The CryptoGraphic Disk Driver

Roland C. Dowdeswell
Metzger, Dowdeswell & Co., LLC

March 8, 2004

The CryptoGraphic Disk Driver

- Why you want it
- What it is
- What it does
- Why I wrote it

Design Goals

- Use of standard crypto techniques
- Modular design
- High performance
- N–factor Authentication
- Simplicity of use

Design Overview, Kernel

- Why a new pseudo disk, rather than using vnd(4)
- Modular cipher/IV gen framework
- Use of CBC and encblockno
- Kernel doesn’t do anything fancy

Design Overview, Userland

- Config files, /etc/cgd/cgd.conf and parameter files
- rc.d framework
- Structure of /etc/cgd/cgd.conf

Design Overview, Parameter files

- Encryption algorithm
- Algorithm key length (if variable)
- IV generation method
- Key generation methods
- Verification method

Design Overview, Key generation

- Methods:
  - pkcs5_pbkdf2
  - storedkey
  - randomkey
  - gssapi_keyserver
- XOR multiple stanzas together
- Provide for N–factor authentication
- Adding additional passphrases
- Does not provide for revoking access

How to Actually Use It

```
# cgdconfig -g -o /etc/cgd/wd0e aes-cbc 192
# cgdconfig cgd0 /dev/wd0e
/dev/wd0e's passphrase:
```

With a Verification Method

```
# cgdconfig -g -o /etc/cgd/wd0e -V disklabel \
>           aes-cbc 256
# cgdconfig -V re-enter cgd0 /dev/wd0e
/dev/wd0e's passphrase:
re-enter device's passphrase:
# disklabel -e -I cgd0
# cgdconfig -u cgd0
# cgdconfig cgd0 /dev/wd0e
/dev/wd0e's passphrase:
```

How to Grant Privileges with a New Passphrase

```
# cgdconfig -G -o newparamsfile oldparamsfile
old file's passphrase:
new file's passphrase:
```

Example Parameters Files (file 1)

```
algorithm aes-cbc;
iv-method encblkno;
keylength 128;
verify_method none;
keygen pkcs5_pbkdf2 {
        iterations 39361;
        salt AAAAgMoHiYonye6Kog \
             dYJAobCHE=;
};
```

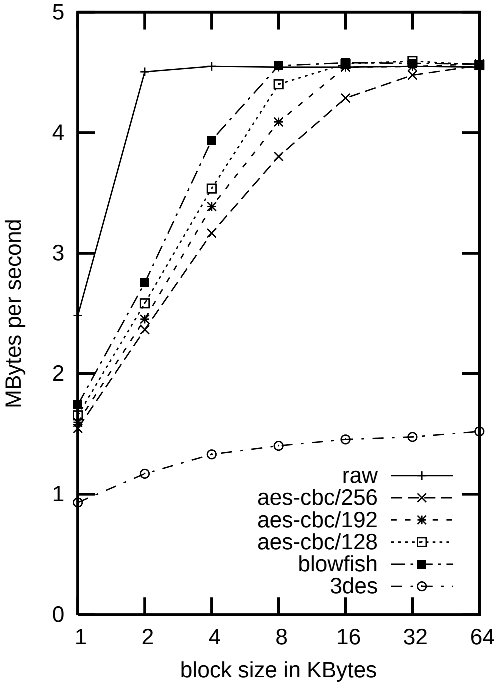
Example Parameters Files (file 2)

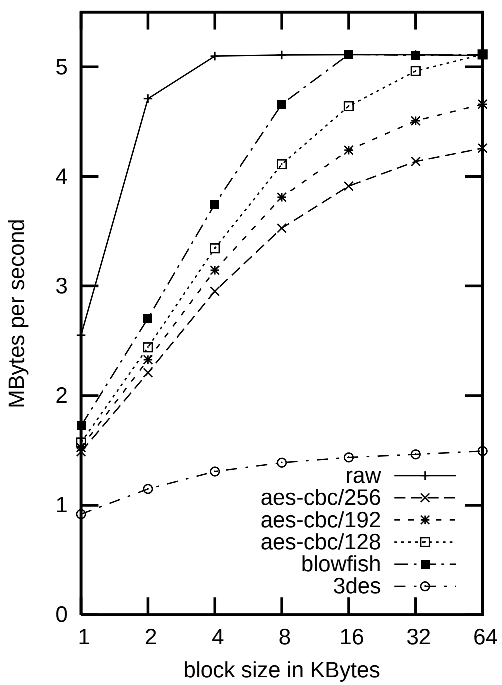
```
algorithm        aes-cbc;
iv-method        encblkno;
keylength        256;
verify_method    none;
keygen storedkey key AAABAK3QO6d7xzLfrXTds \
                     gg4ly2TdxkFqOkYYcbyUK \
                     u/f60L;
```

Example /etc/cgd/cgd.conf

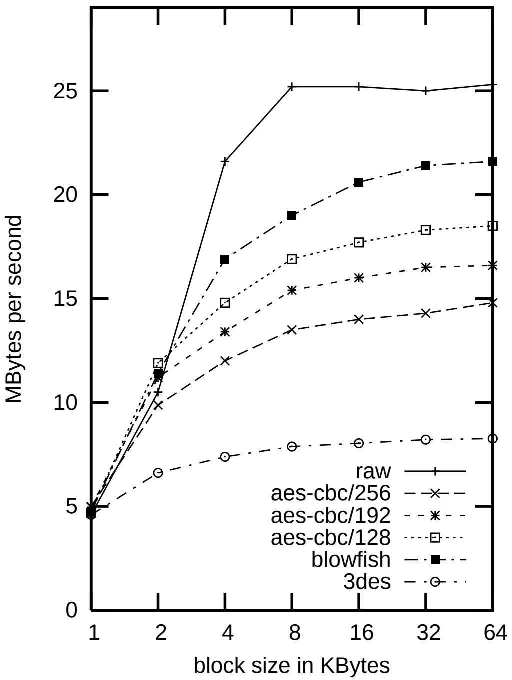
```
#
# /etc/cgd/cgd.conf
# Configuration file for cryptographic
# disk devices
#

# cgd             target            [paramsfile]
cgd0              /dev/wd0e
cgd1              /dev/sd0h         /mnt/cgd/sd0h
```

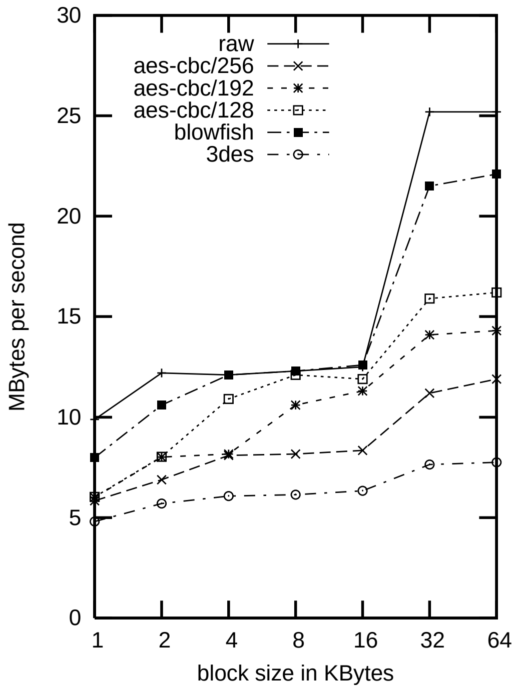
Performance: PWS 500a



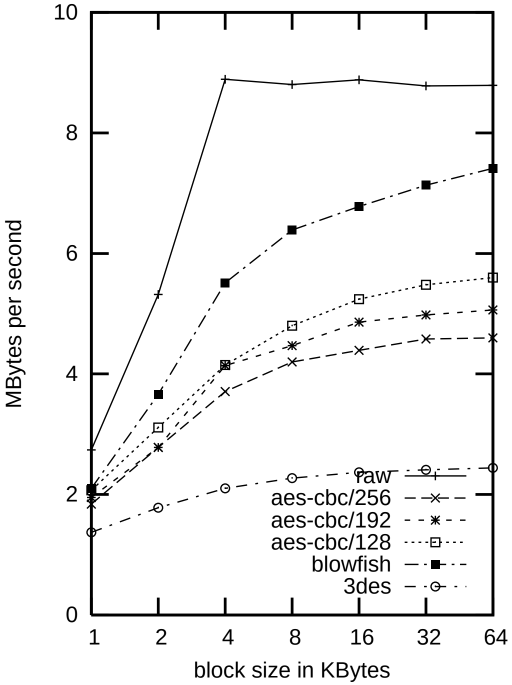


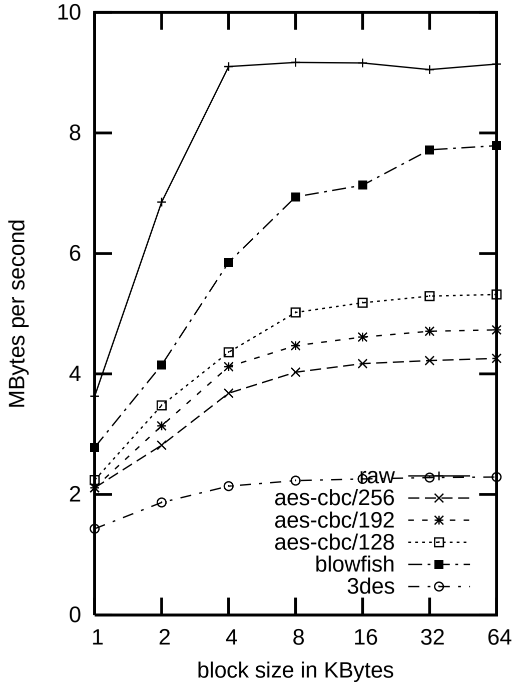
Performance: Random P4





Performance: Thinkpad 600E





Related Work

- OpenBSD's vnd+crypto
- FreeBSD's GBDE
- Linux's loopback encryption
- CFS
- cryptfs and ncryptfs
- tcfs

Future Work

- Fix a couple of bugs
- Add new IV generation methods
- Use hardware accelerated crypto framework
- New keygen methods
- Rekeying cgd's, both on– and off–line
- A little more flexibility in /etc/cgd/cgd.conf

More information

- The FREENIX paper
  `http://www.imrryr.org/~elric/cgd/`
- The man pages (in NetBSD and also the above URL has links)
- Chapter 21 of the NetBSD Guide,
  `http://www.netbsd.org/guide/en/chap-cgd.html`
- Unfortunately, a web search on “cgd NetBSD” is not a useful source of information for various reasons...
- Me.