BOF: Privacy Respecting Incorporation of Values (PRIV)

Virtual Meeting

IETF 112

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully. As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this. listed

Definitive information is in the documents listed on https://www.ietf.org/about/note-well/. For advice, please talk to Working Group Chairs or Area Directors.

Administrative Tasks

- Note Takers
  - Thanks to Peter Saint-Andre
  - It's a long slot – do we have a volunteer willing to take over for the second half?

- Jabber Scribe

Agenda

Wednesday, November 10, 2021; 16:00 – 18:00 UTC

Time	Length	Presenter	Topic
1600 – 1605	5 min	Chairs	Welcome & Administrivia
1605 – 1630	25 min	Eric Rescorla	PPM and How It Differs from Previous Work
1630 – 1635	5 min	Eric Rescorla	Mozilla's Use Cases
1635 – 1640	5 min	Tim Geoghegan	ISRG's Use Cases
1640 – 1645	5 min	Martin Thomson	Advertising Use Cases
1645 – 1650	5 min	Charlie Harrison	Google's Use Cases
1650 – 1705	15 min	Richard Barnes	CFRG Mapping
1705 – 1715	10 min	Chairs	Call for Expression of Interest
1715 – 1800	45 min	Chairs	Discussion of WG Charter & BOF Questions

A Few Notes

- This is a working-group-forming BOF. The goal is to make sure all interested parties understand what problem a corresponding working group would aim to solve. There will be presentation of potential solutions, but the goal is not to refine those solutions in this meeting (that is what a working group would do).
- We will be taking questions *for clarification* after the initial presentation that explains the problem and general proposed solution.
- We then have four presentations on associated use cases. We ask that questions on the use cases be held until all four speakers are done, and be limited to clarification only.
- We conclude the presentations with a discussion of work underway in the CFRG Research group, followed by clarifying questions
- The final 55 minutes of our meeting are reserved for discussion, review of the proposed charter text, and a set of questions to provide information to the Security ADs and the rest of the IESG.

PRESENTATIONS GO HERE

Call for Expression of Interest

Before jumping into the charter discussion, we would like to briefly pause to ask who in attendance is interested in working on this technology?

Proposed Charter (1/2)

There are many situations in which it is desirable to take measurements of data which people consider sensitive. For instance, a browser company might want to measure web sites that do not render properly without learning which users visit those sites, or a public health authority might want to measure exposure to some disease without learning the identities of those exposed. In these cases, the entity taking the measurement is not interested in people's individual responses but rather in aggregated data (e.g., how many users had errors on site X). Conventional methods require collecting individual measurements and then aggregating them, thus representing a threat to user privacy and rendering many such measurements difficult and impractical.

New cryptographic techniques address this gap by splitting measurements between multiple, non-colluding servers which can jointly compute the aggregate value without either server learning the value of individual measurements. The Privacy Respecting Incorporation of Values (PRIV) work will standardize protocols for deployment of these techniques on the Internet. This will include mechanisms for:

- Client submission of individual measurements, including proofs of validity
- Verification of validity proofs by the servers
- Computation of aggregate values by the servers and reporting of results to the entity taking the measurement

Proposed Charter (2/2)

A successful PRIV system assumes that clients and the various servers are configured with each other's identities and details of the types of measurements to be taken. This is assumed to happen out of band and will not be standardized in this working group.

The WG will deliver one or more protocols which can accommodate multiple PRIV algorithms. The initial deliverables will support the calculation of simple predefined statistical aggregates such as averages, as well as calculations of the values that most frequently appear in individual measurements. The PRIV protocols will use cryptographic algorithms defined by the CFRG.

The starting point for PRIV WG discussions shall be draft-gpew-priv-ppm.

BOF Questions

1. Who supports to form a WG with this charter (modulo any changes we discussed today)?
   - If you can't answer with support and haven't already stated why, please put yourself in the mic queue.
2. Do we think the problem statement is clear, well-scoped, solvable, and useful to solve?
   - If you can't answer "yes" and haven't already stated why, please put yourself in the mic queue.
3. Who is willing to review documents? (Answer "review" in the MeetEcho chat.)
4. Who plans to serve as an editor for documents? (Answer "edit" in the MeetEcho chat.)