Header Protection

LAMPS / IETF 111
Daniel Kahn Gillmor, Bernie Hoeneisen, Alexey Melnikov

2021-07-29
Significant changes since IETF 110 (-03):
- ~40 Test vectors (and revised/improved)
- Enumerated problems seen in various legacy clients
- Editors have more asks of the WG!
Test Vectors

• ~40 different e-mail messages, covering:
  - Signed-only vs. signed+encrypted (vs. no S/MIME)
  - Header protection scheme: wrapped vs. injected (vs. no protection)
    • Signed+encrypted Injected messages: Legacy Display vs. no LD
  - Header Confidentiality Policy: hcp_minimal vs. hcp_strong
  - Threaded Replies
  - Signed-only: single part vs. multipart/signed
  - Message body: text/plain vs. complex
    (multipart/alternative + image/png attachment)
Test Vectors – what next?

• Replies to unprotected or plain S/MIME messages?
• Tampered variants of all S/MIME messages?
• Variants using certs issued by pre-installed CAs?
Test Vectors - Ask for WG

- Please test your preferred client!
- https://header-protection.cmrg.net
- Make screenshots!
Complex Problems

- Consequences for compliant MUAs are easy, but legacy MUAs...
- Interactions between different MUAs (at least 2)
- No hope of upgrade for some peers
- Sender does not know which MUA(s) the recipient(s) will use
- Recipient does not know which MUA the sender used
- Different priorities for usability/confidentiality/authenticity tradeoffs
- Level-setting: an improvement to S/MIME, but doesn’t fix all the problems of terrible S/MIME implementations
Legacy Problems

• Created taxonomy of specific concerns
• Broken out by:
  - Type of message (signed-only vs. signed+encrypted)
  - Use context (list vs. render vs. reply)
• Prioritization is unclear
Legacy Problems – Ask for WG

• Review the enumeration of problems in -06 (appendix A)

• Feedback on list!
  – What are we missing?
  – Thoughts about listed concerns?
Screenshots

• Originally had:
  - Thunderbird
  - Evolution
  - Balsa
  - Geary

• Recently added:
  - Outlook 365
  - Mail.app (Apple’s desktop MUA)
Screenshots – Ask for WG

- Screenshot your client!
- Mobile clients especially interesting
Screenshots of Popular Legacy MUAs

- Examples from MS Outlook 365
- A demonstration of identified problems

Legend (meaning of colors / frames in screenshots):
- **Unprotected Subject**
- **Protected Subject**
- **Protected Body**
- **Security indicator**
- **Reply / Forward buttons (unless cropped)**
Outlook – Rendering Signed Only

Wrapped (open attachment first)

Injected (Unprotected Subject only)

This is the smime-one-part-complex-injected message.

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the injected Headers header protection scheme.

--
Alice
alice@smime.example
Wrapped vs. Injected

Wrapped (open attachment first)

Injected (missing Subject)

This is the smime-enc-signed-complex-wrapped-strong message.

This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme with the hcp_strong Header Confidentiality Policy.

--
Alice
alice@smime.example
Outlook – Reply Signed Only

Wrapped (open attachment first)

From: Alice <alice@smime.example>
Sent: Saturday, February 20, 2021 6:04 PM
To: Bob <bob@smime.example>
Subject: smime-one-part-complex-wrapped

This is the smime-one-part-complex-wrapped message.

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme.

--
Alice
alice@smime.example

Injected (Unprotected Subject only)

From: Alice <alice@smime.example>
Sent: Saturday, February 20, 2021 6:06 PM
To: Bob <bob@smime.example>
Subject: smime-one-part-complex-injected

This is the smime-one-part-complex-injected message.

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Injected Headers header protection scheme.

--
Alice
alice@smime.example

Note: Alternative ways to reply not shown here
Outlook – Reply Signed & Encrypted

**Wrapped (open attachment first)**

This is the smime-enc-signed-complex-wrapped-strong message.

This is an encrypted and signed S/MIME message using PKCS#7 envelopeData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme with the hsp_strong Header Confidentiality Policy.

---

**Injected (missing Subject)**

This is the smime-enc-signed-complex-injected-strong message.

This is an encrypted and signed S/MIME message using PKCS#7 envelopeData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the injected Headers header protection scheme with the hsp_strong Header Confidentiality Policy.

---

**Injected Legacy Display (missing content)**

This is the smime-enc-signed-complex-injected-strong-legacy message.

This is an encrypted and signed S/MIME message using PKCS#7 envelopeData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the injected Headers header protection scheme with the hsp_strong Header Confidentiality Policy.

---

Note: Alternative ways to reply not shown here
Next Steps

• The editors have not had as much engagement on the list as we’d like
• Considering formation of a design team
  – Needs to have more than just the editors
• Talking with chairs about this
Next Steps – Ask for WG

• Does a design-team approach seem acceptable?
• Do we have non-editor candidates for a prospective design team?
This is the **smime-one-part-complex-wrapped** message.

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme.

**--
Alice
alice@smime.example**

This is the **smime-one-part-complex-injected** message.

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Injected Headers header protection scheme.

**--
Alice
alice@smime.example**
Wrapped (Protected Subject in Body)

Alice

21.04.21

An: Bob

Betreff: smime-enc-signed-complex-wrapped-strong

Sicherheit: Signiert (Alice Lovelace), Verschlüsselt

Von: Alice <alice@smime.example>

Injected (missing Subject)

This is the smime-enc-signed-complex-injected-strong message.

This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme with the hcp_strong Header Confidentiality Policy.

---

Alice
alice@smime.example

Injected Legacy Display (Protected Subject in Body)

This is the smime-enc-signed-complex-injected-minimal-legacy message.

This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Injected Headers header protection scheme with the hcp_minimal Header Confidentiality Policy with a “Legacy Display” part.

---

Alice
alice@smime.example
Wrapped (Protected Subject in body)

Am 20.02.2021 um 18:11 schrieb Alice <alice@smime.example>:

Von: Alice <alice@smime.example>
Betreff: smime-enc-signed-complex-wrapped-strong
Datum: 20. Februar 2021 um 18:11:02 MEZ
An: Bob <bob@smime.example>

This is the smime-enc-signed-complex-wrapped-strong message.
This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Wrapped Message header protection scheme with the hcp_strong Header Confidentiality Policy.

Alice
alice@smime.example
<Mail-Anhang.png>

Injected (missing Subject)

Am 20.02.2021 um 18:12 schrieb Alice <alice@smime.example>

Von: Alice <alice@smime.example>
Betreff: Re: ...
Datum: 20. Februar 2021 um 18:11:02 MEZ
An: Bob <bob@smime.example>

This is the smime-enc-signed-complex-injected-strong message.
This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Injected Headers header protection scheme with the hcp_strong Header Confidentiality Policy.

Alice
alice@smime.example
<Mail-Anhang.png>

Injected Legacy Display

(Protected Subject in Body)

Am 20.02.2021 um 18:10 schrieb Alice <alice@smime.example>

Von: Alice <alice@smime.example>
Betreff: Re: ...
Datum: 20. Februar 2021 um 18:11:02 MEZ
An: Bob <bob@smime.example>

Subject: smime-enc-signed-complex-injected-minimal-legacy

This is the smime-enc-signed-complex-injected-minimal-legacy message.
This is a encrypted and signed S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Injected Headers header protection scheme with the hcp_minimal Header Confidentiality Policy with a "Legacy Display" part.

Alice
alice@smime.example
<Mail-Anhang.png>
Thunderbird – Rendering Signed only

Wrapped (after open attachment)

Wrapped (display as forwarded)

Injected (Unprotected Subject only)
Thunderbird – Reply Signed & Encrypted

Wrapped (open attachment first) Injected (missing Subject) Injected Legacy Display (protected subject & box in body)

Note: Alternative ways to reply not shown here