GELI – GEOM Disk Encryption

Paweł Jakub Dawidek
<pjd@FreeBSD.org>
FreeBSD committer

Don't we have GBDE already?

Some interesting features

- utilize the crypto(9) framework
- supports many cryptographic algorithms (currently AES, 3DES, Blowfish)
- can create a key from a couple of components (user entered passphrase, random bits from a file, etc.)
- allows to encrypt root partition (!)
- user's passphrase is strengthen by default with PKCS#5 HMAC/SHA1
- allows to use two independent keys (user and company key)

...more features

- it is fast (uses simple sector-to-sector encryption)
- allows to backup/restore Master-Key
- detach-on-last-close-thing or unmount-and-forget
- allows to use one-time keys

Status

- it is finished
- working on manual page
- needs reviews and analysis