Web Services Security Standards Forum

Dr. Phillip M. Hallam-Baker  C.Eng. FBCS
VeriSign Inc.
Web Services Security Standards
For ‘Um

For ‘um: Meeting to tell people that everyone agrees on an issue

• Walk the Walk or just Talk the Talk?
VeriSign is For ‘um

• Provider of Web Services
  – XKMS Service live over 1 year
  – Trust Service Integration Kit
• User of Web Services
  – Integrate multiple IT infrastructures
    • VeriSign
    • Signio
    • Network Solutions
    • Illuminet
    • HO Systems
Why Everyone is For’um

Web Services like email
✓ Anyone can talk to everyone

Not like Power Cord
✖ Different Mains Adapter for Every Device
✖ $600 service fee to repair broken connector
And Security?

Don’t want our Power Cords [Web Services] to catch Fire
Why Are We All For’um?

- Standards Benefits
  - Interoperability
  - Vendor Independence
  - Clearly Defined Intellectual Property
  - Constraints

- Standards should be enablers, not limiters
  - Don’t complain if companies don’t wait for standards to catch up
Why Web Services Security is a Challenge

Theory:
This thing has 4 wheel drive
But we only take it to the Mall

Practice:
In this environment we *need*
4 wheel drive
Why Security Is Needed

Without Trust and Security…
Web Services are Dead on Arrival
Web Services Security Groups

- XML Encryption
- XML Signature
- XKMS
- XrML
- Provisioning
- Biometrics
- XACML
- WS-Security
- SAML
- W3C Architecture
- OASIS Joint Security
- Biometrics
And Don’t Forget…

- Web Services Institute
  - Standards are great
    - Interoperability is better
    - Need Profiles, Testing, etc.
- UDDI
  - Protocol specification now in OASIS
- www.XMLTrustCenter.org
  - Web Services Security Community
- Internet Engineering Task Force
  - Mainly focused on lower protocol stack layers
What Parts of Web Services Security Should Be Infrastructure?
What Parts of Web Services Security Should Be Infrastructure?

- Replicate security context provided by O/S
  - Protected Memory
    - Prevents modification of process state
    - Prevents interception of function calls
    - Prevent disclosure
  - Access Control
    - Authentication
    - Authorization
    - Auditing
## Problem Space

<table>
<thead>
<tr>
<th>Policy</th>
<th>Trust</th>
<th>Funds Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversation</td>
<td>Authorization</td>
<td>Payroll</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Authentication</td>
<td>Inventory</td>
</tr>
<tr>
<td>Integrity</td>
<td>Attributes</td>
<td>Purchasing</td>
</tr>
<tr>
<td>Access Control</td>
<td>Security Infrastructure</td>
<td>Applications</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Services</td>
<td></td>
</tr>
</tbody>
</table>
Solution Space

Applications

Web Services Security Infrastructure

- Conversation
- Access Control
- Rights Management
- Credential Management
- Privacy
- Policy

XML & Web Services Foundation

- XML Signature
- XML Encryption
- SOAP
- WSDL Description

XML & Web Services Security Infrastructure
Part I – XML Infrastructure
• Allow node level security enhancements
  – Sign parts of a document
  – Enveloped signature is inside signed node
  – Detached signature signs referenced content
  – Detached encryption data

• Operate on the XML InfoSet
  – *Not* just a stream of bits
XML Signature Operates on the InfoSet not Just Bits

Source → XML Encoded Bits

XML Encoded Bits → XML Parser

XML Parser → XML Infoset

XML Infoset → Application Code

Traditional PKCS#7

XML Signature
Part II – Web Services Security Infrastructure
Is SSL Enough?

• For some applications
  – Yes

• As Infrastructure
  – No
  • SSL Only supports data in transit, not in storage
  • SSL does not support multi-party transactions
  • SSL is all or nothing
    – Messages are opaque to firewalls
  • SSL does not support non-Repudiation
WS-Security

- SOAP Message Level Security
  - Confidentiality
  - Integrity
  - Authentication

- Builds on XML Standards
  - XML Signature & Encryption
Completing the Picture

• Request / Response Correlation
  – Prevent Message Substitution Attacks
    • Response Modification
    • Response Replay
• Request Replay
• Denial of Service
Part III Web Services Infrastructure

Security Applications

• Key Management
  – XKMS
  – Key Agreement TBA

• Distributed Access Control
  – SAML
  – XACML
  – XrML

• Ancillary
  – Provisioning [SPML]
  – Biometrics [XCBF]
  – Privacy Profile [P3P]
• Management of Public Keys
  – Because all you need to know to communicate securely with anyone is their public key
  – Registration
    • Alice registers her email signature public key
      – [Alice might later request reissue, revocation, recovery]
  – Information
    • Bob looks up the key for alice@somecorp.com
    • Bob checks to see if it is valid

• Core Objective:
  – Shield the client from the complexity of PKI
Distributed Access Control

• Authorization Decision
  – Can ‘Alice’ access the general ledger?

• Authentication
  – Is ‘Alice’ the real Alice?

• Attributes
  – Alice is a Finance department employee

• Authorization Policy
  – Finance department employees may access the general ledger.
Distributed Access Control

- User Attributes
- Authentication: Password, Biometric, Smartcard etc.
- Authorization Policy
- Authorization Decision: Permit or Deny
- User
- Request
- Application

Single Mechanism
SAML

User Attributes

Authentication

Password
Biometric
Smartcard etc.

Authorization Policy

Authorization Decision

Single Mechanism

Permit or Deny

Request

Application
SAML Authentication Statements

I really am Alice

Authentication Authority

Authentication Assertion

Connect as Alice

Member Site
SAML Authorization Decision and Attribute Statements

Service

Should Alice Do X?

Authorization Authority

Is Alice Creditworthy?

Attribute Authority

X
Why Standardize Authorization Policy?

• Support common Authorization Policy API

• Move policy with controlled object
  – Privacy Applications
    • Healthcare (HIPPA)
    • EU Privacy Directive
  – Digital Rights Management
XML Access Control Markup Language

- Allows Access Control Policy to be expressed
  - Encode in XML rules such as:
    1. A person may read any record for which he or she is the designated patient.
    2. A person may read any record for which he or she is the designated parent or guardian, and for which the patient is under 16 years of age.
    3. A physician may write any medical element for which he or she is the designated primary care physician, provided an email is sent to the patient,
    4. An administrator shall not be permitted to read or write medical elements of a patient record.
  - Chief standards issue is naming
    - How to identify ‘patient’, ‘record’, ‘guardian’ etc.
• Allows Digital Rights Policy to be expressed at each level in the value chain
  – Encode in XML rules such as:
    • Consumer can view film 6 times within 6 months
    • Consumer can view any content in super subscription plan for 1 month
    • Consumer can listen to audio track $X$ on the devices $P$, $Q$, $R$.
    • Content Owner can define distributors and their respective rights on the content

• Chief standards issue is naming
  – How to identify content, constraints etc.
Part IV Futures

• Proposals on or near the table to address:
  – Support for Direct Trust
  – WSDL Description of Security Enhancements

• Why not now?
  – Need to standardize dependencies first
  – Maintain focus, momentum on existing work
Support for Direct Trust

- It can’t be turtles *all* the way down.
• We know what to do
  – WSDL description of security enhancements
    • I support WS-Security with AES Encryption
    • The authentication key of my service is X
    • I always authenticate responses with Y
    • You must perform key agreement with Z

• Specification is dependent on:
  – WSDL specification
  – Web Services Security Specifications
Conclusions

• Without Security and Trust:
  Web Services are Dead On Arrival

• Considerable progress has already been made
  – Industry wide consensus on value of standards
  – Basic Infrastructure is in place or in development
  – There is considerable consensus on the roadmap
  – Security need not be the show stopper
Time to Say:

I’m For ‘um