Security Engineering - Winter 2017

Sambuddho Chakravarty

April 6, 2017

Lab Assignment 3 (Total points: 30)

Due date: April 7. Time: 23:59 Hrs.

1 Directory Encryption using `eCryptfs`

The objective of this assignment is to familiarize you with using `eCryptfs` directory encryption scheme. You are expected to perform the following tasks:

1. Install `eCryptfs` on your laptops/desktops.
2. Create a subdirectory which would be encrypted directory.
3. Mount it as an encrypted directory using `eCryptfs`. Use either your or your group mates first name as the passphrase.
4. Once mounted every file subsequently added to this directory would be encrypted and stored.
5. Create a temporary file – `temp1` and add some text to it, while the subdirectory is still mounted using `eCryptfs`.
6. Unmount the directory and validate that the contents of the file `temp1` are encrypted. Print the contents on the screen and take a snapshot of the same (to be submitted).

2 File Encryption and Decryption using

The second part involves the use of `openssl` command line utility to encrypt and decrypt files. You would require to do the following:

1. In your encrypted directory (while mounted), add a new file. The file should be named [Your first name]-[your group mate's name].1.txt. The file should have your name and roll number as contents.
2. Encrypt the above file name using `openssl` command line program using your name as the passphrase which would be used to generate key, salt and IV. The passphrase must be either your or your group mate's firstname (so that we can validate it).

3. The next operation is to create yet another file, named [your name name]-[your group mate's].2.txt. This should be encrypted using a manually derived salt, IV and key, using `openssl` random number generator. Save the randomly generated salt, IV and key values (to be submitted).

4. Print the contents of both the encrypted file on screen and take snapshots.

Make sure both the encrypted files can be decrypted with the passphrase and (Salt, IV, key) tuple respectively.

What to submit

- Screen snapshots of the `eCryptfs` commands, the printed output of the encrypted directory.
- Screen snapshots of the encrypted files.
- Encrypted directory with passphrase (your or your group mate's first name) containing the files encrypted using `openssl`, along with passphrases and (IV, Key,Salt) tuples for the two respective files which have been encrypted.