Unattended Encrypted Kernel Crash Dumps

Konrad Witaszczyk
def@FreeBSD.org

FreeBSD Developer Summit
Hilton Conference Centre
St. Julian's, Malta
September 26 – 28, 2013

Whose idea was this?

PEFS: A Stacked Cryptographic File System

Gleb Kurtsou
gleb@FreeBSD.org

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

TODO

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

Ideas about design

- Paweł Jakub Dawidek
  - Create a script in rc.d that generates an one-time random symmetric key.
  - Use the script to encrypt the key with a public key and store it in /var/crash/dumpkey.
  - Move the symmetric key to kernel via sysctl.
  - Use CBC mode with a random IV to encrypt data.
  - Don't encrypt a crash dump according to GELI/PEFS format.
  - Use savecore to save a crash dump and rename /var/crash/dumpkey to a proper name related to the dump.

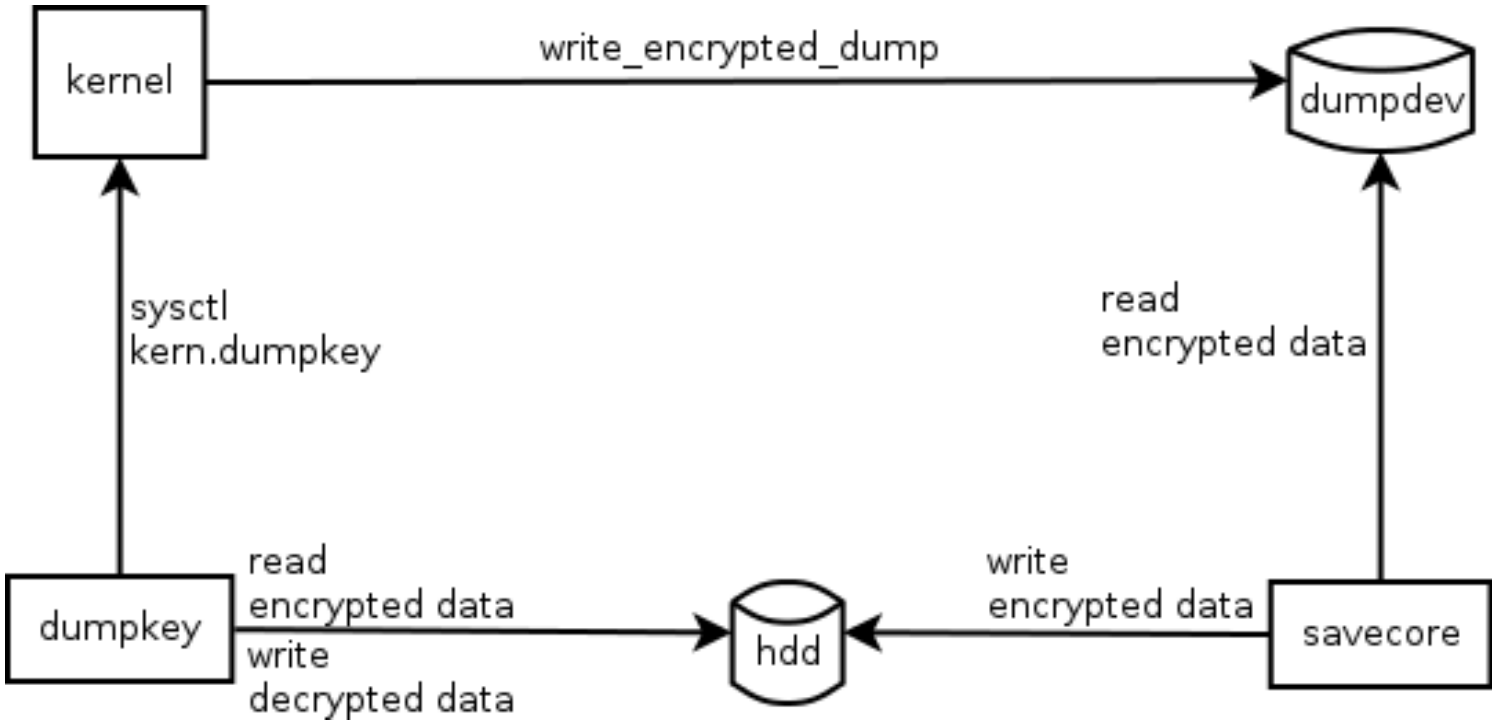
Ideas about design

- Gleb Kurtsou
  - Generate and encrypt a symmetric key.
  - Don't store the symmetric key in a local file system. Keep an unencrypted and encrypted keys in kernel.
  - Write the encrypted key to a dump device alongside a dump.
  - Use XTS mode to encrypt data (compatible with pefs).
  - Make it possible to save a plaintext dump in /var/crash.

Final design

- Generate an one-time random AES key.
- Encrypt the key with another asymmetric key.
- Use XTS-AES to encrypt a crash dump.
- Store an encrypted key and a tweak in a kernel dump header.
- Don't decrypt a crash dump after reboot.
- Don't remove an encrypted dump.
- Make it PEFS-ready (HKDF, 4096-bytes sectors).

Final design



FreeBSD

Changes in kernel

- Import XTS-AES implementation.
- Create `write_encrypted_dump` function.
- Extend `struct kerneldumpheader`.
- Create `struct kerneldumpkey` and a sysctl variable for it.

Changes in userland

- savecore creates key.X for vmcore.X.
- dumpkey configures kernel on startup.
- dumpkey decrypts a key and a crash dump.
- You can specify your own RSA keys in rc.conf.
- If at least one of the RSA keys doesn't exist then dumpkey will generate another pair of them.

What's missing?

- Increase the size of `struct kerneldumpheader`.
- Encrypt file names in savecore to use them with PEFS.
- Encrypt a crash summary.
- Support for Camellia and others if needed.

FreeBSD

Thank you for your attention!

ask questions