Streamed Oblivious HTTP Messages

A discussion

Tommy Pauly
OHAI
IETF 117, July 2023, San Francisco
Status quo OHTTP

OHTTP currently defines a single message in each direction, that

Must be encrypted and decrypted in one chunk

This is great for DNS, and other small messages

However, Binary HTTP (RFC 9292) does support indeterminate messages
Why streamed OHTTP?

Some usage patterns can benefit from allowing encryption/decryption in multiple chunks

Long (or slowly generated) messages that can be processed in multiple parts — large database lookup, etc.

Interactive workflows where the request can be completed after the headers from the response are received
What needs to change?
Changes

1. Chunk encapsulation (HPKE / AEAD)
2. Request/response format
3. Media type
Chunk encapsulation

New requirements:

1. Protect against chunk reordering

2. Protect against truncation/removal of entire chunks

Truncation attacks within a single chunk are already prevented by the AEAD
Chunk encapsulation
Proposal

Sequence of chunks

- Requests: HPKE already has sequence numbers for additional operations
- Responses: Add a counter to the AEAD message nonce

Final chunk integrity

- Add a sentinel AAD value "final" for both the final request and response chunks
Request / response format

Add a varint "length" field before each chunk

Final chunk is indicated by length=0, and extends to the end of the outer stream

Note that the encapsulation does not need to directly authenticate this format, just the content and order of the chunks

Allows flexibility for the formats for sending chunks

Any concerns with this?
Media types

Format is different, so we need a different media type

message/ohttp-streamed-req

message/ohttp-streamed-res
Open questions

Any negotiation or indication of support?

Many uses of OHTTP are some a priori configuration

Implications for discovered support (SVCB)

Must servers reply with streamed if clients send streamed requests?
Next steps

Publish draft

Update implementations for interop

Consider adoption