geli: Allow attaching of multiple providers at once if they use same passphrase and keyfiles

https://reviews.freebsd.org/D9396

EuroBSDcon 2017
Ben Woods
woodsb02@FreeBSD.org

Scratching an itch

I had to enter my geli passphrase 4 times when booting my FreeBSD NAS (once per drive in my raidz2).

This was tedious.

But the boot loader caches passphrases

True, but this was not a boot drive, so it was not being handled by the loader.

Instead in /etc/rc.conf:

geli_devices="ada0 ada1 ada2 ada3”

GELI attaching multiple drives at once with a single passphrase should also be available after boot (on command line or via rc service).

Proposed new rc.conf syntax

```
geli_devices="ada0”
geli_groups="data storage backup"
geli_data_devices="ada1 ada2"
geli_storage_flags="-k /etc/geli/storage.keys"
geli_storage_devices="ada3 ada4"
geli_backup_flags="-j /etc/geli/backup.passfile -k
/etc/geli/backup.keys"
geli_backup_devices="ada5 ada6"
```

sbin/geom/class/eli/geom_eli.c

geli add request (userland):

1. **Reads metadata from the provider** (incl. salt)
2. **Obtains the secret** (keyfiles, passfiles or passphrase)
3. **Generates decryption key** (hmac with salt + secret)
4. **Issues request + key to kernel**

Impact of salt

Same passphrase ≠ same decryption key

Even with the same passphrase and/or keyfile, each provider has a different decryption key because they all have different salt.

Solution Options

Even with the same passphrase and/or keyfile, each provider has a different decryption key because they all have different salt.

Option 1: Single geli request on command line issues multiple geli requests to kernel (one per provider)

Option 2: Convert geli add requests to allow multiple providers (userspace+kernel). **(Like geli detach)**

Implementation

geli add request (userland):

For each provider:

1. **Read metadata from the provider** (incl. salt)
2. **If 1st provider, obtain secret** (keyfiles, passfiles or passphrase)
   otherwise, use cached secret
3. **Generates decryption key** (hmac of salt + secret)

Issues request to kernel with array of providers and corresponding array of decryption keys.

For all the details (including man page)

https://reviews.freebsd.org/D9396

Thank you