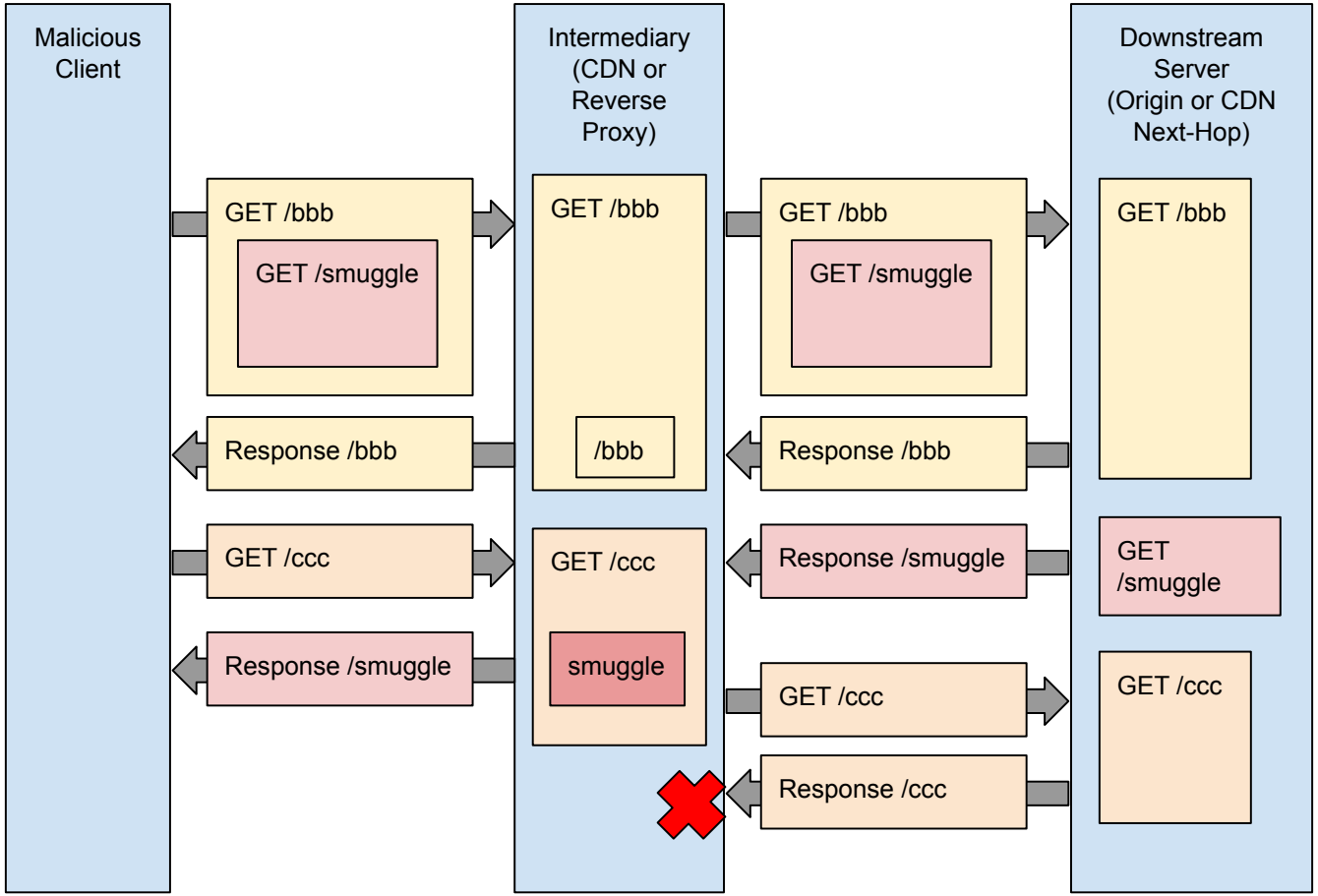
HTTP/1.1 Request Smuggling Defense using Cryptographic Message Binding

Erik Nygren <erik+ietf@nygren.org>
Akamai Technologies

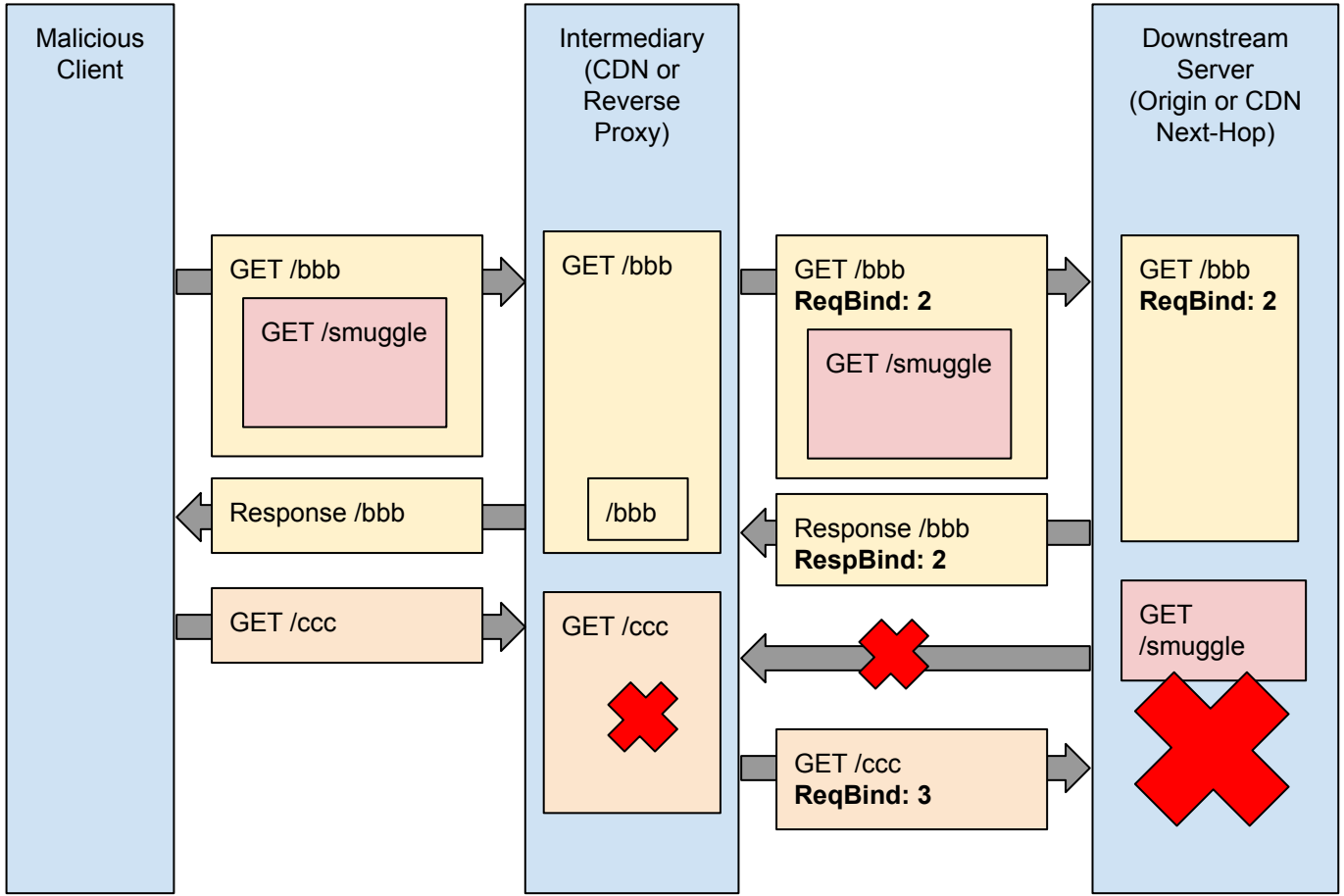
IETF 126 Vienna — July 24, 2026

https://datatracker.ietf.org/doc/html/draft-nygren-httpbis-http11-request-binding-01

Request Smuggling: exploits differences in HTTP/1.1 implementations to bypass controls and poison caches



Idea: use an inband but protected signal to detect and fail when smuggling occurs.



- HTTP/1.1 will be with us for a long time to come
- Multiple vulnerabilities being found each year, especially impacting Intermediary=>OriginServer

- ***Based on Montreal feedback: needs to be simple and easy to implement and deploy.*** *(eg, don't require TLS exporters)*

Changes since -00 based on WG feedback

- Define an explicit Threat Model for what is and isn't intended to be protected
- Bound-Request-Init header field to negotiate a mechanism, including support for crypto agility and for inband communication of a key
  - Enables use without TLS exporters
- Include siphash-2-4 as an alternate hash function for inband
- Suggest a separate ALPN as a possible negotiation mechanism

Properties of a solution

- Easy to implement, low-overhead
- Auto-negotiates (to enable drop-in)
- Protects request Serial (and perhaps other things)
- Provides safeguards against “enough” attacks
- *NOT protecting the assumed-to-be-hostile client-to-intermediary hop*

- ***Is this a problem the WG and implementers are interested in solving?***