The LastPass Hack

R.Abarrota, M.Bandali, S.Merante

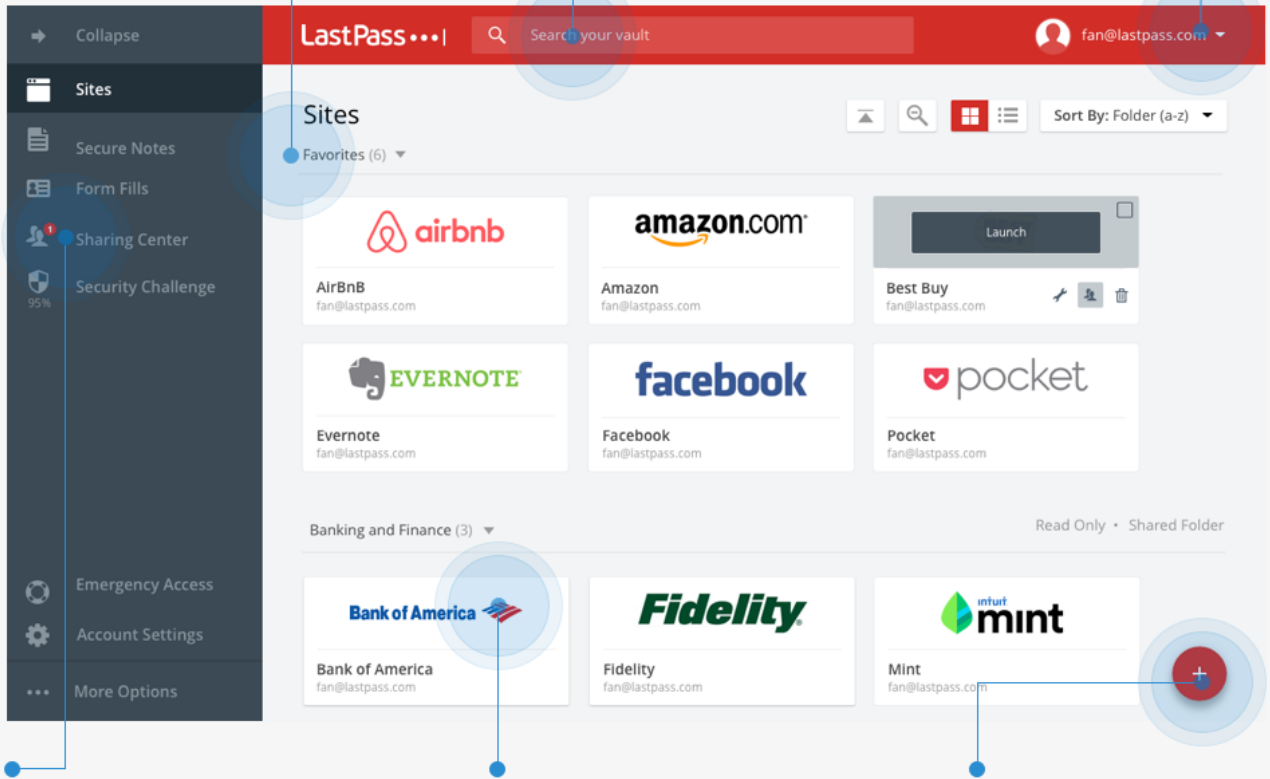
What is LastPass?

- Freemium password management service
- Web-based
- Stores passwords in cloud

Folders
Drag and drop logins into folders to keep them organized.

Search
Easily search for any item stored in the vault.

Sync
Your account is synced and available everywhere you need it.

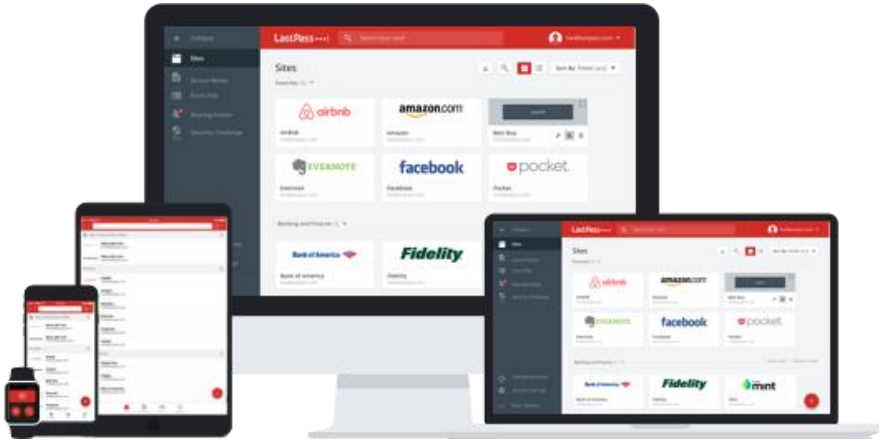


Sharing Center
Share passwords with family and friends that need access to an account.

Sites
LastPass keeps your data secure while helping you login to all your web accounts.

Save
Save new sites, notes, and profiles as you go.

Photo courtesy of LastPass
https://lastpass.com/



Cross Platform

LastPass has apps for most major mobile platforms, with dedicated support for a variety of browsers on the PC.

Photo courtesy of LastPass
https://lastpass.com/

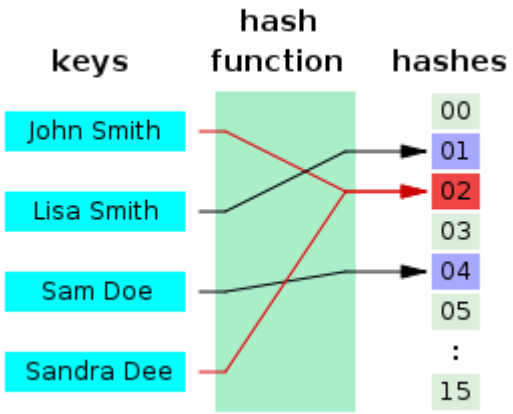
What Happened?

In June 2015, LastPass noticed unusual activity on their network of servers, with evidence showing compromise of some* data

Photo courtesy of Roos-Skywalker
http://roos-skywalker.deviantart.com/art/Data-path-with-glow-335648807

"... The investigation has shown, however, that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised."

Hashes & Salts?

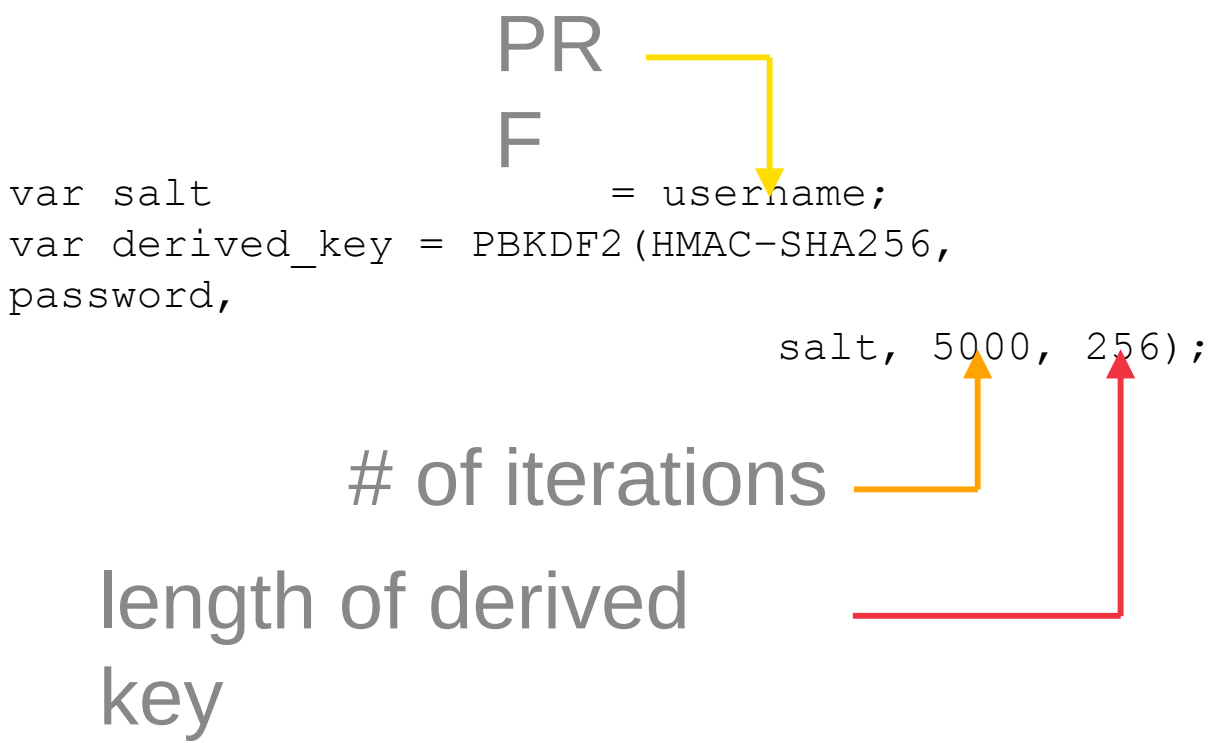


a **Hash Function** maps data of arbitrary size to data of fixed size.

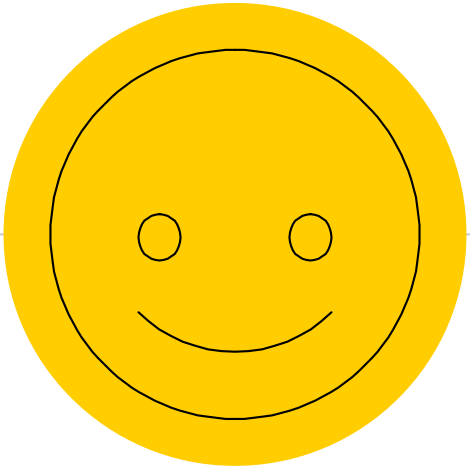
Examples of cryptographic hash functions:

- MD5
- SHA-1
- SHA-2

Salts are [random] data used as additional input to a one-way function that hashes a password or a passphrase.


PR
F
var salt = username;
var derived_key = PBKDF2(HMAC-SHA256,
password,
salt, 5000, 256);
# of iterations
length of derived key

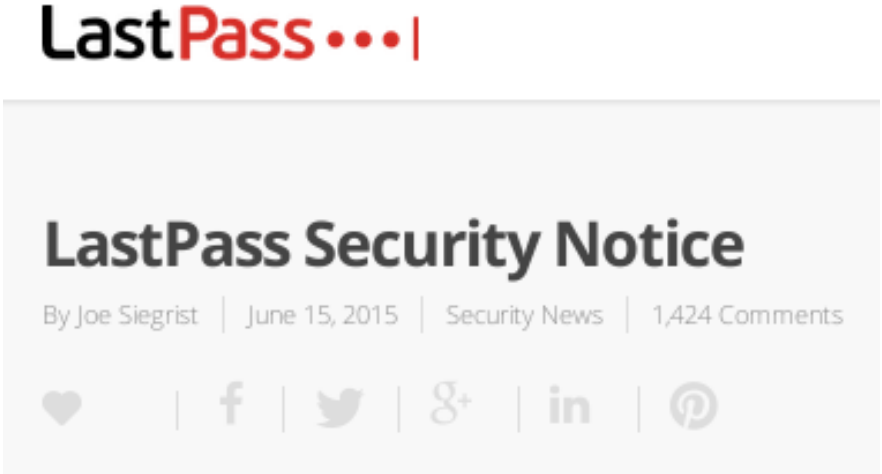
What could hackers do?



Not much!

Because ...

- Passwords were hashed.
- Hashes were salted.
- After the breach, the LastPass team took extra measures to prevent further damage.



LastPass blog post June 2015
Disclosed what happened and how they planned on ensuring to keep data safe.

Summary

LastPass

- Password management service

LastPass Hack

- User information compromised

Questions

Was my master password exposed?

The master password is used to retrieve all other passwords stored by the service.

Yes
No

What Should I do Now?

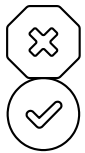
Email your master password to LastPass

Update info

Was information in my vault exposed?

Form fill profiles, secure notes, usernames, emails, etc..

Yes
No



Thanks!

Any questions ?

References

- https://blog.lastpass.com/2015/06/lastpass-security-notice.html
- https://en.wikipedia.org/wiki/LastPass
- https://en.wikipedia.org/wiki/Hash_function
- https://en.wikipedia.org/wiki/PBKDF2
- https://tools.ietf.org/html/rfc2898
- https://en.wikipedia.org/wiki/Salt_%28cryptography%29
- https://en.wikipedia.org/wiki/Pseudorandom_function_family
- http://www.graemenoble.id.au/post/49072807017/lastpass-password-database-explanation
- http://lifehacker.com/lastpass-hacked-time-to-change-your-master-password-1711463571
- http://www.dailytech.com/When+Breaches+Happen+LastPass+Hack+Showcases+Value+of+Strong+Encryption/article37401.htm
- http://www.ibtimes.co.uk/lastpass-hacked-what-you-need-know-about-password-manager-security-breach-1506350

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Presentation icons by SlidesCarnival
- Images from LastPass and other cited sources