Introduction to SAML and claims-based security

Andrea Cogliati
Rochester OWASP President
http://owasp.org/rochester
andrea.cogliati@owasp.org

OWASP
Education Project

The OWASP Foundation
http://www.owasp.org

Agenda

- Defining the problem
- Available technologies
- Claims-based security model
- Why this is important for OWASP

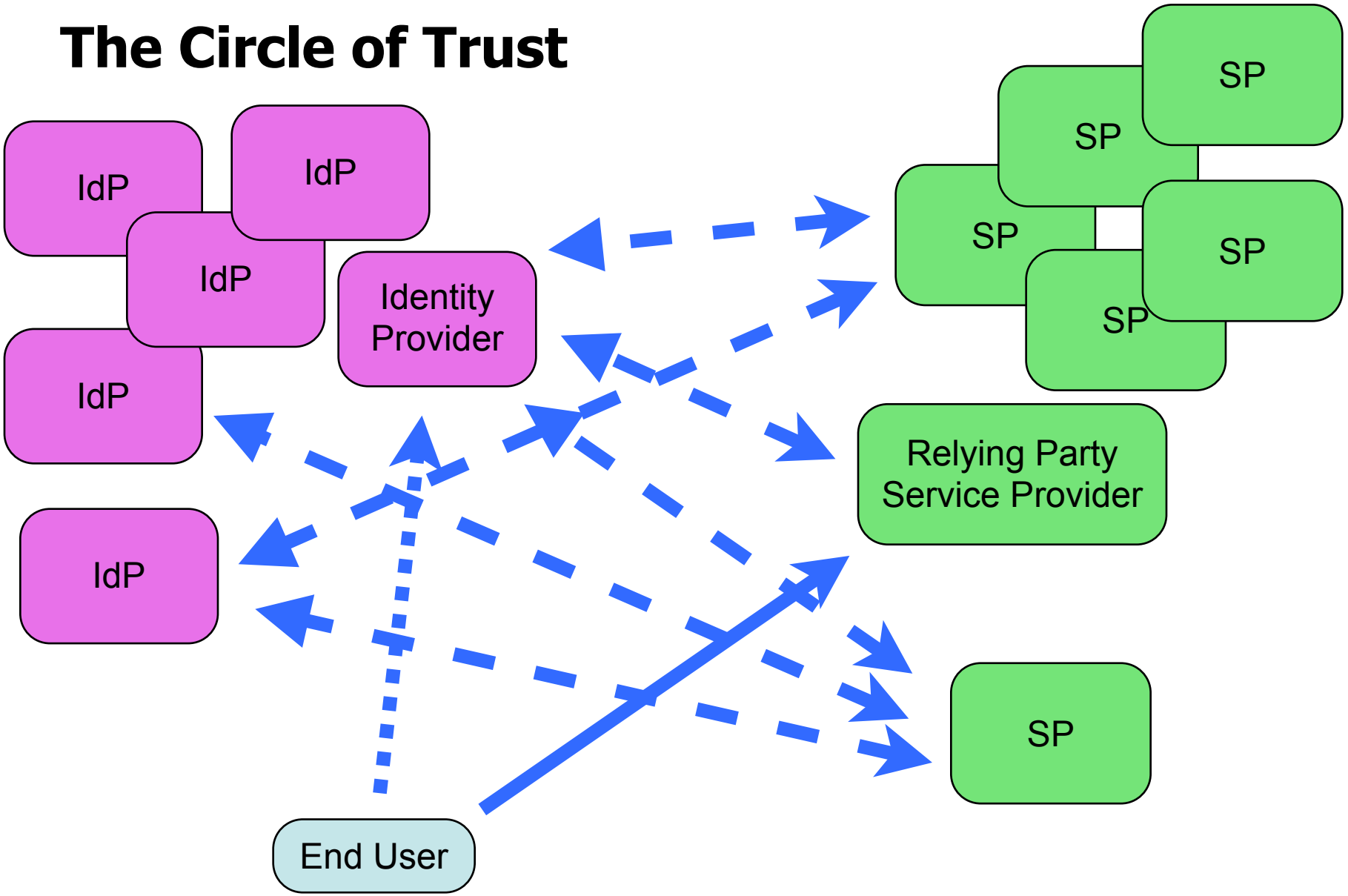
A common scenario

- Vacation: flight, hotel, car, restaurants, spa treatments, ...
- Single stop shop: e.g., Expedia
- Comparison shopping: Priceline, airline websites, establishment websites, ...
- You end up with:
  - Multiple credentials
  - Multiple logins

Enterprise scenario

- A bank has a single directory service: e.g., Active Directory
- Bank creates a remote banking application
  - Where to store customers' credentials?
    - AD?
      - Licensing, security concerns, technical considerations, ...
    - DB?
      - Multiple repositories, declarative security, ...
- Outsourcing, B2B, ...
- The bank merges with another bank...
  - Consolidate employees, customers, contractors, business partners, ...

The Circle of Trust



Current solutions

- Windows Live ID (AKA MS Passport, .NET Passport)
  - Closed, proprietary, centralized
    - It's a "pyramid" of trust!
  - eBay and Expedia stopped supporting it
- OpenID
  - Lots of IdPs
  - Very few Relying Parties
  - User oriented
  - Limited personalization
- SAML
  - XML-based standard by the OASIS Security Services Technical Committee
  - Exchange authentication and authorization assertions between security domains
- Liberty Alliance ID-*
- WS-*

SAML assertions

- Authentication statements
  - assert to SP that a principal authenticated with IdP at a particular time using a particular method of authentication
- Attribute statements
  - assert that a subject is associated with certain attributes
- Authorization decision statements
  - asserts that a subject is permitted to perform action A on resource R given evidence E
  - deprecated in favor of XACML (eXtensible Access Control Markup Language)

Claims-based security model

- MS marketing term
- Part of the Windows Communication Foundation (WCF)
- Decouple authentication and, possibly, authorization from applications
- Consume claims (security assertions)
- Prefer declarative security to programmatic security

Why is this important to OWASP?

- Identity federations and security assertions are likely to become prominent in enterprise webapps
- Nobody has ever done a threat model
  - From OWASP Top Ten 2010 RC1
    - A3 – Broken Authentication and Session Management
    - A6 – Security Misconfiguration (NEW)
    - A8 – Unvalidated Redirects and Forwards (NEW)
  - Trust but check?

Call to action

- Establish best practices for assertions-based security in webapps
- Threat-modeling of current technologies/ products
- Source code analysis of open source products
- Vulnerability assessment of commercial products
- Educate the community
- Lobby for OWASP in SIGs (Concordia, Liberty Alliance, OASIS, ...)
- Showcase ESAPI for assertions-based security

If you're interested...

Drop me an email

andrea.cogliati@owasp.org