Identity Management

Hannes Tschofenig
Motivation

• OAuth was created to allow secure and privacy friendly sharing of data.
• OAuth is not an authentication protocol.
  – Works with any user authentication protocol (e.g., OATH, FIDO, W3C CryptoAPI, etc.)
  – Federated login possible with OpenID Connect
• OAuth is widely used on the Internet.
  – Example: Salesforce, Google, MSFT Azure, Deutsche Telekom, GSMA mobile connect (Orange, Telekom Italia)
$\textbf{Identity}$: Any subset of an individual's attributes, including names, that identifies the individual within a given context. Individuals usually have multiple identities for use in different contexts. \textit{(RFC 6973)}
Players

Resource Owner & User Agent

Authorization Server

Client

Protected Resource

Token

Courtesy to Justin Richer for the figure.
Google OAuth 2.0 Playground

This app would like to:

- View and manage the files and documents in your Google Drive
- View your email address
- Know who you are on Google

Google OAuth 2.0 Playground and Google will use this information in accordance with their respective terms of service and privacy policies.
Players: “Payment Terminology”

- Customer
- Resource Owner & User Agent
- Merchant
- Authorization Server
- Payment Infrastructure
- Protected Resource
- Token

Courtesy to Justin Richer for the figure.
Layering Payment on Top of Identity Infrastructure?
Insights we gained

• It works and is deployed.
  – Even password sharing practice has been significantly decreased.
• High interest to be the identity provider but not necessarily relying party.
• Incentivizing the issuance of strong credentials (i.e., stronger than passwords) is difficult.
• Design for a distributed mechanism can still lead to silos.
• Some companies use the standardized OAuth/OpenID Connect but add extensions that make their solution non-interoperable.
  – Lack of understanding? Mistake? Intention?
Insights we gained, cont.

- Relationship between relying party and identity provider is more than just technology.
  - Influenced by business agreements and legal frameworks → OIX

- Security guidance we provide in our specifications (e.g., RFC 6819) is sometimes “kindly ignored”.

- Privacy:
  - Consent mechanism lead to better privacy.
  - Relying parties still ask for too much but this is a deployment choice rather than something a standard can dictate.
  - Choice offered is often limited → “take it or leave it”
More Info?

- **OpenID Connect** might be a good platform for a payment protocol.
- Look at **IETF OAuth working group** for core specifications.
- OAuth Tutorial:
  - **Slides**
  - **Recording**
    ( Might require to download a Cisco Webex ARF player at [http://www.webex.com/go/down_player_win_arf](http://www.webex.com/go/down_player_win_arf) )