RSA-PSS in XMLDSig

Position Paper

W3C Workshop

Mountain View

25.09.2007

Konrad.Lanz@iaik.tugraz.at

Konrad Lanz

- Digital Signature Services OASIS-DSS
  - IAIK (Inst. f. angew. Informationsverarbeitung und Kommunikation)
  - SIC
    - Stiftung Secure Information and Communication Technology
  - TUG (Technische Universität Graz)
- OASIS-DSS TC Voting Member
- W3C
  - Zentrum für Sichere Informationstechnologie (A-SIT)
  - W3C XML CORE Working Group
    - Canonicalization (c14n)
  - XMSSMWG

Konrad.Lanz@iaik.tugraz.at

Introduction

- Currently RSASSA-PKCS1-v1_5
  - Bleichenbacher implementation vulnerability
- RSA-PSS
  - randomized method
    - tighter security proof

<Signature ID?>
<SignedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>
(<Reference URI? >
(<Transforms/>)?
<DigestMethod/>
<DigestValue/>
</Reference>)+
</SignedInfo>
<SignatureValue>
(<KeyInfo>)?
(<Object ID?>)*
</Signature>

RSA-DSS Recognition/Adoption

- Cryptographic Message Syntax (CMS, [RFC 3852])
  - RSA-PSS signature method ([RFC 4056]).
- DSS Draft [FIPS 186-3 Draft]
  - section 5.5 references [PKCS#1 v2.1] and considers RSA-PSS as approved.

Konrad.Lanz@iaik.tugraz.at

What do we need?

- Namespace and identifiers for RSA-PSS
- XML schema for the algorithm parameters

Namespace Algorithm Identifiers

- Namespace
  - http://www.w3.org/2007/09/xmldsig-pss
- Algorithm Identifiers
  - SignatureMethod
    - http://www.w3.org/2007/09/xmldsig-pss/#rsa-pss
  - Mask Generation Function
    - http://www.w3.org/2007/09/xmldsig-pss/#mgf1
  - Hash Functions
    - specified in XML encryption [XMLEnc] (SHA-256, SHA-512), [RFC4051] SHA-224 and SHA-384
    - specified in [XMLDSig] SHA-1

RSA-PSS Parameters

- the digest method (dm)
- the mask generation function (MGF)
  - the digest method if used in the MGF (mgf-dm)
- the salt length (sl)
- the usually constant trailer field (tf)

Default (fixed values?)

- NIST Drafts - moving away from SHA-1 to longer output lengths of the SHA family.
  - [FIPS 180-3 Draft], [NIST SP 800-107 Draft] and [NIST SP 800-57 Draft]

- dm SHA-256 (SHA-1 [PKCS#1v2.1])
- MGF MGF1
  - mgf-dm = dm (SHA-1)
- sl length(dm)/8=32 byes (20 bytes)
- tf 1 (corresponds to 0xbc)

SHA-1 tarnished

- SHA-1[NIST SP 800-57 Draft]
  - less than 80 bits of security, currently asses the security strength against collisions at 69 bits
- successful collision attacks on SHA-1
  - reduced SHA-1
    - 2005 - 53 steps [WaYiYu]
    - 2006 - 64 steps [CaMeRe]
    - 2007 - 70 steps [MeReRei]
  - theoretical attacks on full version (80 steps)
    - 2005 - 2^{69} op. [WaYiYu] announced 2^{63} [WaYaYa]
    - 2007 - 2^{60} op. announced [MeReRei]

RFC 4055
RSA-PSS parameters

- subjectPublicKeyInfo field of an X.509 certificate
- parameters to be added to the signature
  - unless default values are used

- …
  - dm = dm' as in the key/certificate
  - MGF = MGF' as in the key/certificate
    - dm-mgf = dm-mgf' as in the key/certificate
  - sl >= sl' as the one in the key/certificate
  - tf = tf' as specified by the key/certificate (effective val)

Examples

- Example 1 defaults
  - SHA-256, MFG1 with SHA-256, default salt length 256/8=32 bytes, trailer = 1 (‘0xbc’)
- Example 2
  - **SHA-512**, MFG1 with SHA-512, salt length of 512/8=64 bytes, trailer = 1.
- Example 3
  - **SHA-1**, MFG1 with SHA-1, salt length of 256/8=32 bytes, trailer = 1.
- Example 4
  - SHA-1, MFG1 with SHA-1, **salt length of 32 bytes**, trailer = 1.

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms/>)?
      <DigestMethod/>
      <DigestValue/>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>
```

Conclusion

- RSA-PSS as a signature method
- plain SHA-1 should not be default any more
- SHA-256 as default hash algorithm
- specification and approaches encoding the RSA-PSS parameters with the key or certificate has been discussed

Thanks

- Thanks for your Attention !
- References in position paper.

JAVA

- XML-DSig (JSR 105)
  - http://www.jcp.org/en/jsr/detail?id=105
- XML-Enc (JSR 106)
  - http://www.jcp.org/en/jsr/detail?id=106

Thanks !
SIC – XSect Toolkit

- IAIK XML Signature Library (IXSIL) Successor
- Java XML Digital Signatures APIs (JSR105)
- Java XML Digtial Encryption APIs (JSR106)

- http://www.sic.st
- http://jce.iaik.tugraz.at/sic/products/xml_security

- Thanks for your Attention.