Google Drive Encryption - Project proposal for CSE 207

Sunil Raiyani, Sahil Agarwal

November 10, 2015

1 Idea and Motivation

Google Drive is a secure cloud storage and file backup service for photos, videos, files etc. It allows you to access these files from anywhere, using any compatible device. Although Google ensures privacy of the data in the files that are stored on the drive, there is concern about the fact that the data is still not private as far as Google, itself, is concerned.

We propose the development of an add-on for Google Drive which will enable users to encrypt their files before storing them on the server so that data privacy is maintained with respect to the cloud service provider (Google Inc.) as well. The users can retrieve these files from the drive by downloading them. The add-on will decrypt the downloaded file and return the original file to the user.

Ensuring privacy of data stored on the cloud, from the cloud service provider itself, is the motivation behind our proposed project.

2 Security goals and features

The desired functionality here is that:

- It should provide encryption (and decryption) on a per-file basis
- It should be *easy to use*. The interface should be the normal Google drive plugin with a couple of extra buttons. The user should not be prompted to enter a password each time.
- *Security*: Secure key storage and symmetric encryption should uphold privacy of user's data.

3 Implementation outline

Initialization

- Generate a private key when a file has to be encrypted and uploaded to the drive for the first time.
- Encrypt the key using system password and store the encrypted key in the system. This will be used for encryption and decryption.

Upload

- Encrypt the file that has to be uploaded using AES block cipher in CTR (random IV) mode.
- Use Drive REST API to upload file to drive(in a folder named 'Encrypted Files'). Add an extension (eg. .enc) to distinguish from non-encrypted files

Download

- Download encrypted file from drive using Drive REST API
- Decrypt the downloaded file (if it has been originally encrypted using our software) and return the decrypted file to the user.