

Introduction to WS-Security

Oxford University

Software Engineering Programme

Sep 2015



© Paul Fremantle 2012. Portions © Jeremy Gibbons 2010, © WSO2 2005-2012 used with permission of the author(s).

Licensed under the Creative Commons 3.0 BY-SA (Attribution-Sharealike) license.

See <http://creativecommons.org/licenses/by-sa/3.0/>

Overview

- Introduction
 - WS Security features
- XML Security
 - XML Encryption
 - XML Signature



Introduction

- XML-Signature & XML-Encryption
 - To secure XML documents
- How do we secure SOAP messages ?
- WS-Security specifications
 - Based on XML-Signature and XML-Encryption
- Token profiles to define how different security applications can be used
 - Username Tokens
 - X509 Tokens
 - SAML Tokens



WS-Security Features

- UsernameToken
- Timestamp
- Encryption
 - Encryption parts
 - Elements and element contents
- Signature
 - Signature parts



Some Jargon

- Claim
 - A statement about a subject or resource
- Token
 - A serialized collection of claims



Authentication - UsernameToken

- Two forms
 - Plain text password
 - Digest of a password
- Most popular and recommended is plain text password
 - No need to store the requesters' password
 - LDAP
- The “Security” header contains a “UsernameToken” element with the “Username” and “Password” child elements
- Username Token without passwords



Authentication

- X509 Tokens
 - Signature
- SAML Tokens
 - as a claim
 - as a key pair



Integrity - Signature

- Sign different parts of the SOAP message
 - Add a Timestamp and sign it to protect against replay attacks
- “Signature” element within the “Security” header
- Different key reference mechanisms
 - Direct reference
 - Subject Key Identifier
 - Issuer serial
 - Thumbprint SHA Identifier



Confidentiality - Encryption

- Encrypt elements or element contents of a SOAP message
- An ephemeral key is generated and its used to encrypt content
- Ephemeral key is encrypted with the recipient's public key



Non repudiation

- Does signature always provide non repudiation ?
 - Asymmetric/Symmetric Signature



XML Security

- Confidentiality of XML documents
 - XML Encryption by W3C
 - <http://www.w3.org/TR/xmlenc-core/>
- Integrity and non-repudiation
 - XML Signature by W3C
 - <http://www.w3.org/TR/xmlsig-core/>



XML-Encryption

- Encrypts XML with a symmetric key
- Allows using an asymmetric key



Plain-text XML

```
<RootElement xmlns="http://www.apache.org/ns/#app1">  
  <foo>Some simple text</foo>  
</RootElement>
```



XML Encryption

- Encrypt an XML Element
 - Encrypt the entire Element
- Encrypt an XML Element Content
 - Encrypt the only the content of the Element



Element Encryption

```
<RootElement xmlns="http://www.apache.org/ns/#app1">
  <xenc:EncryptedData
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <ds:KeyInfo/>

    <xenc:CipherData/>

  </xenc:EncryptedData>

</RootElement>
```



Content Encryption

```
<RootElement xmlns="http://www.apache.org/ns/#app1">
  <foo>
    <xenc:EncryptedData
      xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
      Type="http://www.w3.org/2001/04/xmlenc#Content">
      <xenc:EncryptionMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
      <ds:KeyInfo/>
      <xenc:CipherData/>
    </xenc:EncryptedData>
  </foo>
</RootElement>
```



Encrypted Data

```
<RootElement xmlns="http://www.apache.org/ns/#app1">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod ... />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      ...
    </ds:KeyInfo>
    <xenc:CipherData      xmlns:xenc="http://www.w3.org/2001/04/
      xmlenc#">
      ...
    </xenc:CipherData>
  </xenc:EncryptedData>
</RootElement>
```



CipherData

```
<RootElement xmlns="http://www.apache.org/ns/#app1">
  <xenc:EncryptedData ... >
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
      </ds:KeyInfo>
      <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
        <enc:CipherValue>zX60MsDMv2..</enc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedData>
  </RootElement>
```



XML-Signature

- Allows signing an XML document or parts of it
- Canonicalization
- Three types
 - Enveloping
 - Enveloped
 - Detached



Summary

- WS-Security features
- XML Encryption
- XML Signature

