

QAuth2

W E L C O M E

to the Fabulous

RESO PlugFest

MONTE CARLO HOTEL, LAS VEGAS
OCTOBER 21-23
2014

Cal
Heldenbrand

WebOps
FBS



AND THE ROAD TO HELL!

About Cal

- Web Operations at FBS, 9yrs
- Created most of FBS's auth systems
- First RESO conference

Warning, Techno-Babble Ahead!



Goals

- Problem: OAuth2 has negative media attention on security
- Important because: they're (partially) correct
- Resolution: The RESO Web API Security document

OAuth2 Google Search

oauth2 security

Web News Images Videos Shopping More ▾ Search tools

About 234,000 results (0.34 seconds)

[OAuth 2.0 and the Road to Hell | hueniverse](#)

[hueniverse.com/2012/07/26/oauth-2-0-and-the-road-to-hell/](#) ▾

Jul 26, 2012 - To be clear, **OAuth** 2.0 at the hand of a developer with deep understanding of web **security** will likely result is a **secure** implementation.

[Serious security flaw in OAuth, OpenID discovered - CNET](#)

[www.cnet.com/.../serious-security-flaw-in-oauth-and-openid-disco...](#) ▾ CNET ▾

May 2, 2014 - Computer **Security** Beware of links that ask you to log in through Facebook. The **OAuth** 2.0 and OpenID modules are vulnerable. iStockphoto.

[OAuth - Wikipedia, the free encyclopedia](#)

[en.wikipedia.org/wiki/OAuth](#) ▾ Wikipedia ▾

Jump to **Security** - **Security**[edit]. On April 23, 2009, a session fixation **security** flaw in the 1.0 protocol was announced. It affects the **OAuth** authorization ...

[OpenID](#) - [Initiative For Open Authentication](#) - [Access token](#) - [Authorization](#)

[Egor Homakov: The Most Common OAuth2 Vulnerability](#)

[homakov.blogspot.com/2012/07/saferweb-most-common-oauth2.html](#) ▾

Jul 3, 2012 - Disregards its popularity a lot of people don't understand it deeply enough to write proper and **secure** implementation. OAuth1.a and **OAuth2** ...

- RFC lead author quit
- Hated “design-by-committee”, enterprise driven
- Started negative media attention

Negative Publicity

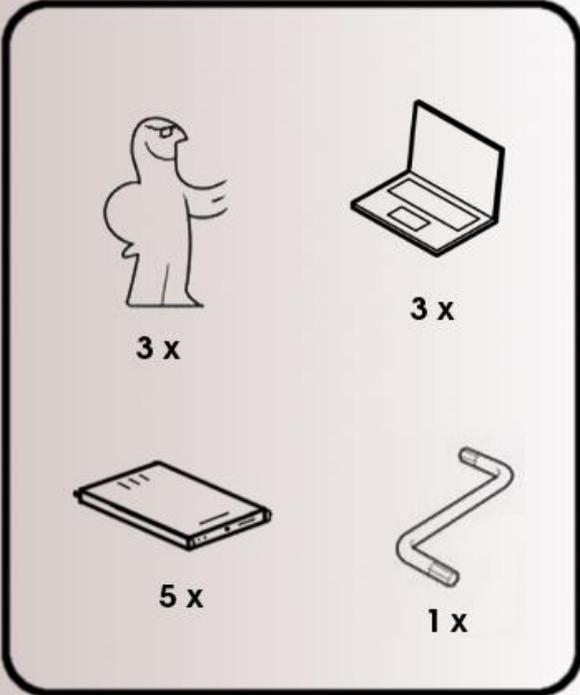
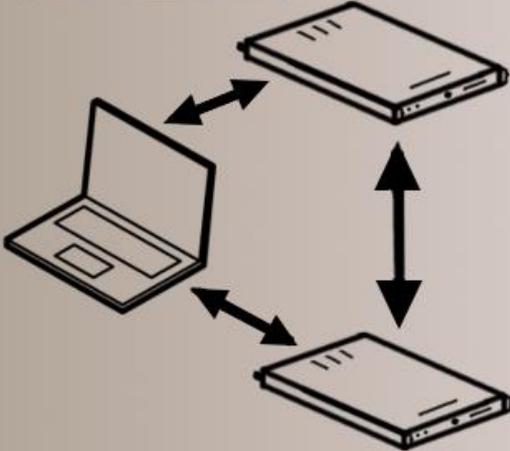
- Security flaws a result from options in the OAuth2 RFC
- Example: redirect_uri enforcement is optional (“Covert Redirect”)
 - Pinterest, ESPN did not enforce this

What is OAuth2, really?

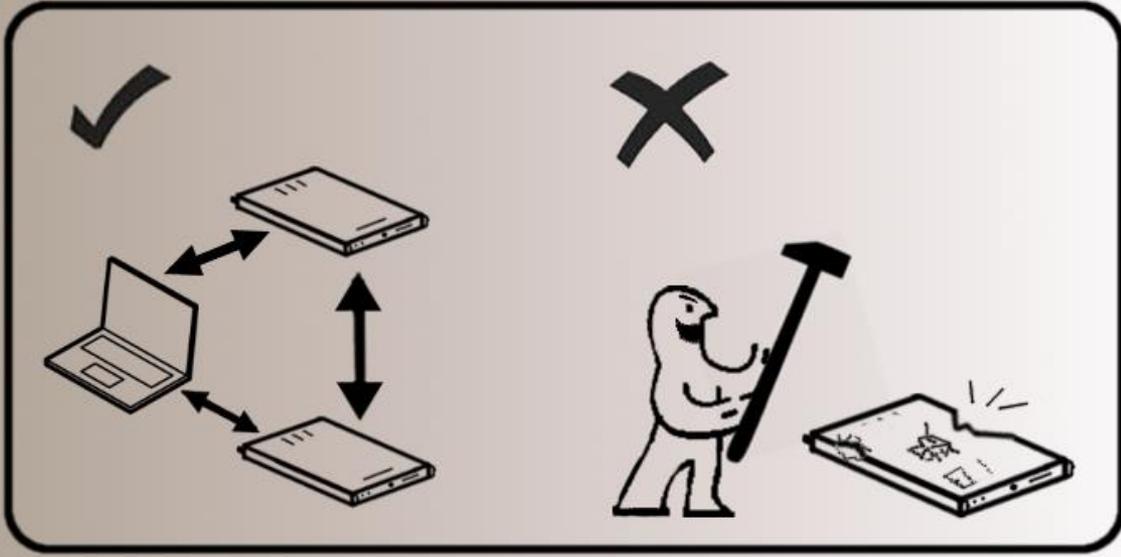
- OAuth2 RFC is a **framework**
- A guide for creating a product
- Provides options for developers
- Not usually interoperable

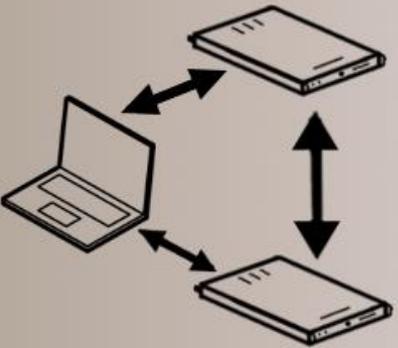
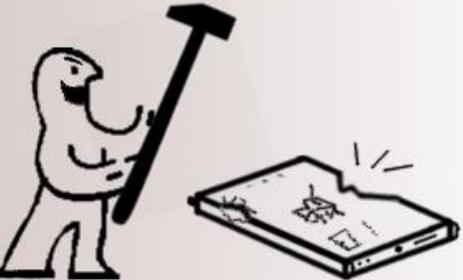
A framework
Is like...

ÖÅûth2



3 x  3 x 
5 x  1 x 



✓  X 

The bottom section is divided into two panels. The left panel, marked with a checkmark, shows the correct assembly diagram from the top section. The right panel, marked with an 'X', shows a person using a hammer to smash an external drive, with a broken drive icon and a lightning bolt symbol indicating damage.

What is a protocol then?

- Protocols are created from frameworks
- Interoperable
- Few options

“To be clear, OAuth 2.0 at the hand of a developer with a deep understanding of web security will result in a secure implementation”

-Eran Hammer,
OAuth2 and the Road to Hell

RESO Web API Security

- Removed options from the RFC
- Required XSS, redirect_uri, SSL (TLS!)
- Secure token format
- Registering a product is a manual process
- Adds extra server-side security
- Still uses standard toolkits client-side

First Phase: One Auth Method

- Goal of 100% interoperability
- Many popular sites use this method
- 80% of RESO use cases are handled
- Purposefully more specific than necessary
- Simple programming, easy start up

The Future of API Security

- **Need** more volunteer activity in the workgroup
- We accept well defined use cases and requirements
- More protocols added if required
- OpenID Connect? Basic over SSL?
- Authorization standards (access control per-user,action,resource)

Questions?

THANK YOU!