Oblivious Relay Feedback

draft-rdb-ohai-feedback-to-proxy-07

Nov 2022

T. Reddy (Nokia)
D. Wing (Citrix)
M. Boucadair (Orange)
R.Polli (Team Digitale, Italian Govt)

Agenda

- Updates to address feedback from the WG

Problem Recap

- Servers often rate-limit incoming requests
- Rate-limiting the relay harms all clients using that relay

Proposal Recap

- Signal overload from target to relay
- Relay uses the feedback to rate limit transactions from overzealous or misbehaving clients.
- Uses draft-ietf-httpapi-ratelimit-headers to publish quotas (or service limits) to clients

New *ohttp-target* Quota Policy Parameter

- Rate-limit quota policy for the Oblivious Relay

```
HTTP/1.1 200 OK
Date: Wed, 27 March 2022 04:45:07 GMT
Cache-Control: private, no-store
RateLimit-Limit: 10
RateLimit-Policy: 10;ohttp-target=2;attack-severity="high"; \
comment="abnormal header matching a WAF rule"
Content-Type: message/ohttp-res
Content-Length: 38 <content is the encapsulated 400 response>

...encrypted content...
```

ohttp-target Parameter values

- 1 => RateLimit fields are applicable to all the clients
- 2 => Ratelimit offending client

How can relay prevent de-anonymization of clients ?

Rate-limit offending client (ohttp-target=2)

- **New Prerequisite to handle malicious target**
  - **Large number of clients sending large volume of requests AND**
  - **number of benign clients ≫ number of offending clients**
- **The relay does not immediately rate-limit requests from the offending client**
- **Rate-limits requests only when the ratio of "potential malicious requests" (value=2) to "legitimate requests" is high (no ohttp-target parameter)**
- Malformed HTTP requests are linkable whereas the valid HTTP requests are not linkable.

The target will not be able to partition the anonymity set of legitimate clients.

ohttp-target Parameter values

- 1 => Ratelimit fields are applicable to all the clients
  - **After rate-limiting continue to forward a high volume of messages from many clients.**
  - **Dividing the rate limit fairly among the active clients, the timing pattern of requests can possibly be strongly correlated by the to gateway to de-anonymize clients.**
    - **Relay can delay requests before forwarding them to mitigate the attack as it will likely increase the anonymity set into which each request is attributed.**

draft-rdb-ohai-feedback-to-proxy-07

- Consider for WG adoption
- Comments and suggestions are welcome.