE is not documented, and may change.

AUTHORS

ld-elf-cap.so.1 is derived from rtld(1), the normal run-time linker, and was developed by Robert N. M. Watson at the University of Cambridge Computer Laboratory with support from a grant from Google, Inc.