# Oblivious HTTP BoF

IETF 111
July 2021

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.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

**NOTE WELL**

# Agenda

| | |
|---|---|
| 5m | Administrivia / Background / How we got here (Chairs) |
| 30m | Use case + technology recap (Martin Thomson) |
| 60m | Proposed Charter Review (Chairs) |
| * | Document discussion (Martin Thomson / Chris Wood) |

# Process history

Jan 2021 - draft-thomson-http-oblivious

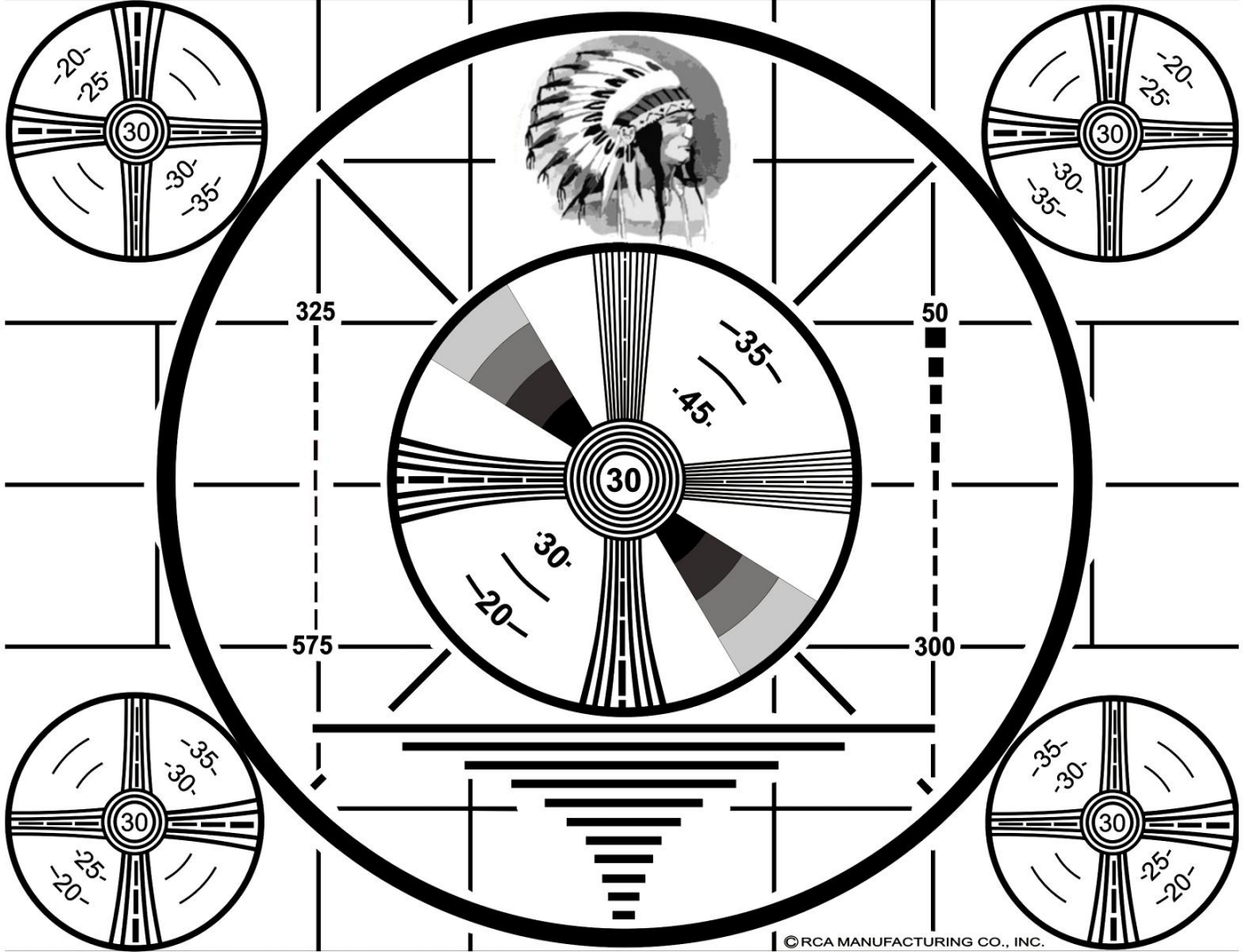
Mar 2021 - SECDISPATCH dispatches to a new, focused WG

Jun 2021 - IESG charter review

=> Discussion on ohttp@ietf.org

=> BLOCKs from INT, OPS, TSV ADs

=> BoF


-20-
-25-
30
-30-
-35-
325
50
-35-
-45-
30
-30-
-20-
575
300
©RCA MANUFACTURING CO., INC.

# Proposed Charter Review

# Proposed Charter (1/3) [Preamble / problem]

# Oblivious HTTP Working Group (OHTTP) Charter

In a number of different settings, interactions between clients and servers involve information that could be sensitive when associated with client identity.

Client-server protocols like HTTP reveal aspects of client identity to servers through these interactions, especially source addresses. Even without client identity, a server might be able to build a profile of client activity by correlating requests from the same client over time.

In a setting where the information included in requests does not need to be correlated, the Oblivious HTTP protocol allows a server to accept requests via a proxy. The proxy ensures that the server cannot see source addressing information for clients, which prevents servers linking requests to the same client. Encryption ensures that the proxy is unable to read requests or responses.

# Proposed Charter (2/3) [Main work product]

The OHTTP working group will define the Oblivious HTTP protocol, a method of encapsulating HTTP requests and responses that provides protected, low-latency exchanges. The working group will define any encryption scheme necessary and supporting data formats for carrying encapsulated requests and responses, plus any key configuration that might be needed to use the protocol.

The OHTTP working group will include an applicability statement that documents the limitations of this design and any usage constraints that are necessary to ensure that the protocol is secure. The working group will consider the operational impact as part of the protocol design and document operational considerations.

# Proposed Charter (3/3) [Caveats]

The working group will prioritize work on the core protocol elements as identified.  In addition, the working group may work on other use cases and deployment models, including those that involve discovery of OHTTP proxies or servers.

The OHTTP working group will work closely with other groups that develop the tools that Oblivious HTTP depends on (HTTPbis for HTTP, CFRG for HPKE) or that might use Oblivious HTTP (DPRIVE for DNS over HTTPS).

[[ Single milestone for the core protocol that was between 4 and 5 meetings / ~18 months out from formation of the working group  ]]

# Discussion