NAME

libcapsicum — library interface to capability-mode services

LIBRARY

library “libcapsicum”

SYNOPSIS

```
#include <sys/types.h>
#include <sys/capability.h>
#include <libcapsicum.h>

int
lc_limitfd(int fd, cap_rights_t rights);
```

DESCRIPTION

libcapsicum implements APIs that allow applications to create, manage, and interact with sandboxed software services running in capability mode, described in cap_enter(2). Applications linked against **libcapsicum** will use one or both of "host" and "sandbox" APIs, depending on whether they consume or produce sandboxed services. **libcapsicum** will start sandboxed components using a sandbox-specific run-time linker, rtld-elf-cap(1), rather than the standard rtld-elf(1).

Host processes use the **libcapsicum** host API, described in libcapsicum_host(3), to launch compartmentalized components in sandboxes. They may also use **libcapsicum** to communication with the sandboxed service based on socket I/O or remote procedure call (RPC).

Sandbox processes run in capability mode, and are only able to use resources either assigned to the sandbox during creation, or later explicitly passed to the process. Sandbox processes use the **libcapsicum** sandbox API, described in libcapsicum_sandbox(3). Sandboxed processes themselves may launch software components in further sandboxes, so a single program may use both host and sandbox APIs.

In addition, the **libcapsicum** file descriptor list API, described in libcapsicum_fdlist(3), may be used to manage the delegation of file descriptors/capabilities to sandboxes using a namespace.

CAPSICUM API

lc_limitfd() is a wrapper around cap_new(2), dup2(2), and close(2). which takes an existing file descriptor and replaces it with a capability with the requested rights mask.

SEE ALSO

rpcgen(1), rtld-elf(1), rtld-elf-cap(1), cap_enter(2), cap_new(2), close(2), dup2(2), libcapsicum_fdlist(3), libcapsicum_host(3), libcapsicum_sandbox(3), unix(4)

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.

AUTHORS

These functions and the capability facility were created by Robert N. M. Watson and Jonathan Anderson at the University of Cambridge Computer Laboratory with support from a grant from Google, Inc.