THE PPSP PEER PROTOCOL (PPSPP)

Arno Bakker
Riccardo Petrocco (Spotify/TU Delft)
Victor Grishchenko (Citrea LLC)

VU UNIVERSITY AMSTERDAM

LOOKING FURTHER

OVERVIEW

- IESG telechat on July 10th
- Released -11:
  - Addressed IANA issues for -10
  - Processed some DISCUSSes
  - Fixed small textual issues

IESG TELECHAT

- IESG Evaluation: AD Followup
- Has 5 YES / NO OBJECTIONs
- Has 4 DISCUSSes.
- Needs 5 more YES or NO OBJECTION positions to pass

- Reviews from:
  - OpsDir
  - GenArt
  - SecDir

DISCUSS FARRELL

“I have a number of discuss points (sorry;-), but most of 'em are pretty simple really.

(1) 3.10: What is a "benign" environment? I actually do understand what is meant, but how could a program evaluate that in order to decicde [sic] whether or not to send a PES_RESv4?”

Reformulated such that PEX_REScert is the only viable option for the Internet

DISCUSS FARRELL

“(2) 6.1.2.2: What exactly are the "munro" bytes that are the first input to the signature? […]”

Added to Terminology and added an explicit reference in this section.

DISCUSS FARRELL

“(3) 7.6 and 13.5: SHA1 as the MTI is wrong. Why is that ok, given the collision resistance is less that designed for?”

SHA-256 is now the default. SHA-1 is still MTI to give content providers a trade-off between performance and security, as the on-the-wire overhead is 37.5% smaller.

“(4) 7.7: Why RSASHA1 and not RSA with SHA256?”

RSASHA256 also MTI.

$$Q^{-1}\sum_{z}\sum_{y}|y\rangle\,|z\rangle\sum_{x:\,f(x)=z}\omega^{xy}.$$

DISCUSS FARRELL

“(6) 8.4: […] two questions:

a) where is the "chunk size used" option in section 7? and
b) do all the swarm metadata options have to be sent each time with no limit on ordering […]?”

Chunk size has now been added as a protocol option.

The HANDSHAKE message and hence protocol options are sent only in the first datagram. Options now sorted on code value, ascending, as a simplification.

DISCUSS FARRELL

“(7) 8.13: Don't you need to register the ppsp URI scheme?”

- ppsp://192.0.2.0:6778/e5a12c…

Not sure. Complicated to encode desired info in X5.09.

Replaced the ppsp: with the file: scheme.

DISCUSS FARRELL

“(8) 13.4: Wouldn't DTLS change the chunk size considerations and also influence how messages map to datagrams?”

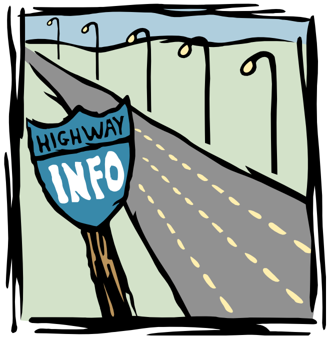
DTLS allows us to know PMTU beforehand. Can fragment when necessary or use small chunk size and send multiple DATA messages per datagram. Added explanation to 13.4.

DISCUSS COOPER

“I'm a little surprised about the choice of LEDBAT for congestion control of live streams. It seems like LEDBAT is not what the receiver would want the sender to use for live-streamed content […]

will yield early, […] no […] acceptable level of quality”

Issue was clarified via email. Updated 8.16 to explain why LEDBAT’s quick reaction to congestion is actually beneficial and that LEDBAT has configurable aggressiveness.

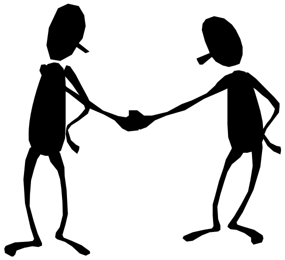


DISCUSS BARNES

“My DISCUSS here is based mainly on the readability of the document, which seems bad enough to be an impediment to interoperability.

As far as I can tell, this document does not define a protocol, in the sense of a set of actions required to achieve a given objective.”

TODO



DISCUSS MORIARTY

“I am still reading this draft, but don't see any response to the SecDir review that raised some very important points for discussion: […]

I'll amend this when I get further into my review and would appreciate a response to the SecDir review.”

SecDir replied to. Awaiting the further amendment ☹

IANA STATUS

IANA Review State: IANA OK - Actions Needed

- Version 0 not defined :-(
- Question one single top-level registry [for] the six new registries defined in this draft?

Internet Assigned Numbers Authority

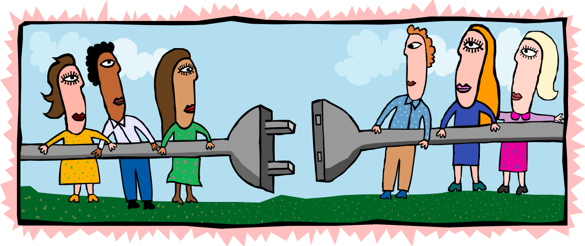
FUTURE

- Discuss our responses with ADs
- Await other AD ballots
  - Been 4 months ☹
- Respond to rest of DISCUSSes
- Process COMMENTs and reviews

- Moving forward!

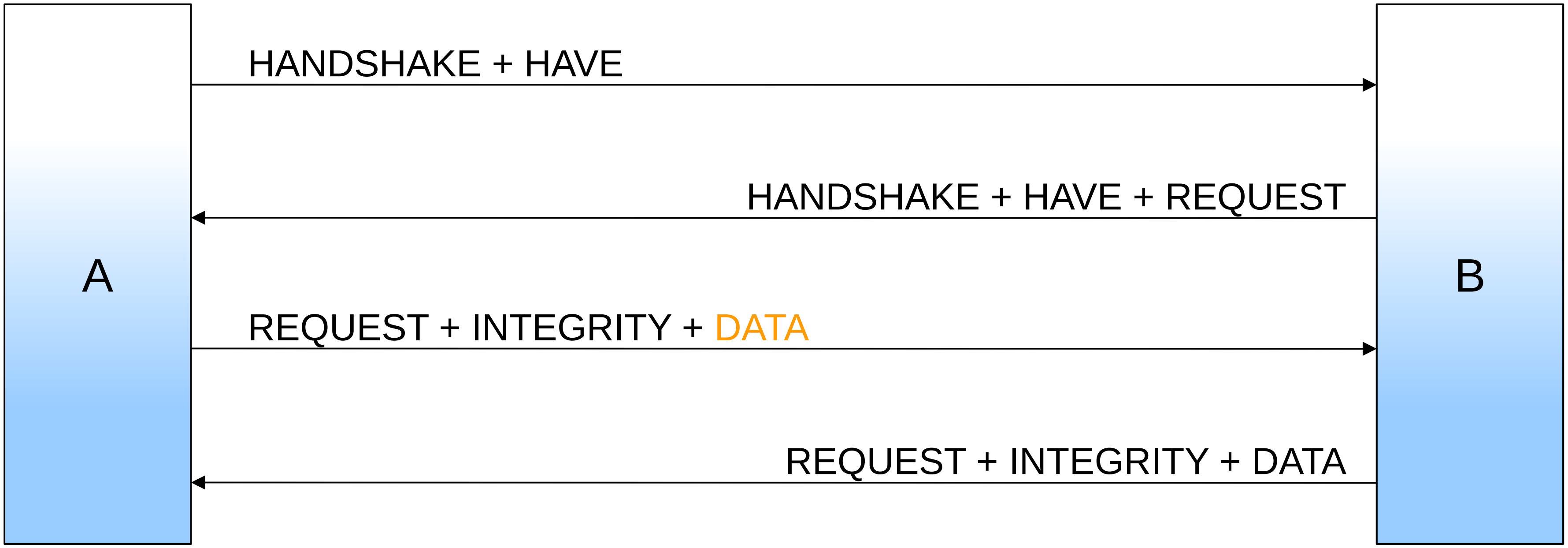
REFRESH: PPSPP MESSAGES

- Basic unit of communication: Message
  - HANDSHAKE
  - HAVE: convey chunk availability
  - REQUEST: request chunks
  - DATA: actual chunk
  - INTEGRITY: hashes to enable integrity verification
  - …
- Messages are multiplexed together when sent over the wire.



EXAMPLE PPSPP ON THE WIRE

- Peer A and B both have some chunks:


HANDSHAKE + HAVE
HANDSHAKE + HAVE + REQUEST
A
B
REQUEST + INTEGRITY + DATA
REQUEST + INTEGRITY + DATA

- Note: low latency, data transfer already in 3rd datagram.