Binary HTTP Messages

draft-thomson-http-binary-message

Martin Thomson* & Chris Wood

OHAI Meeting

IETF 112, not-Madrid, November 2021
Oblivious HTTP protects entire HTTP messages

Binary encoding is
  Unambiguous and deterministic
  Easy to process

Protocol formats (and message/http) are
  Bound to protocols (compression, HTTP/1.1 HEAD responses)
  More complex
How?

Take the format in HTTP/2 and HTTP/3

Simplify

No HPACK

Fixed control data

QUIC variable-length integers throughout

Extend (?)

Fixed vs. indeterminate length

Padding
With Length Prefixes

Known-Length Message {
  Framing Indicator (i) = 0..1,  # request = 0, response = 1
  Known-Length Informational Response (..) ...,  
  Control Data (..),
  Known-Length Field Section (..),
  Known-Length Content (..),
  Known-Length Field Section (..),
}

With Indeterminate Lengths

Indeterminate-Length Message {
  Framing Indicator (i) = 2..3,  # request = 2, response = 3
  Indeterminate-Length Informational Response (..) ...,  
  Control Data (..),
  Indeterminate-Length Field Section (..),
  Indeterminate-Length Content (..) ...,  
  Indeterminate-Length Field Section (..),
}
GET /hello.txt HTTP/1.1
User-Agent: curl/7.16.3 libcurl/7.16.3 OpenSSL/0.9.7l zlib/1.2.3
Host: www.example.com
Accept-Language: en, mi

02034745 54056874 74707300 0a2f6865 ..GET.https../he
6c6c6f2e 7478740a 75736572 2d616765 llo.txt.user-age
6e743463 75726c2f 372e3136 2e33206c nt4curl/7.16.3 l
69626375 726c2f37 2e31362e 33204f70 ibcurl/7.16.3 Op
656e5353 4c2f302e 372e31362e 207a6c69 enSSL/0.9.7l zli
622f312e 322e3304 686f7374 0f777777 b/1.2.3.host.www
2e657861 6d70742d 6c616e67 75616765 .example.com.ace
2e657861 6d70742d 6c616e67 75616765 066562c ept-language.en,
206d6900 0000 mi...
Discussion suggests that this is not for OHAI
Suggest we ask HTTP to take this on