

NAME

capng_lock – lock the current process capabilities settings

SYNOPSIS

```
#include <cap-ng.h>
```

```
int capng_lock(void);
```

DESCRIPTION

capng_lock will take steps to prevent children of the current process to regain full privileges if the uid is 0. This should be called while possessing the CAP_SETPCAP capability in the kernel. This function will do the following if permitted by the kernel:

- Set the NOROOT option on for PR_SET_SECUREBITS.
- Set the NOROOT_LOCKED option to on for PR_SET_SECUREBITS.
- Set the PR_NO_SETUID_FIXUP option on for PR_SET_SECUREBITS.
- Set the PR_NO_SETUID_FIXUP_LOCKED option on for PR_SET_SECUREBITS.

It does not enable PR_SET_KEEPCAPS or the KEEP_CAPS/KEEP_CAPS_LOCKED securebits; after a successful call those usually remain off unless the caller changed them separately.

RETURN VALUE

This returns 0 on success and a negative number on failure. -1 means a failure setting any of the PR_SET_SECUREBITS options. -2 means failure setting PR_SET_NO_NEW_PRIVS. These are additive meaning -3 is a failure of both.

SEE ALSO

capng_apply(3), prctl(2), capabilities(7)

AUTHOR

Steve Grubb