

Identity management terminology



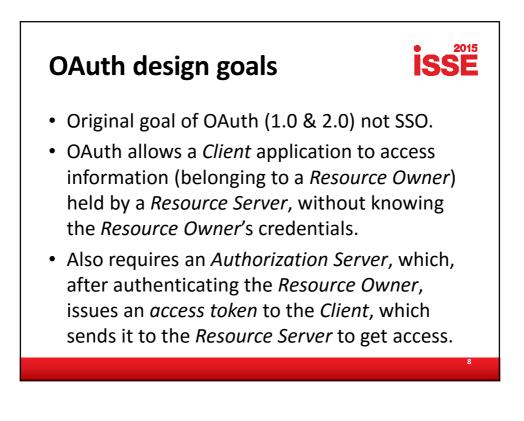
- Identity Provider (IdP) authenticates user and vouches for User identity to ...
- **Relying Parties (RPs)**, which rely on IdP and provide online services to ...
- Users, who employ ...
- User Agents (UAs) (typically web browsers), to interact with RPs.

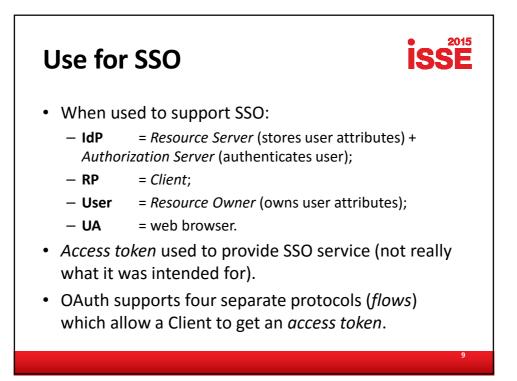


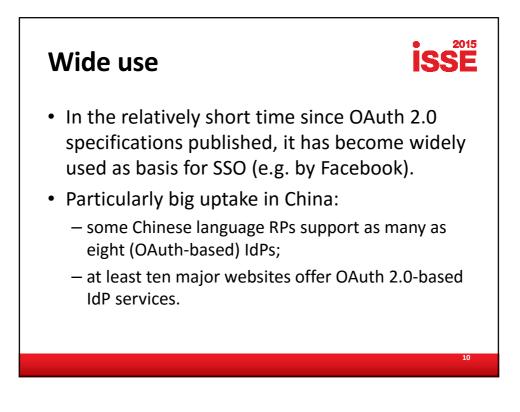
OAuth 2.0

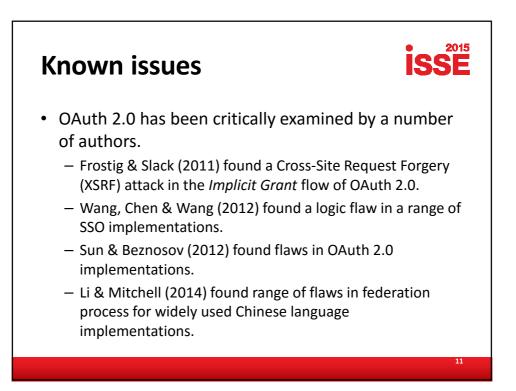


- OAuth 2.0, published in 2012 (RFC 6819), is being widely used as the basis of Englishlanguage SSO services, e.g. for *Facebook Connect*.
- It is also being very widely used for SSO by a range of popular IdPs operating in other languages, notably in China.
- Serious practical issues with use of OAuth 2.0 by Facebook and others have been identified.

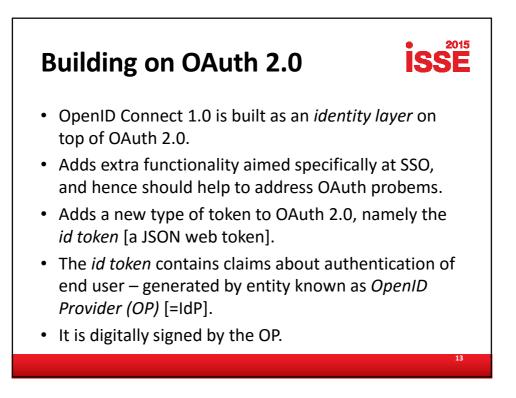










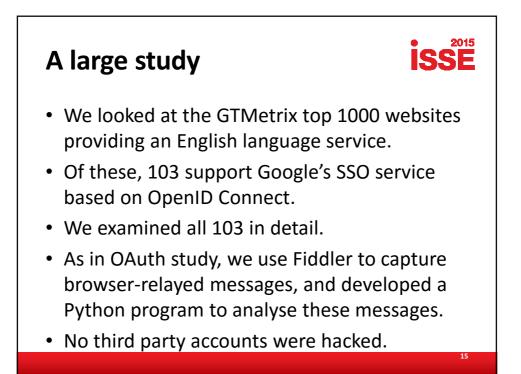


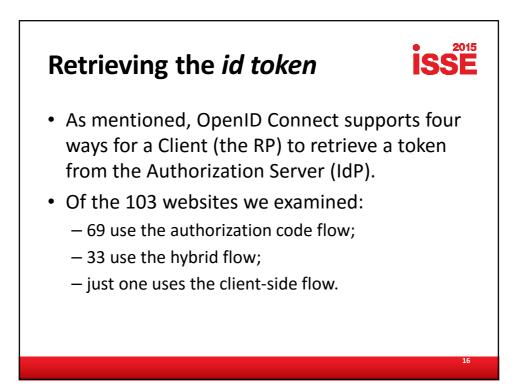
Four ways to retrieve an *id* token

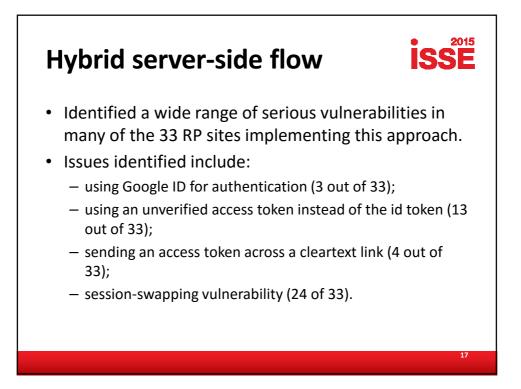
• OAuth (and hence OpenID Connect) supports four ways for a Client (the RP) to retrieve a token from the Authorization Server (IdP):

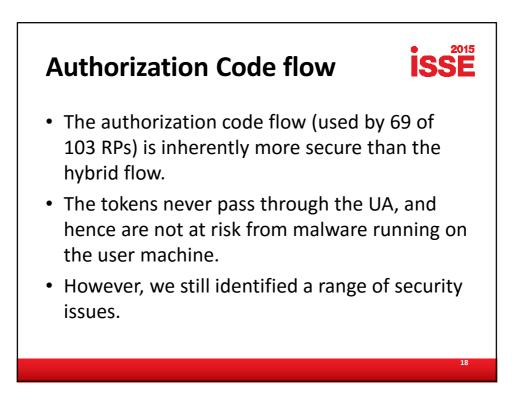
ISSF

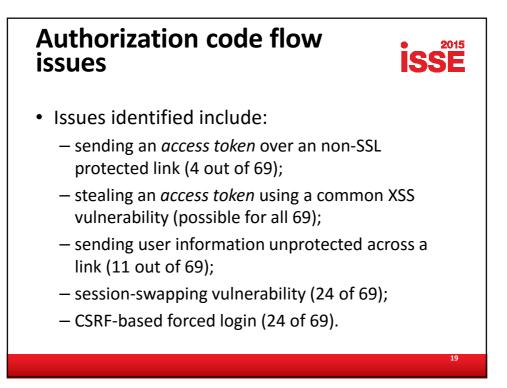
- *hybrid flow* [token sent via the UA, using an RPprovided JavaScript client running on UA];
- *client-side flow* [very similar to hybrid flow];
- *authorization code flow* [token sent directly from authorization server (IdP) to client (RP)];
- pure server-side flow [not supported by Google].

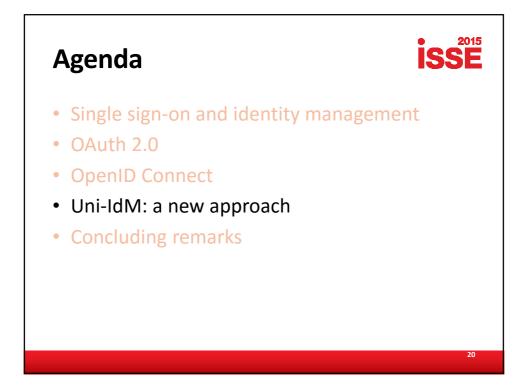


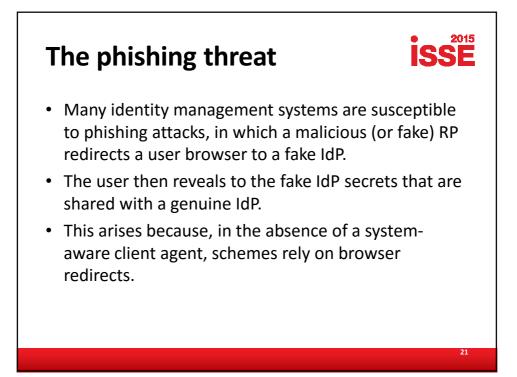


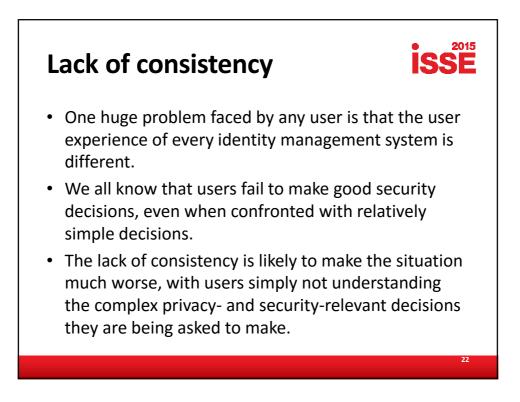


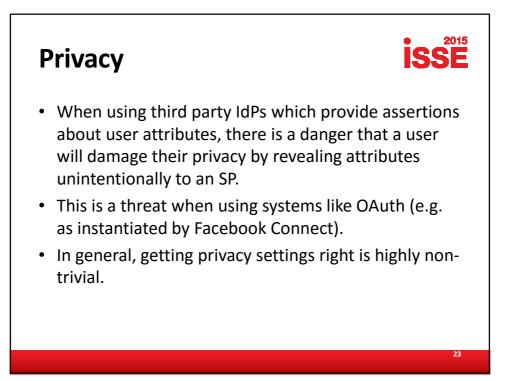






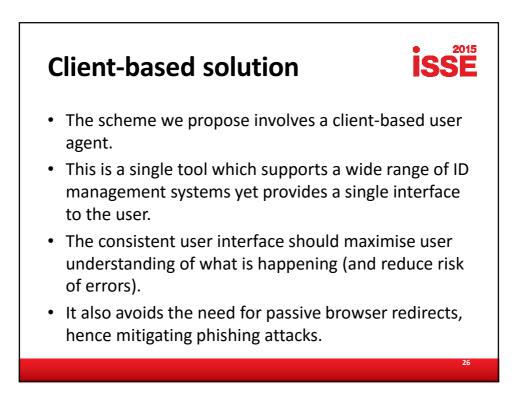












2015



- One motivation for the scheme comes from considering CardSpace (and its open source 'twin', Higgins).
- CardSpace acts as client-based agent, and provides a consistent card-based user interface.
- That is, sets of user credentials (relationships with IdPs) are represented to users as cards.
- CardSpace also defines a set of protocols for interactions between IdPs, Clients (user machines) and SPs.

