Network and System Security

Assignment - 3

By Kaustav Vats (2016048)

Key and Iv for all cases are generated using this command **PKCS5_PBKDF2_HMAC_SHA1.** Hashed password of a user is passed as passphrase and Key are generated with 100 Iteration of length 32 bits. Iv is generated in same way but with 50 iteration of length 16 bits. HMAC is created using hmac library in openssl. I used HMAC function in this file to calculate hmac.

Implemented below commands using openssl library

- **Fput_encrypt:** Encrypts the contents before storing them to the file. I used EVP Library to encrypt content using EVP_aes_256_cbc().
- **Fget_decrypt:** Decrypts the content of encrypted file and dump output on stdout. I used EVP Library to decrypt content using EVP_aes_256_cbc().
- **Fverify:** This program verifies the HMAC signature with the key and IV derived from the owners shadow password. Everytime a file is to be read, if there is a corresponding signature file, it needs to be checked. This is also there for encrypted files which would be decrypted using ‘fget_decrypt’. If the signatures mismatch then an error must be reported, else there is no need to report anything. This should work only for files for which the calling user has read permissions.
- **Fsign:** This program creates a HMAC signature with the key and IV derived from the file owners shadow password. Everytime a file is created either using `fput’ or `fput_encrypt’ the signature should be created. The signature should be separate file with the same file name but a ‘.sign’ extension.

Assumptions

- Only encrypted file will be passed for encrypted and decrypted command.
- For all hmac related queries, HMAC file of corresponding input file should be present in the directory.
- Rest at the time of demo :)