School of Computer Science & Statistics (SCSS)
Faculty of Engineering, Mathematics and Science

Secure Dropbox

Juntao Gu. Supervisor: Hitesh Tewari

Introduction

- Current storage systems secure data either via encrypting data on the wire, or through data encryption on the physical disk. Cryptographic protection of single file instances could prevent data modification or leakage during storage.

- The goal of the Secure Dropbox is to investigate the feasibility of gaining users' confidence towards the security of cloud storage service by utilization of a hybrid encryption mechanism in terms of data security and key management.

- Secure Dropbox is designed as a client end encryption tool over the Dropbox service. The main idea is to provide a file encryption service with symmetric cryptography where key is not known to Dropbox and ciphered with asymmetric cryptography for sharing encrypted file.

Design

Encrypted File Storage

$Cipher = E_{AES}(Plaintext, K)$

$K_{secure} = E_{RSA}(K, RSA_{public})$

Encrypted File Read

$K = E_{RSA}(K_{secure}, RSA_{private})$

$Plaintext = E_{AES}(Cipher, K)$

Encrypted File Storage

- In the file encrypted storage procedure, plain text is ciphered in AES with a random generated file encryption key. Then the file encryption key is ciphered in RSA with file owner's RSA public key as K_{secure}.

- In encrypted file reading procedure, firstly the ciphered K_{secure} should be deciphered in RSA with file owner's RSA private key. After retrieving the raw file encryption key K, the cipher text could be decrypted in AES.

Encrypted File Sharing

$K = E_{RSA}(K_{secure}, RSA_{private}\_A)$

$K_{sharing} = E_{RSA}(K, RSA_{public}\_B)$

Encrypted Shared File Reading

$K = E_{RSA}(K_{sharing}, RSA_{private}\_B)$

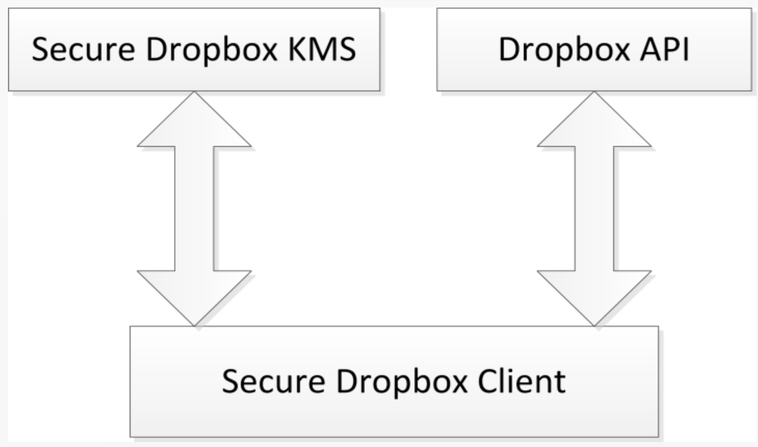
$Plaintext = E_{AES}(Cipher, K)$

Encrypted File Sharing

- A wants to share an encrypted file with B. In order to enable B to decipher the key ciphered by A, A should encrypt the raw doc key K in RSA with Bob's RSA public key. $K_{sharing}$ is generated and then transmitted to Bob via secure tunnels.

- After receiving the $K_{sharing}$, B will decrypt it in RSA with his own RSA private key and then get the raw doc key. Now the plain text of the shared encrypted file could be retrieved by decrypting in AES with the raw doc key.

Implementation



Secure Dropbox Architecture

- Secure Dropbox performs file operations like uploading, downloading and sharing via Dropbox Core API and Dropbox application. It performs cryptographic computations in the local host.

- Key Management Service (KMS) mainly processes key management requests and storage requests. No cryptographic computation involves in KMS.

Application Scenario	Target	Algorithm
Authentication	User password	SHA1
Plaintext file loading	File content / AES key	AES-256 / RSA-2048
Cipher file reading	Cipher AES key / Cipher file content	RSA-2048 / AES-256
Cipher file sharing	Cipher AES key / AES key	RSA-2048

Cryptography Application in Secure Dropbox

Conclusion

- Secure Dropbox accomplishes a client end encryption tool and the key ideas in accordance with security have been explained.

- Security of data in Secure Dropbox is based on strength of symmetric cryptography and key management with asymmetric cryptography.

- It gains users' confidence when using public cloud storage service to store their confidential documentations according to the user testing feedback.

M.Sc. in Computer Science

(Mobile and Ubiquitous Computing)

Contact Information

- Email: juntao.gu@gmail.com
- Mobile:083 1675390

TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH
THE UNIVERSITY OF DUBLIN

NDP National Development Plan 2007 - 2013