Single Sign on with SAML

Madhu Siddalingaiah
madhu@madhu.com
http://www.madhu.com
301-801-9122

Outline

- What is single sign-on?
- Introduction to SAML
- SAML solutions
- Walmart benefits application
- Wrap up

About the Presenter

- Independent IT consultant
  - More than 15 years professional experience
    - Wireless, enterprise, embedded systems
  - Apple computer, Blue Cross/Blue Shield, Food & Drug Administration, Department of Defense, Sun Microsystems
- Authored three books and numerous articles
  - Java, XML, Web development
- Delivered more than 100 presentations at venues worldwide
  - North America, Europe, Asia, Australia
  - EclipseCon 2006, March 20-23, 2006, Santa Clara
    - *Eclipse vs. Visual Studio*
- Private pilot since 1987
  - Rotorcraft-helicopter rating

Recent Project

- Handheld e-Prescribing app
  - PalmOS and PocketPC
- Features
  - View patient history
  - Prescribe new medications
    - Bluetooth printing
  - Flags drug interactions
  - Suggests preferred alternatives
  - Integrates with backend DB
- In the works
  - Wireless direct to pharmacy

What is Single Sign-on?

Sounds simple…

- Send username/password to second website!
  - Not secure
  - Both websites must share authorization credentials
    - Difficult to manage
    - Two sites are tightly coupled
  - Plaintext passwords must be available
    - Not a good idea
- OK, send a ticket or something…
  - Requires architecting a solution
  - Is it secure?
  - What about a standard?

Security Assertion Markup Language (SAML)

- Emerging standard for exchanging authentication, entitlement, and attribute information
  - Developed by OASIS
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- Enjoys industry support
  - RSA, IBM, SUN, Novell, Oracle etc.
  - Commercial products exist
    - RSA federated identity management (FIM)
- Well engineered
  - Secure (so far!)
- Relatively straightforward
  - Not hard to roll your own solution

SAML Concepts

- SAML 1.0 terminology
  - SAML 2.0 is slightly different, but conceptually similar
- Asserting party (AP)
  - The site you are logged into
  - Send assertions to relying party
- Relying party (RP)
  - The site you want to go to
  - Receives assertions from AP
- Assertion
  - Data exchanged from AP to RP
    - XML data
  - Can include users identity, authentication data, or any other attributes
  - Information agreed upon by AP and RP
    - Not specified by SAML proper

Assertion Example

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
    <env:Body>
        <samlp:AuthnRequest
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
            ForceAuthn="true"
            AssertionConsumerServiceURL="https://www.sp.example.com/SSO"
            AttributeConsumingServiceIndex="0"
            ProviderName="CarRentalInc.com"
            ID="abe567de6" Version="2.0"
            IssueInstant="2005-01-31T12:00:00Z"
            Destination="https://www.idp.example.com/">
            <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
                    j.doe@acompany.com
                </saml:NameID>
            </saml:Subject>
        </samlp:AuthnRequest>
    </env:Body>
</env:Envelope>
```

This is the important bit

How Does it Work?

- Browser post profile (BPP)
  - AP posts assertions to RP in HTML form
  - SSL post for confidentiality
- Browser artifact profile (BAP)
  - AP issues a redirect with SAML artifact
    - Large, volatile random number
      - Like a secret ticket
    - http://www.rpsite.com?SAMLart=34229AFS403AM44532
  - RP issues a SOAP call to AP and supplies artifact
    - AP returns assertions

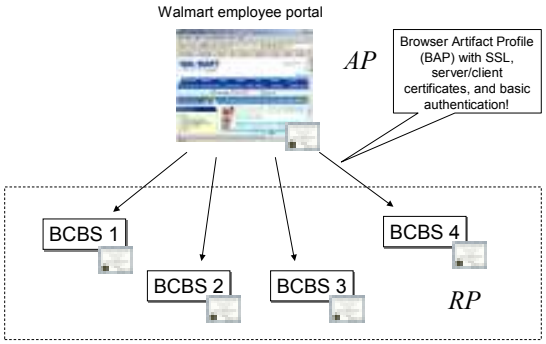
Implementing a Solution

- OpenSAML
  - http://www.opensaml.org/
  - Comprehensive Java framework
  - Does a lot, you probably won't need all of it
- Commercial products
  - IBM Tivoli Access Manager
  - Oblix NetPoint
  - SunONE Identity Server
  - Baltimore, SelectAccess
  - Entegrity Solutions AssureAccess
  - Internet2 OpenSAML
  - Netegrity SiteMinder
  - Sigaba Secure Messaging Solutions
  - RSA Security ClearTrust
  - VeriSign Trust Integration Toolkit
  - Entrust GetAccess 7

Challenges

- SAML proper is not a big deal
  - Protocols are straightforward
  - OpenSAML is a good starting point
  - Many vendors are available to help
- Integration with your enterprise is probably hard!
  - Multiple, heterogeneous systems
    - How do you manage authentication?
  - Must establish trust between AP and RP
    - SSL and mutual certificates often used
    - Configuration and testing takes time

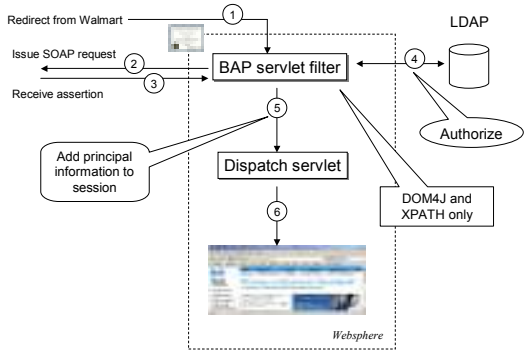
Real World Implementation



Initial Prototype

- Start with OpenSAML
  - Originally did not fully support browser artifact profile (BAP)
  - Some support code needed
- Developed prototype using Jetty
  - Worked well
- Test with with Websphere before implementing production solution
  - Crash and burn!!!
  - OpenSAML required DOM 3.0 APIs
    - Default implementation does not work
    - Would have caused too many ripples in IBM JVM
- Time to fall back…

Final Solution



Testing and Production Challenges

- Client and Server certificates
  - Configuration is time consuming
    - Requires close communication between both parties
      - Test certs expired many times!
    - Lots of *hurry up and wait*
  - Default Websphere 5.1 HTTPS implementation is old
    - Need to add HTTPS package –D JVM parameter
      - Where is that documented?!?!
  - Debugging is difficult
    - Exception: Bad certificate
      - Which one?
- Did I mention basic authentication?
  - *I thought I sent you the password…*

End Result

- It actually worked!
  - Delivered on time and within budget
- Customer (Walmart) was very happy
  - Saves employees considerable time and effort

JUG Promotion

- Half day free onsite consultation
  - Available to all JUG members
- Typical services
  - Design/code review
  - Architect a solution
  - Technology overview
  - Solve challenging problems
  - Rapid prototype
- Contact
  - madhu@madhu.com
  - http://www.madhu.com
  - 301-801-9122

Free to all JUG members!