The Emperor’s New Password Manager: Security Analysis of Password Managers

Zhiwei Li
* collaborated with Warren He, Devdatta Akhawe, and Dawn Song from UC Berkeley

Research Scientist
Shape Security
@liwaius
20 years later ...

"On the Internet, nobody knows you're a dog."
EBay Urges New Passwords After Breach

White-hat hackers lifted 560,000 corporate passwords in 31 days. We’re all screwed

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH

A Russian criminal gang has amassed more than a billion Internet credentials, according to researchers studying the data.

The records, which were lifted from an Internet café in Russia, include confidential household numbers, Login and password combinations, and more.

Thousands Of Passwords Exposed
Kids Cyber Safe?
Password Managers to the rescue

- Physically Effortless
- Resilient to Phishing
- Memorywise Effortless
- Scalable for Users
- Resilient to Physical Observation
- Resilient to Throttled Guessing
- Resilient to Unthrottled Guessing
- Resilient to Leaks from Other Verifiers
- ...

#RSAC
XXX is a must-use freeware tool that supports multiple operating systems and browsers

XXX Offers NSA-Level Protection for Your Passwords

Keep All of Your Logins Secure With XXXX

XXX Never Forget a Password Again

XXX: Unbreakable Passwords That You Don’t Have to Remember

XXX Surpasses Gmail for Top Productivity App

XXX Wins Best Mobile App at CES 2014
Password Security, Protection, and Management

Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase. It is one of the best ways to keep track of each unique password or passphrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master passphrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.
Are they truly secure?

- LastPass
- RoboForm
- My1login
- PasswordBox
- NeedMyPassword
How does it work?
Security Goals

- Master Account Security
  - impossible for an attacker to authenticate as the user to the password manager

- Credential Database Security
  - ensure the CIA of the credential database

- Unlinkability
  - use of password manager should not allow colluding web applications to track a single user across websites
Threat model

- Web attacker
  - control web servers
  - DNS domains
  - get a victim to visit controlled domains
Four classes of vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>Bookmarklet Vulnerabilities</th>
<th>Web Vulnerabilities</th>
<th>Authorization Vulnerabilities</th>
<th>UI Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastPass</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RoboForm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My1Login</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PasswordBox</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NeedMyPassword</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vulnerable**

**Not discovered**

**NA**

**NO** product was safe against all four
Bookmarklet Vulnerabilities
Bookmarklet

- A bookmarklet is a snippet of JavaScript code
  - install as a bookmark
  - when clicked, run in the context of the current page
  - interact with a login form
Alice clicks bookmarklet, which includes \_LASTPASS\_RAND and h
Bookmarklet code is a stub that loads the main code from lastpass.com
Bookmarklet loads a LastPass page in an iframe
The iframe loads Alice’s encrypted master key and encrypted credential for dropbox.com (specified by a URL parameter).

This is done using a `<script>` tag in the iframe.
PostMessage communicates the decryption key to the iframe, which decrypts the credential and sends it back through PostMessage.
LastPass Bookmarklet Attack

1. Bookmarklet Click

2. GET bml.php?payload

3. Extract the credential for u from d, alice, _LASTPASS_RAND, and key_rand_encrypted
Leaking sensitive data into untrusted pages

- All password managers that support bookmarklet leak their credentials
  - LastPass
  - RoboForm
  - My1login
Classic Web Vulnerabilities
Web Vulnerabilities

- Subtleties of the web platform
- Focus on CSRF and XSS
- CSRF vulnerabilities
  - LastPass, RoboForm, and NeedMyPassword
- XSS vulnerability
  - NeedMyPassword
LastPass CSRF Vulnerability

- OTP feature
  - authentication code for the master account
  - only valid for one use

- Design flaw
Alice

lastpass.com/otp.php

1. locally generate an OTP otp
2. POST otp.php
3. validate user by checking cookies
4. save (email, h, rand_encrypted_key) to the backend storage

h = hash(hash(email|otp)|otp)
rand_encrypted_key = encrypt(masterkey, hash(email|otp))

Alice

lastpass.com/otp.php?forcelogin=1

1. type email and OTP otp
2. compute h = hash(hash(email|otp)|otp)
3. POST otp.php
4. check if (email, h, rand_encrypted_key) exists in the backend storage
5. extract local_key by decrypting rand_encrypted_key using hash(email|otp)
OTP Attack

h = hash(hash(alice | otp) | any_otp)
rand_encrypted_key = encrypt(dummy, hash(alice | any_otp))

The attacker can then log into Alice’s master account to view unencrypted information and delete credentials.
Authorization Vulnerabilities
Collaboration

- Ability to share passwords with a collaborator

- Alice requests to share a credential with Bob
- Password manager forwards the credential to Bob
- Both need accounts with the password manager
Authorization Vulnerabilities

- 3 support credential sharing
- Both My1login and PasswordBox mistook authentication for authorization
(a) Sharing an asset

Alice
passwordbox.com

POST /api/0/secrets

shared|encrypted_key|contact_id|asset_id

check cookies

asset_id|contact_id|created_at|...

(b) Accessing a shared asset

Bob
passwordbox.com

GET /api/0/assets

check cookies

[assets]
PasswordBox

(a) Sharing an asset

1. Alice
   - passwordbox.com
   - `POST /api/0/secrets`
   - `shared|encrypted_key|contact_id|asset_id`

2. PasswordBox
   - check cookies
   - `asset_id|contact_id|created_at|`

(b) Accessing a shared asset

1. Bob
   - passwordbox.com
   - `GET /api/0/assets`
   - `[assets]`

2. PasswordBox
   - check cookies
User Interface Vulnerabilities

- Resilient to Phishing
  - a major benefit of password managers
  - detects application
  - (auto-)fill the right password

- Vulnerable
  - LastPass
  - RoboForm
Logging into RoboForm

- Creates an iframe in the current web application to log in the user

- Attack
  - block the iframe
  - spoof an authentication dialog
  - steal master credentials
You are currently logged out of LastPass. Login then click the bookmarkSet again.
Apply Slide

- **Bookmarklet Vulnerabilities**
  - loads the password manager code in an iframe
  - `postMessage` with the right target
  - consider DJS (Defensive JavaScript) proposed by Karthikeyan Bhargavan

- **Web Vulnerabilities**
  - Content Security Policy (CSP)
  - CSRF prevention

- **Authorization Vulnerabilities**
  - simplify sharing logic

- **UI Vulnerabilities**
  - manually open a new tab
Take Homes

- Design and implement with security in mind
- Formalizing (better yet verifying) protocol pays off
Conclusions

- A wide spectrum of discovered vulnerabilities
  - logic mistakes
  - misunderstanding about the web security model
  - typical vulnerabilities like CSRF and XSS

- A single solution is unlikely

- Developing password manager entails a systematic, defense-in-depth approach
Stay Tuned.

http://pepperword.com