Clarification of Privacy Mechanism for SIP

draft-munakata-sip-privacy-clarified-00

Mayumi Munakata (NTT)
Shida Schubert (NTT)
Outline of the draft

As a result of incorporating the comments we got in San Diego...

<table>
<thead>
<tr>
<th>Draft name</th>
<th>draft-munakata-sip-privacy-clarified-00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Redefine and clarify the privacy mechanism (Update or obsolete RFC 3323 and clarify RFCs 3325/4244)</td>
</tr>
<tr>
<td>priv-values</td>
<td>Newly define nw-level, all, none. Maintain id, history as they are. The other priv-values defined in RFC 3323, header, session, user, and critical are NOT RECOMMENDED to be used and kept solely for the backward compatibility reason.</td>
</tr>
</tbody>
</table>
Basic concept

• User's privacy request is based on a binary decision (Privacy ON or OFF).
  The user either requests privacy for the whole message or no privacy at all.

• Privacy functions are executed at two points (UA and Privacy Service).

• Even when a UA can anonymize the user inserted information (From, Contact, etc.), it still needs to ask a privacy service to deal with the intermediary inserted information (Via, Record-Route, etc.)
  Privacy functions are executed at UA/PS or PS alone.
New priv-values

• Defines two new priv-values "nw-level" and "all".

- Privacy ON or OFF?
  - ON
    - UAC anonymizes itself?
      - YES: nw-level
      - NO: all
  - OFF: none or no Privacy header
Way forward

- Is the direction of the draft right?

- We got a comment that new privacy mechanism should define privacy function executed solely on UA.
Options

1. Obsolete or update RFC 3323 and redefine the Privacy header with new priv-values.

2. Separate the draft into two drafts. One updating RFC 3323 with details on privacy treatment on pre-existing priv-values. One defining end point oriented privacy mechanism that does not use B2BUA; uses GRUU and TURN.
Next Step:
- Incorporate the comments on mail list.
- Needs more feedbacks.
- WG item?

Thank you.
New priv-values

<table>
<thead>
<tr>
<th>nw-level</th>
<th>Request that PS anonymizes intermediary inserted/modified information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Request that PS anonymizes all user privacy related information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use cases</th>
<th>Privacy ON/OFF</th>
<th>priv-value</th>
<th>Who anonymizes ...</th>
<th>intermediary inserted information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user can anonymize the message by itself.</td>
<td>ON</td>
<td>nw-level</td>
<td>UAC</td>
<td>PS</td>
</tr>
<tr>
<td>All the privacy functions are expected in a privacy service.</td>
<td>ON</td>
<td>all</td>
<td>PS</td>
<td>PS</td>
</tr>
<tr>
<td>Privacy is not required.</td>
<td>OFF</td>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PS: Privacy Service
Examples

In the case of Privacy: nw-level

From: anonymous
Contact: anonymous
Via: anonymous
Privacy: nw-level

From: anonymous
Contact: anonymous
Record-Route: Proxy1
Via: anonymous
Via: Proxy1
Privacy: nw-level

Privacy function
Only for the intermediary inserted user information

From: anonymous
Contact: anonymous
Record-Route: stripped
Via: stripped

In the case of Privacy: all

From: UAC
Contact: UAC
Via: UAC
Privacy: all

From: UAC
Contact: UAC
Record-Route: Proxy1
Via: UAC
Via: Proxy1
Privacy: all

Privacy function
For all the user information

From: anonymous
Contact: anonymous
Record-Route: stripped
Via: stripped

reference information
Issue

Any time a privacy service modifies a Call-ID header, it SHOULD retain the former value, then restore the value in Call-ID in the response and in other SIP headers such as In-Reply-To and Replaces in any subsequent messages that refers the modified Call-ID.

• Should this draft solve the problem on how to include the privacy service in the path?