NAME

ecryptfs-recover-private − find and mount any encrypted private directories

SYNOPSIS

ecryptfs-recover-private [--rw] [encrypted private dir]

DESCRIPTION

This utility is intended to help eCryptfs recover data from their encrypted home or encrypted private partitions. It is useful to run this from a LiveISO or a recovery image. It must run under **sudo**(8) or with root permission, in order to search the filesystem and perform the mounts.

The program can take a target encrypted directory on the command line. If unspecified, the utility will search the entire system looking for encrypted private directories, as configured by **ecryptfs-setup-private**(1).

If an encrypted directory and a *wrapped-passphrase* file are found, the user is prompted for the login (wrapping) passphrase, the keys are inserted into the keyring, and the data is decrypted and mounted.

If no *wrapped-passphrase* file is found, the user will be prompted for their mount passphrase. This passphrase is typically 32 characters of [0-9a-f]. All users are prompted to urgently record this randomly generated passphrase when they first setup their encrypted private directory.

The destination mount of the decrypted data is a temporary directory, in the form of */tmp/ecryptfs.XXXXXXXX*.

By default, the mount will be read-only. To mount with read and write permission, add the --rw parameter.

SEE ALSO

ecryptfs-setup-private(1), **sudo**(8)

http://blog.dustinkirkland.com/2009/03/mounting-your-encrypted-home-from.html

http://ecryptfs.org/

AUTHOR

This manpage was written by Dustin Kirkland <kirkland@ubuntu.com> for Ubuntu systems (but may be used by others). Permission is granted to copy, distribute and/or modify this document under the terms of the GNU General Public License, Version 2 or any later version published by the Free Software Foundation.

On Debian and Ubuntu systems, the complete text of the GNU General Public License can be found in /usr/share/common-licenses/GPL.