Security Issues with Sharing (Cloud Storage Services)

Kalyani Haridasyam
EECS710: Information Security and Assurance
University of Kansas

Topics

- Introduction
- Data Sharing
- Dropbox and Sharing
- Dropbox Security Weaknesses
- Google Drive and Sharing
- Google Drive Security Weaknesses
- Microsoft SkyDrive and Sharing
- SkyDrive Security Weaknesses
- The Security of Secret-URL Sharing
- Acknowledgement

Introduction

- Cloud storage and synchronization services let users access their digital content any time, from anywhere, and with any device.
- To ensure the security of a cloud storage service, all communications between users and the CSP(Cloud Service Provider) are encrypted, so nobody can eavesdrop on the data during uploading or downloading.
- However, once users hand over their data to the CSP and begin sharing it with others, the security of that data can move beyond their control.
- Several **security weaknesses in sharing mechanism that could lead to data leakage without users' awareness** are presented here.

Data Sharing

- **Public Sharing –** the data is intended for the public, so there's no access control
- **URL Sharing –** the owner shares the data with others by sending them a sharing URL generated by the CSP.
- **Secret Sharing –** the owner must specify who can access the shared data

Dropbox and Sharing

- Hosted on Amazon Simple Storage Service.
- **Public Sharing URL –** http://dl.dropbox.com/u/10312344/cloud1.pdf, where **"10312344"** is a sequence of decimal numbers identifying a **user's public folder**.
- Secret URL – https://www.dropbox.com/s/192tmt67scsel57/cloud.pdf, where **"192tmt67scsel57"** is an alphanumeric sequence identifying **exactly a file**.
- The private sharing is only provided for folders

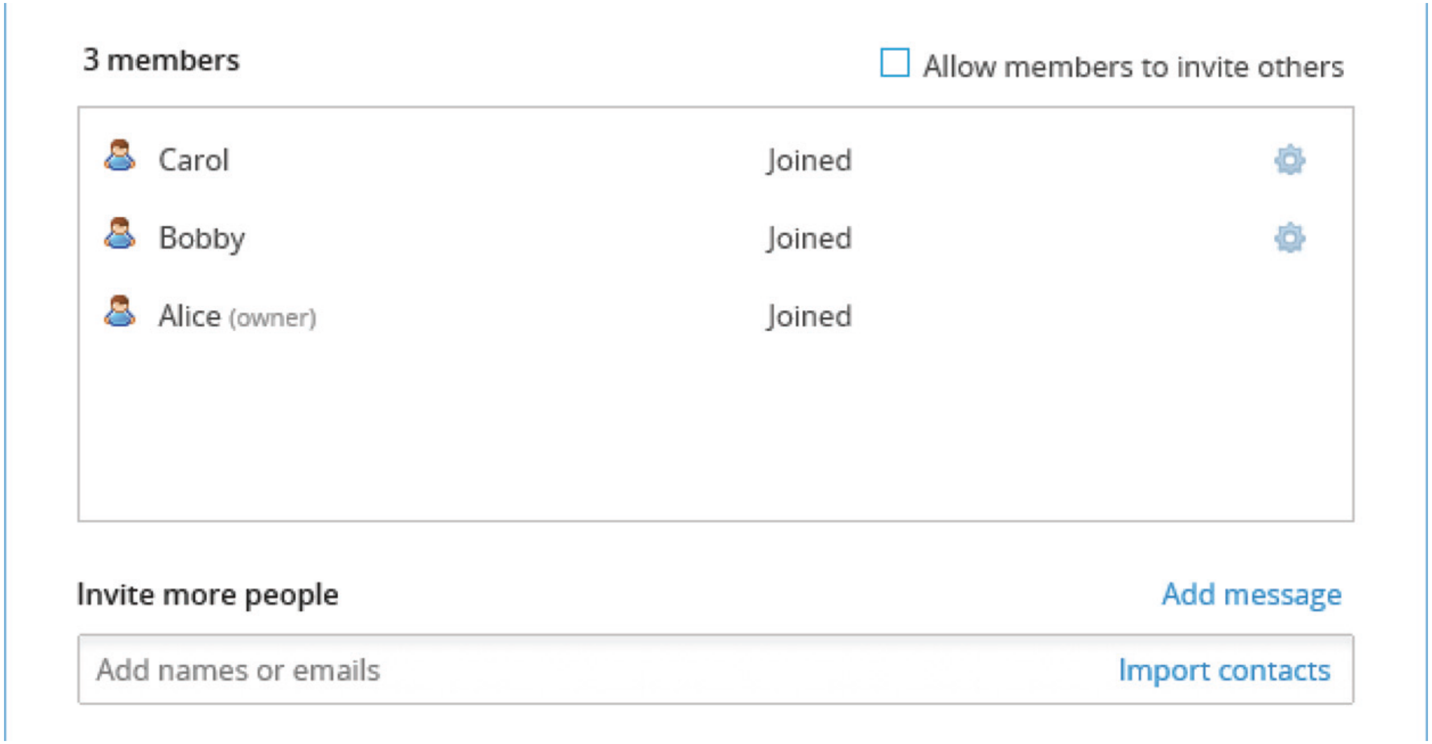
Dropbox Security Weaknesses

- **Nondead**
  - The Secret URL link remains **“nondead,” after the file is removed**. Later, if some other file object is associated with the same file name, user with Secret URL can access the new object even when the new object is ‘private’.
- **NonHTTPS shortened URL**
  - The **shortened URL isn’t SSL protected**, and an eavesdropper could acquire the link and access the file.

Dropbox Security Weaknesses Contd.

- **Unauthorized resharing**
  - User with whom a folder is shared **can share the folder or some of its files** using secret-URL sharing.
- **No privacy on sharing**
  - Anyone with access to sharing folder can learn **the identities of other people** with access to the folder.
- **Uncertain identities**
  - The invitation link to register a new account with any email address to access the sharing folder

The private sharing options for a folder named "paper" in Dropbox.



3 members

□ Allow members to invite others

Carol	Joined	⚙
Bobby	Joined	⚙
Alice (owner)	Joined	

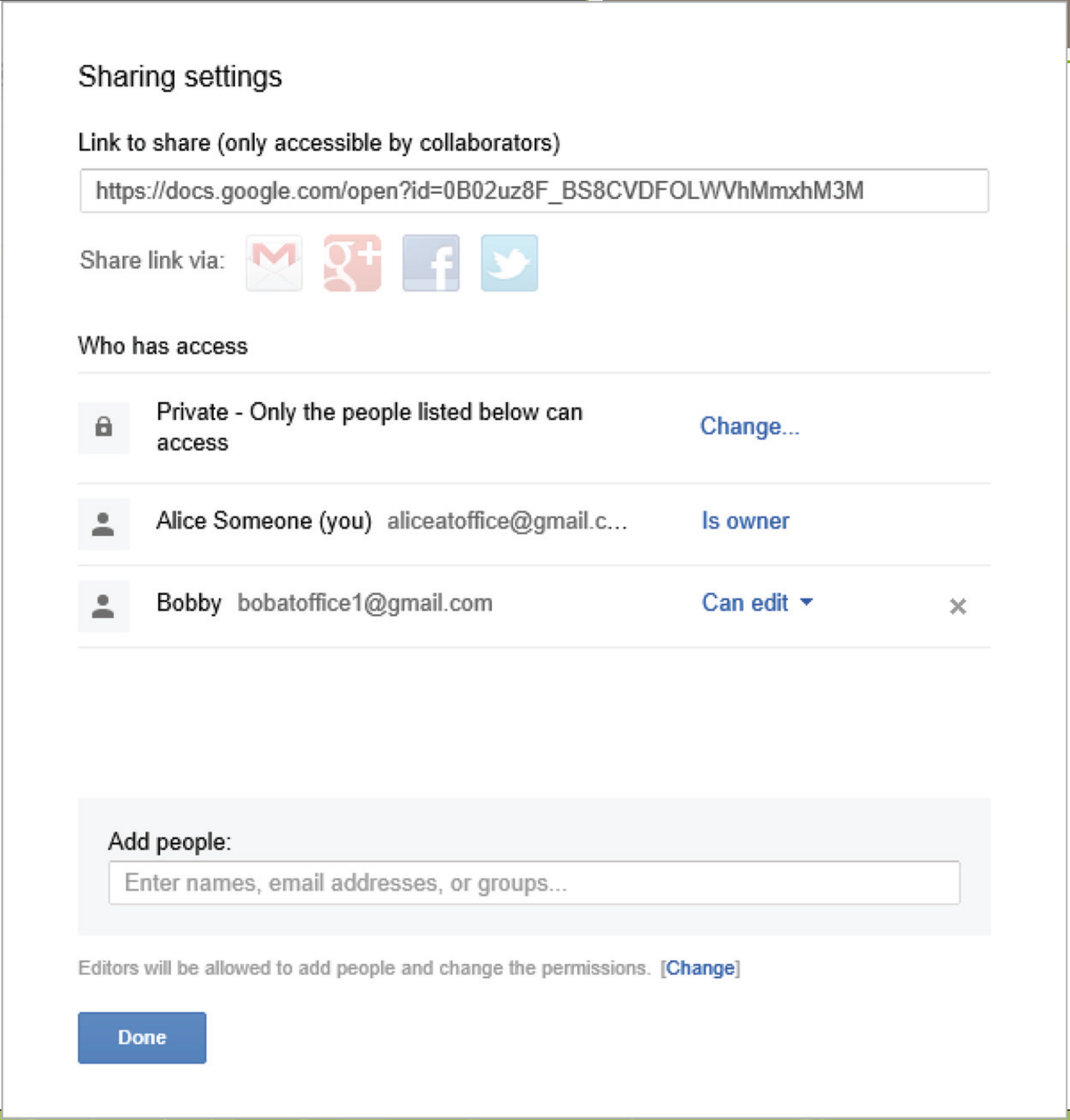
Invite more people

Google Drive and Sharing

- Each file, once uploaded, is associated with a unique URL.
- Regardless of the sharing method employed, **the file's associated URL remains fixed**. Access to the file depends on the file's sharing settings.
- The visibility option are "private" ,"public on the Web" and "anyone with the link".

Google Drive Security Weaknesses

- **Sharing of trash files**
  - People can access the deleted file (in the trash folder) via the same URL as before, no matter the share mechanism.
- **Fixed URL**
  - Once the URL is published, it’s not possible to recall this public information. Someone who already got the URL can still access the file even after it is made private.
- **Unauthorized resharing**
  - The invitation URL can be used multiple times. The invitation URL can be redistributed to let other people sign in to the system with other Google accounts and can access the file.



Sharing settings

Link to share (only accessible by collaborators)

https://docs.google.com/open?id=0B02uz8F_BS8CVDFOLWVhMmxhM3M

Share link via:

Who has access

Private - Only the people listed below can access — Change...

Alice Someone (you) aliceatoffice@gmail.c... — Is owner

Bobby bobatoffice1@gmail.com — Can edit ▾ ×

Add people:

Enter names, email addresses, or groups...

Editors will be allowed to add people and change the permissions. [Change]

Google Drive Security Weaknesses Contd.

- **Indiscriminate accessing URL**
  - Any file is accessed via the associated URL, even for the file owner. If the file is accessed while using a projector, **the URL will be shown in the browser's address bar**.
- **No privacy on sharing**
  - As in Dropbox, people who have access to files **can learn each other's identities**.
- **Uncertain identities**
  - Some email addresses shown on the sharing list might be confusing because invitations were not sent to those addresses.

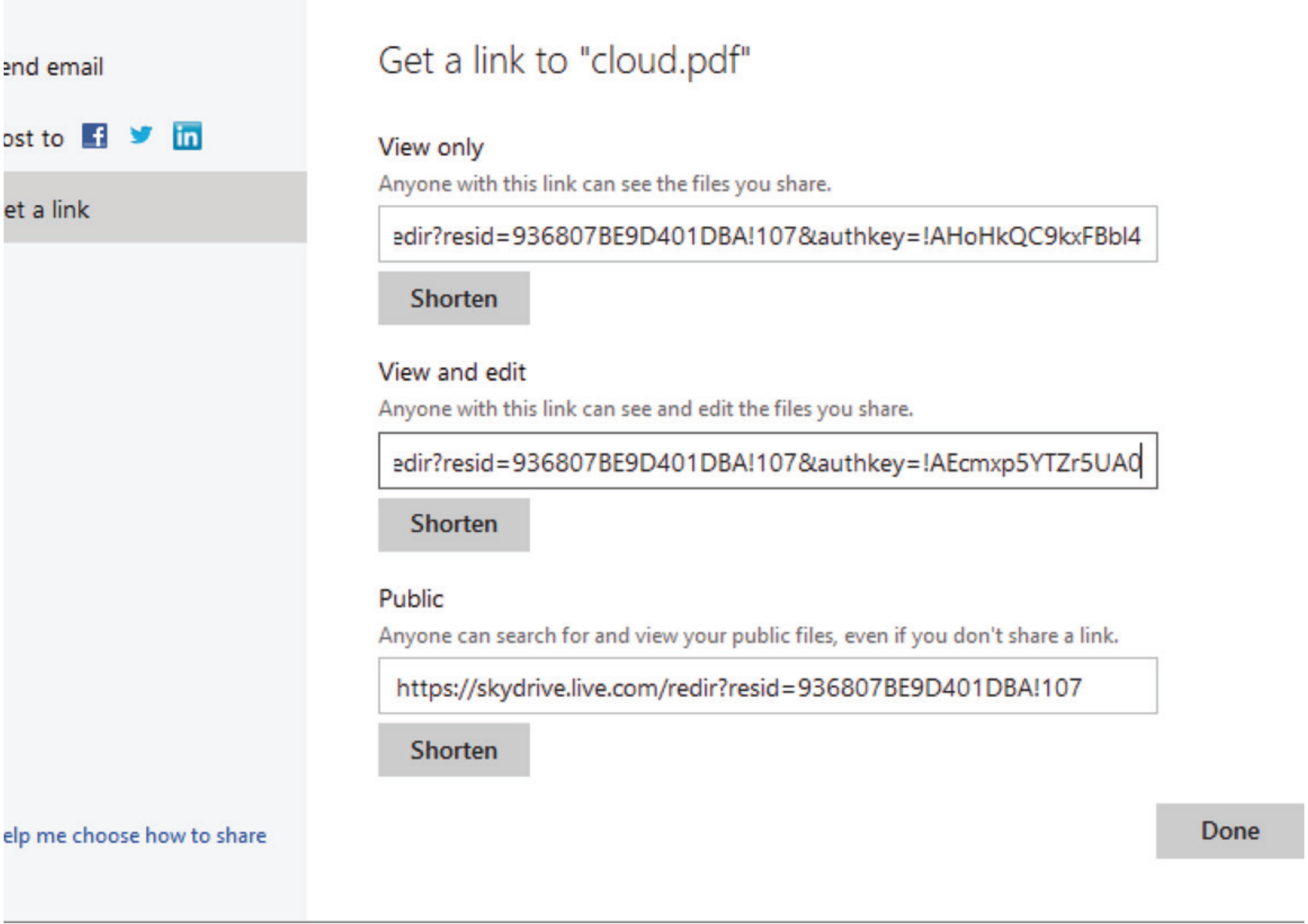
Microsoft SkyDrive and Sharing

- Microsoft SkyDrive also supports the three sharing methods, but in a relatively more secure way.
- In Microsoft SkyDrive, **each file is has a fixed resource ID which can be made public**. All users, including the file owner, must access the file via a URL containing the resid.
- The access permission of a shared file is controlled by an **additional secret authentication key (“authkey”)**, which can be appended to the sharing URL.

Microsoft SkyDrive and Sharing Contd.

- Owner can control user’s permission by sending the URL with the corresponding authorization key. **This key can be revoked when owner wants to stop sharing** the file, and it can be regenerated when owner wants to share it again.
- User will need to sign into the system using Microsoft account (in the form of an email address) before accessing a shared fie.
- The system lets owner send a URL with an authorization key to user via email. **The authorization key can only be used once**.

The sharing settings for a file in Microsoft SkyDrive. Each file is associated with a fixed resource ID (“resid”).



Get a link to "cloud.pdf"

View only

Anyone with this link can see the files you share.

edir?resid=936807BE9D401DBA!107&authkey=!AHoHkQC9kxFBbl4

View and edit

Anyone with this link can see and edit the files you share.

edir?resid=936807BE9D401DBA!107&authkey=!AEcmxp5YTZr5UA0

Public

Anyone can search for and view your public files, even if you don't share a link.

https://skydrive.live.com/redir?resid=936807BE9D401DBA!107

SkyDrive Security Weaknesses

- **NonHTTPS shortened URL**
  - Microsoft SkyDrive provides a URL-shortening service for **secret-URL sharing which is not protected by SSL**. The URL is in a form such as http://sdrv.ms/WEkgCn, where "WEkgCn" is a case-sensitive alphanumeric sequence. With the the number of possible combinations it's not hard for an attacker to perform an exhaustive search.
- **Uncertain identities**
  - Even if owner sends the sharing email to one of user's Microsoft accounts, **user can still sign in with any Microsoft account**. This makes it difficult for owner to identify the users with whom the file is shared.

The Security of Secret-URL Sharing

- Obtaining the URL is equivalent to obtaining the data. There are many possible “covert” channels where the secret URL might be revealed.
- **Browsing Logs**
  - URLs are saved in log files on various servers. The logs aren’t well protected. **Secret URLs will likely be saved in plaintext in the log files** and thus can later be divulged. In case of Internet access via a proxy, even if the connection to the destination server is protected by SSL the intermediate proxy server, independent of the CSP, can still record in its log file the entire URL in plaintext.

The Security of Secret-URL Sharing Contd.

- **Browser History**
  - **Web browsers save the entire URL** which cause situation where the URL can be leaked.
  - JavaScript Web applications, exploiting "history sniffing," **could reveal the user's browser history to third parties**.
  - The **browser send the browsing history** to its software developer for analysis which could cause inadvertent leakage of secret URLs.
  - **Not clearing browsing history**, even after using a public computer to access the shared data.
  - The URL might be sent in the **referral request header**

The Security of Secret-URL Sharing Contd.

- **Bookmark**
  - Users may bookmark a secret URL sent by an owner securely. The URL will be stored in plaintext and might then be **synchronized with user's other computers**, because browsers can save bookmarks in the cloud.
- **URL Shortening**
  - The **URL will be sent out in plain text** and is subject to eavesdropping.

Acknowledgement

- Cheng-Kang Chu; Wen-Tao Zhu; Jin Han; Liu, J.K.; Jia Xu; Jianying Zhou
- "Security Concerns in Popular Cloud Storage Services,"
- *Pervasive Computing, IEEE* , vol.12, no.4, pp.50,57, Oct.-Dec. 2013