• Generic Use Cases for Header Protection (HP)

• Requirements
  – First draft as basis for discussion

• pEp implementation experience and description of HP
  – Progressive Header Disclosure (pEp message format version 2)
  – Not covered in these slides
Background

- New Work Item on Header Protection (HP) to be added to the LAMPS Charter requested from IESG:

*Update the specification for the cryptographic protection of email headers -- both for signatures and encryption -- to improve the implementation situation with respect to privacy, security, usability and interoperability in cryptographically-protected electronic mail. Most current implementations of cryptographically-protected electronic mail protect only the body of the message, which leaves significant room for attacks against otherwise-protected messages.*
HP in S/MIME since version 3.1

Privacy by Default.

Wrap message

Cannot be protected

Can be protected

Content (orig)

Header (orig)

Content (outer)

Header (outer)

Content (orig)

Privacy by Default.
Privacy by Default.

Content (orig)

Header (orig)

Content (outer)

Header (outer)

Public Key

Wrap message

Cannot be protected

Can be protected

Cannot be protected

Can be protected
Protection Levels

- Which protection level use cases are in scope?

  a) signature and encryption

  b) signature only

  c) encryption only

  (unclear whether this is relevant or whether it can be treated the same as a)

Note: In pEp only a) is relevant

Privacy by Default.
### Interaction Cases (1/2)

- Which interaction cases are in scope?

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

1)  

2)  

3)  

4)*

* trivial case

Privacy by Default.
Interaction Cases (2/2)

- 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></th>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>5)</td>
<td>Supports legacy HP</td>
<td>Supports new HP</td>
</tr>
<tr>
<td>6)</td>
<td></td>
<td>Supports legacy HP</td>
</tr>
</tbody>
</table>

Privacy by Default.
General Requirements (High Level)

- G1: Format (MIME structure, Content Type, etc.)
- G2: Transport of Public Keys
- G3: Easily implementable
- G4: Mitigation of MITM (incl. downgrade) attacks

- B1: Distinguish between forwarded and wrapped messages [depends on solution]
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)

- BS1-BS2: Indication / detection for support of new HP
- BS3: Ensure Subject HF can be displayed to users of HP unaware clients

Privacy by Default.
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
- BR1: Indication / detection for support of new HP
Interoperability Requirements legacy HP

- Not covered in this presentation
MEDUP Mailing List / Non-WG Meeting

- New mailing LIST for MEDUP
  - Missing Elements for Decentralized and Usable Privacy
  - https://www.ietf.org/mailman/listinfo/medup

- Non-WG meeting, Thursday, 18:15 - 19:30, Room Tyrolka (Mezzanine floor), including:
  - Introduction to MEDUP / pEp
  - Privacy Threat Modeling (Uni Luxembourg)
  - User Interfaces to Support Privacy (Uni Luxembourg)
  - Status Update on documents

Questions / Discussion