NAME

unveilro - unveil(2) a read-only view of the filesystem hierarchy

SYNOPSIS

unveilro *cmd ...*

DESCRIPTION

unveilro executes commands with an initial read-only unveil(2) set. To allow a larger number of applications to run without any additional config, write operations are permitted in */dev*, and create in */tmp*.

As such, it is *NOT* supported to use **unveilro** as root, or recommended with programs that already apply unveil(2) or pledge(2) themselves.

By default, execute permissions are *NOT* permitted unless overridden by the per-program unveil config. Note that because of unveil(2) semantics, execute permissions are not necessary to simply enter or traverse a directory. Effectively this only removes the ability to exec(3) arbitrary files, similar to dropping the "exec" promise from pledge(2).

The **unveilro** program should only be used as a last resort, if possible, greater protection and safety can be better attained through careful observation and direct source modification of programs.

EXAMPLES

unveilro will optionally check for additional paths to unveil in

```
~/.config/unveilro/<cmd>.unveil
```

For example:

```
# Example comment
# path  permissions (any combination of rwcx, or noperm)
~/games r
~/.savedir rwc

# apply quirks
quirks mkdir_home
```

SEE ALSO

unveil(2), ld.so(1)

CAVEATS

unveilro does not support setuid programs. **unveilro** utilizes several implementation-specific details on OpenBSD. For example, LD_PRELOAD and PIE (Position Independent Executables). Static binaries are NOT supported for those reasons. **unveilro** must be installed in *$HOME/bin* as **unveilro** to operate correctly.

AUTHORS

Bryan Steele <*brynet@gmail.com*>