Client-side Attacks on the LastPass Browser Extension

Derk Barten

supervised by Cedric Van Bockhaven

Master Security and Network Engineering, UvA

LastPass

“Cloud based” password manager

13 Million users, 33k businesses

Browser extension in Javascript

Custom implementation of AES/SHA/PBKDF2

https://droid-life.com/wp-content/uploads/2015/04/lastpass-android.jpg

Research Question

What client-side attacks be used on the LastPass extension for the Chrome browser?

1. File system based attacks
2. Memory based attacks
3. ~~Javascript attacks, XSS, CSRF~~

The Scenario

Post exploitation phase

Jumping point for Red Team operations

Internet criminals

Lab Setup

Windows 10 VM, Virtualbox

Google Chrome

LastPass extension

Two Lastpass accounts, victim_alice & victim_bob

Filesystem based Client-side attack

Local database under chrome UserData

Site accounts stored in a binary blob base64 encoded

Master password encrypted (AES) with SHA256 of the email

Vault key is 100100 iterations of PBKDF2 with email & master password

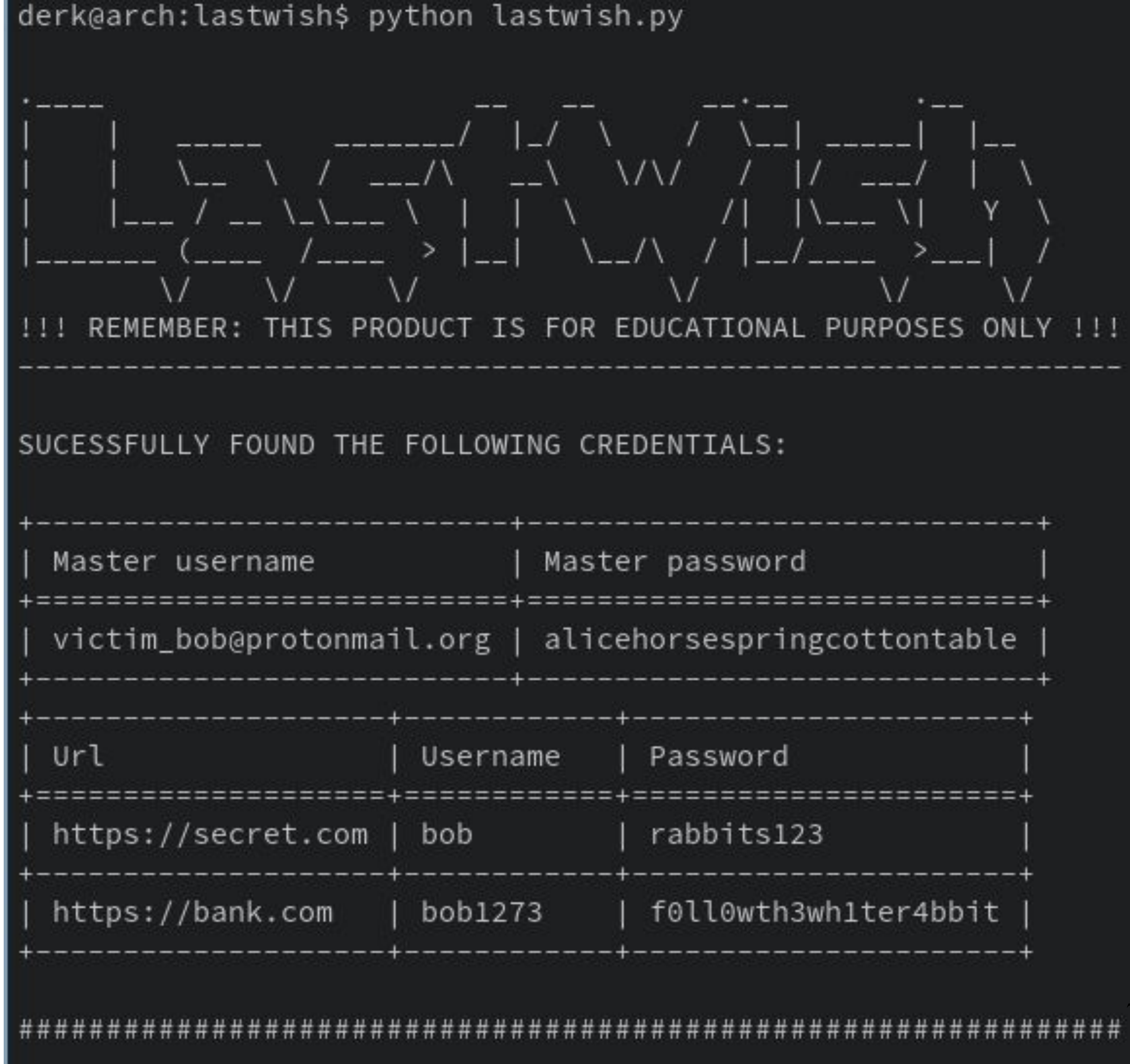
Vault key used to decrypt accounts in local database

LastWish

Automated Python script

Decrypts every site in the local database

Works when browser is closed



```
derk@arch:lastwish$ python lastwish.py

.____                   __   __      __.__       .__
|    |   _____    _______/  |_/  \    /  \__| _____|  |__
|    |   \__  \  /  ___/\   __\   \/\/   /  |/  ___/  |  \
|    |___ / __ \_\___ \  |  |  \        /|  |\___ \|   Y  \
|_______ (____  /____  > |__|   \__/\  / |__/____  >___|  /
        \/    \/     \/              \/          \/     \/
!!! REMEMBER: THIS PRODUCT IS FOR EDUCATIONAL PURPOSES ONLY !!!
---------------------------------------------------------------

SUCESSFULLY FOUND THE FOLLOWING CREDENTIALS:

+---------------------------+-----------------------------+
| Master username           | Master password             |
+===========================+=============================+
| victim_bob@protonmail.org | alicehorsespringcottontable |
+---------------------------+-----------------------------+
+--------------------+------------+----------------------+
| Url                | Username   | Password             |
+====================+============+======================+
| https://secret.com | bob        | rabbits123           |
+--------------------+------------+----------------------+
| https://bank.com   | bob1273    | f0ll0wth3wh1ter4bbit |
+--------------------+------------+----------------------+

###############################################################
```

Limitations of the File system attack

Remember password needs to be enabled

Offline mode needs to be enabled or MFA needs to be disabled

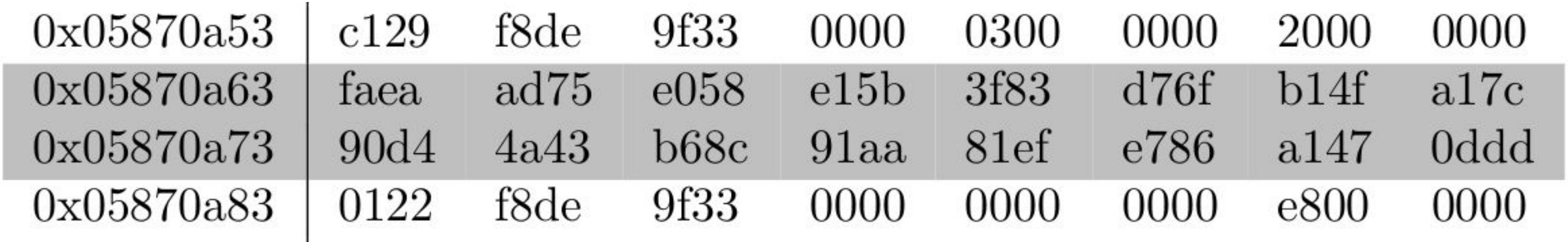
Memory based Client-side attack

Previous research suggest plaintext usernames/passwords

Chrome devtools, WinDBG, strings, radare2 :)

Found site name, username and vault key

18363 Matches -> 224 Matches -> 90 Matches



```
0x05870a53 | c129 f8de 9f33 0000 0300 0000 2000 0000
0x05870a63 | faea ad75 e058 e15b 3f83 d76f b14f a17c
0x05870a73 | 90d4 4a43 b68c 91aa 81ef e786 a147 0ddd
0x05870a83 | 0122 f8de 9f33 0000 0000 0000 e800 0000
```

Limitations of the Memory attack

Offline mode needs to be enabled

Browser/extension must be open

Implications

File system attack:

- ❑ Passwords can be stolen when remember password
- ❑ Same approach already performed 4yrs ago
- ❑ Likely low priority for Lastpass

Memory attack:

- ❑ Passwords can be stolen when the extension is active
- ❑ Have not found functional previous research
- ❑ May be included in the threat model of LastPass

Conclusion

What client-side attacks be used on the LastPass extension for the Chrome browser?

Remembered password function can be abused to decrypt the locally stored database accounts.

The encryption key of the accounts can reliably be found in the memory of the extension

Discussion

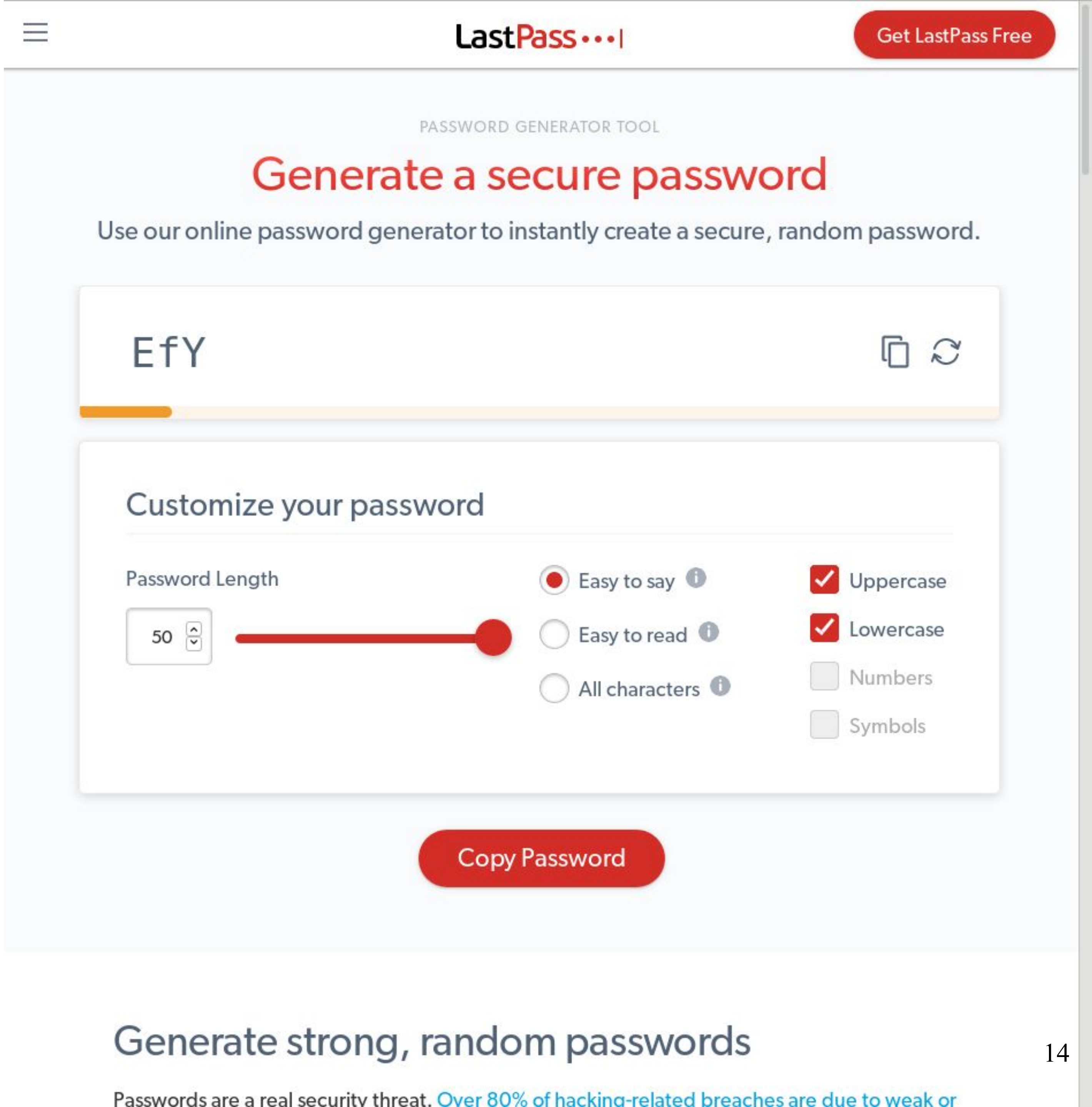
Could also just get the vault key from the chrome dev tools

Observation: Offline access can only be DISABLED when MFA is ENABLED

Advice: With MFA, offline access should always be DISABLED when remember password is ENABLED.

Silly Bug

“Easy to say” may result in very short passwords



PASSWORD GENERATOR TOOL

Generate a secure password

Use our online password generator to instantly create a secure, random password.

EfY

Customize your password

Password Length 50

● Easy to say
○ Easy to read
○ All characters

☑ Uppercase
☑ Lowercase
□ Numbers
□ Symbols

Generate strong, random passwords

Passwords are a real security threat. Over 80% of hacking-related breaches are due to weak or