Analysis and decryption of Apple's FileVault 2

Omar Choudary, Felix Gröbert and Joachim Metz

About FileVault 2 and our work

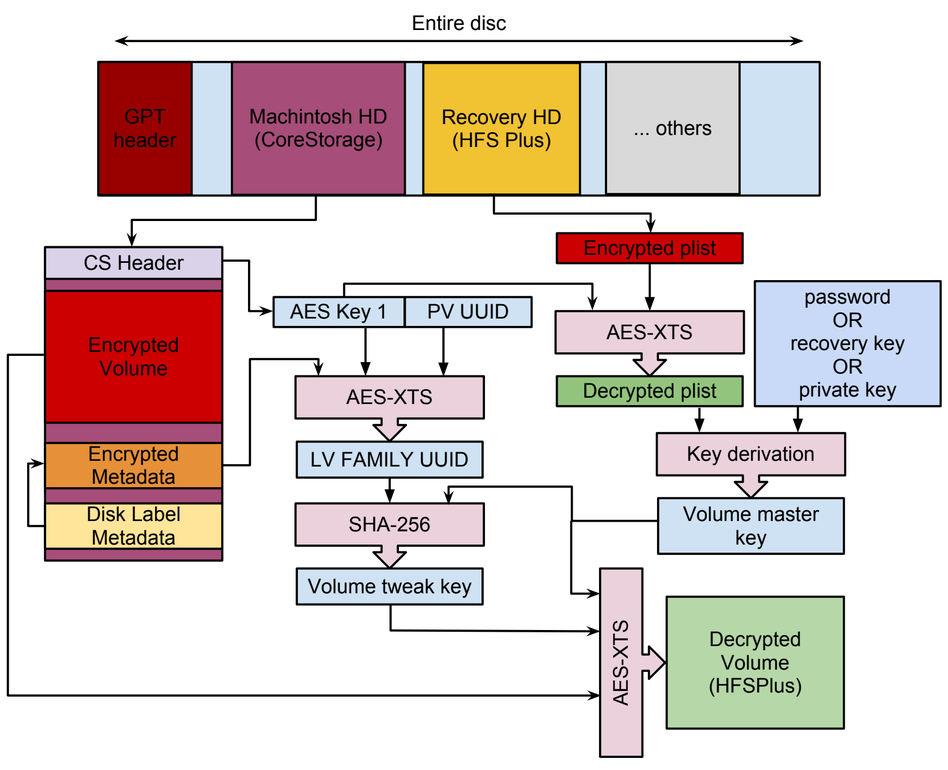
FileVault 2 is a volume encryption system, which Apple introduced with the launch of Mac OS X 10.7 in their operating system. While the previous version of FileVault (introduced with Mac OS X 10.3) only encrypted the home folder, FileVault 2 can encrypt the entire volume containing the operating system. This allows to protect all the data in the hard disk including both the user data and the OS.

This work is described in more detail in *Security Analysis and Decryption of FileVault 2*, to appear at IFIP WG 11.9 international conference on digital forensics, Orlando, FL, 2013.

Our work provides the first publicly available technical description and security evaluation of FileVault 2. We also maintain an open-source library to decrypt and mount FileVault 2 encrypted volumes. These contributions are very useful to forensic practitioners as they can now use their own tools to analyse data from FileVault 2 encrypted volumes (if some recovery token is known).

Recovery key snapshot

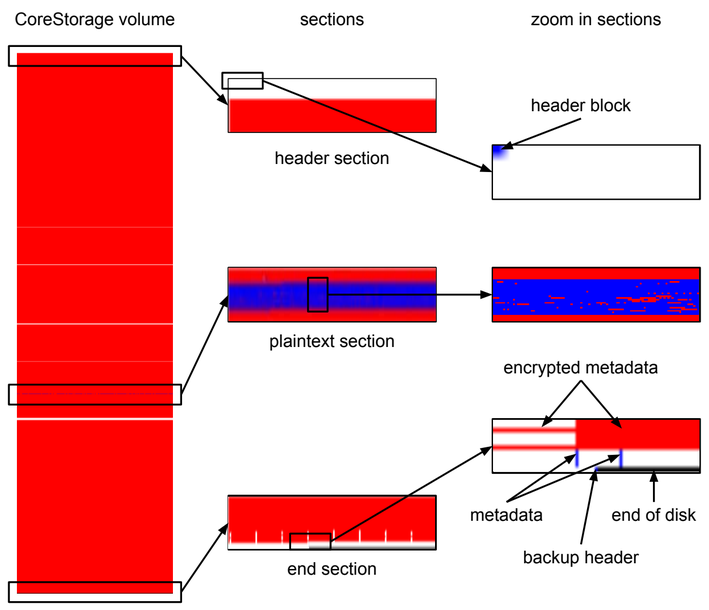
Overall architecture



FileVault 2 uses AES-XTS to encrypt the volume data. The encryption keys are stored in encrypted form in the disk itself, on a separate volume. To decrypt these encryption keys it is possible to use a user password, the recovery key or some key escrow in form of a private key. Some additional information needed for decryption is stored in metadata sections near the end of the encrypted volume. These contain details such as the start of the encrypted volume, its size and also additional decryption parameters.

Security Evaluation

One of our main purposes was to perform a security evaluation of FileVault 2 to determine if it is secure, as it will be used potentially on many corporate computers that contain sensitive data. We found that FileVault 2 uses good cryptographic algorithms with adequate parameters. We analysed in detail the random number generator that is used for the computation of the recovery key and found that it is a variant of Yarrow, providing 332 bits of entropy every 10 minutes. Additionally we performed an entropy scan of the entire encrypted volume and we found that there was a significant portion of plaintext (around 250 MB) in the middle of the encrypted volume, containing among others also user data. We have advised Apple about this issue and it was fixed in the next OS update (CVE-2011-3212).



Entropy bitmap showing plaintext (blue), ciphertext (red) and blank (white).

Libfvde: open-source lib for FileVault 2

We have developed an open-source library that can be used to decrypt and mount (via fuse) FileVault 2 encrypted volumes if the user password or some recovery token are known. This library can be useful to any forensic investigator as it allows to examine the contents of a FileVault 2 encrypted volume without having to trust a possibly compromised system.

The library, along with extensive documentation on FileVault 2, is available on Google Code:

`https://code.google.com/p/libfvde/`

Mounting a FileVault 2 encrypted volume can be done in just a few steps:

```
fvdemount -e EncryptedRoot.plist.wipekey -r 35AJ-AC98-TI1H-N4M3-HDUQ-UQFG /dev/sda2 /mnt/fvdevolume/
mount -o loop,ro /mnt/fvdevolume/fvde1 /mnt/hfs_file_system
```

Contact

Omar Choudary (PhD student, Computer Laboratory, Security Group)
omar.choudary@cl.cam.ac.uk
`http://www.cl.cam.ac.uk/~osc22/`

Online free version of the paper available at ePrint:

`https://eprint.iacr.org/2012/374/`