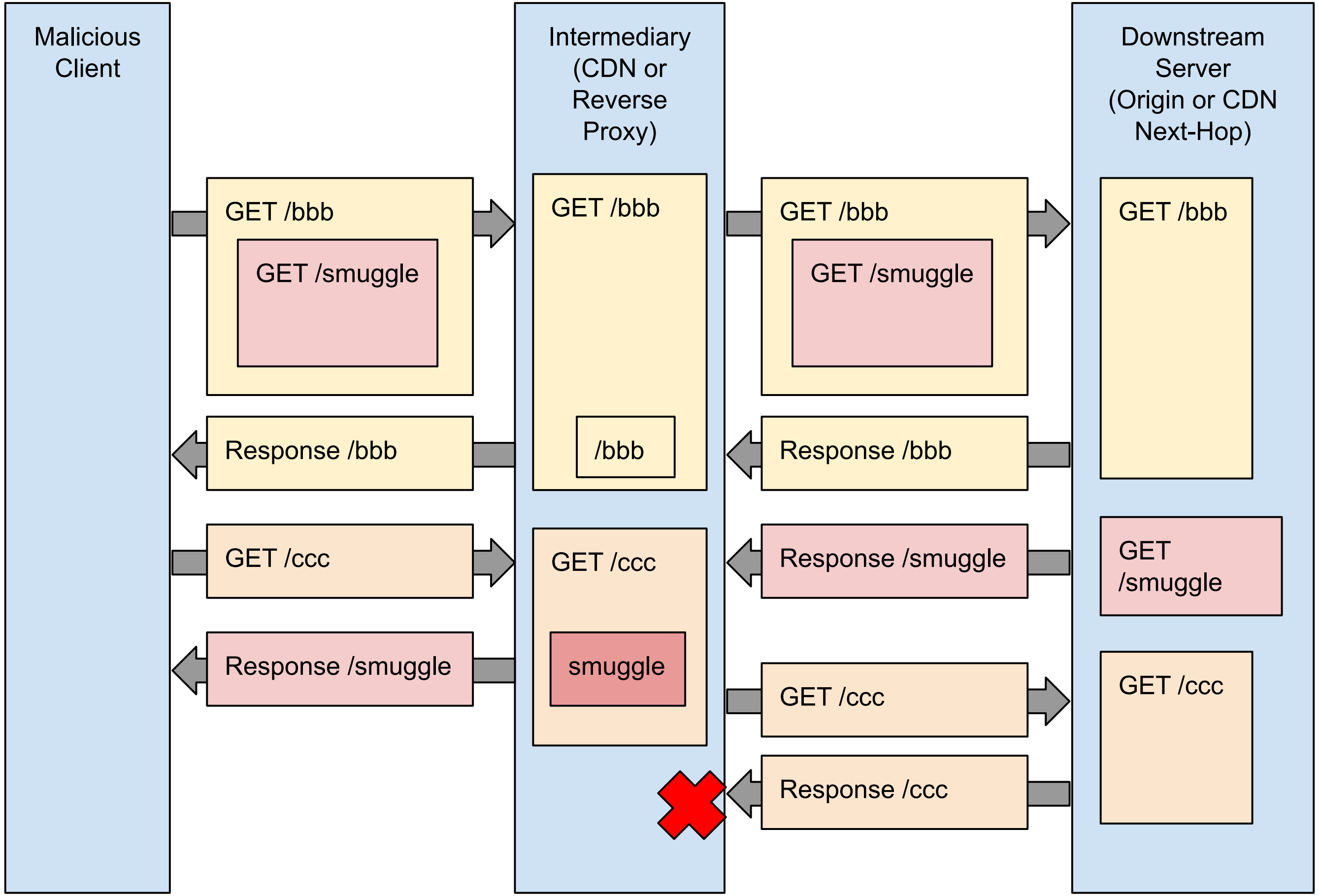
HTTP/1.1 Request Smuggling Defense using Cryptographic Message Binding

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

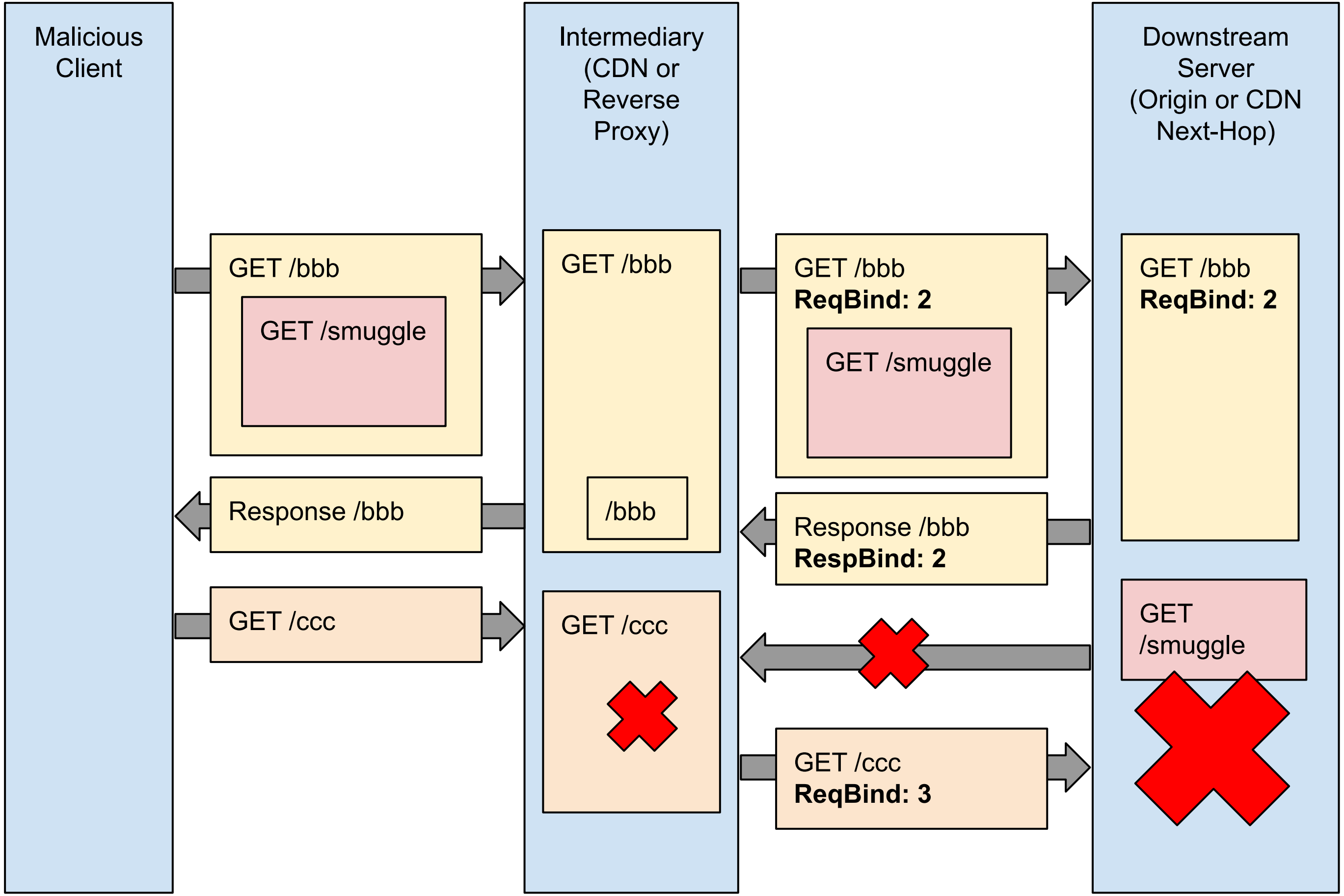
IETF 124 Montreal — Nov 5, 2025

https://datatracker.ietf.org/doc/html/draft-nygren-httpbis-http11-request-binding-00

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

- Draft proposes one proof-of-concept approach using TLS Exporters to protect Request Serial (equivalent of H2/H3 stream ID)

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

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