UA-Driven Privacy Mechanism for SIP

draft-ietf-sip-ua-privacy-02

Mayumi Munakata
Shida Schubert
Takumi Ohba

Changes from 01 (1/3)

- **Incorporated the result of last meeting (Anonymous From header)**

  From header must be "anonymous@anonymous.invalid"
  unless RFC4474 is provided/is to be used,
  in which case it must be "anonymous@{user's domain name}".

- **Deleted the Requirement section**

  All the requirements seemed too obvious.
  (UA MUST anonymize a SIP message by itself,
  and the backward compatibility MUST be secured.)

- **Organized the text in Sec 4 (Treatment of Privacy-Sensitive Information)**

Changes from 01 (2/3)

- **Added instructions to treat each SIP headers**

  Such as Contact, From, and Via, as well as SDP and host name.

- **Deleted the citations from RFC3323**

  The draft **does not obsolete RFC3323**,
  but defines UA-driven anonymization that is independent.

  The draft now focuses on providing a **guideline for UA to conceal the privacy-sensitive information utilizing GRUU and TURN**.

Changes from 01 (3/3)

1. Deleted the text on the need of the indication of UA-driven privacy

The purposes of indication were:

1. To request intermediaries not to add any extra privacy-sensitive information
2. To request intermediaries not to anonymize the already-anonymized message

For the first purpose;

P-Asserted-Identity is the only privacy sensitive information that can be considered critical which is added by the network entity.

As the privacy on P-Asserted-Identity can be addressed by setting "id" in the Privacy header, no additional indication is necessary.

For the second purpose;

We understand that the **redundancy of anonymization is not a problem.**
(Intermediaries could anonymize the message that is already anonymized.)

Next Step

- **Intended status**

  Informational or BCP?

- **What to do next**

  - Update the draft to incorporate comments on SIP-ML

  - WGLC?