Header Protection

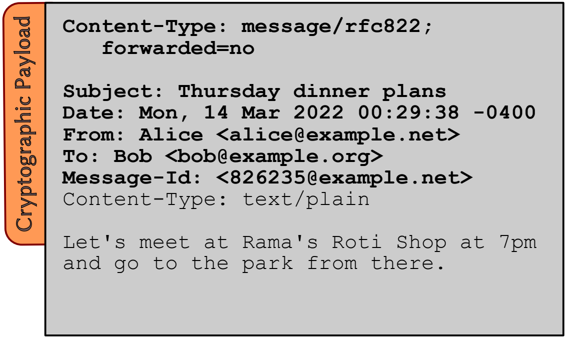
IETF 113 / LAMPS

March 2022

Daniel Kahn Gillmor
Bernie Hoeneisen
Alexey Melnikov

Recap: two schemes

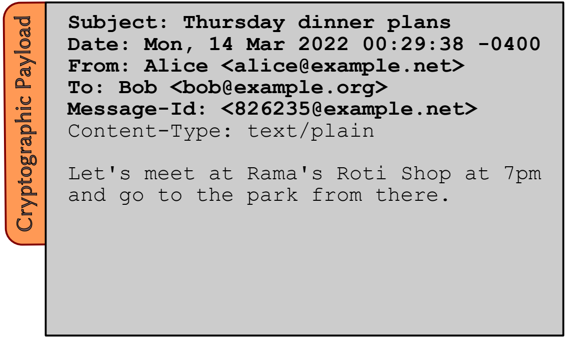
Wrapped Message



```
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)

Recap: legacy problems

Wrapped Message

Looks like a forwarded message to legacy clients

Strange UI/UX "click to see attachment", or save message to read

In some cases, totally unreadable

Injected Headers

Obscured header fields invisible to legacy clients

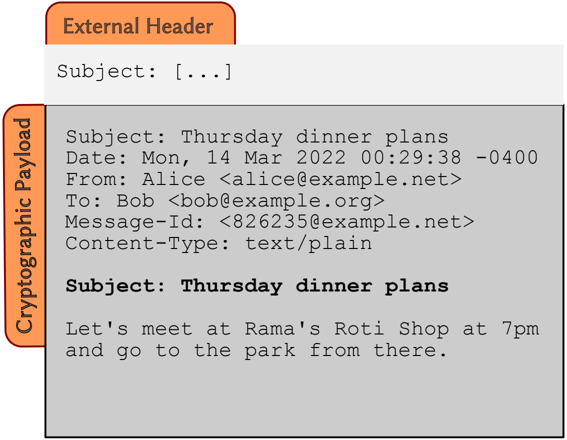
Fix: decorative "Legacy Display" MIME part inserted

But "Legacy Display" MIME part makes the whole message unreadable in Outlook

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"**

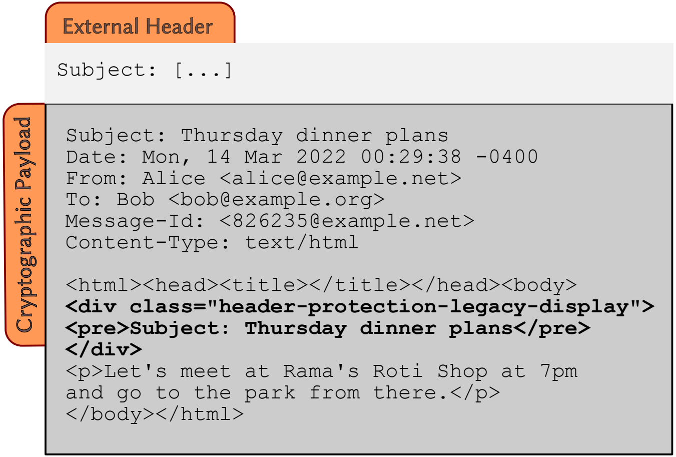


```
Subject: [...]
```

```
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.
```

Update: Legacy Display Evolved

… or main text/html part:



```
Subject: [...]
```

```
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

Qs for the WG 2

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!

https://gitlab.com/dkg/lamps-header-protection/-/issues/20

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?

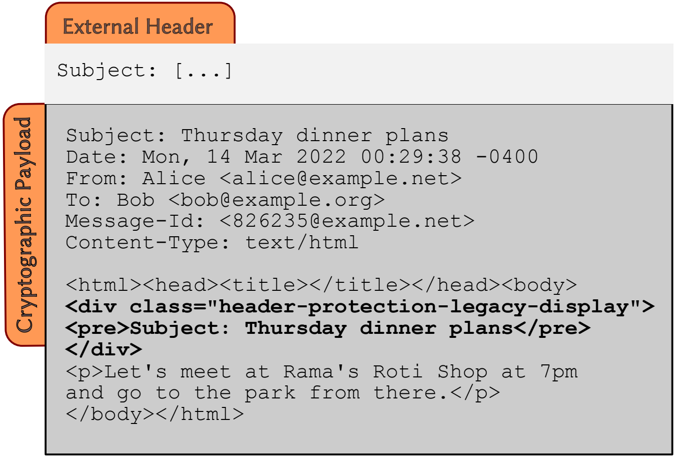
- Mailing lists (e.g., Schleuder)
- Bug trackers (e.g., RT, Debbugs)
- DNS control (e.g., Joker.com)

4 Qs for the WG

Legacy Display in `text/html`

Is this easy enough for clients to insert?

What kind of problems might this change to html cause?



```
Subject: [...]
```

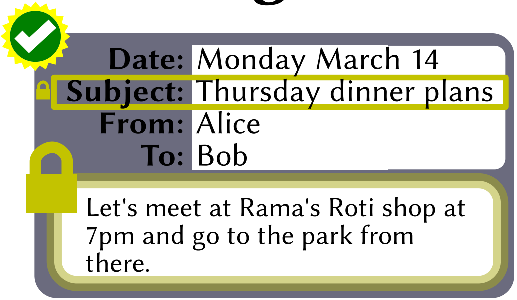
```
Subject: Thursday dinner plans
Date: Mon, 14 Mar 2022 00:29:38 -0400
From: Alice <alice@example.net>
To: Bob <bob@example.org>
Message-Id: <826235@example.net>
Content-Type: text/html

<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>
```

Qs for the WG 5

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.



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.

But unprotected copy can change in transit.

gitlab issues 25 &26

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

Questions?

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