Security Considerations for Optimistic Use of HTTP Upgrade

Ben Schwartz, Meta Platforms, Inc.

HTTPBIS @ IETF 119

Document Status

- Recently adopted
- No changes yet from pre-adoption text
- Some proposed changes and topics of interest:
  - “Connection: close” on Upgrade failure (#2739, slide 3)
  - Restricting message bodies on Upgrade requests and/or responses (#2738, slide 4)
  - Status of “Upgrade: HTTP/2.0” (#2737, slide 5)

“Connection: close” on Upgrade failure

draft-00 only makes recommendations to *standards authors*, not client or server implementors. The standards recommendations largely bind clients, not servers.

Proposal: Server implementors SHOULD treat any failed Upgrade as if it carried a “Connection: close” request header.

Pro: Prevents this category of issues while staying compatible with existing and future Upgrade tokens.

Con: Adds 2 RTT to the HTTP/1.1 authentication flow for MASQUE and WebSockets, and any other Upgrade reject-retry path.

Restricting Request (or Response?) Bodies with Upgrade

All Upgrade Tokens in active use are limited to the HTTP GET method. An Upgrade request containing a body could result in confusion for servers that transfer control of the input stream between separate components.

Proposal: General-purpose gateways MAY remove the Upgrade header from any request containing a non-empty body.

Pro: Reduces the likelihood of security issues from confused backends.

Con: Restricts creativity for future uses of Upgrade.

Status of “Upgrade: HTTP/2.0”

RFC 9110 §18.10 defines the “HTTP” Upgrade Token family, which carries a “Version Token” that can be “any DIGIT.DIGIT (e.g., "2.0")”. This text is carried over from RFC 7230, which predates HTTP/2 (RFC 7540). **There are no known implementations.**

The “h2c” Upgrade Token was defined in RFC 7540 and deprecated in RFC 9113. It had slightly different behavior from the (presumed) semantics of “HTTP/2.0”:

- It was restricted to the insecure “http” scheme.
- It used an “HTTP2-Settings” header instead of the SETTINGS frame.

Proposal: Mark the “HTTP”* Upgrade Token as “OBSOLETE” in IANA.

*and how about deprecating “Upgrade: TLS” too while we’re at it.

```
0\r\n
\r\n
```