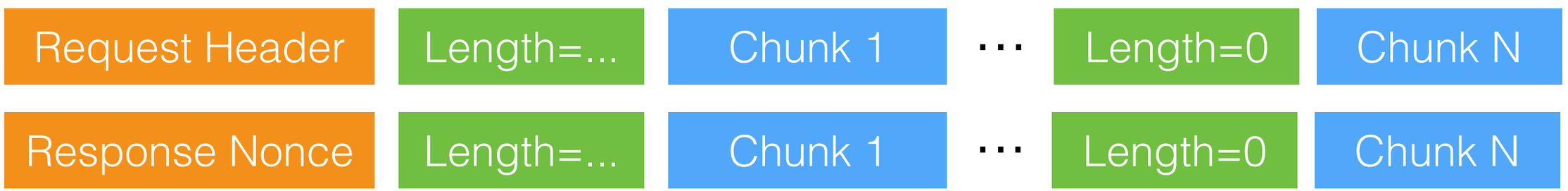
Chunked Oblivious HTTP Messages

draft-ietf-chunked-ohttp-02

Tommy Pauly & Martin Thomson
OHAI
November 2024, Dublin

Chunked OHTTP

Chunked OHTTP allows encrypting and decrypting requests and responses in separate chunks



Allows the use of Binary HTTP's "indeterminate" mode

Takes advantage of HPKE's support for multiple messages

Still is a **single** HTTP request-and-response transaction

Updates in -02

Guidance for incremental processing by relays

- Links to `draft-kazuho-httpbis-incremental-http`

Reiterate security properties around forward secrecy

- Like "basic" OHTTP, messages are not forward secret until the key configuration changes
- Don't assume that incremental processing of chunks gives you forward secrecy between chunks

The "Incremental" header field

Signal to relays in both requests and responses that the content should be forwarded incrementally

```
POST /request.example.net/proxy HTTP/1.1
Host: proxy.example.org
Content-Type: message/ohttp-chunked-req
Incremental: ?1
```

Without this, intermediaries will often pend up POST request and response bodies

This provides a signal separate from the content type to request incremental delivery

Remaining issues

Issue #5: Negotiating use of chunked

Issue #7: Maximum chunk size

Issue #27: Replayability & interactivity

Negotiating use

Issue #5

We had a discussion at IETF 119

- Media types are enough to signal what is being used
- "Just try" using chunking seems like the consensus option
- We need to provide some guidance still

Proposal:

- If you know you need to use Chunked OHTTP for a particular use case, use it (via the media type); if it fails, that's the same as OHTTP failing overall
- If you want to use Chunked OHTTP opportunistically, try using the media type. Add a privacy/security note that without consistency checks this could lead to differentiated behavior between clients
- If the client uses the chunked media type for a request, the gateway MUST use the chunked media type for the response, for simplicity

Maximum chunk size

Issue #7

We also discussed this at 119

> Add a minimum supported maximum chunk size for interoperability — the value an implementation will assume peers are willing to hold in memory and decrypt at once

Proposal:

> "Implementations MUST support 2^{16}-byte chunk sizes. Implementations SHOULD limit chunk sizes to that value unless otherwise configured."

Replayability & interactivity

Issue #27

If chunked messages are not interactive (all request chunks end before any response chunks start), then a malicious relay replaying chunks won't have an impact

If messages are interactive (interleaved request and response chunks), we need to add considerations for the impact of a malicious relay replaying chunks

Next steps

Complete formal analysis and test vectors — please help if possible!

More interop testing

Track dependency on Incremental header field

Are we almost done?