Web Services
Security Issues

Gerald Edgar & Pranab Baruah
BCA IS
e-Business & Architecture

March 5, 2002
Introduction

• Web Services – a new technique
  • For integrating applications
• Where before interfaces were for the most part
  • A shared secret
    – Not publicly known
    – No readily accessible
    – Unless each application knew of the other
• Now interfaces are well specified
  • Publicly listed
  • Open specification
Where Security Fits

- User Applications
  - Tools and Applications
    - Directory brokering, diagnostics, and monitoring
    - Secure access to resources and services
- Collective Services
  - Resource and Connectivity Protocols
    - Diverse resources such as computers, storage media, networks and other data
- Fabric

Source: Ian Foster: Private Communication
A Need for Security

• Security controls risk, it does not eliminate it
• Information systems have vulnerabilities
• Vulnerabilities have countermeasures
• Countermeasures control risk

• Three major aspects of security
  • Integrity
  • Availability
  • Confidentiality
Integrity

• Protection against malicious or accidental attempts to alter data
• Perform unauthorized data modification
• Bypass steps to preserve data integrity
  • in an automated process flow
• Integrity covers data
  • in storage
  • in processing
  • in transit
Availability

• Availability is protection against unauthorized deletion
• Or otherwise cause a denial of access to the data or service
Confidentiality

• Confidentiality is protection from unauthorized attempts to read data.

• Confidentiality covers data
  • in storage
  • in processing
  • in transit

• Confidentiality is NOT privacy
Privacy

• Privacy to the right of an entity
  – Normally a person, acting in their own behalf,
• How much it will interact with its environment
• The entity determines how much information to share information about itself with others
Accountability

• Event tracking
• Alerts for significant events
• Identification of event source
• To support
  – Detection
  – Isolation
  – Deterrence
  – Prevention
  – After-action recovery
  – Legal action
Assurance

• Confidence that accountability and the three main security objectives have been met

• This includes
  • Functionality that performs correctly
  • Sufficient protection from errors (user or software)
  • Resistance to malicious penetration or by-pass
Another view

• Divide security goals into
  • Communications (COMMUNICATIONS SECURITY)
  • Protecting systems (SYSTEMS SECURITY).
Communications Security

• Partition goals of communications security
• Three major categories:
  • CONFIDENTIALITY,
  • DATA INTEGRITY and
  • END-POINT AUTHENTICATION.

Security Levels

• Object security apply to entire data objects.
• Channel security measures provide a secure channel
  • transparently to data transmitted
  • channel has no special knowledge about objects
Systems Security

• Reduce risk by not overloading functions
• Control Exposure by constraining functionality
• Limiting functionality also makes testing easier
• Thorough testing enhances quality
  • providing a measure of assurance for security as well
What is Needed

- End-User Device
- Web Server
- Application Server
- Internet connection
- Processing/data Service

Confidentiality

Integrity

Accessibility
What is Needed

**Integrity**
- Signed XML
- Encrypted data load

**Confidentiality**
- Authentication
- Authorization
- Encryption
- SSL

**Accessibility**
- Fail-over
- DOS defenses

**What is Needed**
- End-User Device
- Web Server
- Application Server
- Internet connection
- Cloud
- Processing/data Service
What Groups are Working On
What is Available – Or Will be

Confidentiality

Authentication
Authorization
(X.509 certificates)

Channel Encryption
(SSL)

Object Encryption
(SAML)

End-User Device

Integration

Signed XML
(ebXML, W3C, SAML)

Encrypted data load
(SAML DES RSA)

Internet connection cloud

Accessibility

Fail-over
(Commercial products, UDDI)

Denial Of Service defenses
(Network monitoring Server log monitoring Server network connection monitoring)

Application Server

Processing/data Service

Gerald Edgar/Pranab Baruah Web Services Security
References and Resources

• IETF Security considerations
  • Covers Security issues for RFC 2026 (Internet Standards Process)
  • http://www.ietf.org/internet-drafts/draft-rescorla-sec-cons-03.txt
  • RFC 2828

• IETF/W3C XML Signature
  • Built into SAML for digitally signing assertions
  • www.w3.org/Signature/

• W3C XML Encryption and Canonicalization
  • Not quite ready yet, but encryption will be important
  • www.w3.org/Encryption/2001/

• XKMS and its relatives
  • An XML-based mechanism for doing PKI
  • SAML traffic might be secured by XKMS-based PKI, by other PKI, or by other means entirely
  • www.w3.org/TR/xkms/
References and Resources

- OASIS XACML
  - XML-based access control/policy language
  - Could be the way PDPs talk to back-end policy stores
  - www.oasis-open.org/committees/xacml/
- OASIS Provisioning
  - XML-based framework for user, resource, and service provisioning
  - www.oasis-open.org/committees/provision/
- UDDI
  - A Web services registry:
References and Resources

- **WSDL**
  - Web Services Description Language
  - http://www.w3.org/TR/wsdl
- **ebXML**
  - Main resource site run by UN/CEFACT and OASIS:
    - http://www.ebxml.org
- **SOAP**
  - Working draft of version 1.2 on the W3C site:
    - http://www.w3.org/TR/2001/WD-soap12-20010709/