S/MIME Updates

Jim Schaad
August Cellars
IETF 96

Completed Work

- Updates to Allow for Authenticated Encryption Algorithms
  - Add sections on "How to do …"
  - Add AEAD algorithms to the list of SMIME Capabilities
- Add AEAD MUST algorithm
- Errata updates

- Charter: Specify the way to use authenticated encryption in S/MIME.

2

New sections callout
- Insert new section 2.4.4 – Here is an AEAD structure to use
- Add section 3.4 on creation of AEAD method

Add one new AEAD algorithm
- Add AES-GCM in three key sizes
- Increases the MUST encryption algorithms from 1 to 2 – both 128-bits.

Errata:
- Two reported by me dealing with 1) inner content on a certs-only message and 2) Example use of micalg parameter
- One reported and not done by Peter Gutmann – dealing with examples which are not examples.

OPEN Issues for Message Draft

- What is the version number?
  - 3.3, 3.5 or 4.0
- Correct examples to be real examples
  - Open errata from Gutmann
  - AEAD examples
  - Reference to RFC 4134 (does it need updates?)
- Change ASN.1 versions for the module
- Additional security considerations

3

- Version number 3.3, 3.5 or 4.0
  - Sean would like to use 3.5. I don't care. Jumping all of the way to 4 seems to be a stretch.
- Current examples in the draft are not real messages but "Looks like this" messages
  - Open Errata on the issue
  - Fix to have real examples or just change the text to say "Looks Like this"
  - Refer to RFC 4134 the examples draft?
  - What about AEAD examples? Do we add any?
  - No recommendations on EC key sizes since no such algorithms mentioned.
- Are there any changes needed for the ASN.1 module – currently none. Do we upgrade the module to use "current" syntax.
- Security advice on the use of compression and traffic analysis

OPEN Issues for Message Draft (2)

- Change current algorithm requirements?
  - AEAD algorithms to add (AES-GCM, AES-CCM, ChaCha20-Poly1305)
  - Encryption algorithms (tripleDES, AES-CBC)
  - Hash Algorithms (SHA-1, SHA-256)
  - Signature Algorithms (RSA v1.5, RSA PSS, DSA, ECDSA, EdDSA)
  - Key Transport Algs (RSA v1.5, RSA-OAEP)
  - Key Agree Algorithms (DH, ECDH NIST, ECDH CFRG)
- Change recommendations on key lengths?
  - 128 MUST others SHOULD for AES
  - 1024 to 2048 inclusive for RSA and DH MUST

4

- Algorithm changes
  - Remove tripleDES down from SHOULD-
  - Remove/downgrade any SHA-1
  - Remove DSA support as we are just an ECDSA SHOULD
  - Talk about using deterministic ECDSA and/or DSA
  - Get into the v1.5 vs PSS arguments for RSA
  - Require ECDH rather than DH support
  - Change length of AES keys
  - Add ChaCha20-Poly1305
- Hash algorithms of SHA-1 plus SHA-224, 256, 384 and 512 are permitted for content hashing in signatures
  - The set of algorithms permitted in signatures is restricted to SHA-1 and SHA-256
- Key Length Questions
  - Basically says 1024 to 2048 inclusive is MUST anything else is a perhaps of some level.

Open Issues Work for Message Draft (3)

- Update 2.7 advice on selection of encryption algorithm to use
  1. I know what you can do – use from that list
  2. I don't know what can do
     1. SHOULD use AES-128 CBC
     2. Else SHOULD use tripleDES
  3. Implied rule – Don't use a level of encryption that is too low

5

- Do we worry about the difference between sending EnvelopedData and AuthenticatedEnvelopedData in terms of what the failure condition is for the receiver.
- Should we add a step which says that UA should have capability to assign algorithm recipient or to default for unknown recipients.

Open Issues Work for Message Draft (4)

- Header Protection?
  - May wrap in message/rfc822
  - RFC 7508 – Carry in Signed Attribute, Domain Policy based
  - draft-melnikov-smime-header-signing
  - DKIM
- Problems:
  - Stating absence of a header
  - Merging header sets
  - Conflicting headers
  - Selecting the list of headers
  - Forwarded messages, Mailing Lists

6

Header protection is a problem that some people have expressed an interest in addressing.

Some existing solutions are known

- Currently wrap in message/rfc822 – no rules on merging, no guidance on usage, implementation level unknown
- RFC7508 – Domain oriented – uses an authenticated attribute – applied/removed at domain boundary – allows for absence and removal of items – clear rules on precedence
- Draft – uses mime wrapping, attempts to address forward issues – no negatives –
- DKIM – Domain oriented – new domains can change and not integrated into the S/MIME message

Problems that need to be looked at:

- Do we need to be able to state that a header is/should be absent from the message
- What do we do with conflicting headers. In some cases these are desirable to have such as the Subject field
- Different headers may have different rules – how is this approached?
- How does this affect certificate checking for From if there are different from fields?
- Fixed header may increase spaming input as that can be used for all spam

messages. Must open to find out if it is a real encrypted message.

Potential Future Work

- Update RFC 5750
  - Look at the new email address attribute in certificates
  - Algorithms and key sizes

Discussions – As Time Permits