The Emperor's New Password Manager

Security Analysis of Web-based Password Managers

Zhiwei Li, Warren He, Devdatta Akhawe, Dawn Song

University of California, Berkeley

"On the Internet, nobody knows you're a dog."

20 Years later ...

HOME SEARCH

The New York Times

EBay Urges New Passwords After Breach

By

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

TIME Subscribe

Watch David Letterman Pay Tribute to Robin Williams

Breakin Control

TECH SECURITY

Here's How Hackers Stole Over $1 Million From 1,600 StubHub Users

Sam

The New York Times | http://nyti.ms/1zRDzOm

U.S.

far-fl

Six i

inter

purc

In M

com

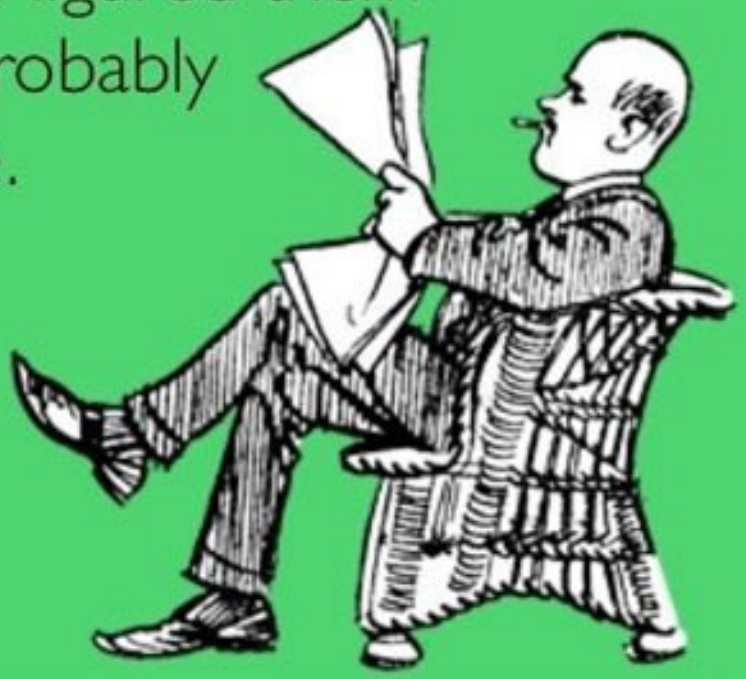
TECHNOLOGY | NYT NOW

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

50% of my time online is spent clicking "forgot password" links.

I have one or two passwords for everything if you figured them out you could probably take over my life.



Benefits of Password Managers

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

XXXX is a must-use freeware tool that supports multiple operating systems and browsers

The New York Times

Apps to Protect Your Array of Passwords

7x7SF

XXXX Offers NSA-Level Protection for Your Passwords

c|net

Keep All of Your Logins Secure With XXXX

lifehacker

XXXX Never Forget a Password Again

xconomy

XXXX: Unbreakable Passwords That You Don't Have to Remember

TECHVIBES

XXXX Surpasses Gmail for Top Productivity App

TRENDHUNTER
FIND BETTER IDEAS, FASTER

XXXX Wins Best Mobile App at CES 2014

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

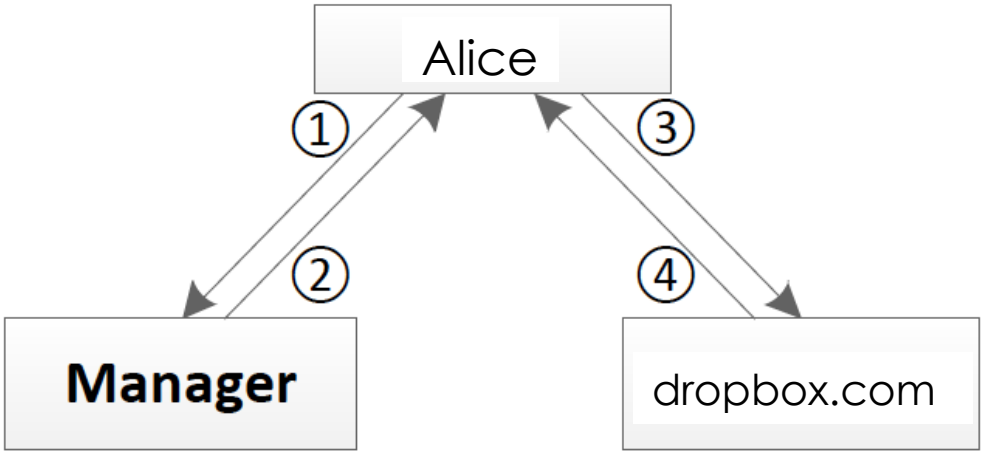
Password Security, Protection, and Management

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.

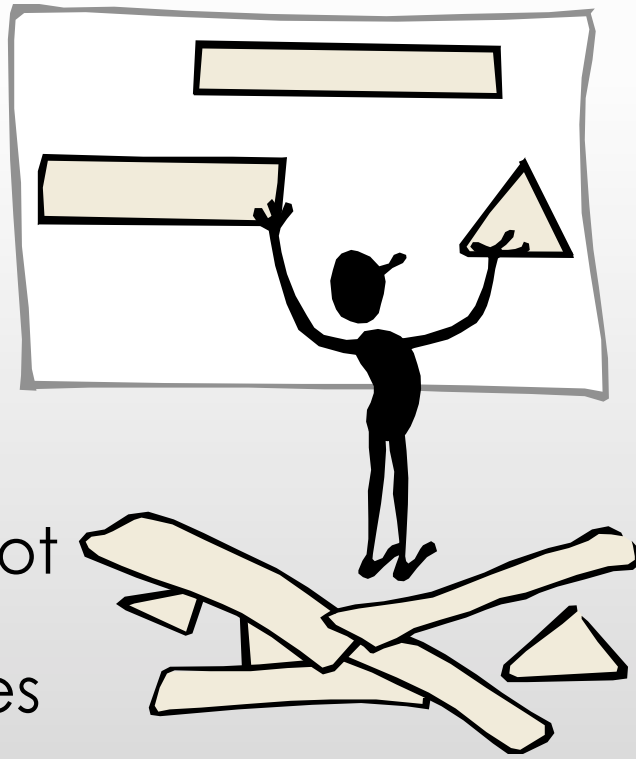
Are they truly secure?

How it works



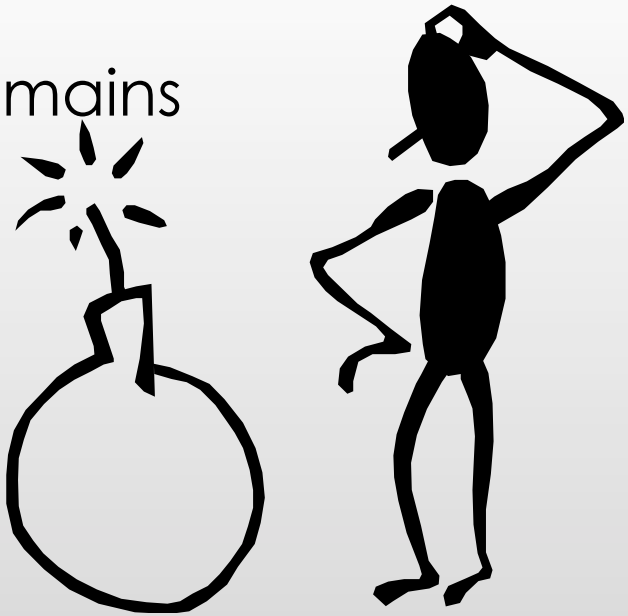
Security Goals

- 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

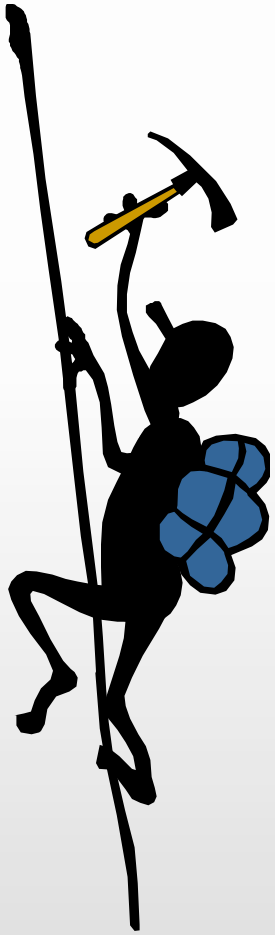
3/3 bookmarklet vulnerabilities

3/5 classic web vulnerabilities

2/3 authorization vulnerabilities

2/5 user interface vulnerabilities

NO product was safe against all four



bookmarklet vulnerabilities

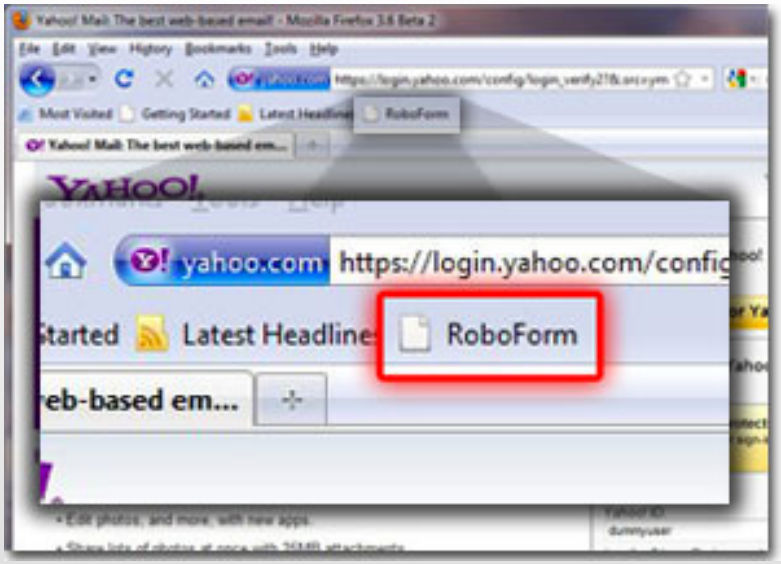
classic web vulnerabilities

authorization vulnerabilities

user interface vulnerabilities

Bookmarklet

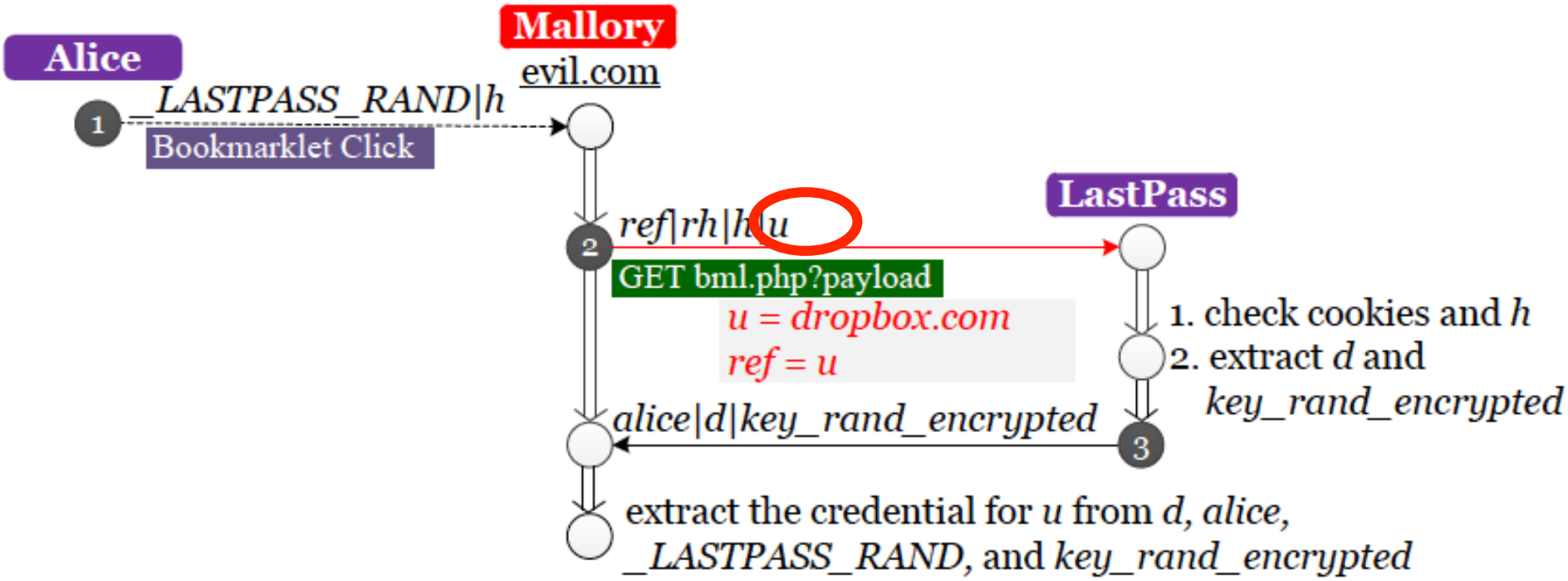
- A bookmarklet is a snippet of JavaScript code
  - installs as a bookmark
  - when clicked, runs in the context of the current page
  - interact with a login form



Alice clicks bookmarklet, which includes _LASTPASS_RAND and h

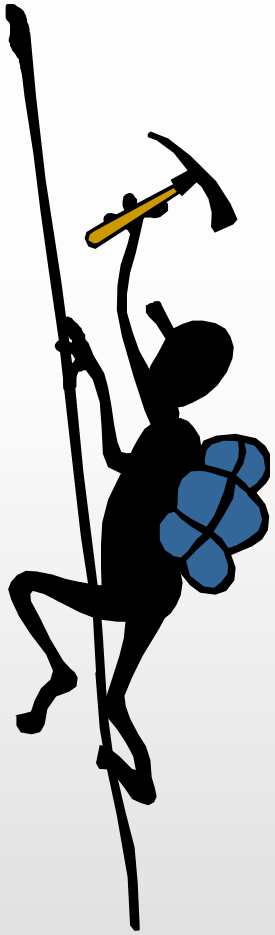
PostMessage communicates the decryption key to the iframe, which decrypts the credential and sends it back through PostMessage.

LastPass Bookmarklet Attack



Leaking sensitive data into untrusted pages

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



bookmarklet vulnerabilities

classic web vulnerabilities

authorization vulnerabilities

user interface vulnerabilities

Web Vulnerabilities

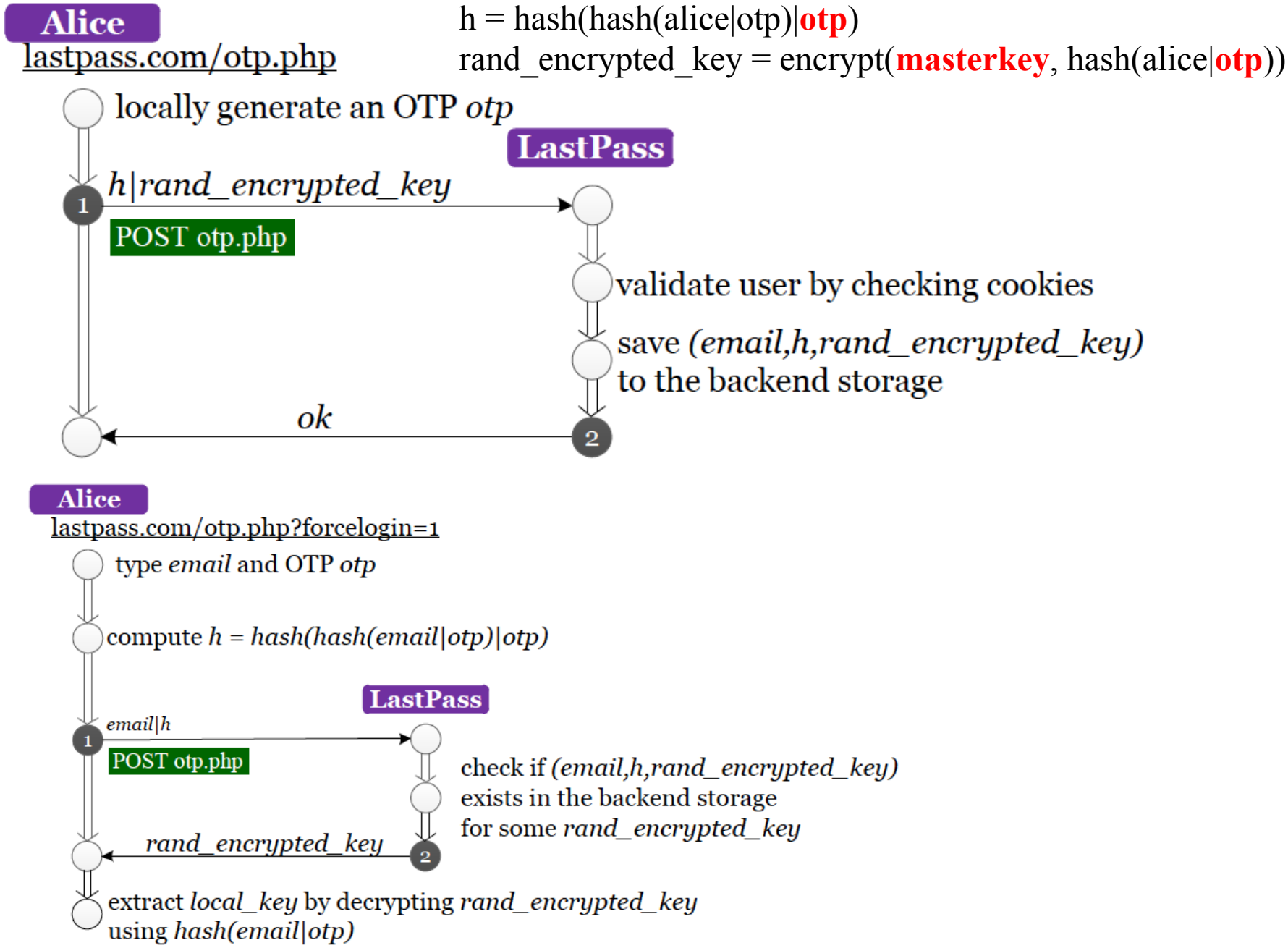
- Subtleties of the web platform
- Focus on CSRF and XSS

- CSRF vulnerabilities
  - LastPass, RoboForm, and NeedMyPassword

- XSS vulnerability
  - NeedMyPassword

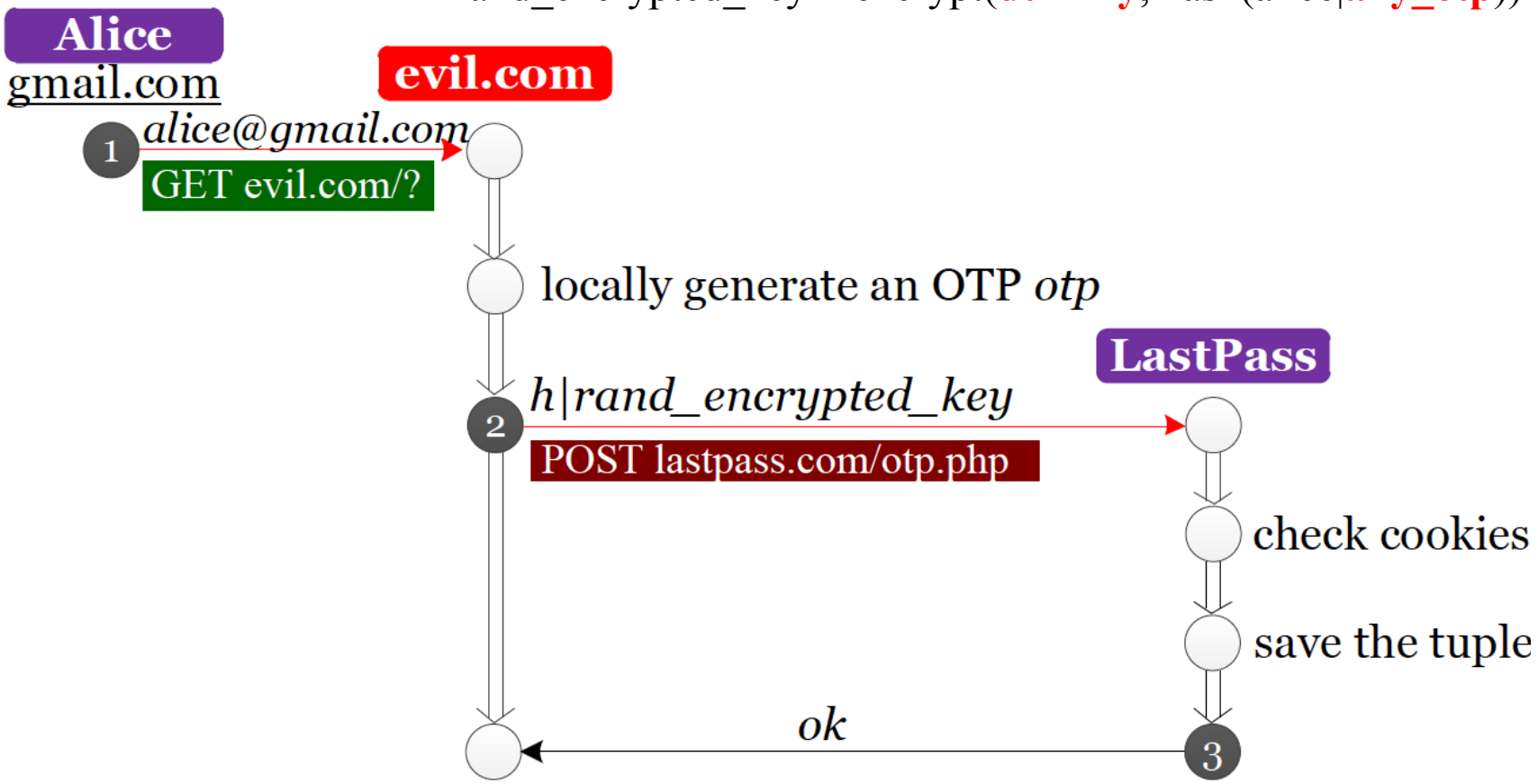
LastPass One-Time Password

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

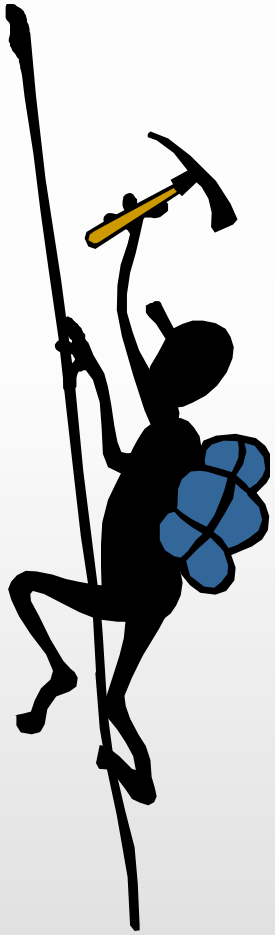

Alice
lastpass.com/otp.php
h = hash(hash(alice|otp)|otp)
rand_encrypted_key = encrypt(masterkey, hash(alice|otp))
locally generate an OTP otp
LastPass
h|rand_encrypted_key
1
POST otp.php
validate user by checking cookies
save (email,h,rand_encrypted_key)
to the backend storage
ok
2
Alice
lastpass.com/otp.php?forcelogin=1
type email and OTP otp
compute h = hash(hash(email|otp)|otp)
LastPass
email|h
1
POST otp.php
check if (email,h,rand_encrypted_key)
exists in the backend storage
for some rand_encrypted_key
rand_encrypted_key
2
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



bookmarklet vulnerabilities

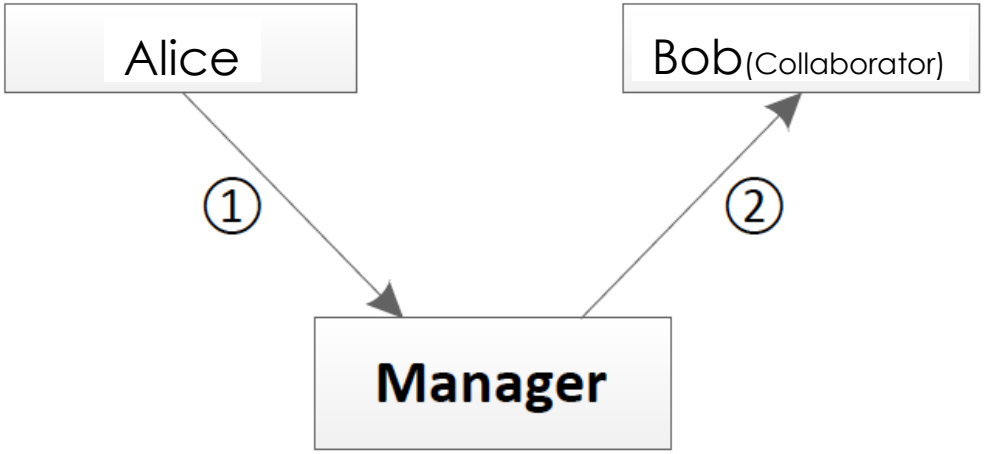
classic web vulnerabilities

authorization vulnerabilities

user interface vulnerabilities

Collaboration

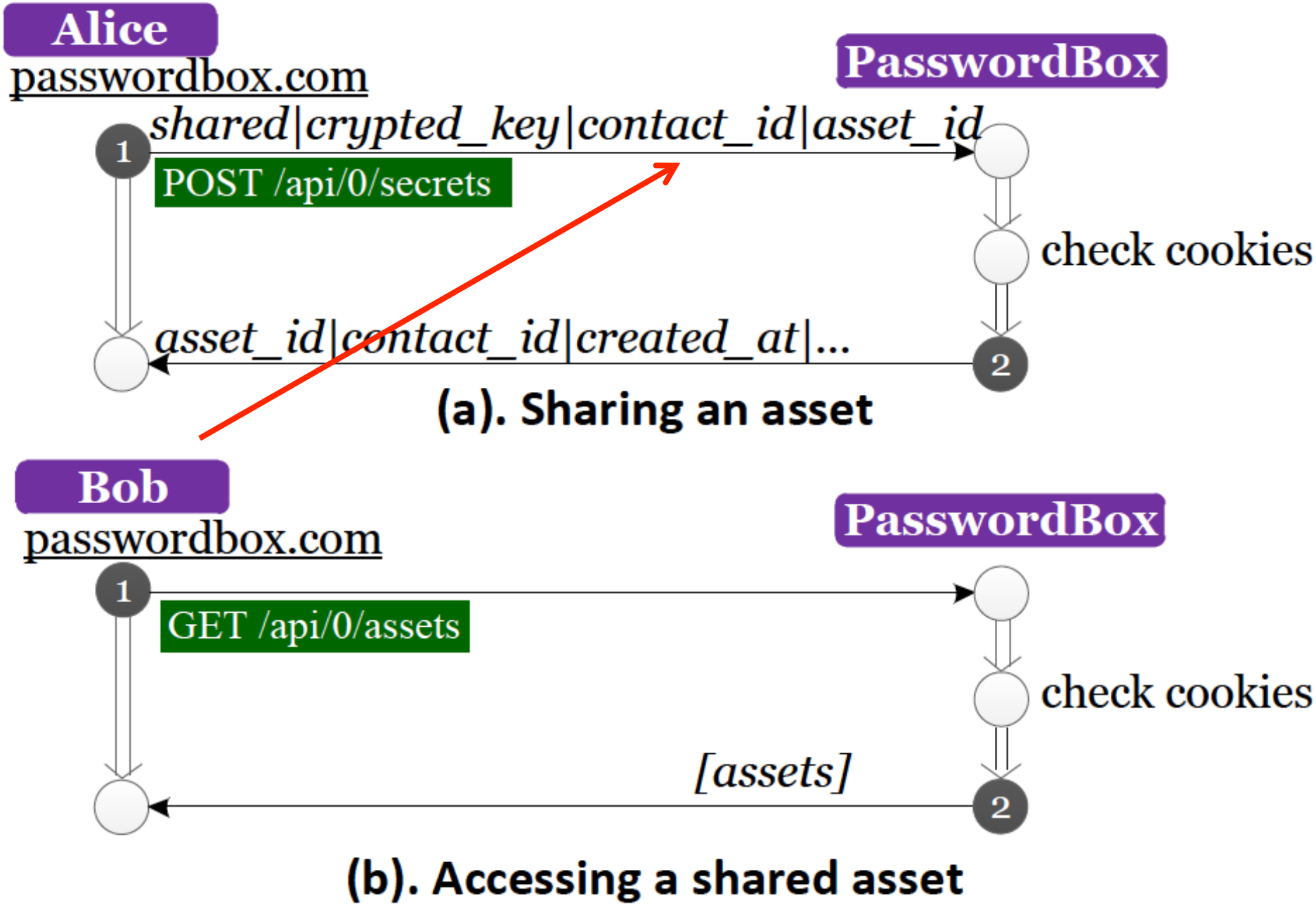
- Ability to share passwords with a collaborator

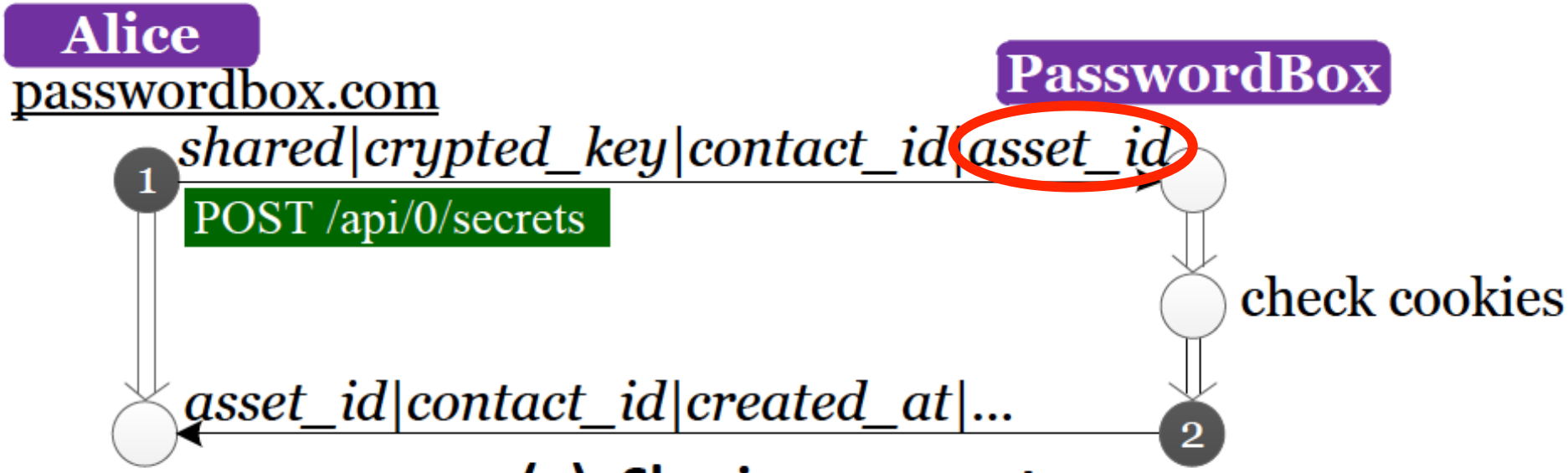


  - Alice requests to share a credential with Bob
  - Password manager forwards the credential to Bob
  - Both need accounts with the password manager

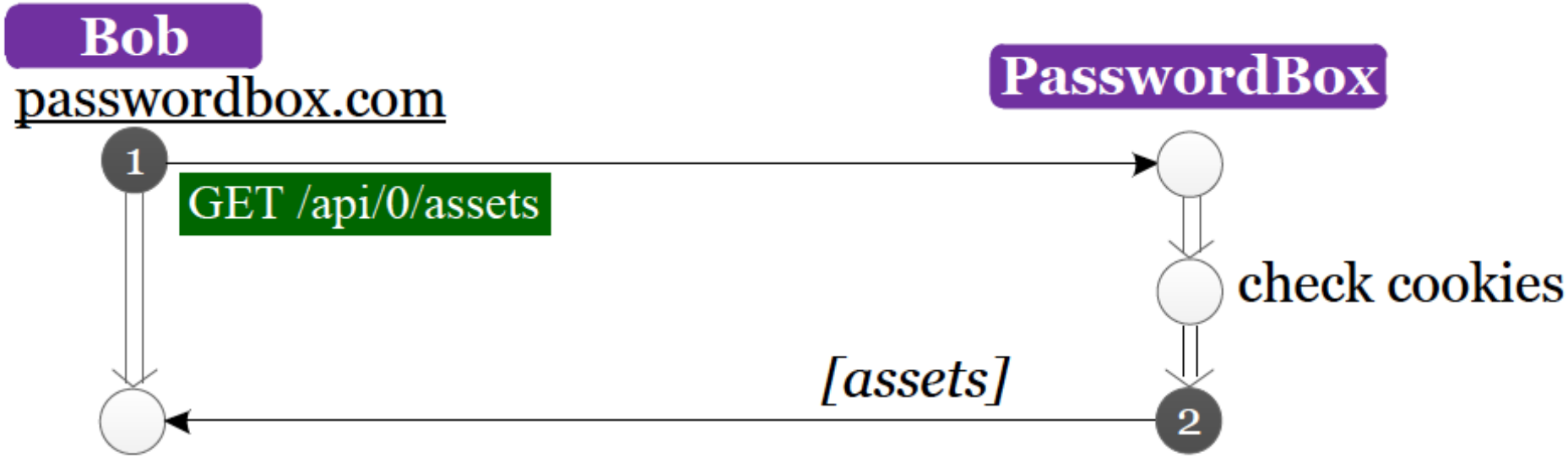
Authorization Vulnerabilities

- Three support collaboration
- Both My1login and PasswordBox mistook authentication for authorization

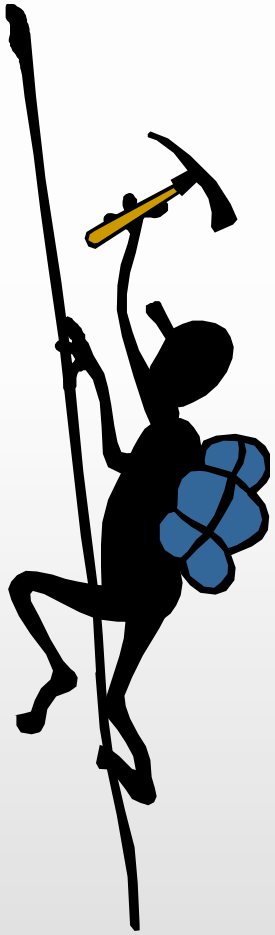

Alice
passwordbox.com
PasswordBox
shared|crypted_key|contact_id|asset_id
1
POST /api/0/secrets
check cookies
asset_id|contact_id|created_at|...
2
(a). Sharing an asset
Bob
passwordbox.com
PasswordBox
1
GET /api/0/assets
check cookies
[assets]
2
(b). Accessing a shared asset



(a). Sharing an asset



(b). Accessing a shared asset



bookmarklet vulnerabilities

classic web vulnerabilities

authorization vulnerabilities

user interface vulnerabilities

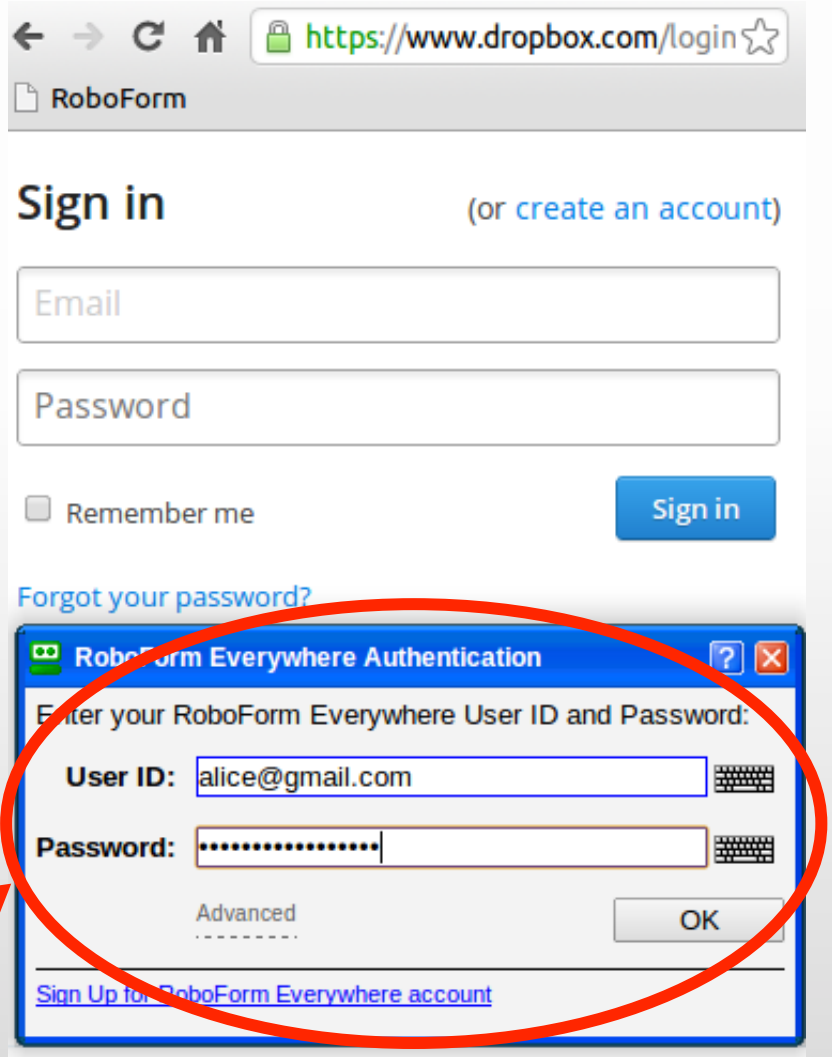
User Interface Vulnerabilities

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

Logging into RoboForm

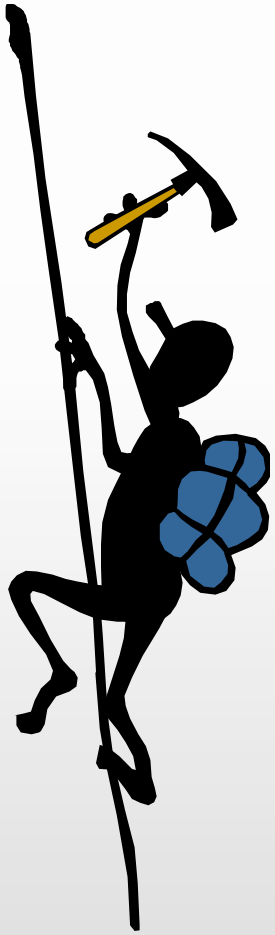
- Creates an iframe in the current web application to login the user

- Attack
  - block the iframe
  - spoof an authentication dialog
  - steal master credentials



LastPass UI Vulnerability

- (Demo)



bookmarklet vulnerabilities

classic web vulnerabilities

authorization vulnerabilities

user interface vulnerabilities

Mitigations

Mitigations

- Bookmarklet Vulnerabilities
  - loads the password manager code in an iframe
  - postMessage with the right target
- Web Vulnerabilities
  - Content Security Policy (CSP)
  - CSRF prevention
- Authorization Vulnerabilities
  - a simpler sharing mode
- UI Vulnerabilities
  - manually open a new tab

Conclusions

- The wide spectrum of discovered vulnerabilities
  - logic mistakes
  - misunderstanding about the web security model
  - typical vulnerabilities like CSRF and XSS
- A single solution unlikely
- Developing password manager entails a systematic, defense-in-depth approach