Header Protection (HP)
Use Cases / Requirements

LAMPS @ IETF-106 / Monday, 18 Nov 2019
draft-ietf-lamps-header-protection-requirements-01

Bernie Hoeneisen / Alexey Melnikov
HP in S/MIME since version 3.1

Privacy by Default.

Cannot be protected

Can be protected

Wrap message
Moved Implementation Considerations to Appendix
Simplified GS3 (Header Fields not to include in clear text)
Added GR3 ('encryption only' on receiving side)
Added example for Option 2.1 (pEp)
Added more information on Bcc (feedback IETF-105)
Shortened abstract
More editorial changes
Open Issues

1) Confirm we are not addressing ‘encryption only’ on sending side (i.e. document receiving side only)

2) Should G3 remain in the document (single format that covers all protection levels)?

3) To what extent are we addressing Backward Compatibility?

4) Any further issues / comments (or is this the set of requirements are we going to address in LAMPS)?
   - Completeness
   - Adjustments (as needed)
Solution Considerations: “Weird artifacts”

- How to deal with rendering issues at receiving side “Weird artifacts”?
  - Mitigate confusion of receiving users
  - Help broken clients that do not handle encapsulated (and forwarded) messages correctly

- Observations in the past:
  - Rendered as empty message with attachment
  - Attachment (inner message) cannot be opened
Solution Considerations: “Work-around”

- **Fix broken implementations** (in code of receiving side) as opposed to “work-around” (to standard)
- “Work-around” suggests to add new MIME node (containing protected headers)
  - Legacy Display: draft-autocrypt-lamps-protected-headers-01
  - Deviation from current S/MIME standards
- More research needed, in particular on receiving side
  - Impact of “work-around” on existing implementations
    - Adverse side effects (e.g. MIME libraries)
    - Newly introduced “weird artifacts” on receiving side (by suggested “work-around”)
  - Update existing research on “weird artifacts”
Next steps

- Close open issues
- Confirm the set requirements on mailing list
- Reach out to implementers of clients and libraries to gain feedback
- Update requirements I-D
- More research on “weird artifacts”
- Start new I-D on solutions
Questions / Discussion

Privacy by Default.
Backup Slides
Interaction Cases (1/3)

• Which interaction cases are in scope?

<table>
<thead>
<tr>
<th></th>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unaware of HP</td>
<td>Supports new HP</td>
</tr>
<tr>
<td>1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4)*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* trivial case
Interaction Cases (2/3)

- Which interaction cases for interoperability with legacy HP are in scope?
- S/MIME HP since version 3.1
- Other implementations (incl. PGP)?

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports legacy HP</td>
<td>Supports new HP</td>
</tr>
<tr>
<td>5)</td>
<td></td>
</tr>
<tr>
<td>6)</td>
<td></td>
</tr>
</tbody>
</table>
Interaction Cases (3/3)

- Interactions between clients not supporting new HP
  - Probably out-of-scope
  - Though, may need to be documented

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unaware of HP</td>
<td>Supports legacy HP</td>
</tr>
<tr>
<td>Supports legacy HP</td>
<td>Unaware of HP</td>
</tr>
</tbody>
</table>

Privacy by Default.
General Requirements (High Level)

- G1: Format (MIME structure, Content Type, etc.)
- G2: Easily implementable
- G3: Only one format for all protection levels
- G4: Mitigation of MITM (incl. downgrade) attacks
Requirements Sender (High Level)

- GS1: Which Header Fields (HF) to protect [signature case]
- GS2: Which HF to send in clear [encryption case]
- GS3: Which HF to not to send in clear (Data Minimization) [encryption case]
- GS4: Which HF to not to include to any HP part (e.g. Bcc)
Requirements Receiver (High Level)

- GR1: Conflicting information between protected and unprotected HF? What to present to the user?
- GR2: Detection of MITM (incl. downgrade) attacks
- GR3: how to treat 'encryption only' on receiving side
Requirements Backward Compatibility

General:
- B1: Distinguish between forwarded and wrapped messages

Sender:
- BS1: Indicate full HP support
- BS2: Define how full HP support of the receiver can be detected or guessed.
- BS3: Ensure Subject HF can be displayed to users of HP unaware clients

Receiver:
- BR1: Detection for support of new HP

Privacy by Default.