Data Minimization

draft-arkko-iab-data-minimization-principle

IETF-114, Philadelphia

Jari Arkko
+ others who have helped (Martin, Mirja, …)

Context

- The IAB does not focus on detailed protocol issues, but tries to identify broader trends and establish principles
- Examples:
  - RFC 8546 – observable parts of a protocol's wire image will be used
  - RFC 8558 – avoid implicit signals, use explicit signals if sharing info
  - iab-protocol-maintenance – robustness principle vs. protocol maintenance
- Is there guidance to give with respect how we share data about users?
- Increased encryption limits the number of parties that get information, but we still provide a lot of information to various services & servers
  - Perhaps too much, and that data may be shared further
- This is a hard issue to improve, but perhaps there are some things to say
- We've also seen some emerging IETF work in this space

The data minimization principle

- What can we say about passing data to various protocol participants?
  - Obviously we need to avoid giving information to unintended parties
  - … but what about the the actual primary protocol participants?

- Can the **principle of least privilege** be applied?

  "Every program and every user of the system should operate using the least set of privileges necessary to complete the job.”

  =>

  ”Protocol participants should minimize the information they share. I.e., they should provide only the information to each other that is necessary for the function that is expected to be performed by the other party.”

- D’Oh! But perhaps needs to be said

Example applications of the principle

- Oblivious DNS & HTTPS – avoid giving full information to any single participant
- Privacy preserving measurements – avoid giving a single user's data data to any party, while still being able to derive aggregate statistics
- End-to-end message encryption between users, only providing recipient routing information to servers even when the servers relay the encrypted messages