PEFS: A Stacked Cryptographic File System

Gleb Kurtsou
gleb@FreeBSD.org

FreeBSD Developer Summit
Meeting Plaza
Maarssen, The Netherlands
October 6 – 8, 2011

Introduction

```
% pefs mount ~/.private.enc ~/private
% pefs addkey ~/private
```

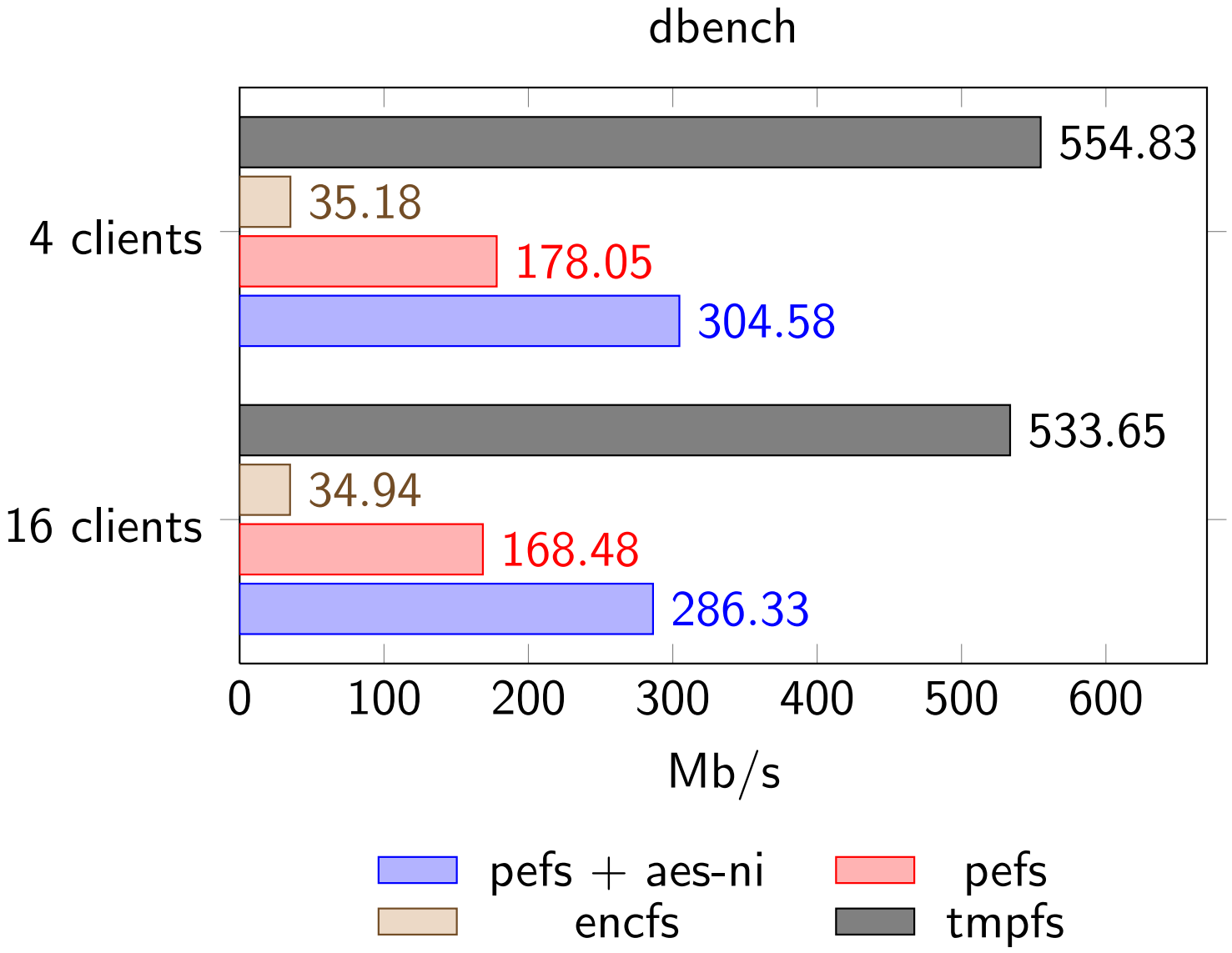
Home directory encryption

- pam_pefs module
- Transparent mode (ZFS snapshots access)

Incremental backups

- File size, owner and permissions are not altered
- Files are self consistent

Benchmark



FreeBSD

Crypto algorithms

Keys

- PBKDFv2 and HKDF (HMAC-SHA512)
- Separate keys for encryption and authentication

Data encryption

- AES or Camellia (or another 128 bit block cipher)
- XTS mode (recomended by NIST)

File name

- AES-128 in CBC mode for encryption
- 64-bit VMAC for authentication

Design

Keep it simple

- No metadata in file itself
- eCryptfs: CVE-2009-0787, CVE-2009-2406/2407, CVE-2010-2492
- Per file random tweak

4096-bytes data units

- Decrypt – Update – Encrypt
- Special handling of small data units ($<$ 16 bytes)
- Sparse files support

No data authentication (yet)

Design

Multiple keys

- No "master key"
- Default directory key
- Emulate access levels
- Key order is undefined (flexibility vs restrictions)

Encrypted file name

- Unique encrypted names
- Use VMAC to detect encryption key
- Max file name length ≈ 180

Implementation issues

Name cache

- Not cached directory lookup is slow in PEFS
- Invalidated too often
- No change notification
- nullfs recycles inactive vnodes
- ZFS inode generation number
- PEFS dircache

No data change notification mechanism

- nullfs reuses vnode buffer objects
- PEFS avoids data caching: no buffer cache
- ZFS-style mmap implementation

FreeBSD

Thank you for your attention!

ask questions

Download

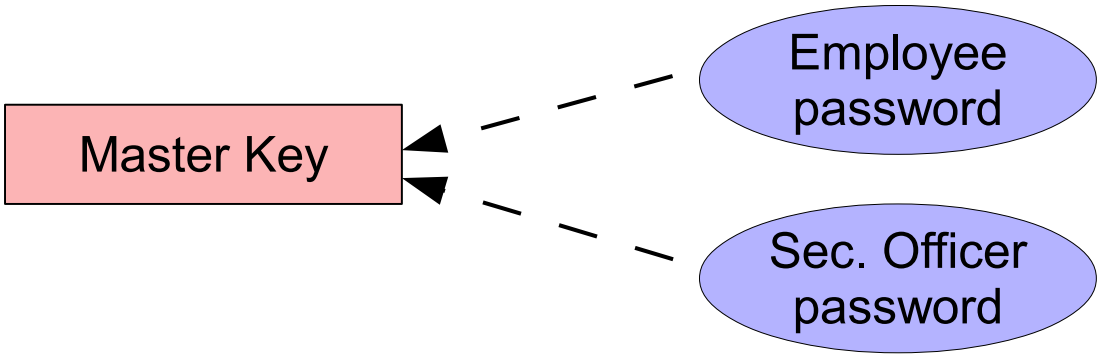
port sysutils/pefs-kmod

gihub github.com/glk/pefs

FreeBSD

Master key

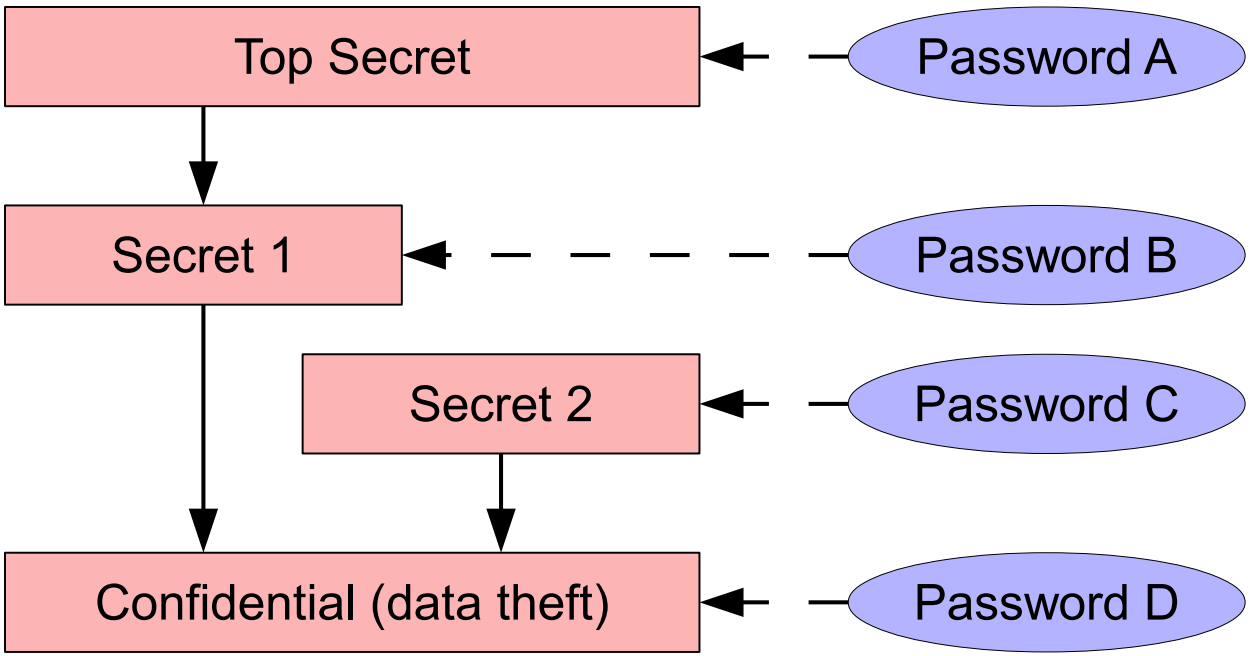
- Several passwords for a single encryption key
- Storage password policy $\neq$ login password policy
- Intruder can decrypt old data after password change



FreeBSD

Key chains

- User level concept
- Directed acyclic graph



FreeBSD

TODO

- GPG/PKCS#11 integration
- One time keys
- Unattended encrypted crash dumps
- Deniability