Secure Systems Group, Aalto University

Sanzhar Yeleuov, Jose Luis Martin Navarro, Tuomas Aura

Double-edged sword: DoS attacks using CDN

Problem

- CDNs need to decide on a forward strategy for the fragments received in the request. Options are:
  1) Wait for the whole packet.
  2) Forward fragments immediately.
- Waiting is vulnerable to Convex Attack [1] while forwarding is susceptible to Pre-Post Slow Attack [2]. Our hypothesis is that no CDN is safe from both attacks.

Convex Attack

- Attacker can accumulate the packet on CDN node to magnify the bandwidth.
- Timing requests forwarded via different CDN nodes allows to compensate limited bandwidth, resulting in a pulsing attack.

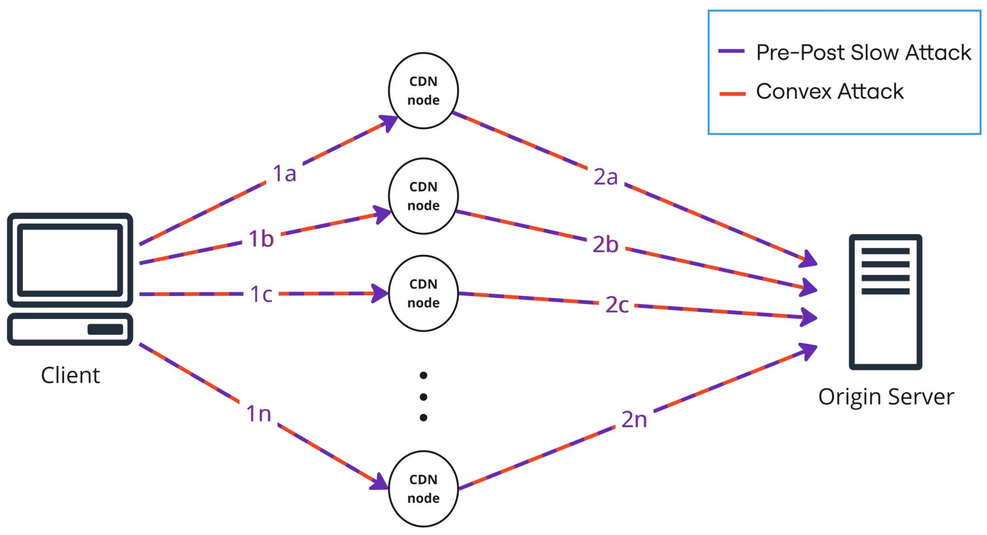

Figure 1. General Diagram of Attacks

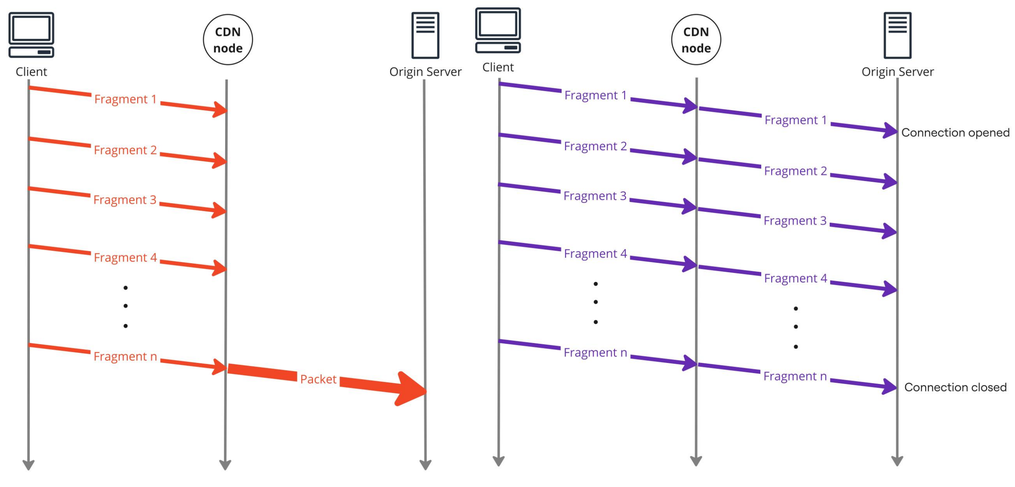

Figure 2. Time Diagrams of Attacks

Pre-Post Slow Attack

- Attacker can slowly send packet fragments to multiple CDN nodes forcing them to maintain connection with the origin server resulting in connection resources exhaustion

Evaluation

- Among four tested CDN providers one was susceptible for Convex Attack and two for Pre-Post Slow attack. Remaining CDN provider does not support POST requests and fragmented requests.
- Since most applications need POST requests, the origin server will be vulnerable to either Convex or Pre-Post Slow Attack depending on the CDN forwarding strategy.

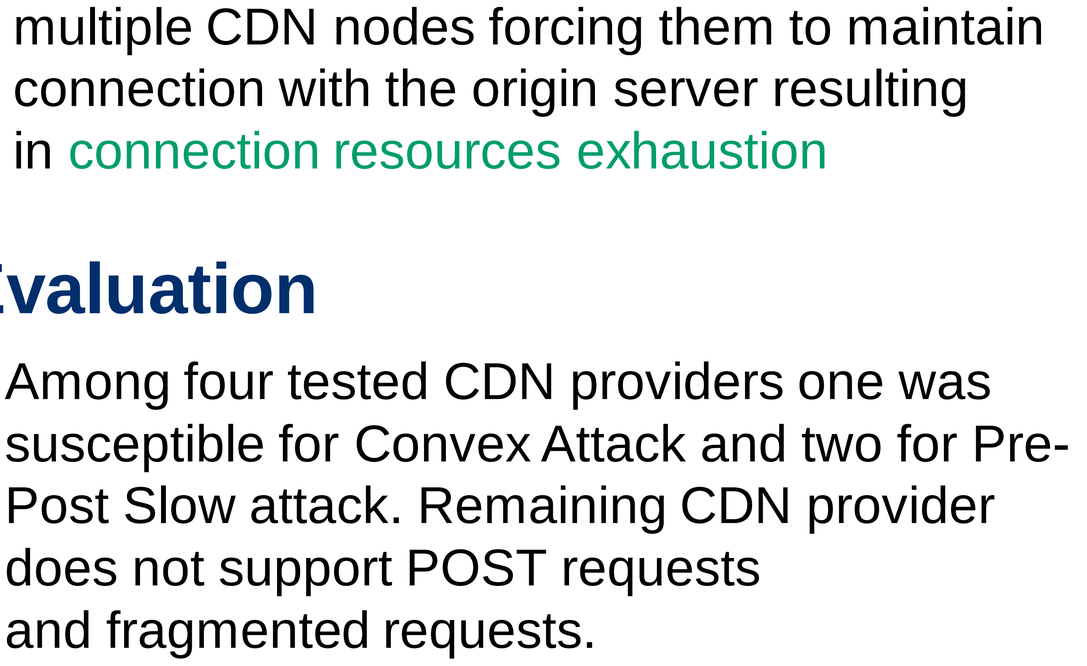

Figure 3. Bandwidth of Attacker and Server during Convex Attack

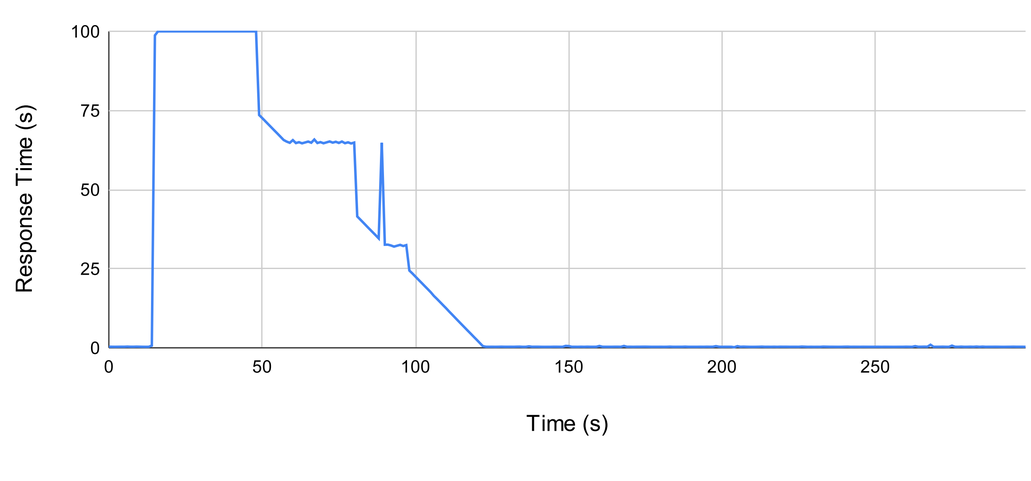

Figure 4. Response time during Pre-Post Slow Attack

Aalto University

Contact: {sanzhar.yeleuov, jose.martinnavarro}@aalto.fi

References:

[1] R. Guo *et al.*, “Temporal {CDN-Convex} lens: a {CDN-Assisted} practical pulsing {DDOS} attack,” 2023.

[2] R. Guo *et al.*, “CDN Judo: Breaking the CDN DoS Protection with Itself,” *Network and Distributed Systems Security (NDSS) Symposium*, 2020