Security Problems (and Solutions) for Service Oriented Applications

Daniel Kulp, Talend
dkulp@talend.com
My Background

J. Daniel Kulp
Talend
VP - OpenSource Development

ASF Member
PMC for CXF, Camel, WebService, Maven, Aries.
Committer for ServiceMix
What I Will Cover

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

Addresses most of the security problems (performance may be the exception)

Very complex

Several “Profiles” defined to attempt to clarify and simplify things
Apache CXF - WS-*

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

HTTPS

Basic Authentication
NTLM/Digest Authentication

OAuth

Really, very few “standards”
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](http://cxf.apache.org)
- Distribution contains several security samples

Talend - [http://talend.com](http://talend.com)
- Talend ESB has several code examples, tech notes and webinars covering security topics

Blogs - [http://coders.talend.com](http://coders.talend.com)
- Colm - [http://coheigea.blogspot.com/](http://coheigea.blogspot.com/)
- Sergey - [http://sberyozkin.blogspot.com/](http://sberyozkin.blogspot.com/)
Contact

▪ Daniel Kulp

▪ dkulp@talend.com

▪ http://dankulp.com/blog

▪ @DanKulp on Twitter
Thank You