CryptoFS Security Note

footoredo

May 6, 2018

1 Basic structure

```
.cfs
  / keys
      / 79
          / 3220291197.key
      / df
          / c7027894e1.key
        ......
  / structure.sec
  / contents
      / 79
          / 3220291197.sec
      / df
          / c7027894e1.sec
        ......
```

2 How to obtain the master key?

STEP 1 Retrive motherboard UUID `$UUID`.

STEP 2 Ask for user passpharse `$PASS`.

STEP 3 Compute `$KEY = hashsum($UUID + $PASS)`.

STEP 4 Compute `$ID = hashsum($KEY + $PASS)`.

STEP 5 Find the key file `keys/$ID[0:2]/$ID[2:12].key` and decrypt it using `$KEY`.

3 What's in the decrypted key file?

PART 1 Symmetric key `$SIMKEY`

PART 2 Public-key encryption key-pair

KEY 1 Public key `$PUBKEY`

KEY 2 Private key `$PRIKEY`

4 `.sec` file

A `.sec` file is the ecrypted version of the original file combined with digital signature to check its integerity.

PART 1 Signature over hashsum of encrypted content (using `$PUBKEY` and `$PRIKEY`).

PART 2 Encrypted content (using `$SIMKEY`).

5 `structure.sec`

This file stores the directory structure of all original files. It is intended for implementation of `ls` command and operation validity check. Furthermore, it also stores the `$SALT` for each file, which is needed in the section below.

6 Where to find a file?

STEP 1 Assume the dir for the file is `$DIR`. First of all check if it is valid in `structure.sec`.

STEP 2 If it is valid, we can retrive `$SALT` of this file. This file's identity can be computed in `$ID = hashsum($DIR + $SALT)`.

STEP 3 Find the corresponding `.sec` file `contents/$ID[0:2]/$ID[2:12].sec` and decrypt it.