Partial Identities and Credentials

A report on work in progress for Primelife

Dave Raggett

<dsr@w3.org>

What is Online Identity for?

- Enable websites to provide a customized experience for each user
- Enable delivery of messages to specific people and organizations
- As a means to find friends and build networks
- As a means to make statements about specific people and organizations

Privacy

- About avoiding harm through inappropriate disclosure and use of personal information
  - Discrimination
  - Loss of face
- We willingly trade personal information for services
  - Customized experience adds value
  - To sustain free services based on ads
- We trust that personal information will be used responsibly
  - Constraints on access, purpose and retention
  - How is this trust maintained?
- Principle of minimal disclosure

Identity and Credentials

- Credential
  - Entity X attests that person Y has property Z
    - Properties like age, location, membership of group
    - Credential used as condition for access to service
- Static credentials
  - Physical credentials
    - Passport, driving license
  - Digital credentials
    - Tied to public Identifier

Identities, Credentials & Privacy

- Static credentials compromise privacy
  - Reliance on public identity
  - Which makes it easy to link information to build a more detailed picture about you
- Dynamic credentials to the rescue …
  - Credentials tied to partial identities
  - Minimal disclosure

Dynamic Credentials I

- Website indicates what credentials are needed
  - e.g. proof your age > 18 for purchase of crate of wine, or you are a current student at the University of Southampton for access to social network
  - Variety of mechanisms possible
    - JSON/XML/JavaScript via HTTP header, HTML link or web page script
- Browser extension requests credential from issuer
  - User is first asked for permission
  - Credential tied to website user name or session ID
  - Issuer isn't told why or who this is needed for
- Credential passed to website
  - Using mechanism described by website
- Practical Implementation as Firefox extension (due Jan 2011)

Dynamic Credentials II

- Avoid need to contact issuer for dynamic credential
- Start from conventional static credential
- Generate zero-knowledge proof of possession of static credential tied to partial ID
  - But only disclose selected subset of properties
  - And not your public identity!
- Open source crypto magic from IBM *(idemix)*
  - http://www.zurich.ibm.com/security/idemix/
- Implemented with LiveConnect and Java library

Related Work

- Firefox account manager
  - Simplifies management of site user id/password
    - http://www.mozilla.com/en-US/firefox/accountmanager/
- Privacy Dashboard
  - Firefox extension that tracks how websites gather personal info and lets you set privacy preferences on per site basis
    - http://www.primelife.eu/results/opensource/76-dashboard
- Fresh take on P3P
  - Firefox extension that matches privacy preferences with site policies for information disclosed through HTTP request headers during a browser session
    - http://www.w3.org/2010/09/raggett-fresh-take-on p3p/