Header Protection

IETF 113 / LAMPS

March 2022

Daniel Kahn Gillmor
Bernie Hoeneisen
Alexey Melnikov
Recap: two schemes

Wrapped Message

- Content-Type: message/rfc822; forwarded=no

  - Subject: Thursday dinner plans
    - Date: Mon, 14 Mar 2022 00:29:38 -0400
    - From: Alice <alice@example.net>
    - To: Bob <bob@example.org>
    - Message-Id: <826235@example.net>
  - Content-Type: text/plain

    Let's meet at Rama's Roti Shop at 7pm and go to the park from there.

(RFC 3851, S/MIME 3.1)

Injected Headers

- Subject: Thursday dinner plans
- Date: Mon, 14 Mar 2022 00:29:38 -0400
- From: Alice <alice@example.net>
- To: Bob <bob@example.org>
- Message-Id: <826235@example.net>
- Content-Type: text/plain

  Let's meet at Rama's Roti Shop at 7pm and go to the park from there.

(deployed in Enigmail, etc)
<table>
<thead>
<tr>
<th>Recap: legacy problems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wrapped Message</strong></td>
</tr>
<tr>
<td>Looks like a forwarded message to legacy clients</td>
</tr>
<tr>
<td>Strange UI/UX &quot;click to see attachment&quot;, or save message to read</td>
</tr>
<tr>
<td>In some cases, totally unreadable</td>
</tr>
<tr>
<td><strong>Injected Headers</strong></td>
</tr>
<tr>
<td>Obscured header fields invisible to legacy clients</td>
</tr>
<tr>
<td>Fix: decorative &quot;Legacy Display&quot; MIME part inserted</td>
</tr>
<tr>
<td>But &quot;Legacy Display&quot; MIME part makes the whole message unreadable in Outlook</td>
</tr>
</tbody>
</table>
Update: Legacy Display Evolved

Instead of inserting a MIME part, modify the content of the main text/plain part...

The inserted text fragment is a "Legacy Display Element"

Subject: Thursday dinner plans
Date: Mon, 14 Mar 2022 00:29:38 -0400
From: Alice <alice@example.net>
To: Bob <bob@example.org>
Message-Id: <826235@example.net>
Content-Type: text/plain

Subject: Thursday dinner plans
Let's meet at Rama's Roti Shop at 7pm and go to the park from there.
Subject: Thursday dinner plans
Date: Mon, 14 Mar 2022 00:29:38 -0400
From: Alice <alice@example.net>
To: Bob <bob@example.org>
Message-Id: <826235@example.net>
Content-Type: text/html

<html><head><title></title></head><body><div class="header-protection-legacy-display">
<pre>Subject: Thursday dinner plans</pre>
</div><p>Let's meet at Rama's Roti Shop at 7pm and go to the park from there.</p></body></html>

The inserted html fragment is also a "Legacy Display Element"
Update: Choice of Scheme

For backward compatibility.

Conformant MUAs **MUST** be able to generate **Injected Headers**.

Conformant MUAs **MAY** generate **Wrapped Message**.

Conformant MUAs **MUST** be able to consume and render both schemes.
Design Team Process

Voice check-in about every 2 weeks
https://gitlab.com/dkg/lamps-header-protection

- draft authors (Alexey, Bernie, dkg)
  plus Hernâni from p≡p
- We welcome additional parties, especially any implementer of a major MUA (Outlook, Mail.app, etc)
More Help Needed

Test vectors
- Test other MUAs
- Send sample messages through MTAs
- Test automated systems
- Route messages through mailing lists

https://header-protection.cmrg.net/
Recommended Default HCP

hcp_minimal(name, val_in):
    if name is 'Subject':
        return '[[[...]]]
    else:
        return val_in

hcp_strong(name, val_in):
    if name in ['From', 'To', 'Cc', 'Date']:
        return val_in
    else if name is 'Subject':
        return '[[[...]]]
    else if name is 'Message-ID':
        return gen_new_message_id()
    else:
        return null

Design team leans toward hcp_minimal for deliverability and threading

https://gitlab.com/dkg/lamps-header-protection/-/merge_requests/19
Signalling for Legacy Display?

We would like to eventually abandon Legacy Display elements.

When composing an encrypted message with Injected Headers, how does a MUA infer the need for Legacy Display?

- General ecosystem survey?
- Signalling from recipients that the recipient can render obscured injected headers?

Signalling is challenging!

Automated Mail Systems

How are systems that use e-mail as a control channel affected by either scheme?

Do Legacy Display Elements interfere with command processing?

- Mailing lists (e.g., Schleuder)
- Bug trackers (e.g., RT, Debbugs)
- DNS control (e.g., Joker.com)
Legacy Display in text/html

Is this easy enough for clients to insert?

What kind of problems might this change to html cause?
Header Field Cryptographic Status for Encrypted Messages

When should a rendering MUA indicate that a header field is encrypted?

When the protected copy of the field doesn't match the unprotected copy.

But unprotected copy can change in transit.

- What is a "match"?
- This calculation uses untrusted data.

Date: Monday March 14
Subject: Thursday dinner plans
From: Alice
To: Bob

Let's meet at Rama's Roti shop at 7pm and go to the park from there.
Questions?

https://gitlab.com/dkg/lamps-header-protection