OAuth Spec

- Defined protocol
- Undefined:
  - (e.g. Developer registration, Approval Page etc)
Protocol Challenges

- Already discussed a lot. Not the focus of this talk. e.g.
  - Dynamic registration
  - Safe code/token delivery on devices
  - App Auth
  - Session management
  - Token binding
  - Token revocation
Challenges with “Undefined”

- Developer registration,
- Approval Page
- Notification
- Usage
- User controls, Revocation
- Admin Controls
OAuth Life cycle

Register
Developer creates app

Grant
User grants access

Usage
Use the token to get data

Revoke
User revokes token
OAuth Challenges @ Google

- Several hundred scopes, APIs
- Different types of data
- Users with varied understanding of security
- Enterprises on Google
  - Users could grant access to malicious apps
  - Enterprise should be able to limit OAuth grants
The OAuth Phishing attack (What happened?)

Joe Bernstein has shared a document on Google Docs with you

Joe.bernstein@buzzfeed.com

Joe Bernstein has invited you to view the following document:

Open in Docs

Google

Choose an account

to continue to Google Docs

Developer info

Email: eugene.pupov@gmail.com

Choosing an account will redirect you to: https://googledocs.gdocs.pro

GOT IT

Use another account
Developer Registration
What is required for developer registration?

- Different info for different platforms (Web, Android, iOS, Windows)
- Developer Information
  - Domain ownership & verification (introduces friction)
- App Information (Logo, Name etc.)
  - What can be verified?
- Scopes
  - Part of the request or at registration
- Justification for the data?
- Privacy policy/ToS
Future

- More verification
- Justification required for sensitive data
- Manual review required
  - If exceeding certain threshold of users
- Learnings from Manual reviews
Approval page

- What metrics should you optimize?
  - Approval rate?
- Amount of info/data/txt on the page
  - Most users don’t read
- Controls on the page?
- **Do users understand?**
- Design -> Study -> Launch -> Data -> Repeat
The *Photo Editor* application on your computer is requesting access to your Google Account for the product(s) listed below.

![Picasa Web Albums](http://picasaweb.google.com)

If you grant access, you can revoke access at any time under 'My Account'. The Photo Editor application will not have access to your password or any other personal information from your Google Account. Learn more

⚠️ The application that directed you here claims to be "Photo Editor". We are unable to verify this claim as the application runs on your computer, as opposed to a website. We recommend you deny access unless you trust the application.

[Grant access] [Deny access]
Example App would like to:

- View your basic profile info
- View your email address

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Deny  Allow
Guardian would like to:

- Know your basic profile info and list of people in your circles.
- Allow Google to let the people in these circles know that you have signed in to this app with Google:

Only you

By touching Sign in, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies.

CANCEL   SIGN IN
No approval page for “Sign-in”
Hi Naveen

nvnagr@gmail.com

Pinterest.com wants to

Know your age range and language

Allow Pinterest.com to do this?

You may review this app’s terms of service and privacy policies. You can remove this or any other app connected to your account in My Account.

CANCEL  ALLOW
It says Google, so it’s safe.

Manage? Oh, I see, delete.

Files on my device?

Will it still work if I say no?

Verified? Great, it won’t spam me.

Why does it want all these things?

App, like app on my phone?
Future

- Give user more guidance
  - Based on various signals
- Differentiated consent page
  - Account chip for just “sign-in”
  - Risk based e.g. Danger, warning, normal
- Quota/Limits
User Notification
Notify user

- Mitigation for hijacked user
- Sensitive data approval reminder
Usage of token
Token Usage

- What does the app actually do?
- Is the developer compromised?
- Monitor for abnormal behavior
Revocation
Token revocation

- Remove inactive apps
- Discovery of token revocation page
- Give more info
  - App activity
- Highlight risky apps
- Guide the user with decision
Admin Controls
Give G Suite admins more controls

- Recent Launch
Summary

- OAuth Abuse has arrived
- Verify info about the app and developer
- Guide user through the consent process
- Notify user
- Monitor activity
- Enforce Limits/Quotas
- Give users information and controls on revocation
- Build admin controls
Questions?

naa@google.com

https://plus.google.com/+NaveenAgarwal