Update to the CMS for Algorithm Identifier Protection

draft-housley-lamps-cms-update-alg-id-protect-00

Russ Housley

IETF 106

LAMPS WG

Algorithm Identifier Protection

The CMS Signed-data Content Type can be vulnerable to algorithm substitution attacks

- the attacker changes either the algorithm identifier or the parameters associated with the algorithm identifier to change the verification process used by the recipient
- the attacker looks for a different algorithm that produces the same result as the algorithm used by the originator
- Example: the signer uses SHA-256, then the attacker finds weaker hash algorithm that produces a 256-bit result
- RFC 6211 offers part of the solution

Proposed Update to RFC 5652

- Section 5.3: … the same digest algorithm MUST be used to compute the digest of the SignedData encapContentInfo eContent …
- Section 5.6: … using the same digest algorithm to compute the digest of the the encapContentInfo eContent OCTET STRING and the message-digest attribute.

Backward Compatibility

- The new requirement might lead to compatibility with an implementation that allowed different digest algorithms to be used to compute the digest of the message content and the digest of signed attributes.
- I do not know any such implementations.
- Do you?

Timestamp Compatibility

The new requirement might lead to compatibility issues for timestamping systems [RFC3161] when the originator does not share the message content with the Time Stamp Authority (TSA)

- In this situation, the originator sends a TimeStampReq to the TSA that includes a MessageImprint, which consists of a digest algorithm identifier and a digest value, then the TSA uses the digest in the MessageImprint.
- As a result, the signature algorithm used by the TSA needs to be the same as the digest algorithm selected by the originator for the MessageImprint.

Security Considerations

- Section 14: add a SHOULD for RFC 6211 …

  While no known algorithm substitution attacks are known at this time, the inclusion of the algorithm identifiers used by the originator as a signed attribute or an authenticated attribute makes such an attack significantly more difficult. Therefore, the originator of a Signed-data content type that includes signed attributes SHOULD include the CMSAlgorithmProtection attribute [RFC6211] as one of the signed attributes. Likewise, the originator of an Authenticated-data content type that includes authenticated attributes SHOULD include the CMSAlgorithmProtection attribute [RFC6211] as one of the authenticated attributes.

Next Steps

- LAMPS WG recharter allows small updates
- Call for adoption after recharter is complete

- Of course, Tim will make all consensus calls for this document