SAML basics
A technical introduction to the Security Assertion Markup Language

Eve Maler
XML Standards Architect
XML Technology Center
Sun Microsystems, Inc.
Agenda

I’m hoping to cover a lot in an hour!

• The problem space
• SAML concepts
• Walking through scenarios
• Status of SAML and related standards efforts

(thanks to Prateek Mishra (Netegrity) and RLBob Morgan (UWWashington) for some material in this presentation)
Agenda

- The problem space
  - Why invent SAML at all?
- SAML concepts
- Walking through scenarios
- Status of SAML and related standards efforts
What problems does SAML try to solve?

- Permissions management data is shared in mostly proprietary ways
  - Integrating new security features may require developing a lot of new code
  - The different systems that generate and use security data are very tightly coupled
- Web-based applications show the need for more federation
  - We need to cross domains more easily
Two common web application scenarios

• Logged-in users of analyst research site SmithCo are allowed access to research produced by sister site JonesCo

• Employees at SmithCo are allowed to order office supplies from OfficeBarn if they are authorized to spend enough
SAML use cases in more detail

- SAML developed three “use cases” to drive its requirements:
  - Single sign-on (SSO)
  - Authorization service
  - Back office transaction
- Each use case has one or more “scenarios” that provide a more detailed roadmap of interaction
Authorization service use case

User → Access Resource → Policy Enforcement Point

Policy Enforcement Point → Check Permission → Policy Decision Point
Back office transaction use case

Authenticate, Qualify

Buyer

Transact Business

Authority Known to Both

Seller
What’s needed

• A standard XML message format
  – It’s just data traveling on any wire
  – No particular API mandated
  – Lots of XML tools available

• A standard message exchange protocol
  – Clarity in orchestrating how you ask for and get the information you need

• Rules for how the messages ride “on” and “in” transport protocols
  – For better interoperability
Agenda

- The problem space
- **SAML concepts**
  - SAML in a nutshell
  - Producers and consumers of assertions
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and related standards efforts
SAML in a nutshell

- It’s an XML-based framework for exchanging security information
  - XML-encoded security “assertions”
  - XML-encoded request/response protocol
  - Rules on using assertions with standard transport and messaging frameworks

- It’s an emerging OASIS standard
  - Vendors and users are involved
  - Codifies current system outputs rather than inventing new technology
Agenda

- The problem space
- **SAML concepts**
  - SAML in a nutshell
  - SAML assertions
  - Producers and consumers of assertions
  - Message exchange protocol
  - Bindings and profiles
- Walking through scenarios
- Status of SAML and related standards efforts
SAML assertions

• An assertion is a declaration of fact about a subject, e.g. a user
  – (according to some assertion issuer)

• SAML has three kinds, all related to security:
  – Authentication
  – Attribute
  – Authorization decision

• You can extend SAML to make your own kinds of assertions

• Assertions can be digitally signed
All assertions have some common information

- Issuer and issuance timestamp
- Assertion ID
- Subject
  - Name plus the security domain
  - Optional subject confirmation, e.g. public key
- “Conditions” under which assertion is valid
  - SAML clients must reject assertions containing unsupported conditions
  - Special kind of condition: assertion validity period
- Additional “advice”
  - E.g., to explain how the assertion was made
Authentication assertion

- An issuing authority asserts that:
  - subject S
  - was authenticated by means M
  - at time T

- **Caution:** Actually checking or revoking of credentials is not in scope for SAML!
  - Password exchange
  - Challenge-response
  - Etc.

- It merely lets you link back to acts of authentication that took place previously
Example authentication assertion*  
*draft syntax

```xml
<saml:Assertion
    MajorVersion="1" MinorVersion="0"
    AssertionID="128.9.167.32.12345678"
    Issuer="Smith Corporation"
    IssueInstant="2001-12-03T10:02:00Z">
    <saml:Conditions
        NotBefore="2001-12-03T10:00:00Z"
        NotAfter="2001-12-03T10:05:00Z" />
    <saml:AuthenticationStatement
        AuthenticationMethod="password"
        AuthenticationInstant="2001-12-03T10:02:00Z">
        <saml:Subject>
            <saml:NameIdentifier
                SecurityDomain="smithco.com"
                Name="joeuser" />
        </saml:Subject>
    </saml:AuthenticationStatement>
</saml:Assertion>
```
Attribute assertion

- An issuing authority asserts that:
  - subject S
  - is associated with attributes A, B, ...
  - with values “a”, “b”, “c”...

- Typically this would be gotten from an LDAP repository
  - “john.doe” in “example.com”
  - is associated with attribute “Department”
  - with value “Human Resources”
Example attribute assertion

<saml:Assertion ...>
  <saml:Conditions .../>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="joeuser" />
    </saml:Subject>
    <saml:Attribute
      AttributeName="PaidStatus"
      AttributeNamespace="http://smithco.com">
      <saml:AttributeValue>
        PaidUp
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
Authorization decision assertion

• An issuing authority decides whether to grant the request:
  – by subject S
  – for access type A
  – to resource R
  – given evidence E

• The subject could be a human or a program

• The resource could be a web page or a web service, for example
Example authorization decision assertion

```xml
<saml:Assertion ...>
  <saml:Conditions .../>
  <saml:AuthorizationStatement
    Decision="Permit"
    Resource="http://jonesco.com/rpt_12345.htm">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="joeuser"/>
    </saml:Subject>
  </saml:AuthorizationStatement>
</saml:Assertion>
```
Agenda

• The problem space

• SAML concepts
  – SAML in a nutshell
  – SAML assertions
  – Producers and consumers of assertions
  – Message exchange protocol
  – Bindings and profiles

• Walking through scenarios

• Status of SAML and related standards efforts
SAML producer-consumer model
This model is conceptual only

• In practice, multiple kinds of authorities may reside in a single software system
  – SAML allows, but doesn’t require, total federation of these jobs
• Also, the arrows may not reflect information flow in real life
  – Information can be pulled or pushed
  – Not all assertions are always produced
  – Not all potential consumers (clients) are shown
Agenda

• The problem space
• **SAML concepts**
  – SAML in a nutshell
  – SAML assertions
  – Producers and consumers of assertions
  – Message exchange protocol
  – Bindings and profiles
• Walking through scenarios
• Status of SAML and related standards efforts
SAML protocol for getting assertions

Asserting Party

SAML

Request for Assertion of Certain Type

Response Assertion

Relying Party
Assertions are normally provided in a SAML response

- Existing tightly coupled environments may need to use their own protocol
  - They can use assertions without the rest of the structure
- The full benefit of SAML will be realized where parties with no direct knowledge of each other can interact
  - Via a third-party introduction
Authentication assertion request

- “Please provide the authentication information for this subject, if you have any”
- It is assumed that the requester and responder have a trust relationship
  - They are talking about the same subject
  - The response with the assertion is a “letter of introduction” for the subject
Example authentication assertion request

```xml
<samlp:Request
    MajorVersion="1" MinorVersion="0"
    RequestID="128.14.234.20.12345678">
    <samlp:AuthenticationQuery>
        <saml:Subject>
            <saml:NameIdentifier
                SecurityDomain="smithco.com"
                Name="joeuser" />
        </saml:Subject>
    </samlp:AuthenticationQuery>
</samlp:Request>
```
Attribute assertion request

• “Please provide information on the listed attributes for this subject”

• If the requester is denied access to some of the attributes, there are options for what gets returned
  – Only the partial list of accessible attributes
  – Either all of the attributes requested, or none
Example attribute assertion request

```xml
<samlp:Request ... >
  <samlp:AttributeQuery
    CompletenessSpecifier="Partial">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="joeuser" />
    </saml:Subject>
    <saml:AttributeDesignator
      AttributeName="PaidStatus"
      AttributeNamespace="http://smithco.com"/>
  </samlp:AttributeQuery>
</samlp:Request>
```
Authorization decision
assertion request

• “Is this subject allowed to access the specified resource in the specified manner, given this evidence?”

• This type of request is the most complex
Example authorization decision assertion request

```xml
<samlp:Request ...>
  <samlp:AuthorizationQuery
    Resource="http://jonesco.com/rpt_12345.htm">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="smithco.com"
        Name="joeuser" />
    </saml:Subject>
    <saml:Actions Namespace="http://...">
      <saml:Action>Read</saml:Action>
    </saml:Actions>
    <saml:Evidence>
      <saml:Assertion>
        ...some assertion...
      </saml:Assertion>
    </saml:Evidence>
  </samlp:AuthorizationQuery>
</samlp:Request>
```
Example response

<samlp:Response
   MajorVersion="1" MinorVersion="0"
   RequestID="128.14.234.20.90123456"
   InResponseTo="128.14.234.20.12345678"
   StatusCode="Success">
   <saml:Assertion
      MajorVersion="1" MinorVersion="0"
      AssertionID="128.9.167.32.12345678"
      Issuer="Smith Corporation">
      <saml:Conditions
         NotBefore="2001-12-03T10:00:00Z"
         NotAfter="2001-12-03T10:05:00Z" />
      <saml:AuthenticationStatement ...
      </saml:AuthenticationStatement>
   </saml:Assertion>
</samlp:Request>
Agenda

• The problem space
• **SAML concepts**
  – SAML in a nutshell
  – SAML assertions
  – Producers and consumers of assertions
  – Message exchange protocol
  – Bindings and profiles
• Walking through scenarios
• Status of SAML and related standards efforts
Bindings and profiles connect SAML with the wire

• This is where SAML itself gets made secure

• A “binding” is a way to transport SAML requests and responses
  – SOAP-over-HTTP binding is a baseline
  – Other bindings will follow, e.g., raw HTTP

• A “profile” is a pattern for how to make assertions about other information
  – Web browser profile for SSO
  – SOAP profile for securing SOAP payloads
The SOAP-over-HTTP binding
By contrast, the SOAP profile
Web browser profiles

- These profiles assume:
  - A standard commercial browser and HTTP(S)
  - User has authenticated to a local source site
  - Assertion’s subject refers implicitly to the user

- When a user tries to access a target site:
  - A tiny authentication assertion reference travels with the request so the real assertion can be dereferenced
  - Or the real assertion gets POSTed
Agenda

• The problem space
• SAML concepts

• Walking through scenarios
  – SSO pull using web browser profile
  – Back office transaction using SOAP binding and SOAP profile

• Status of SAML and related standards efforts
SSO pull scenario

authenticate (out of band)

access inter-site transfer URL

redirect with artifact

get assertion consumer URL

request referenced assertion

supply referenced assertion

provide or refuse destination resource (out of band)
• “Access inter-site transfer URL” step:
  - User is at: http://smithco.com
  - Clicks on a link that looks like it will take her to http://jonesco.com
  - It really takes her to inter-site transfer URL: https://source.com/intersite?dest=jonesco.com

• “Redirect with artifact” step:
  - Reference to user’s authentication assertion is generated as a SAML “artifact” (8-byte base64 string)
  - User is redirected to assertion consumer URL, with artifact and target attached: https://jonesco.com?SAMLart=<artifact>
Agenda

• The problem space
• SAML concepts
• **Walking through scenarios**
  – SSO pull using web browser profile
  – Back office transaction using SOAP binding and SOAP profile
• Status of SAML and related standards efforts
Back office transaction scenario

Authenticate (out of band)
Request authentication and attribute assertions
Receive authentication and attribute assertions
Attach assertions to P.O.

Send P.O.
Process assertions and P.O.

Send P.O. response (out of band)
More on the back office transaction scenario

- An example of attaching SAML assertions to other traffic
- Asymmetrical relationship is assumed
  - Seller is already known to buyer, but buyer is not known to seller, a common situation
  - E.g., server-side certificates might be used to authenticate seller
- If it were symmetrical, additional SAML steps would happen on the right side too
  - This would likely be a different scenario
Agenda

- The problem space
- SAML concepts
- Walking through scenarios
- Status of SAML and related standards efforts
SAML status

• Work started on 9 January 2001
  – From a base of S2ML and AuthXML
• “Beta” specs are due by end of December
  – “Core” assertion and protocol spec
  – Bindings/profiles spec
  – Conformance spec
  – Security/privacy considerations spec
  – Glossary
  – www.oasis-open.org/committees/security/
• Implementations are starting to appear
  – JSAML Toolkit from Netegrity
  – www.netegrity.com
Important efforts related to SAML

- IETF/W3C XML Signature
  - Built into SAML for digitally signing assertions
  - www.w3.org/Signature/

- W3C XML Encryption and Canonicalization
  - Not quite ready yet, but encryption will be important
  - www.w3.org/Encryption/2001/

- XKMS and its relatives
  - An XML-based mechanism for doing PKI
  - SAML traffic might be secured by XKMS-based PKI, by other PKI, or by other means entirely
  - www.w3.org/TR/xkms/
More efforts related to security and identity

- **OASIS XACML**
  - XML-based access control/policy language
  - Could be the way PDPs talk to back-end policy stores
  - [www.oasis-open.org/committees/xacml/](http://www.oasis-open.org/committees/xacml/)

- **OASIS Provisioning**
  - XML-based framework for user, resource, and service provisioning
  - [www.oasis-open.org/committees/provision/](http://www.oasis-open.org/committees/provision/)

- **Liberty Alliance**
  - Identity solution for SSO of consumers and businesses
  - [www.projectliberty.org](http://www.projectliberty.org)

- **Internet2**
  - Higher-ed effort to develop advanced network applications and technologies
  - [http://www.internet2.edu/](http://www.internet2.edu/)
Agenda

• The problem space
• SAML concepts
• Walking through scenarios
• Status of SAML and related standards efforts
• Questions?
Thank you

Eve Maler
eve.maler@sun.com