MIT FinTech Cybersecurity Summit, January 11, 2018

OPAL: Connecting Identity & Data

Thomas Hardjono
MIT Connection Science
MIT Trust::Data Consortium
Identity Providers: What, Who & Why

• Problem of multiple accounts & passwords (late 1990s)
• Problem of repeated re-entering of passwords
• Solution: Authenticate once to “Identity Provider” (IdP)
• IdP issues Assertion or Token
• Userields Assertion or Token to desired Service Provider

Source: Venn of Federated Identity, Forrester, 2011

1) Request service

2) Redirect user

3) Mutual Authentication

4) Issue Assertion

Identity Provider

IdP

User

Relying Party

RP

Service

5) User gets service

- Avoid multiple logins
- User authenticates once only to IdP
- Browser use-case ("front channel")
- Session duration (user is present)
- Services “relies” on IdP for true assertions
Mobile Apps: OAuth & OpenID-Connect 1.0 (2011)

1) AuthN & request token

User (Resource Owner)

2) OP issues Access Token

(Token Provider)

3) Access Token

App (Client)

4) App gets access

Files (Resource)

• Delegated model
• User authenticates to OpenID Provider (OP)
• Token issued to Client (3rd party app)
• App holds token for long time
• Refresh tokens
But Identity Providers don’t have rich user data

- Same attributes collected (repeatedly)
- Fixed information

“It’s a data problem”
Extend the Model: Sharing Insights using OPAL

1) Request service

3) Mutual Authentication

4) Assertion & Identifier

5) User gets service

User

IdP

Relying Party

Data Repo

Data Repo

Data Repo

RP

Service

OPAL
Example: User obtaining Mortgage

(1) User authenticated & gets Identifier

(2) Request Mortgage

(3) OPAL Queries

(4) Safe Answers

Mortgage Provider

Identity & Data Provider

IdP

OPAL

Credit Card Data

Data Repo

Tax Data

Data Repo

Telco Data

Consortium for Data Sharing

Bob

Volunteer

Identifier

RP Service
What’s gained

- Service Providers obtain better insights about users & customers
- Improved risk management
- Raw data stays where it is
- User’s privacy maintained (safe answers)
- Regulatory compliance

- Broader insights across industry verticals
- Information derived using algorithms belongs to data owners
- Incentives to create better algorithms
- Market for algorithms
- AI and Machine Learning
Share Algorithms & Insights, not raw data

Trust Network of Data Providers (OPAL Network)

Finance Data
Telecoms Data
Social Data
Health Data

1. Issue an Identifier for User
2. Request Service using Identifier
3. Buy Insights about User using OPAL Algorithms & Identifier
4. Safe Answers

Service Providers (e.g. Mortgage Provider)
Questions
Core Identities, Personas & Transaction Identifiers

Trust Network for Data Sharing

Data and Core Identities

Personas

Transaction Identifiers
Identity Standards

- **SAML2.0**: universal language for B2B identity federation
- **OAuth2.0**: “token-based” authorization for Web Applications, Mobile Apps and RESTful APIs
- **OpenID-Connect**: Attribute Exchange using OAuth2.0 model
- **UMA1.0**: User-centric consent management (over OAuth2.0)

Source: Eve Maler, UMA WG, Kantara Initiative, 2011