Privacy Terminology

draft-hansen-privacy-terminology-03.txt

Hannes Tschofenig
Status

• Lots of community feedback on -02.
• Version -03 addresses this feedback:
  – Additional co-author: Rhys Smith
  – Major re-write
  – Introduction changed
  – Document further shortened
  – Examples added
• Will become an IAB document soon.
Anonymity

• **Definition**: Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set.

• **Example**: P-Asserted-Identity (PAI) used in SIP with privacy extensions.

• **Uses**
  From: "Anonymous"
  <sip:anonymous@anonymous.invalid>' rather than the subject's address-of-record
Unlinkability

• **Definition**: Unlinkability of two or more Items Of Interest (e.g., subjects, messages, actions, ...) from an attacker's perspective means that within a particular set of information, the attacker cannot distinguish whether these IOIs are related or not (with a high enough degree of probability to be useful).

• Additional terms: profiling, relationship anonymity, unlinkable session, linking identifier

• **Example**: A property typically desired in authentication and key exchange protocols where individual protocol runs are independent of each other. A counter example is a ticket that is used to resume a previous session or a cookie (as a non-cryptographic version of the ticket).
Undetectability

• **Definition**: Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

• **Example**: steganographic systems (to make a message undetectable), or cryptographic systems that inject dummy traffic to conceal traffic content patterns.
Pseudonymity

- **Definition**: A pseudonym is an identifier of a subject other than one of the subject's real names.
- **Example**: Systems that allow identifiers to get re-generated (e.g. SIP CERT – RFC 6072) or replace long-term user identifiers with short lived identifiers (RADIUS Chargeable User Identity – RFC 4372)
Next Steps

• Submit doc as draft-iab-privacy-terminology
• Next draft revision – Early December 2011
  – Add more examples
  – Sync with privacy considerations draft
  – Add missing terms
• Last call – Early 2012