XML Security
Issues and Requirements

W3C Workshop on the Future of XML Security
September 25, 2007

Hal Lockhart
Office of the CTO
BEA Systems
BEA Experiences with XML Security

- Implementations of XML Signature & Encryption in products
- Comments reflect
  - Implementation experiences
  - Customer usage experiences
  - Development of Standards which normatively reference them
    - OASIS: SAML, XACML, DSS, SPML, WS-Security
    - WS-I: Basic Security Profile
General Requirements

- Use in network protocols
- Structured data w/o formatting
  - Use of XML Schema
- Messages constructed by distinct software components
  - Within same node
  - Multiple nodes – intermediaries
- Distinct namespaces
- Unaware of other namespaces or message semantics
- Digital signatures over independently created portions
- Overlapping signatures and encryptions
- Data added after signatures – new or duplicate namespaces
XML Security Benefits

- Generally positive experiences
- More flexibility than TLS or IPSec
- Particularly useful capabilities
  - The ability to selectively encrypt and integrity protect portions of messages.
  - The ability to integrity protect data without encrypting it.
  - The ability to construct overlapping digital signatures using different keys.
  - The ability to digitally sign and encrypt data in either order as application needs dictate.
Issues Overview

XML Signature Issues

- No Completely Satisfactory Canonicalization Algorithm
  - Spurious Validation Errors
  - Qnames in Content
- No Satisfactory Way to Reference Arbitrary Inserted Content
  - XPath expressions not guaranteed to work
  - Id Attributes present other problems
- Other security threats
- Performance

XML Encryption Issues

- Encrypted data not schema valid
- Security threats
Canonicalization Issues

- (Inclusive) XML Canonicalization generally not suitable
- Exclusive XML Canonicalization
  - Works for moving intact chunks – SAML Assertion
  - Less satisfactory for messages constructed incrementally
  - Spurious validation errors possible (suggested by Melvin Hughes)
    
    ```xml
    <SomeEnclosingElement>
      <ToBeSigned wsu:Id="tbs">
        <Data xmlns:foo="urn:foo" Something="foo:Bar"/>
      </ToBeSigned>
    </SomeEnclosingElement>
    ```
  - Qnames in content
    - Still used
    - Application / security layer isolation
    - Preprocessing – ugly & inefficient
Referencing Arbitrary Inserted Content

- XPath expressions without Id attribute not certain to work
- Use of Id attributes is problematic
  - Flat namespaces – behavior with conflicts undefined
  - Uniqueness scheme – no standard
  - Insertion or deletion of Id attribute breaks signatures
  - Id Attributes can cause security threats

XML Signature Element Wrapping Attacks and Countermeasures, Michael McIntosh, Paula Austel
Other Issues

- Security risks in the use of Signature and Encryption
  - Not inherent flaws, mostly consequence of flexibility
  - Many found, probably there are more
  - W3C should collect and document

- Performance
  - Mostly Canonicalization
  - Requires study
  - Special algorithms
  - Special purpose hardware

- Encrypted data is not Schema valid
Recommendations

- Charter a new working group, not constrained to be backwards compatible.
- One guiding principle: always specify algorithms and versions explicitly.
- Chartered to collect and analyze information about threats.
- Liaise with other W3C Working Groups to address problems outside the scope of XML Security.