Complexity as the Enemy of Security

W3C Workshop on Next Steps for XML Signature and Encryption
25/25 September 2007

Brad Hill - iSEC Partners

brad@isecpartners.com

The adversary is the *raison d'etre* for XML Digital Signatures and Encryption.

The specification forgot this somewhere along the way.

Many things that are difficult to harden against malicious input:

- XSLT
- Remote references
- XPath
- C14N

Denial of Service matters!

One broken implementation,
blame the team.

Five broken implementations,
blame the spec.

Security considerations section is plainly inadequate.

And the implied order of operations is wrong.

Knowledge of correct practice is scattered and hard to find.

(important to clients, not just implementers)

Many signature profiles exist, none are shared across verticals.

(except SAML, indirectly)

Proposal 1: Update the Security Considerations section of the core specification.

1. Warn against and disable XSLT Transform by default.

2. Provide ability to enable/disable transforms in general, and distinctly for RetrievalMethods and References.

3. Ability to set hard timeout values and limit resource consumption.

4. Ability to use distinct resource resolvers for KeyInfo and SignedInfo.

5. Order of Operations:
    1. Process KeyInfo and return key
    2. Validate signature calculated over SignedInfo
    3. Verify references

6. MUST provide ability for relying applications to retrieve the verified Reference material EXACTLY as processed by the validator.

7. C14N of SignedInfo SHOULD exclude comments.

Two main goals for XML Security:

- Safe to use in presence of adversary
- Interoperable
  - Features are important, but anyone can build features
  - Interoperability is why you use the W3C “standard”

Q.E.D. Proposal 2:

The core specification should include a common minimal profile that is maximally robust vs. adversarial messages.

What do people want?

Look at “best practices” elsewhere XML is consumed from potential adversaries.

Messages should self-contain all necessary context for evaluation.

Total resource consumption for evaluation can be constrained to a “sane” value by limiting input message size.

1. Reference URIs MUST be either whole document (URI=“”) or same-document bare XPointers identifying content by xml:Id (URI=“#ref1”)

2. Only Enveloped, Enveloping, Base64 and C14N Transforms allowed.

3. Each Transform may appear in its relevant context EXACTLY ONCE.

4. Same constraints on URIs and Transforms for KeyInfo as for References.

5. Use Exclusive C14N

6. Documents must be entity-normalized prior to signing. All entities other than standard XML single-character escapes cause immediate failure.

7. SignedInfo C14N excludes comments.

Thank you!

brad@isecpartners.com