
OAuth2
WELCOME
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

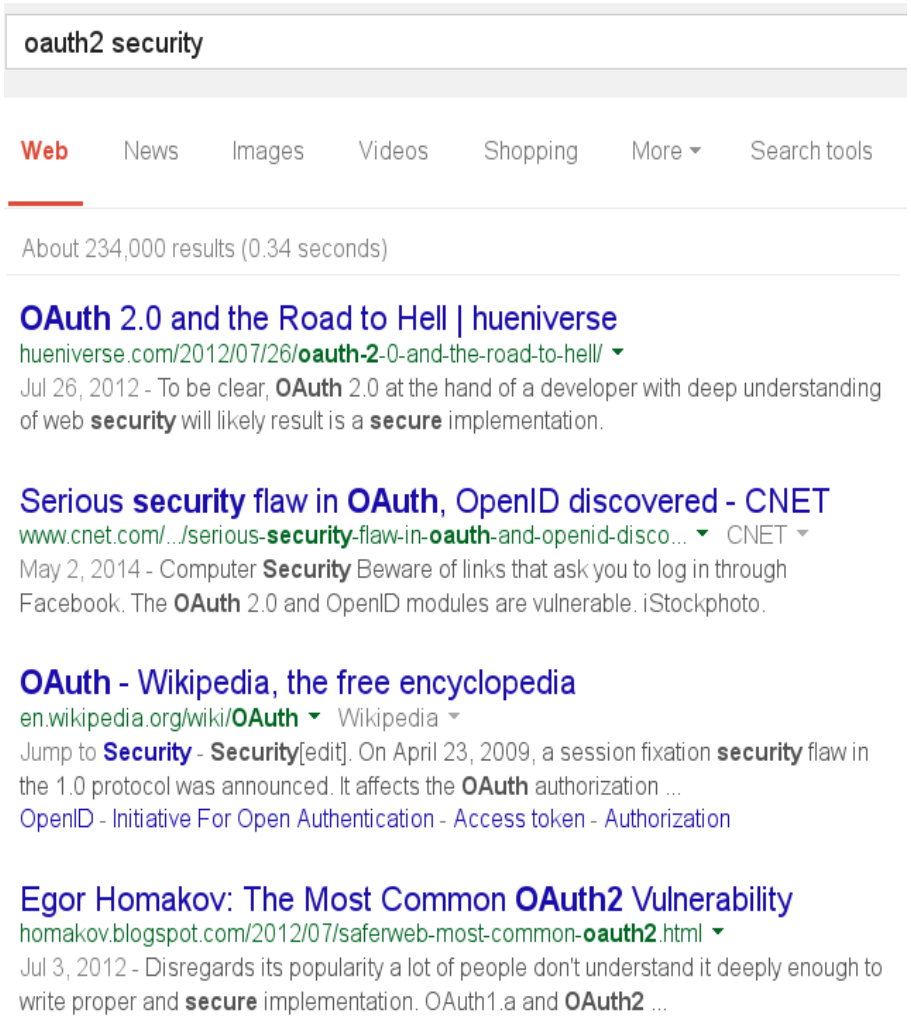
- Web Operations at FBS, 9yrs
- Created most of FBS's auth systems
- First RESO conference

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



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

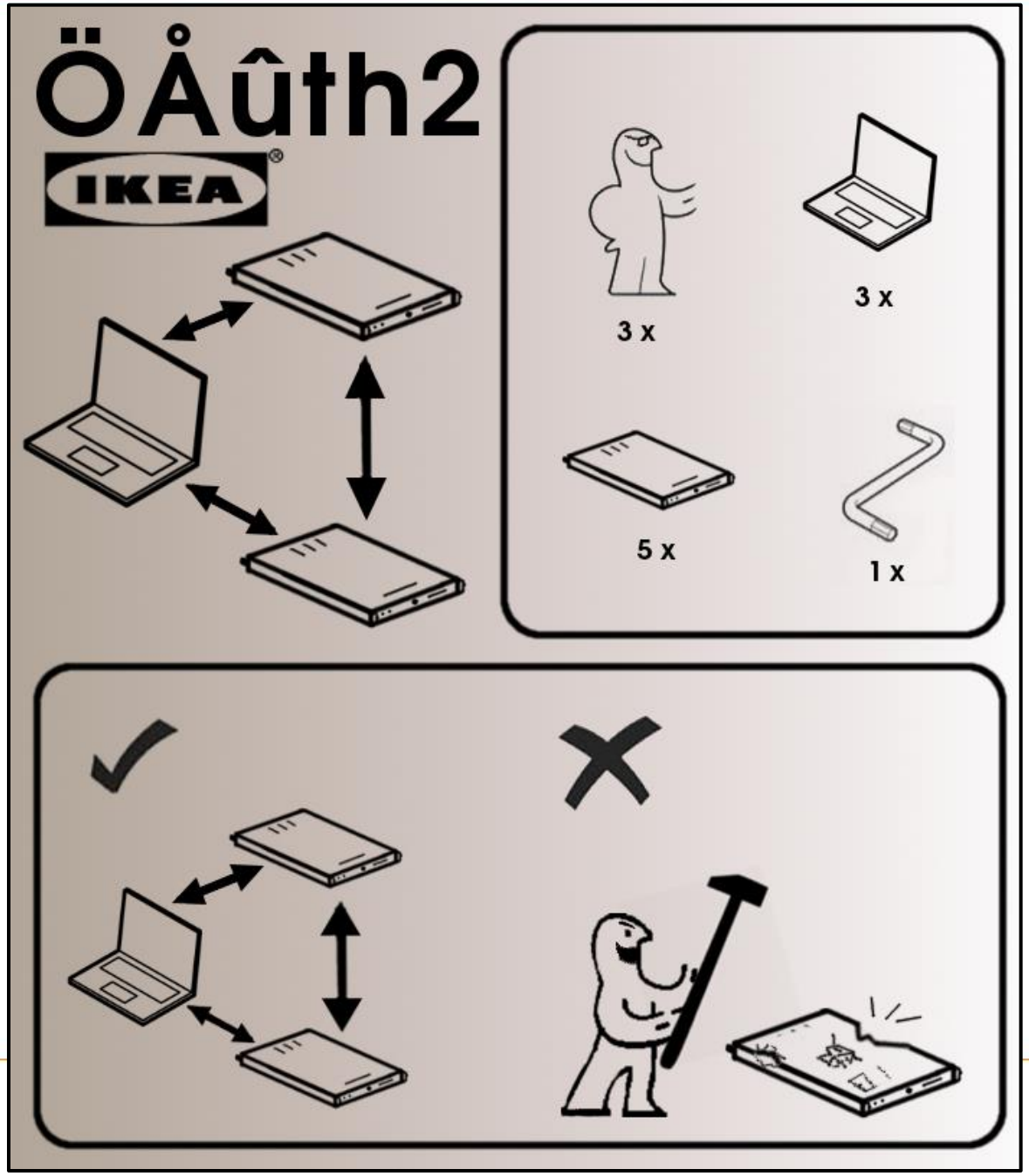
Negative Publicity

- 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...



RESO

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!