Web Services Security

Application attacks and defense
in the SOA world

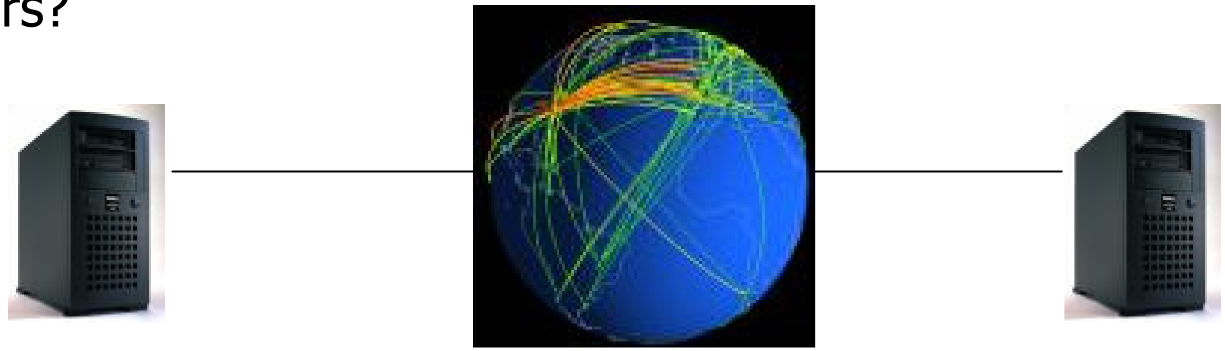
Rohit K. Sethi, CISSP
Manager, Security Compass
April 12th, 2006

Agenda

- Basics of web services
- ….

Why Web Services?

- Web services provide standard protocols that allow systems in a heterogeneous environment to communicate within an organization or across organizational boundaries
- Promotes loose coupling and code-reuse
- Vendor independent (supposedly)
- Based on XML, so easy for humans to understand
- Functionality during transport (i.e. message brokers, WS-Routing expressions, etc.)
- Others?



Security Implications – High Level

- Standard implementations of web services essentially provide an API to application logic over port 80
  - Seen as legitimate traffic from firewalls
  - As with standard web applications, places most of the security responsibility at the application tier
- API documents (i.e. WSDL files) are readily available – shortens the information-gathering phase of an attack
- XML is plain-text – password and other sensitive data that is not encrypted can be sniffed by anyone during routing
- Security standards are still maturing, and although some are officially recommended, they have not necessarily gained widespread adoption

Web Services – Base Standards

- Web services are based upon the following standards
  - XML
  - SOAP
  - WSDL
  - Optionally, UDDI
- There are now hundreds of other open and vendor specific standards and technologies related to web services

```
<?xml version='1.0' ?>
<SOAP-ENV:Envelope
xmlns:SOAP-
      ENV="http://s.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Body>
..
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

```
<schema targetNamespace="http://e.com/quote.xsd"

      xmlns="http://www.w3.org/2000/XMLSchema">
        <element name="TradePriceRequest">
          <complexType>
             <all>
                <element name="tiSym" type="string"/>
             </all>
          </complexType>
        </element>
```

Breaking Web Services

- The OWASP Top Ten still apply!
- Access control – how do we handle authentication in a WS-world?
  - HTTP authentication?
  - X509 or Kerberos Tokens?
  - WS-Security or SAML?
  - Custom coding?

- Authorization is primarily done in the business logic layers below the web services wrapper
  - As long as the end user can be identified in the SOAP request, you should be able to leverage existing authorization techniques
  - However, trusting the contents of the message implies the need for message signing (covered in WS-Security)
- XML is text-based – credentials are passed in the clear, unless messages and/or channel are encrypted

Other Major Vulnerabilities

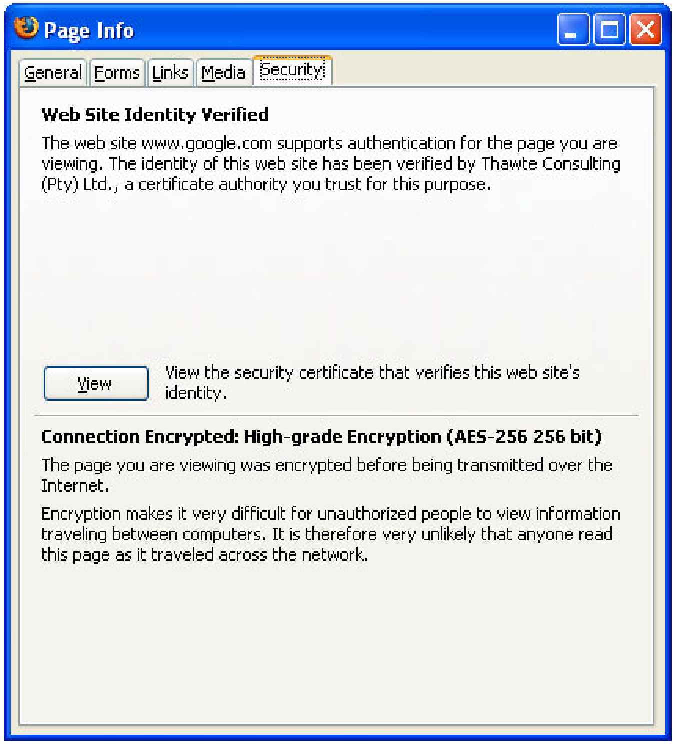
- Input validation – probably biggest security issue facing web services today
  - SQL Injection still possible!

```
<soap:Body>
        <login xmlns="urn:enterprise.soap.sforce.com">
           <username>fakeuser’ or ‘1=1’ -- </username>
           <password>whocares</password>
```

- Session management – can be tricky due to asynchronous nature of web services
  - WS-Secure Conversation meant to address this, amongst other issues
  - Web service containers often provide this, but need to ensure that sessions are sound and not guessable. Everyone who can read the message can see the session id!
  - Ask yourself – Do we really need to maintain state? If services are being consumed asynchronously, consider forcing authentication on each call

Standards

- What’s wrong with using SSL to solve all WS confidentiality and integrity requirements?
- XML-Encryption defines how to encrypt all or part of a message
- XML-Digital Signature defines how to sign a message
  - Neither defines how or when to use these, and are not specific to SOAP
- WS-Security Provides message integrity, message confidentiality, and single message authentication
- Question – How do we know a key belongs to a particular entity? In server-side SSL it’s easy because we associate key with the DNS name of the web server



Web Site Identity Verified

The web site www.google.com supports authentication for the page you are viewing. The identity of this web site has been verified by Thawte Consulting (Pty) Ltd., a certificate authority you trust for this purpose.

View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Cost of WS-Security

- Message level security adds considerable overhead to a message – so much so that several vendors now offer hardware appliances called 'XML Security Gateways' to speed up processing
  - Data Power's XS40 Security Gateway
  - Reactivity XML Security Gateway
  - Layer 7 Secure Span Gateway
  - Intel XML Security Gateway
- MSRP around the $65,000 ballpark per appliance

Exponential Growth of Technology

- Just some examples of Web Services related terms and acronyms

  - XML
  - WSDL
  - SOAP
  - UDDI
  - WSS
  - WS-I
  - XPath
  - XOP
  - XML-Encryption
  - XML-Signature
  - SOA
  - DISCO
  - WS-Trust
  - WS-Security
  - WS-Federation
  - WS-Polling
  - WS-Atomic Transactions
  - WS-Business Activity
  - WS-Coordination
  - WS-Manageability
  - WS-Brokered Notification
  - WS-Base Notification
  - WS-Attachments
  - WS-Addressing
  - WS-Eventing
  - WS-Topics
  - WS-Security Policy
  - WS-Resource Properties
  - WS-Resource Lifetime
  - WS-Reliable Messaging
  - WS-Policy Framework
  - WS-Policy Attachments
  - WS-Policy Assertion
  - WS-Inspection
  - WS-Secure Conversation
  - WS-Provisioning
  - WS-Distributed Management
  - WS-Transfer
  - WS-Enumeration
  - WS-Eventing
  - WS-Enhancements
  - BPEL4WS
  - WSXL
  - WSRP
  - Java WSDP
  - Java-WS
  - JAX-RPC
  - JAXR
  - JAXP
  - JAXB
  - SAAJ
  - XWSS
  - JAX-WSA
  - OASIS
  - SAML
  - XACML
  - AXIS
  - EBXML
  - RPC
  - DOC
  - DOM
  - XSLFO
  - XQuery
  - WSCI
  - WSDM
  - MTOM
  - RAMP
  - BICS

- Are you WS-Confused yet?