Security Problems (and Solutions) for Service Oriented Applications

Daniel Kulp, Talend
dkulp@apache.org, November 10, 2011

Presented by

Produced by

What I Will Cover

- SOA Security Concerns
- Types of Security Problems
- WS-* Solutions
- REST Solutions
- Apache CXF extensions
- Thoughts for the future

My Background

- J. Daniel Kulp
- Talend
- VP - OpenSource Development
- ASF Member
- PMC for CXF, Camel, WebService, Maven, Aries. Committer for ServiceMix

SOA Security Concerns

- Collection of Services that make up a complex application that solves complex problems.
- Primarily Web Services
  - NOT just SOAP
  - Includes REST
- Can include other technologies like CORBA, JMS, etc...

Security Problems

- Authentication
- Authorization
- Message Protection
  - Data encryption
  - Signatures
- Intermediaries
- Security Tokens
- Performance

WS-* Solutions

- "Well Defined" (OK: overly complex) specifications
  - WS-Security
  - WS-SecureConversation
  - WS-SecurityPolicy
  - WS-Trust
  - Etc....

WS-Security

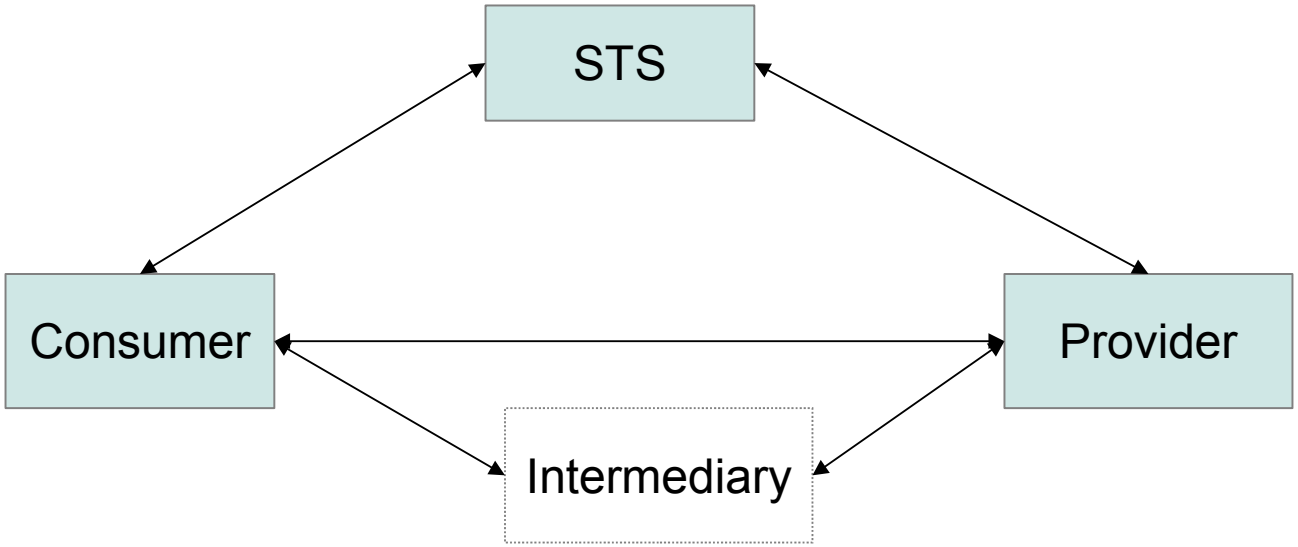
- How to sign SOAP messages to assure integrity.(based on XMLDsig)
- How to encrypt SOAP messages to assure confidentiality. (based on XML-Enc)
- How to attach security tokens to ascertain the sender's identity.
  - X.509, Kerberos, UserNameToken, SAML

WS-SecurityPolicy

- Tries to address the “contract” of the Security requirements
- XML based WS-Policy fragments that describe the Security requirements of the service
- Contains the information about what needs to be includes, what needs to be signed, what needs to be encrypted, algorithms, etc...

WS-Trust

- Managing Security Tokens
  - Issue, Renew, Cancel, Validate
- Support brokering trust relationships



WS-SecureConversation

- Attempt to address the “performance problem” of the WS-Security specifications.
- XML Signatures and Encryption using strong asymmetric keys is very expensive. WS-SecConv allows for a simpler symmetric key to be used after establishing a “session”.
- Extends WS-Trust

WS-*

- Addresses most of the security problems (performance may be the exception)
- Very complex
- Several “Profiles” defined to attempt to clarify and simplify things

REST

- HTTPS
- Basic Authentication

- NTLM/Digest Authentication
- OAuth

Really, very few “standards”

Apache CXF – WS-*

- Covers the WS-* stuff very well
  - Very well tested
  - Very actively developed
  - Highly interopable
  - High performance (relative)
  - New in 2.5.0 is an Enterprise Ready Security Token Service

Apache CXF - REST

- JAX-RS
  - OAuth 1.0 Flows
  - XML Message Protection
    - Enveloped
    - Enveloping
    - Detached
  - SAML
    - Auth Header
    - Token in Message
    - Form value

Future Work

- OAuth 2.0
- Single Sign-On / SAML
- SAML for Bearer token in OAuth 2.0 flows
- Performance (Streaming)
- WS-Federation for SSO
  - Apache Fediz proposal to the Incubator

More Information

- CXF - http://cxf.apache.org
  - Distribution contains several security samples
- Talend – http://talend.com
  - Talend ESB has several examples and webinars covering security topics
- Blogs
  - Colm - http://coheigea.blogspot.com/
  - Glen - http://www.jroller.com/gmazza/
  - Sergey - http://sberyozkin.blogspot.com/

Contact

- Daniel Kulp
  - **dkulp@apache.org**
  - **http://dankulp.com/blog**
  - **@DanKulp on Twitter**