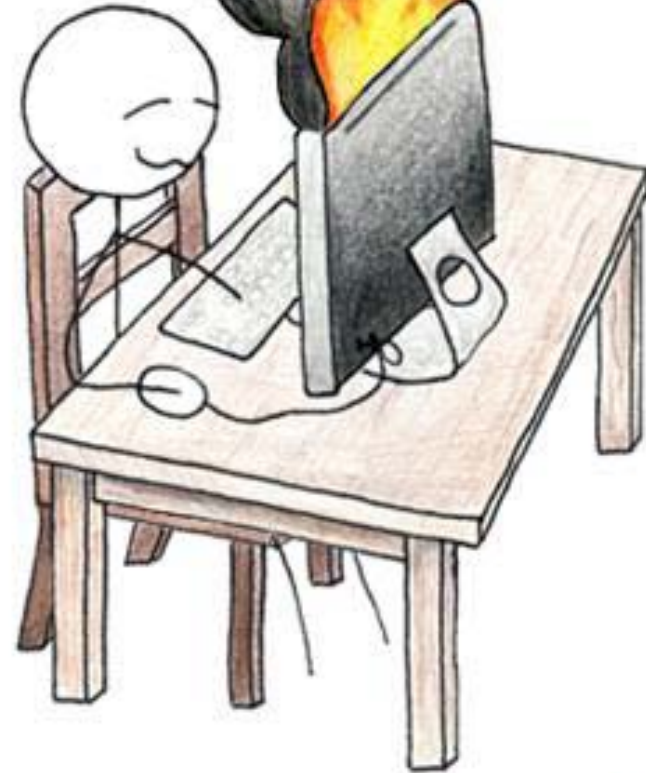


UM... ISN'T YOUR  
COMPUTER ON FIRE?



IT'S OKAY, MY FILES ARE  
SAVED ON **DROPTBOX**.  
IT WAS GETTING KINDA  
COLD IN HERE ANYWAY.



# SECURITY ISSUES WITH DROPTBOX

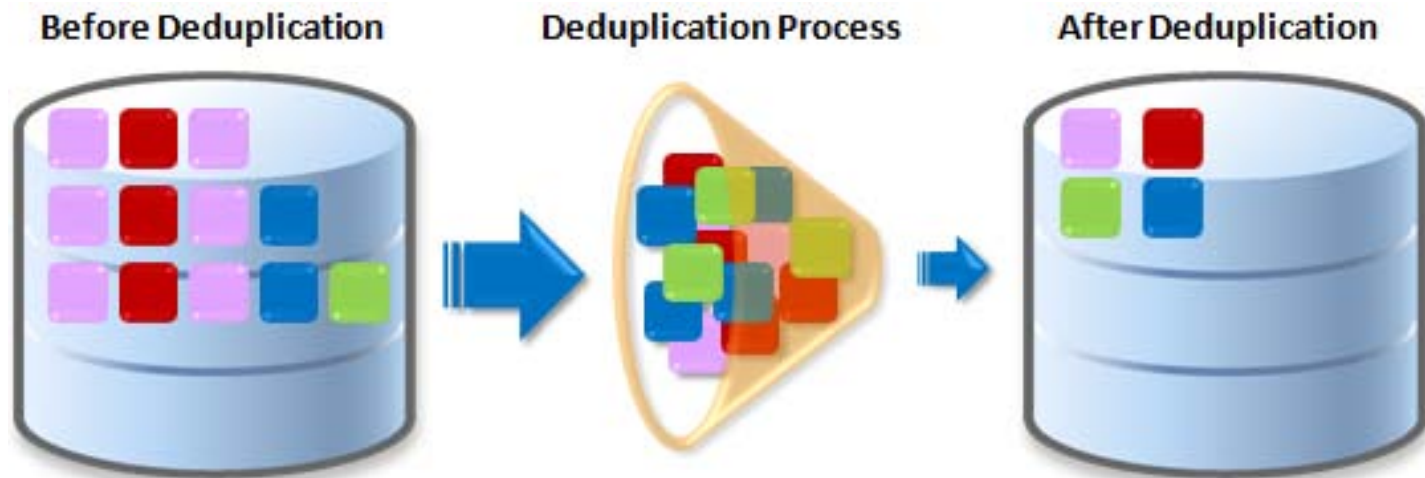


Sanaz Bahargam

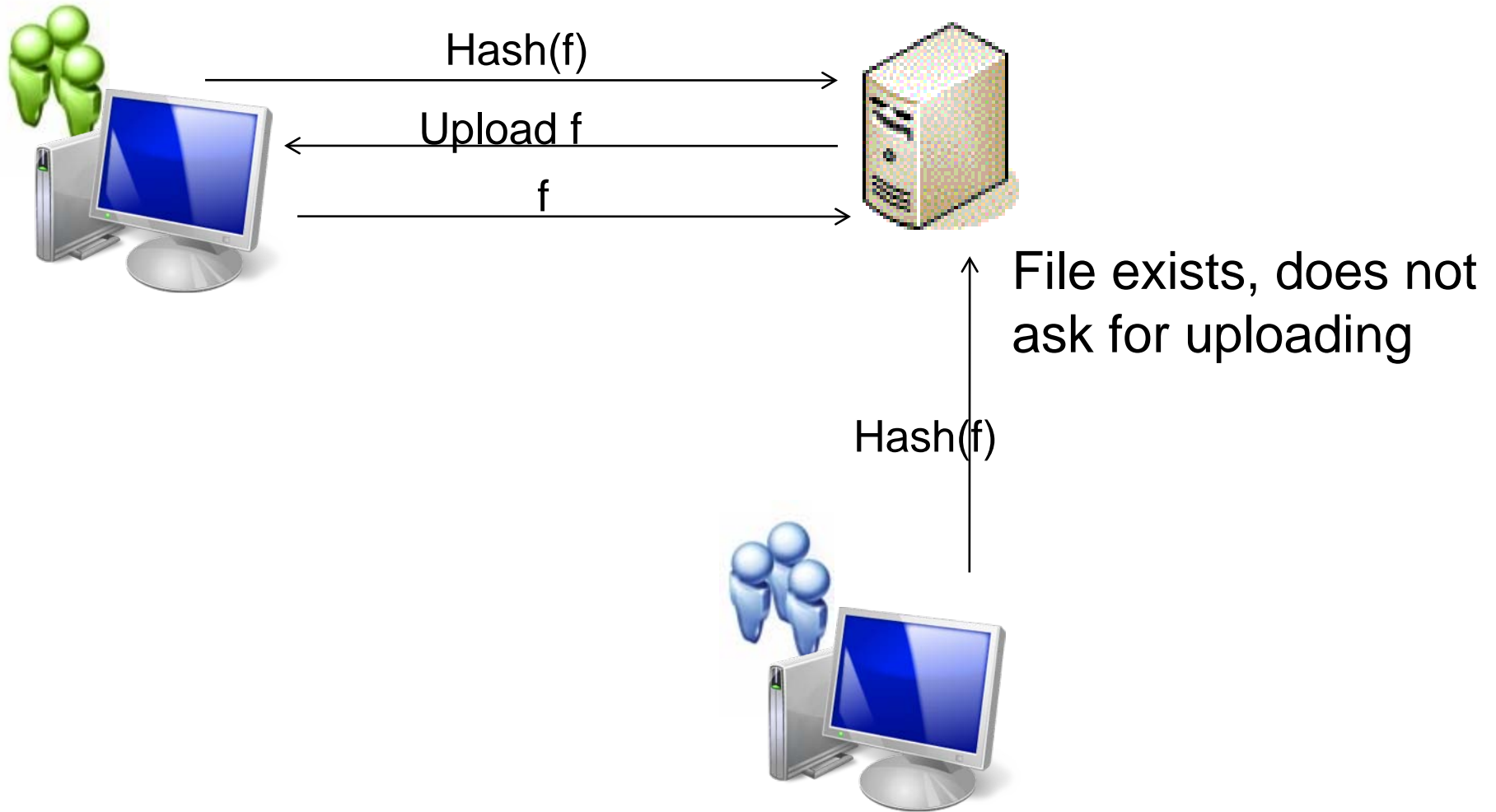
# How Dropbox works?

**Dropbox** is a Web-based file hosting service operated by *Dropbox, Inc.* that uses networked storage to enable users to store and share files and folders with others across the Internet using file synchronization

Using deduplication to save *storage space* and *bandwidth*



# Deduplication



# Is deduplication Secure?!



No!

It is possible to determine if any given file is already stored by one or more Dropbox users

If you have the hash of file, you have the file itself.

You can guess a hash and tell Dropbox you want to upload a file with that hash, if a file with that hash exists, you are the file's owner.

# Any solution?

Proof-of-ownership is a protocol in two parts between two players on a joint input  $F$ .

First the verifier summarizes the input file  $F$  and generates a verification information  $v$ .

Later, the prover and verifier engage in an interactive protocol in which the prover has  $F$  and the verifier only has  $v$ , at the end of which the verifier either accepts or rejects.

# Encryption



The service tells it "uses the same secure methods as banks and the military to send and store your data" and that all files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without users' password.

Dropbox does not ask for Key! Is key stored at Dropbox??

But Dropbox claims its employees do not have access to encrypted files

Is it possible to have both encryption and deduplication!?

# Authentication

SQLite Database Browser - C:/Users/Alex/Dropbox/Projects/db hack/config.db

File Edit View Help

Database Structure Browse Data Execute SQL

Table: config

New Record Delete Record

	key	value
1	config_schema_version	1
2	show_bubbles	1
3	last_update	(F1301572909.2149999
4	host_id	
5	dropbox_path	C:\Users\Alex\Dropbox
6	root_ns	11475598
7	email	
8	stats_dont_send_until_upgrade	
9	stats_next_report_time	1303776605.712
10	stats_next_report_id	153692481
11	stats_build	S'Dropbox-win-1.0.28'
12	ns_p2p_key_map	(dp1...
13	sandboxes	(lp1
14	recently_changed3	(lp1...

< 1 - 14 of 14 >

Go to: 0

# Any problem?



In Windows, the config.db file is completely portable and is **not tied** to the system in any way

If you gain access to a person's config.db file (or just the host\_id), you gain complete access to the person's Dropbox until such time that the person removes the host from the list of linked devices via the Dropbox web interface



# Reference:

- <http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/>
- <http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html?showComment=1302661727678>
- <http://seoonlinesource.blogspot.com/2012/01/how-dropbox-sacrifices-user-privacy-for.html>
- [http://www.discourse.net/2011/04/dropbox-is-much-less-private-than-i-thought.html?doing\\_wp\\_cron=1334762919](http://www.discourse.net/2011/04/dropbox-is-much-less-private-than-i-thought.html?doing_wp_cron=1334762919)
- [http://en.wikipedia.org/wiki/DropBox#cite\\_note-76](http://en.wikipedia.org/wiki/DropBox#cite_note-76)
- *Proofs of Ownership in Remote Storage Systems*, Shai Halevi, Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, ACM-CCS 2011