User Centric Authentication for Web Applications

Michal Procházka, Daniel Kouřil, Luděk Matyska
Masaryk University, Brno, Czech Republic

The 2010 International Symposium on Collaborative Technologies and Systems
Outline

• Introduction
• Identity federations
• Drawbacks of current identity federations
• Problems need to be addressed
• Aditi
• Conclusion
Introduction

- Web based collaborative environments
  - Users from different domains
- Problem of user identification (authentication)
- Managing access to the restricted resources (authorization)
- Promising solution is federated identity, but current implementations possess several problems
Identity federations (IF)

- Basically consists of Service providers (SP) and Identity providers (IdP)
- User authentication is done on the IdP, SP only receives acknowledge from the IdP
- Allows to interconnect users' identity management systems with SP in a standard manner (using IF middleware)
- IF Middlewares: SAML based IF (Shibboleth), OpenID, CardSpace
Drawbacks of current IF (1)

- SAML based
  - Static central configuration (Metadata)
  - Painful SP provisioning
  - Users cannot control information released about them, IdPs decide, therefore IdPs needs to take care of all accepted SPs
  - Information from one IdP cannot be combined with information from other IdP
Drawbacks of current IF (2)

- OpenID
  - User needs to maintain his/her unique identifier
  - User provides his/her identifier to the SP
  - Missing protection against DNS, MITM and phishing attacks
  - Missing validation of the IdP trustworthiness → missing validation of the source of the information
  - Information from one IdP cannot be combined with information from other IdP
Drawbacks of current IF (3)

- **CardSpace**
  - SPs and IdPs have to know each other in advance
  - SP has to agree with IdP on the underlying protocol (CardSpace is protocol agnostic)
  - Requires client software – Card selector
  - Information from one IdP cannot be combined with information from other IdP
Problems need to be addressed

- Complete user control over information released by the IdP
- Implement trust only where is needed (SP → IdP)
- Support for trust computation (trustworthiness of IdPs)
- Leverage current implementation as much as possible (SAML is promising solution)
Aditi

- New view on the IF concept (SAML based)
- User becomes both SP and IdP (user's SP and user's IdP)
- User decides which information will be released and can add its own
- Uses card selector (locally or remotely managed)
- IdPs communicates only with user's SP
  - IdPs are not connected with SPs anymore
Aditi design

Attributes flow
Trust link
User authentication

Trust Network

Trust Processor
IdP
User's SP
User
Card Selector
User's IdP

Trust Processor
SP
Login process

- User accesses SP (Aditit enabled)
- SP replies with authN request to the user, specifying which attributes are needed
- User selects card which fits SP needs or creates new one
  - If the attributes are expired or hasn't been cached, IdPs are connected to get fresh one
- User sends appropriate set of attributes back to the SP
- SP can verify each attribute, because it is signed by the IdP
Aditi trust and Trust Network

- Each SP can operate Trust Processor
  - Maintains trust information about IdP
  - Provides list of trusted IdPs gathered from SAML Metadata, manual configuration, PKI, …
  - Can operate Trust Network node

- Trust Network
  - P2P based network used to share trust information about its members
  - Reputation based computation of the trust
Aditi trust and Trust Network
Aditi complementary features

- Support of non-web applications
  - As user operates SP and IdP, it can also operate credential transformation service (e.g. federated identity → PKI)
- Aditi can work without using cookies
  - New EU regulation law requires user's consent to store the cookie in her browser
  - Aditi can sends set of user's attributes along with each request to the SP
Conclusion

- Aditi introduces new view on the IF with these features:
  - Complete user control over her information released by her IdP(s)
  - Easy SP provisioning
  - Helps SPs to compute trust of each IdP
Thank you.

Questions?