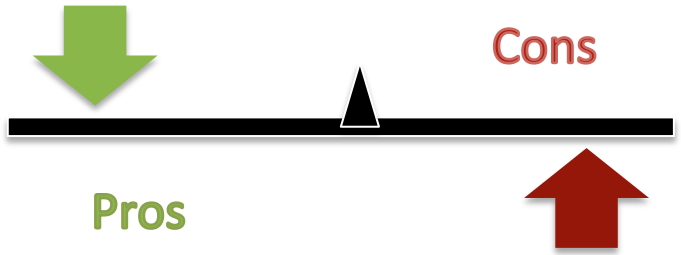
Analyzing the Security Schemes of Various Cloud Storage Services

ECE 646
Project Presentation
Fall 2014
12/09/2014

Team Members
Ankita Pandey
Gagandeep Singh Bamrah

Pros and Cons of Cloud Storage Services



PROS

- Flexibility
- Reliability
- Scalability
- Cost Effectiveness

CONS

- Users are unaware of the specific location of the data stored
- Third party (cloud service provider)access

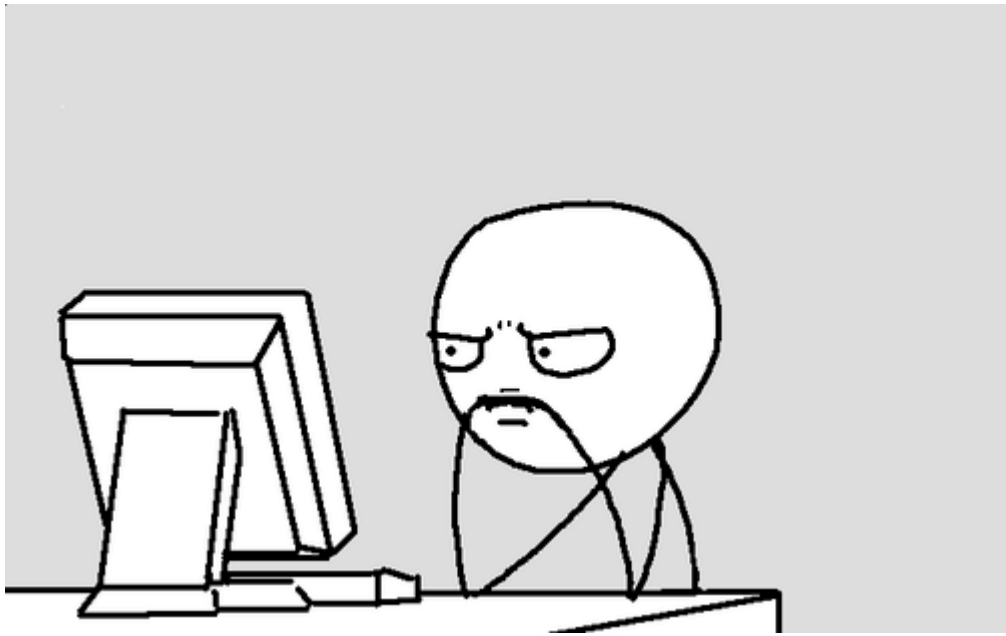
Security Standpoints

- Protecting the data in transit: From the hackers and eavesdroppers
- Protecting the data at rest
- Protecting the data from the cloud provider

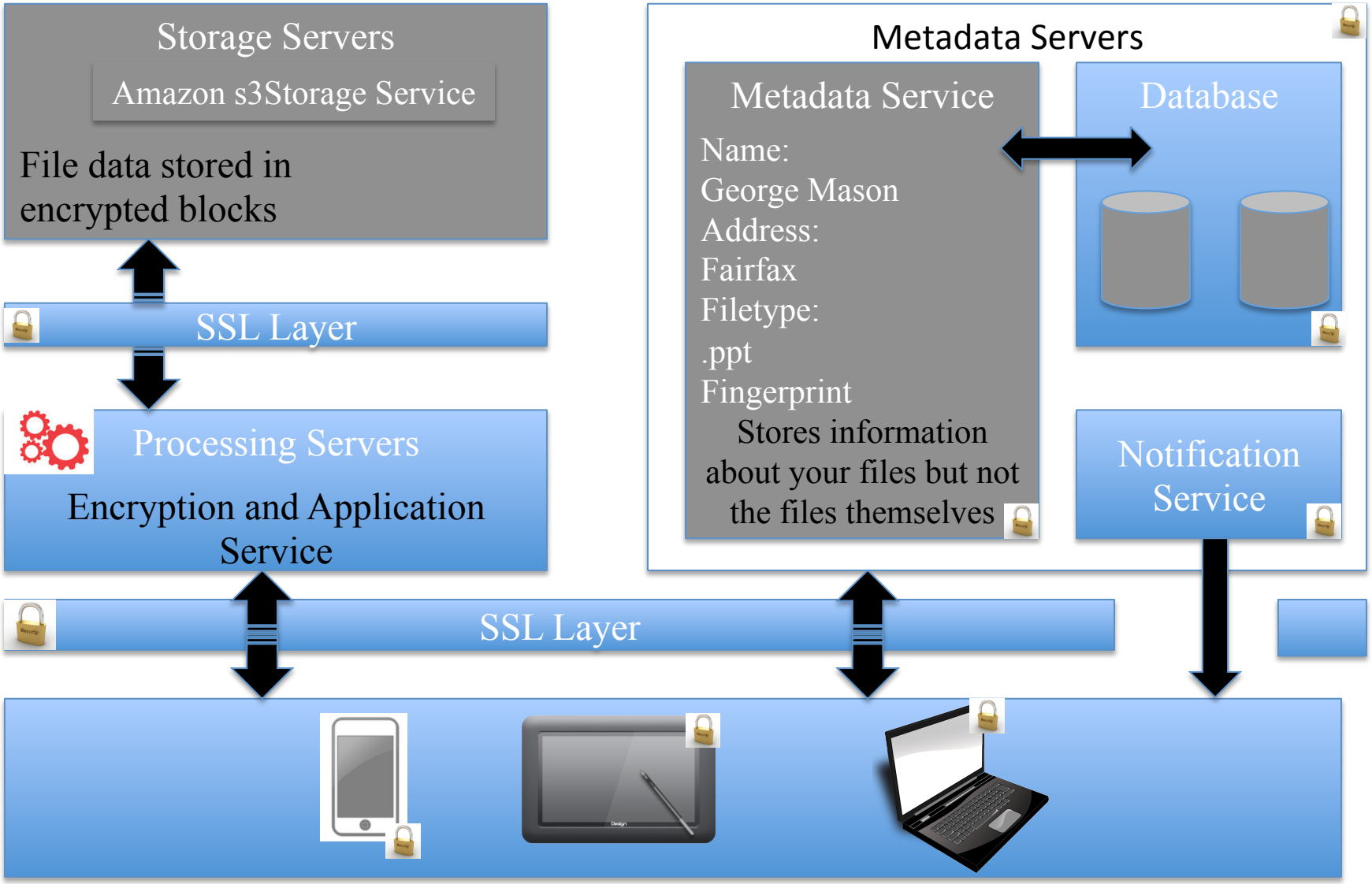
Encryption keys management

Options

- APPLE iCLOUD
- DROPBOX
- SPIDER OAK



Dropbox High Level Secure and Private Architecture



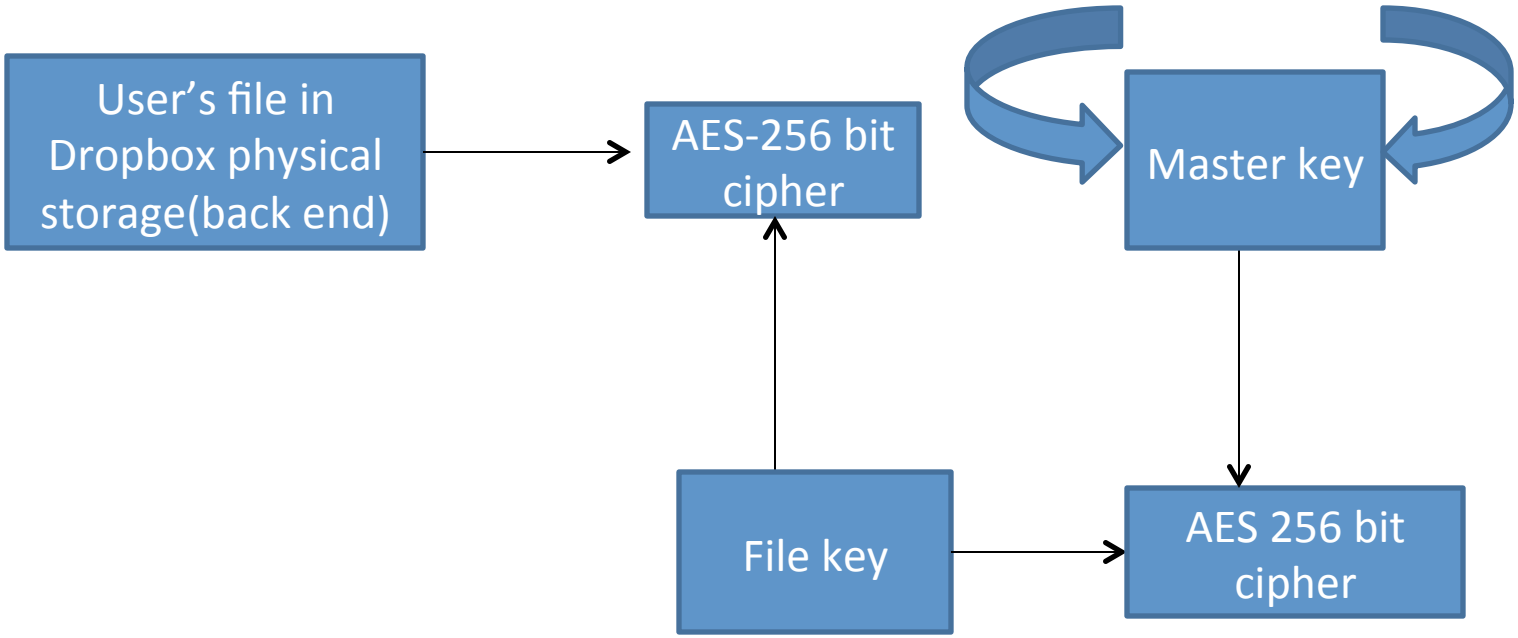
Securing Data in Transit

SSL/TLS : Provide a secure communication channel

- Identification and Authentication: Exchange of certificates to avoid man-in-the-middle attacks
- ECDHE_RSA : Key agreement protocol to establish the shared secret between the client and server
- Personal forward secrecy: Use of ephemeral RSA public-private key pair
- AES-128 bit GCM: Authenticated encryption algorithm using the shared secret key to provide data integrity and confidentiality

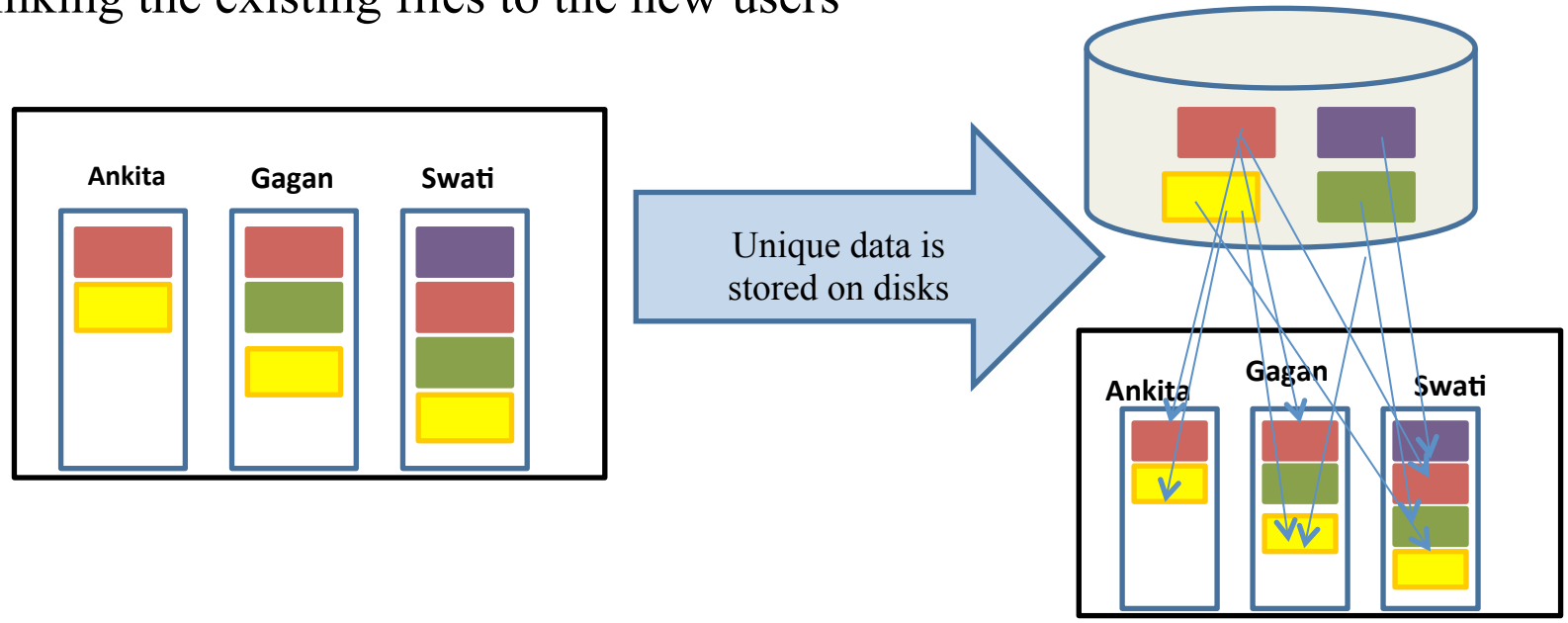
Securing Data at Rest (Server Side Encryption)(1)

- Each file(object) is encrypted using AES-256 bit cipher using a unique key which itself is encrypted through a periodically rotated master key using AES-256 bit cipher.



Data De-duplication in Dropbox

- Cryptographic hash function is generated (fingerprint) for every stored file
- The server just keep a database of file fingerprints and compare any new data to these fingerprints preventing the storage of any duplicated files and linking the existing files to the new users



Loopholes Analyzed in Dropbox

- For the data de-duplication dropbox looks in to the encrypted files with the possibility that the adversary (internal malicious employee) having access to backend storage can decrypt the file, if he acquires the key.

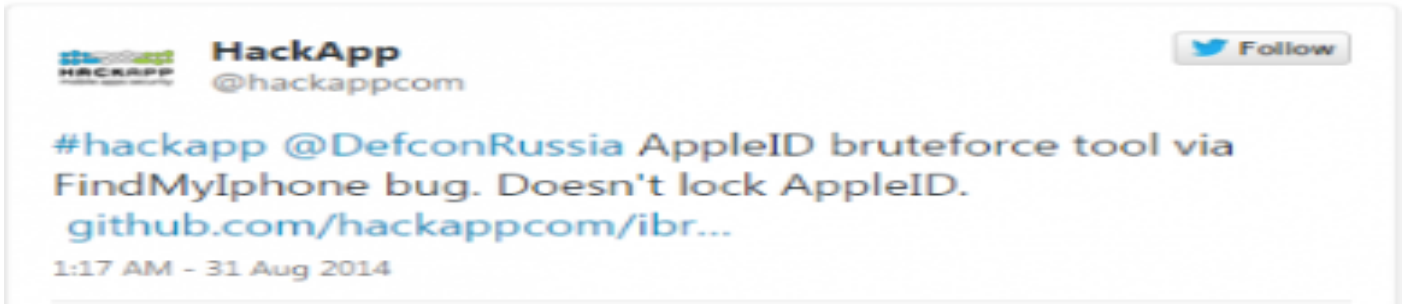
- Security issues with the shared links: Leaking private information of the dropbox users

Apple iCloud

Data	Encryption In Transit	Encryption On Server	Comments
Contacts	Yes	Yes	A minimum of 128-bit AES encryption
Reminders	Yes	Yes	A minimum of 128-bit AES encryption
Photos	Yes	Yes	A minimum of 128-bit AES encryption
Find My iPhone	Yes	Yes	A minimum of 128-bit AES encryption
iCloud Keychain	Yes	Yes	Uses 256 bit AES encryption to store ad transmit passwords and credit card information. Also uses Elliptic Curve Asymmetric cryptography and key wrapping.
iTunes in the iCloud	Yes	N/A	Purchased music files are not encrypted on server because they do not contain any personal information.

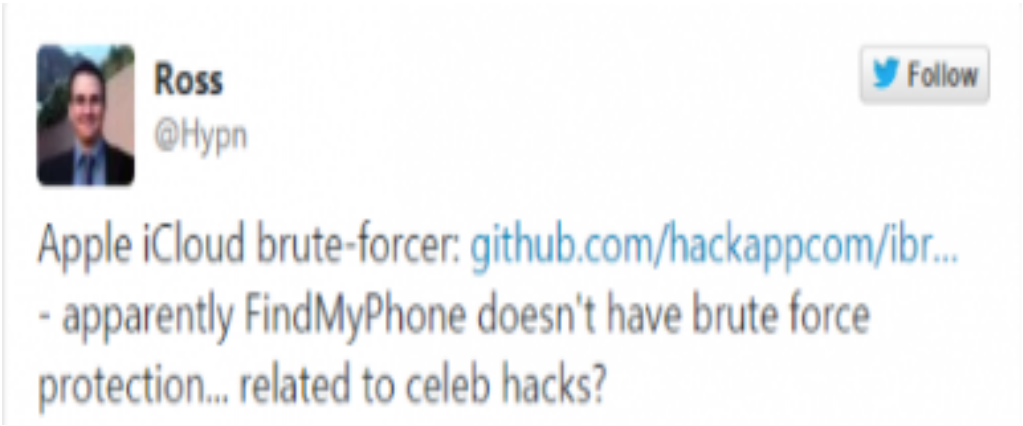
Loophole in iCloud

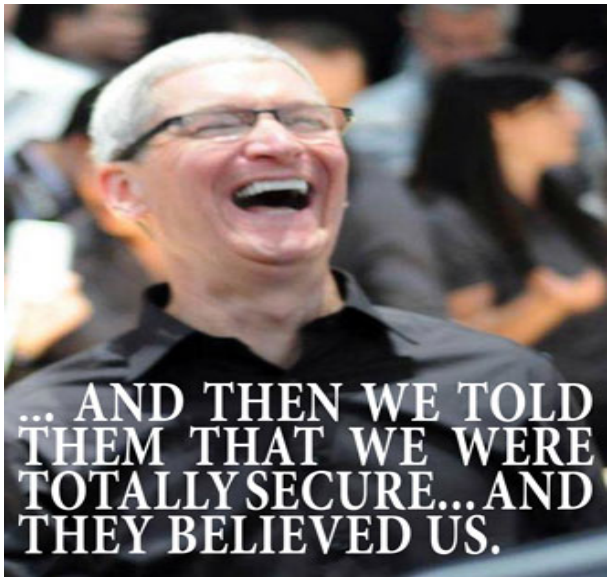
- According to post on Github.com, the Apple ID can be prevented from being locked after a certain number of attempts. This tool attempts to make an attack on Find My iPhone Services. So one can use brute force attack to get the access to the attack.

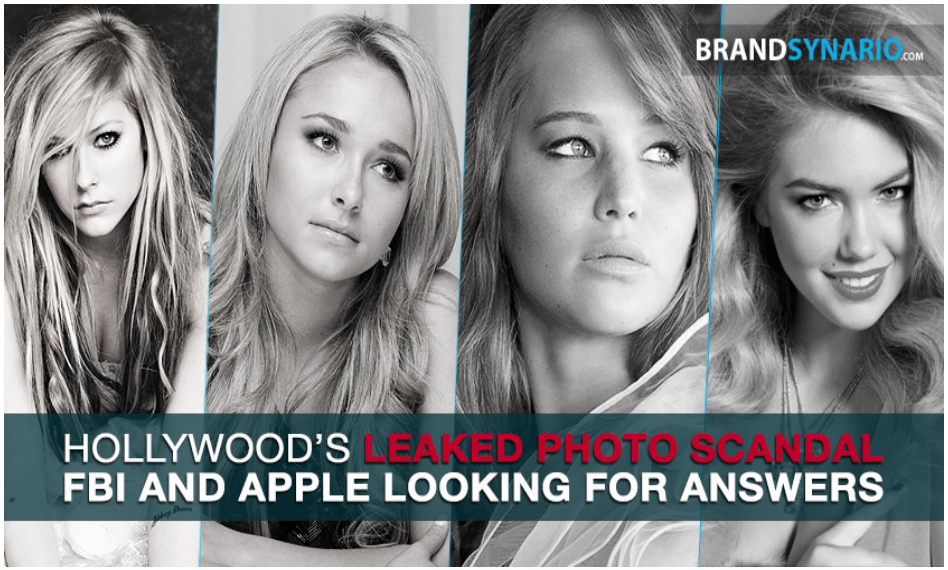


Recent Data Breaches(1)

Apparently, the adversary was believed to have the knowledge of the Apple IDs and was able to get through the security questions







Recent Data Breaches(2)

2012: Users were receiving spam emails on their email IDs

Investigation revealed that a Dropbox employee's password was compromised and was used to get access to the email IDs of the Dropbox users

15 October, 2014: Dropbox urged users to use two step authentication amid reports that the login attempts of millions of users have been compromised

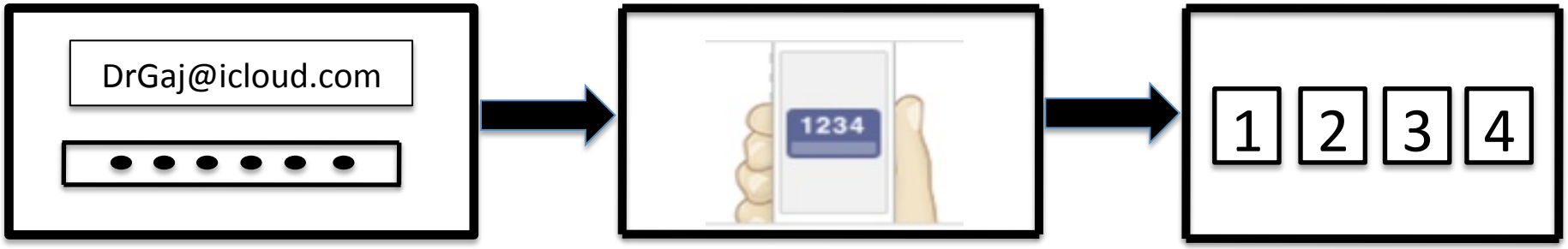
Source: Edward Snowden Interview with The New Yorker.

"**Dropbox is hostile to privacy**"

"Get rid of Dropbox, use SpiderOak

Reducing Susceptibility to Attacks

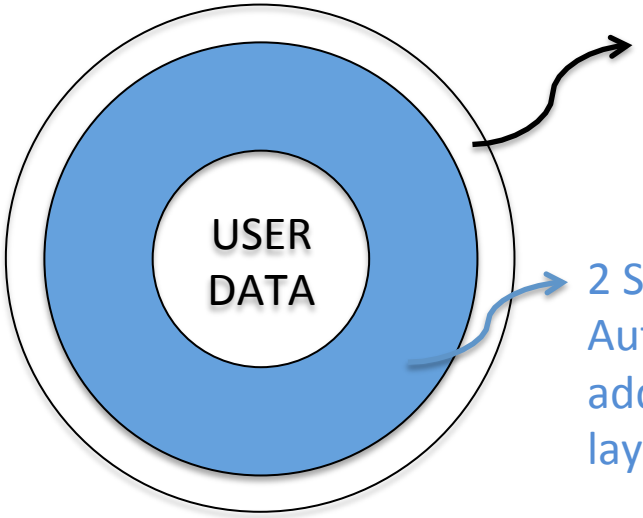
2 STEP AUTHENTICATION :



The User enters the ID and Password.

The cloud service provider sends a verification code.

The User enters the code to verify identity.

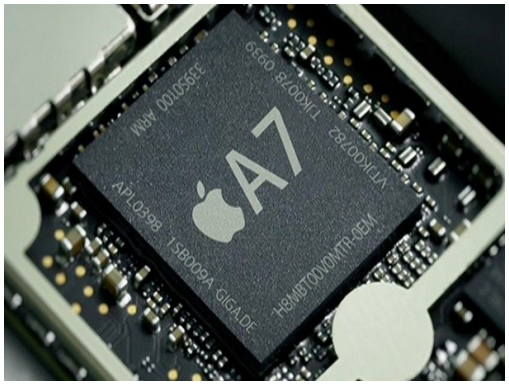


Security by password

2 Step Authentication adds an extra layer of security

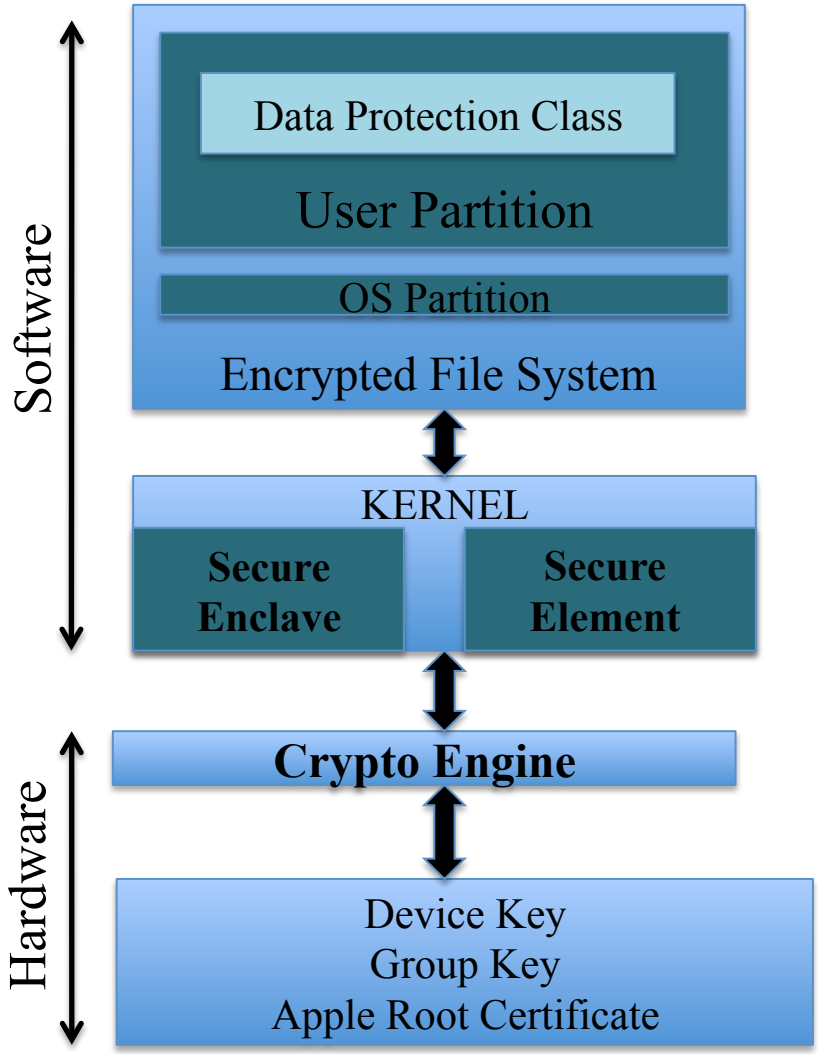
- Security code (Time Based One Time Password)
- TOTP: Hash based message authentication code HMAC(K,C)

Implementation of Secure Enclave in iPhones



Source: Apple iOS Security Guide (pdf)

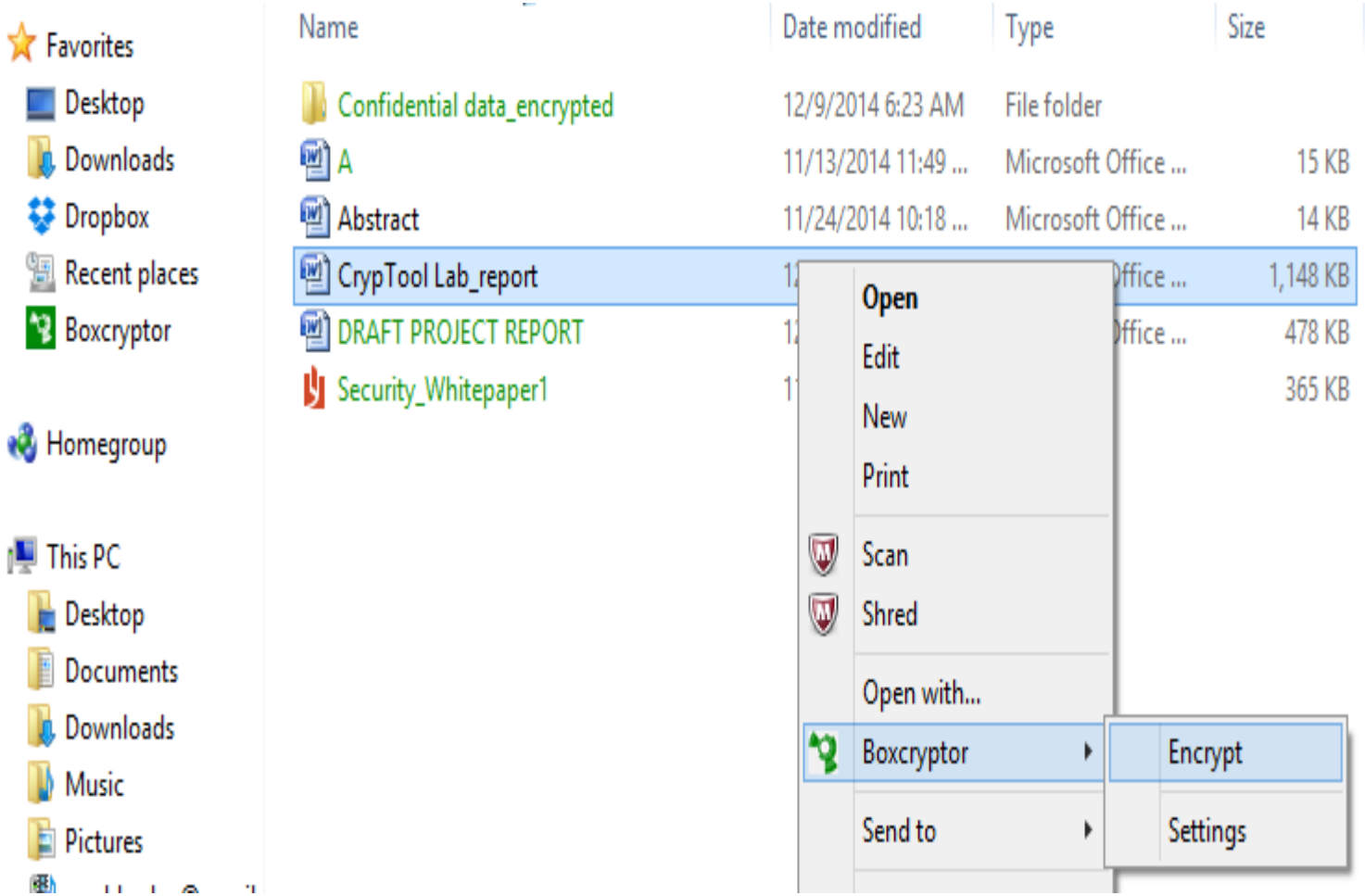
- Secure Enclave is a coprocessor within the A7 chip
- Contains a unique ID (UID) inaccessible to other parts of the system.
- Inaccessibility to Apple and any other third party
- Used to prevent access to Apple ID (and thus iCloud) by storing the fingerprint data.



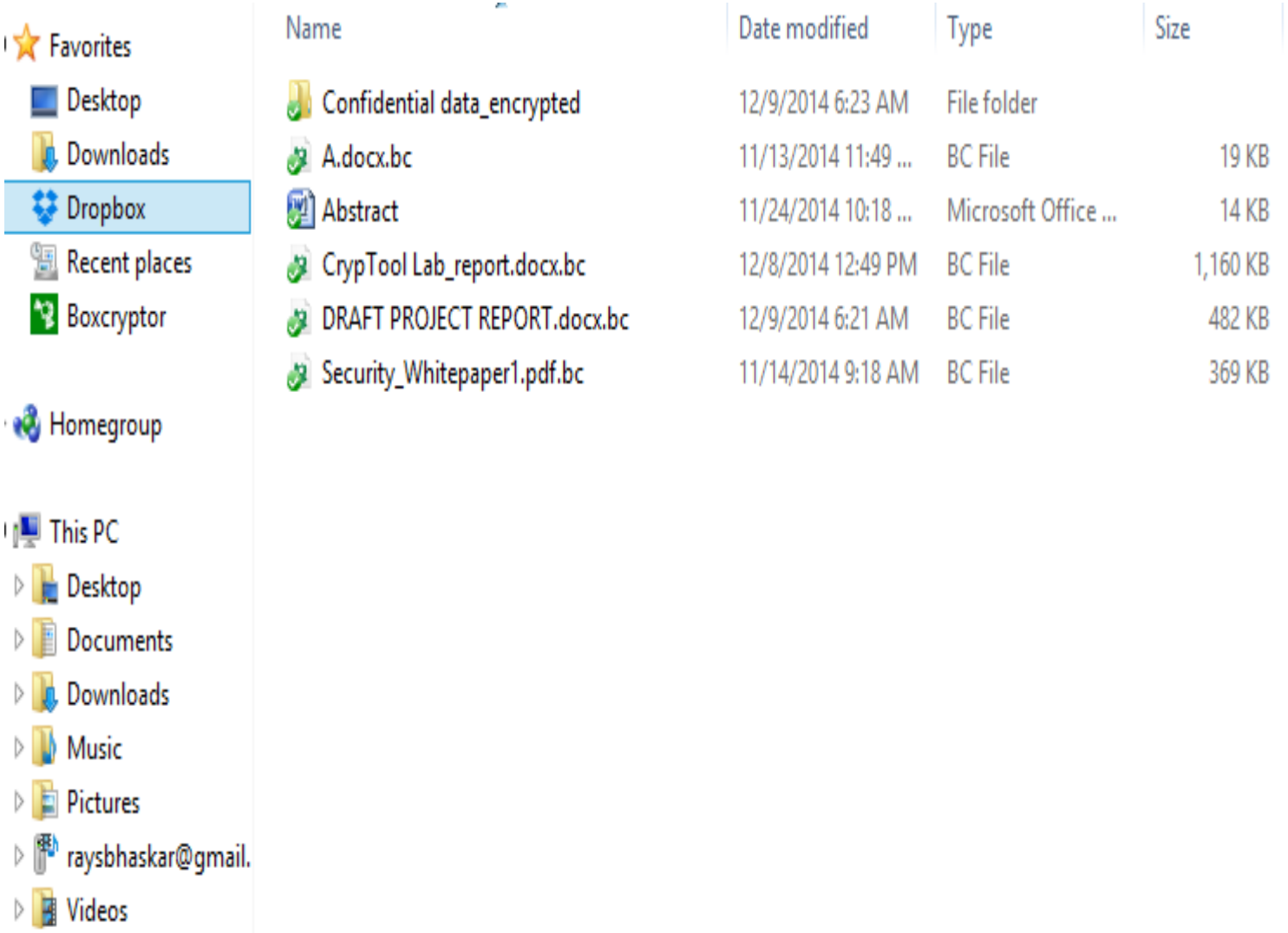
Boxcryptor (Client Side Encryption for Dropbox)

- Secure use of Dropbox cloud storage services
- Creates a virtual drive in the computer for encrypting the files locally before storing them in the cloud
- Boxcryptor uses AES 256-bit cipher and Asymmetric RSA cipher to encrypt the files stored in the cloud
- Zero knowledge software: Any information that is stored is encrypted by the user's password

Encrypting Files for Dropbox



Dropbox view using Boxcryptor



Encryption in Boxcryptor

Username and password

Hash of the password

Password key is derived using PBKDF2 with HMAC_SHA512 along with the 24 bytes salt

Public key of user

Private key of user

RSA-4096

RSA-4096

Password Key

Data in cloud

File Key

AES-256 bit cipher

AES-256 bit cipher

AES-256 bit cipher

Wrapping Key

Boxcryptor (Securing Dropbox)

- Internal attacks (malicious employees): The encrypted data cannot be decrypted without the user's password

- External attacks (hackers): Even if the adversary gains the knowledge of a user's dropbox account (by resetting the password), all he can view are the group of encrypted files

SpiderOak Cloud Storage Services

- Client Side Encryption + Data Storage
- Zero knowledge privacy
- Only the owners of data have access to encryption keys
- Encryption keys generated on computer instead of browser
- Data is safe from employees as well as hackers

No option for Password Resetting

Password loss results in data loss

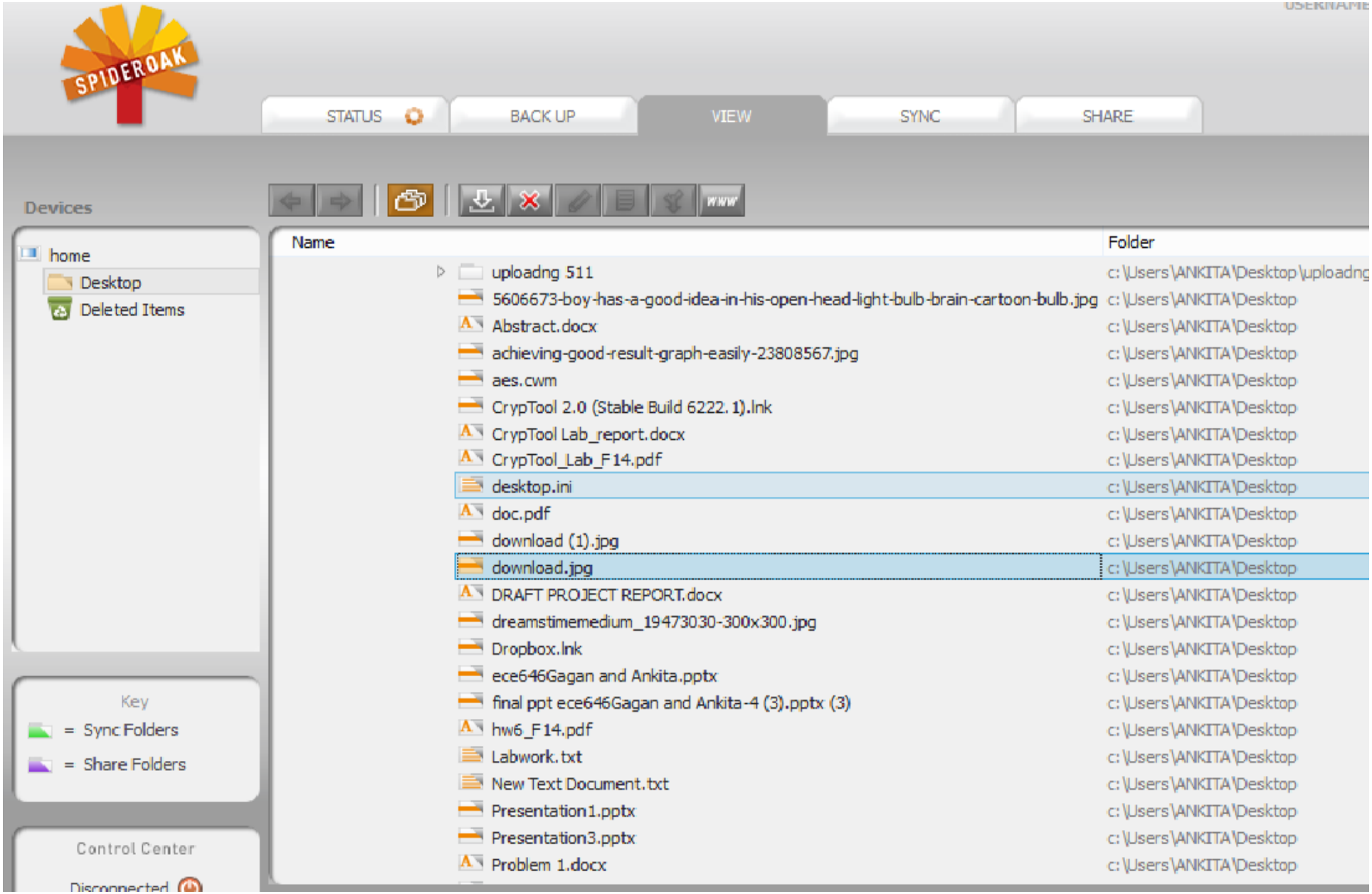
SPIDEROAK SECURITY

Uses AES-256 in CFB mode to encrypt the data with a unique key.

Unique key is secured with the key derived from the user's password by using PBKDF2

PBKDF2 = SHA-256 (Password, salt)

Encrypted File Storage in SpiderOak



Comparison of the Cloud Services

Tool	Securing Data At Rest	Securing Data In Transit	Platforms	Storage Facilities
	Cipher for encryption	**Cipher for encryption**		
Dropbox	Server side encryption and storage AES-256 bit cipher	SSL: AES-128 Galois counter mode, ECDHE_RSA	Windows, Linux, Mac OS X , Android, Blackberry, iOS	Uses Amazon Cloud Storage facilities
Boxcryptor (software tool for encrypting dropbox)	Client side encryption software AES- 256 bit cipher and RSA-4096	SSL:AES-128 Galois counter mode, ECDHE_RSA	Window, Mac OS X, Android, Blackberry, iOS	Not Applicable
SpiderOak	Client side encryption and storage AES-256 bit cipher and 3072-bit RSA	SSL:AES-128 Galois counter mode, ECDHE_RSA	Window, Mac OS X, Blackberry, iOS	Own Storage Facilities
iCloud	Server side encryption AES-256 or 128 bit cipher	SSL:AES-128 Galois counter mode, ECDHE_RSA	Windows, MAC, iOS Linux, Blackberry, Android: via storage made easy client	Own Storage Facilities

Conclusion

Based on the cryptographic point of view

- All the cloud storage services are using the best cryptographic algorithms available to keep up with the competitors. Differentiating them on the basis of cryptographic algorithms is inappropriate.

Based on the number of attacks

- Dropbox is facing strong criticism from the users due to increased number of attacks.
- iCloud offers more security than dropbox but the past data breach raises questions on its secure environment.

Based on the nature of the clouds

- User's data is always in a vulnerable state in the cloud storage services supporting server side encryption.
- Try to use clouds that are less popular but use strong ciphers for encryption. Hackers keep their eyes on services that are popular in the market.

Client side encryption: Best way to ensure data privacy and security (strong passwords)

- SpiderOak is gaining popularity over Dropbox and iCloud
- No notable attacks on SpiderOak so far
- Boxcryptor encryption tool provides refinement to the server side encryption based cloud storage services


Thank you


Q&A