Securing Web Services with Apache CXF

PROGRESS SOFTWARE

Daniel Kulp
Software Fellow
Progress Software
dkulp@progress.com

Who am I?

- Employed by IONA (now Progress) for 10 years working in Web Services space.
  - XMLBus, Artix, Celtix, CXF/Fuse
  - Currently in the Open Source group at Progress
  - http://fusesource.com
- Original “founders” of Apache CXF project
- Current PMC Chair of Apache CXF
- Also contribute to Apache Web Services and Apache Maven projects.

Agenda

- What is Apache CXF?
- What type of Security?
- Standards in the space
- Recommendations
- Demonstration
- Questions and answers

Apache CXF - http://cxf.apache.org

- One of the premier services frameworks for Java
- Started as merger of XFire (codehaus) and Celtix (ObjectWeb) in 2006 as incubator project at Apache
- Strong support for standards (including API standards)
- Not just “SOAP” framework
  - CORBA/IIOP
  - REST (JAX-RS)
- Graduated to TLP in May 2008
- Embedded in ServiceMix, Camel, JBoss, Mule, Pramati, JOnAS, Eclipse Swordfish, etc...
- Commercially supported: http://fusesource.com

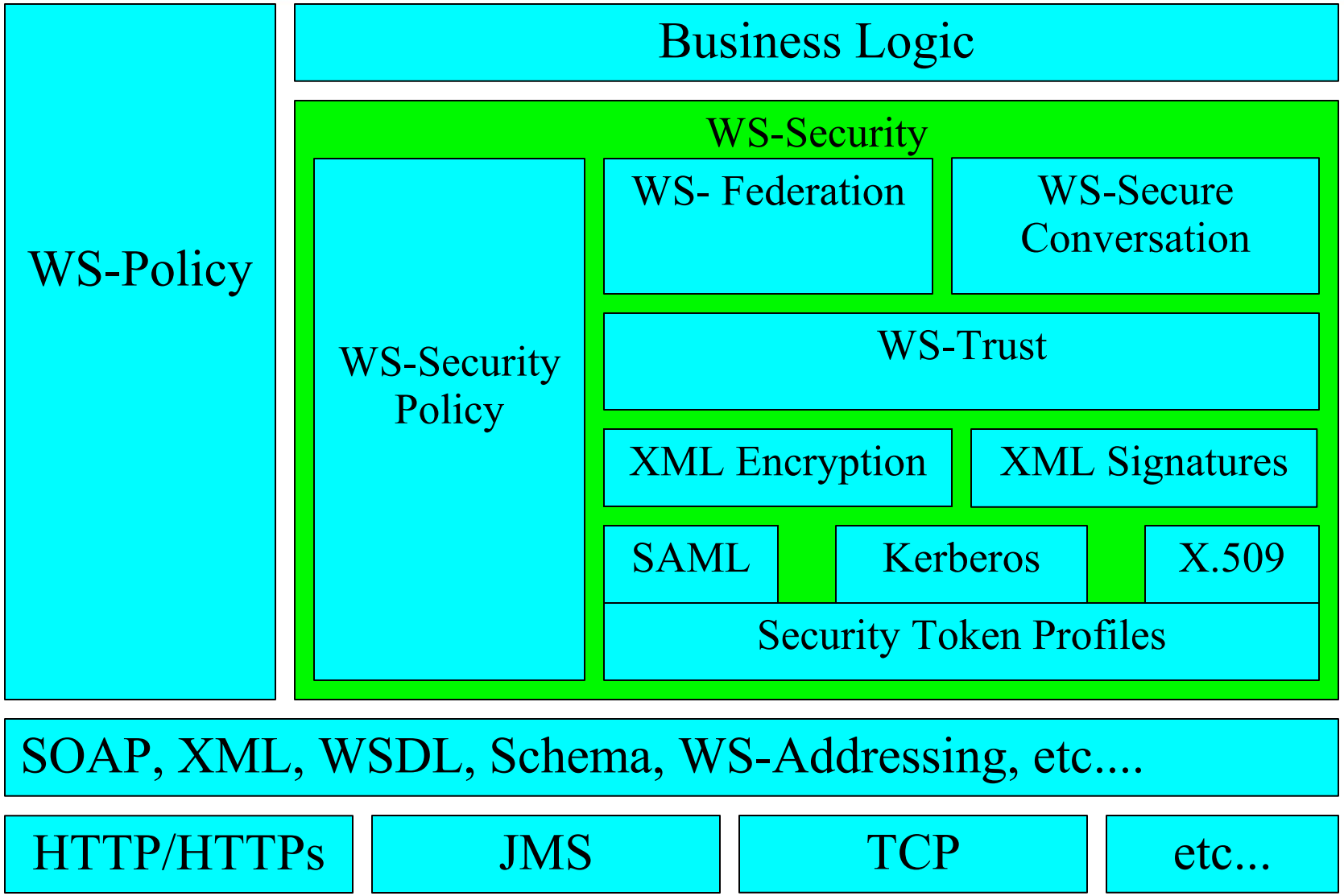
Security options

- Authorization/Authentication
- Privacy
  - Encryption
- Message validation
  - Signatures

Security Standards

- HTTPs
- WS-Security/WS-SecurityPolicy
- WS-Trust
- WS-SecureConversation

- XML Encryption
- XML Digital Signatures



HTTPs

- Best known way of security web services
- Highest performance
- Most inter-operable
- Also usable for REST services

HTTPs (part 2)

- BORING
  - No buzz words – SOA, “Messaging”, etc...
  - No differentiator – everyone does it. No money to be made.
- Does not work well for intermediaries
- Connection oriented, not Messaging oriented
- Hard to implement “Trust” domains

WS-SecurityPolicy

- WS-Policy assertions to describe security requirements
  - Which parts (elements) are signed
  - Which parts (elements) are encrypted
  - Sign before encrypt or encrypt before sign
  - Types of token required (UsernameToken, X509Token, etc...)
  - Symmetric or Asymmetric protection
  - Encryption algorithms
  - Use of derived keys
  - MUCH more
- Requires external information to fill in details
  - Names/Passwords, keystores, certs

WS-Trust

- Provides a mechanism to exchange security credentials.
- Methods for issuing, renewing and validating security tokens.
- Allows use of security tokens across domains.

WS-SecureConversation

- Defines extensions to allow creations of security contexts and sessions keys
- Helps the performance of WS-Security as more efficient keys can be exchanged

Security in CXF

- CXF 2.0/2.1
  - HTTPs
  - WS-Security through WSS4J Interceptors
- 2.2
  - WS-SecurityPolicy
  - WS-Trust
  - WS-SecureConversation

CXF 2.2

- Policy driven, configuration to add missing data

```
<jaxws:client name="{http://InteropBaseAddress/interop}MySecureClient">
  <jaxws:properties>
    <entry key="ws-security.username" value="Alice"/>
    <entry key="ws-security.callback-handler"
           value="interop.client.KeystorePasswordCallback"/>
    <entry key="ws-security.signature.properties"
           value="etc/alice.properties"/>
    <entry key="ws-security.encryption.properties"
           value="etc/bob.properties"/>
  </jaxws:properties>
</jaxws:client>
```

- No code changes to secure stuff – Policy + Config
- Significant testing with .NET/WCF

Demonstration

Sample sources:
http://svn.apache.org/repos/asf/cxf/trunk/distribution/src/main/release/samples/ws_security/interopfest/

Shipped in the CXF 2.2 download in:
samples/ws_security/interopfest

Performance

- Do you REALLY want to know?

Performance

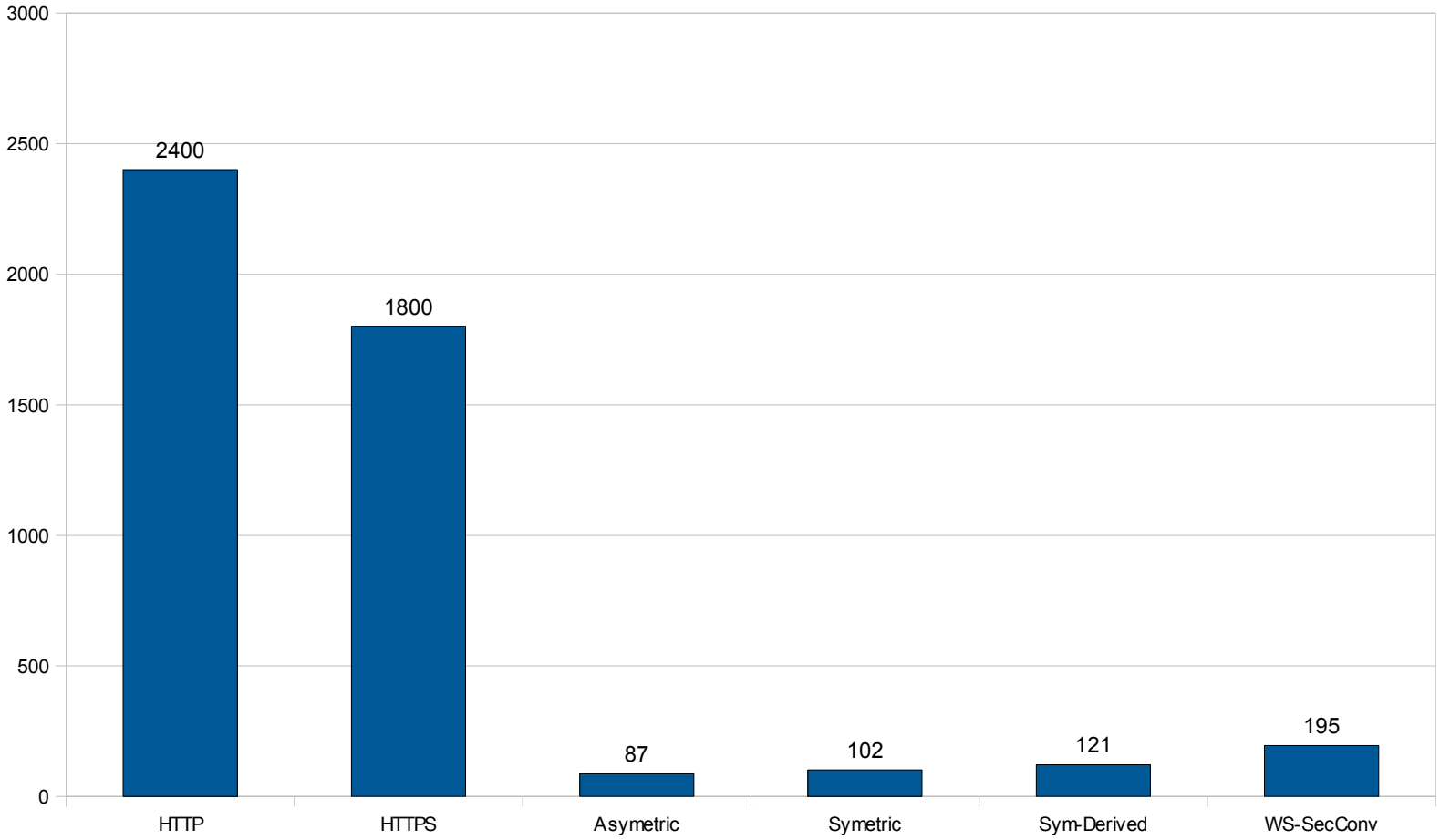
- Do you REALLY want to know?

- XML C14N is not “free”
- Signatures are not “free”
- Encryption is not “free”
- Message size increase is not “free”
- Loss of streaming is not “free”

Performance

- Do you REALLY want to know?
- I'm serious, do you REALLY want to know?

Performance



Recommendations

- HTTPs whenever possible
- For clients making multiple requests, consider WS-SecureConverstation
- WS-SecurityPolicy fragments are complex. Use pre-canned policies by reference or use a good GUI policy editor. (Netbeans, Actional, etc...)

Questions?

http://cxf.apache.org
users@cxf.apache.org
dev@cxf.apache.org

http://fusesource.com
dkulp@progress.com
http://dankulp.com/blog