



**1Password protects you,
but who protects 1Password?**



/>\$ whoami

Adi Ludmer

Research Team Leader @ PerimeterX

Previous work places : Akamai, McAfee, 8200

The password problem

1. Too many passwords to remember
2. Choosing a simple password
3. Password re-use

Suggested solution - Password manager

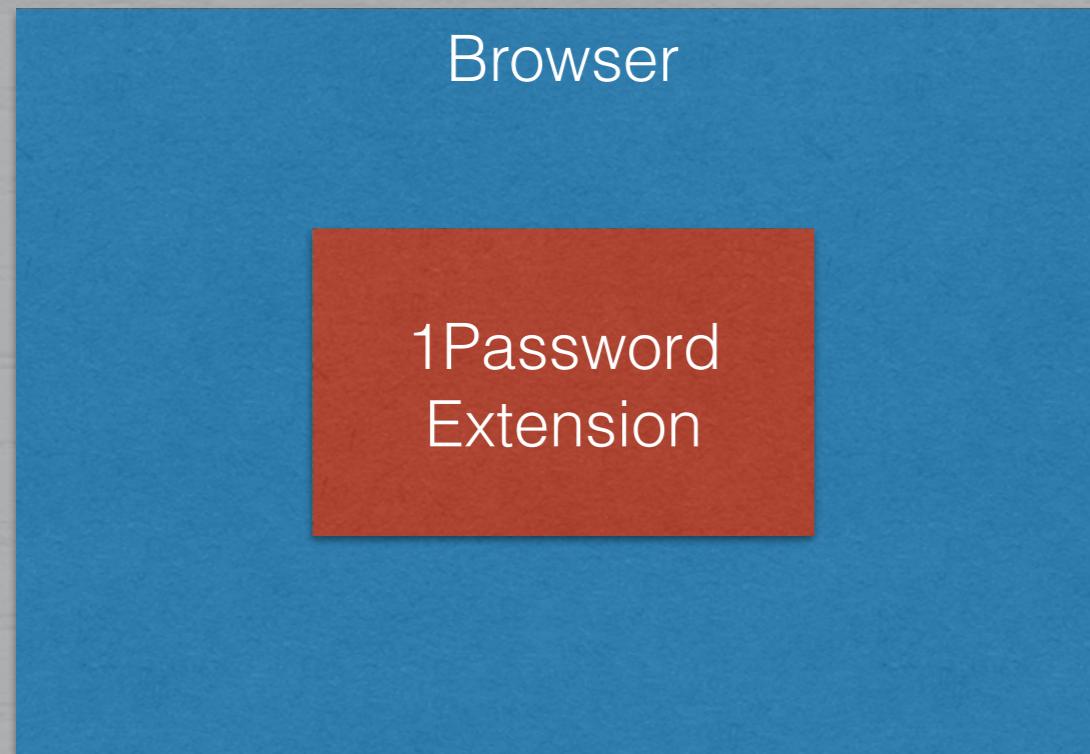
1. All passwords stored in an encrypted file
2. Requires to remember only the Master password
3. Password generator
4. Auto-fill via browser extension

1Password's browser extension

- The main goal of this extension is to ease the process of copying the password from the 1Password's application to the browser
- The credentials transferred from 1Password process to the browser via a WebSocket based communication channel.
- But there is a little problem ...

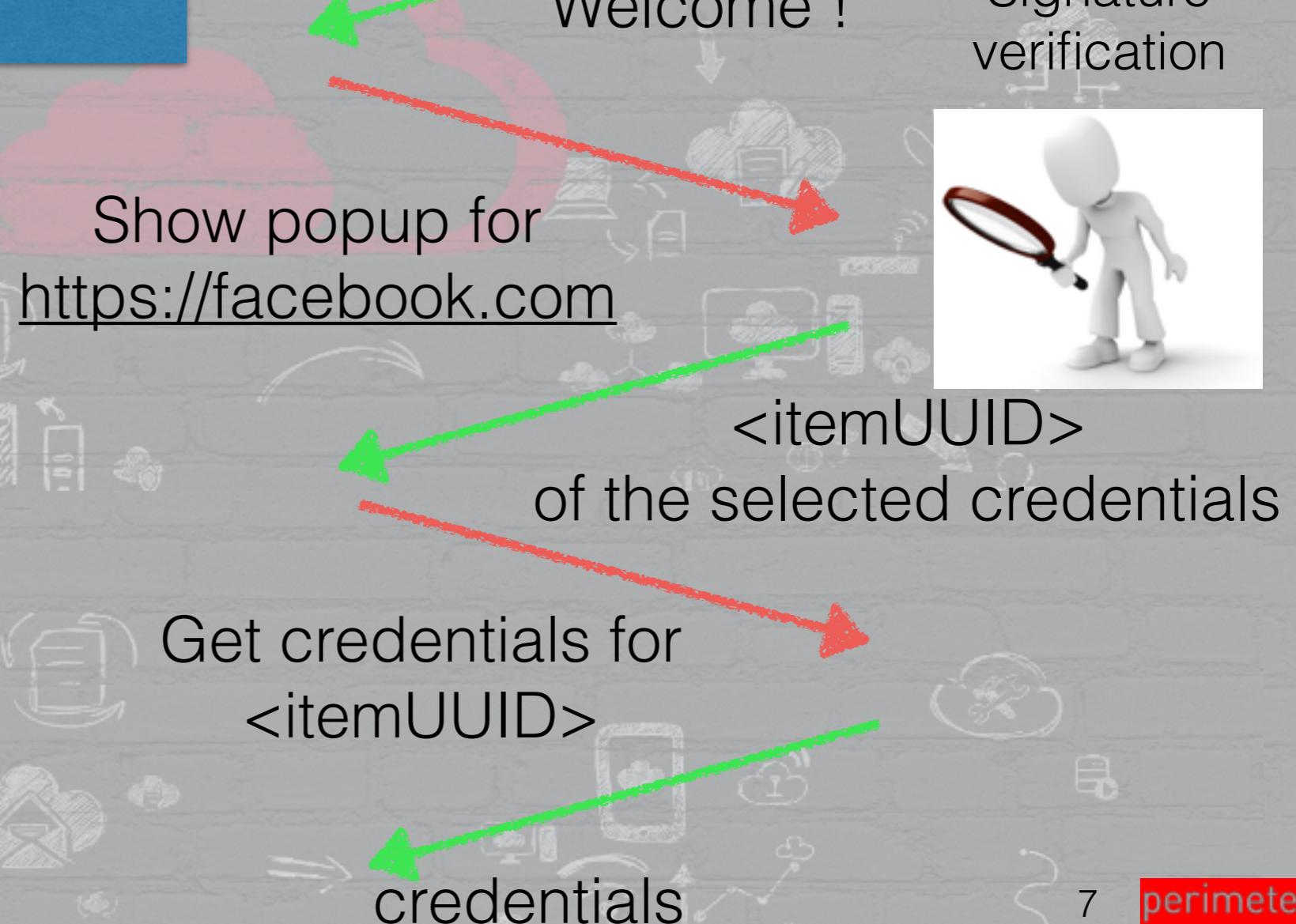
The problem

- The authentication between the extension & 1Password process is weak
- Which lets an attacker to write an evil extension that communicates with 1Password process and grabs the credentials.
- In some cases the user even doesn't notice that it happened



1Password Protocol

1Password Process



We have to pass the following checks

1. Origin check - The origin header should contain the extension's ID
2. Signature check - The process that initiated the connection must be a signed Chrome browser

The attack vectors

	External process	xss	Chrome Extension	Chrome App
Signature check	X	V	V	V
Origin Header check	V	X	X	V



It's demo time!

Questions ?

Thank you!

Join us! We are looking for:

- Web Data Analysis Team Leader
- Web Data Analysts
- Senior Malware Researchers
- Web Security Researchers



adi@perimeterx.com



[@adi_ludmer](https://twitter.com/adi_ludmer)



[/adi.ludmer](https://facebook.com/adi.ludmer)



Adi Ludmer