

## Re: GELI – disk encryption GEOM class committed.

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2005-07/1357.html>

---

**From:** Mike Tanca (mike\_at\_sentex.net)

**Date:** 07/30/05

Date: Fri, 29 Jul 2005 22:21:05 -0400

To: Pawel Jakub Dawidek <pjd@freebsd.org>, freebsd-current@freebsd.org

At 04:54 PM 28/07/2005, Pawel Jakub Dawidek wrote:

> – Utilize the crypto(9) framework, so when there is a crypto hardware  
> available, geli(8) will make use of it automatically.

Hi,

Any plans to add Via's AES support to crypto(9) ? This would potentially speed it up quite a bit when using AES

```
[via]# openssl speed -evp aes-256-ecb -engine padlock  
engine "padlock" set.
```

To get the most accurate results, try to run this program when this computer is idle.

```
Doing aes-256-ecb for 3s on 16 size blocks: 10620355 aes-256-ecb's in 3.00s
```

```
Doing aes-256-ecb for 3s on 64 size blocks: 10108173 aes-256-ecb's in 2.99s
```

```
Doing aes-256-ecb for 3s on 256 size blocks: 6917320 aes-256-ecb's in 2.99s
```

```
Doing aes-256-ecb for 3s on 1024 size blocks: 3004029 aes-256-ecb's in 3.00s
```

```
Doing aes-256-ecb for 3s on 8192 size blocks: 478383 aes-256-ecb's in 3.00s
```

```
OpenSSL 0.9.7e 25 Oct 2004
```

```
built on: Fri Jul 29 17:03:29 EDT 2005
```

```
options:bn(64,32) md2(int) rc4(idx,int) des(ptr,risc1,16,long) aes(partial)
```

```
blowfish(idx)
```

```
compiler: cc
```

```
available timing options: USE_TOD HZ=128 [sysconf value]
```

```
timing function used: getrusage
```

The 'numbers' are in 1000s of bytes per second processed.

```
type 16 bytes 64 bytes 256 bytes 1024 bytes 8192 bytes
```

```
aes-256-ecb 56735.66k 216464.53k 592534.15k 1026953.66k 1308336.36k
```

```
[via]# openssl speed -evp aes-256-ecb
```

To get the most accurate results, try to run this

program when this computer is idle.

```
Doing aes-256-ecb for 3s on 16 size blocks: 1390266 aes-256-ecb's in 3.00s
```

```
Doing aes-256-ecb for 3s on 64 size blocks: 364037 aes-256-ecb's in 2.99s
```

```
Doing aes-256-ecb for 3s on 256 size blocks: 92390 aes-256-ecb's in 3.00s
```

```
Doing aes-256-ecb for 3s on 1024 size blocks: 23185 aes-256-ecb's in 3.00s
```

freebsd-current: Re: GELI – disk encryption GEOM class committed.

Doing aes-256-ecb for 3s on 8192 size blocks: 2902 aes-256-ecb's in 2.99s  
OpenSSL 0.9.7e 25 Oct 2004  
built on: Fri Jul 29 17:03:29 EDT 2005  
options:bn(64,32) md2(int) rc4(idx,int) des(ptr,risc1,16,long) aes(partial)  
blowfish(idx)  
compiler: cc  
available timing options: USE\_TOD HZ=128 [sysconf value]  
timing function used: getrusage  
The 'numbers' are in 1000s of bytes per second processed.  
type 16 bytes 64 bytes 256 bytes 1024 bytes 8192 bytes  
aes-256-ecb 7424.03k 7796.16k 7893.39k 7923.14k 7952.16k  
[via]#

This is with a

CPU: VIA C3 Nehemiah+RNG+ACE (1199.80-MHz 686-class CPU)

Origin = "CentaurHauls" Id = 0x698 Stepping = 8

Features=0x381b83f<FPU,VME,DE,PSE,TSC,MSR,SEP,MTRR,PGE,CMOV,PAT,MMX,FXSR,SSE>

real memory = 251592704 (239 MB)

avail memory = 236732416 (225 MB)

---

freebsd-current@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-current>

To unsubscribe, send any mail to "freebsd-current-unsubscribe@freebsd.org"