NAME

cgd − cryptographic disk driver

SYNOPSIS

pseudo-device cgd [*count*]

DESCRIPTION

The **cgd** driver provides the capability of encrypting blocks on their way to and from a disk or partition.

In order to compile support for the **cgd** into your kernel, you must add the driver to your kernel configuration file. To do this, add a line similar to:

```
pseudo-device   cgd    4      # cryptographic disk driver
```

The count argument defines how many **cgd**'s may be configured at a time.

Encryption Algorithms

Currently the following cryptographic algorithms are supported:

aes-cbc
: AES in CBC mode. AES uses a 128 bit blocksize and can accept keys of length 128, 192, or 256. The default key length is 128.

3des-cbc
: Triple DES in CBC mode. Triple DES uses a 64 bit blocksize and is performed in EDE3 mode with a 168 bit key. The key passed to the kernel is 192 bits but the parity bits are ignored.

blowfish-cbc
: Blowfish in CBC mode. Blowfish uses a 64 bit blocksize and can accept keys of length 128.

IV Methods

Currently, the only IV Method supported is *encblkno* (Encrypted Block Number). This method encrypts the block number of the physical disk block with the cipher and key provided and uses that as the IV for CBC mode. This method should ensure that each block has a different IV and that the IV is reasonably unpredictable.

IOCTLS

A **cgd** responds to all of the standard disk `ioctl`(2) calls defined in `sd`(4), and also defines the following:

CGDIOCSET
: configure the **cgd**. This `ioctl`(2) sets up the encryption parameters and points the **cgd** at the underlying disk.

CGDIOCCLR
: unconfigures the **cgd**.

These `ioctl`(2)'s and their associated data structures are defined in `/usr/include/dev/cgdvar.h`.

WARNINGS

It goes without saying that if you forget the passphrase that you used to configure a **cgd**, then you have irrevocably lost all of the data on the disk. Please ensure that you are using an appropriate backup strategy.

FILES

/dev/{,r}cgd∗ **cgd** device special files.

SEE ALSO

`ioctl`(2), `sd`(4), `MAKEDEV`(8), `cgdconfig`(8), `config`(8)

HISTORY

The **`cgd`** driver was written by Roland C. Dowdeswell for NetBSD. The **`cgd`** driver originally appeared in NetBSD 2.0.