Part 2: DDoS Discovery: Industry and Academic perspective

Q1

The monitoring technologies mentioned in the paper are Network telescopes, Flow monitoring, Honey pots and hybrid approaches combining them together.

Differences in monitoring DDoS attacks across technologies arise from:

- Vantage Point

  The position of technology within the network influences what portions of traffic it can observe.

- Detection

  Distinguishing legitimate traffic peaks from attack traffic is challenging, as each technology highlights unique traffic or attack attributes using varied feature sets.

- Scope

  A technology monitoring range defines its capabilities. Monitoring range shapes capabilities. Telescopes target spoofed direct-path attacks, missing reflection attacks, while flow monitoring at IXPs broadly captures attacks but is path-limited (as it captures only specific ones)

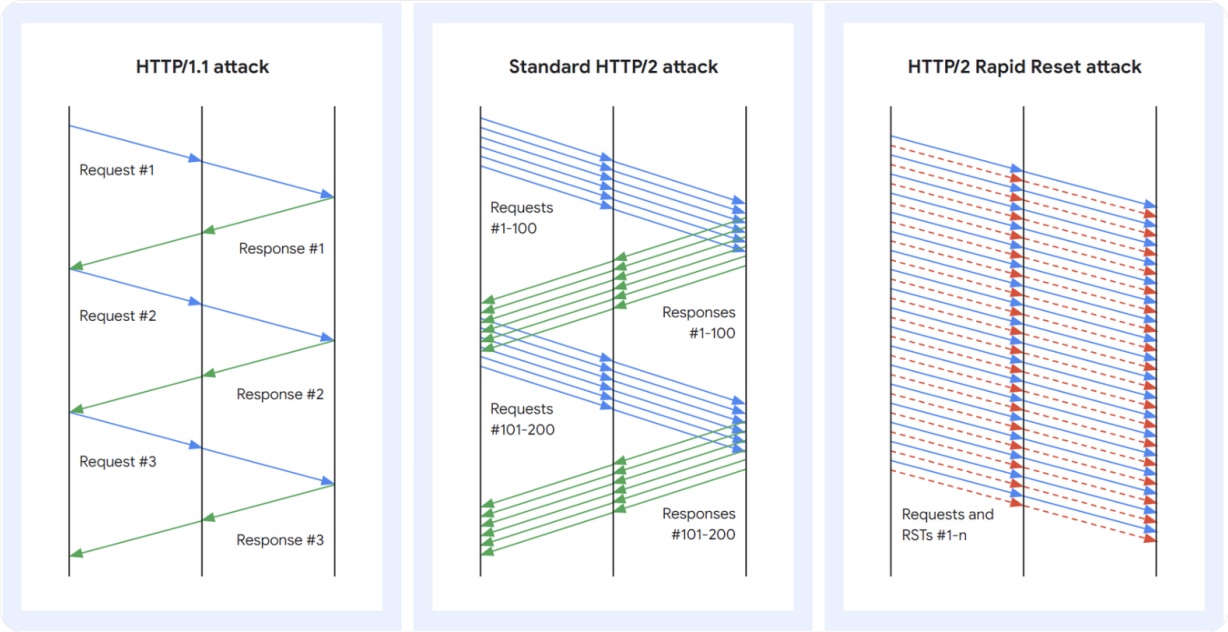
- Data Access

  Data sharing impacts attack visibility. For example the authors of the paper mentioned Flow monitoring by Netscout integrates ISP data for broader insights, but proprietary limits restrict sharing, unlike shareable but narrower telescope data

Q2

The HTTP/2 Rapid Reset attack is application layer DDoS attack exploiting HTTP/2's stream multiplexing. An Attacker sends and cancel numerous requests using `RST_STREAM` within a single TCP connection, overwhelming servers with high request volumes using minimal resources. It's non-spoofed, direct-path, and targets HTTP/2 servers.

Here's a scheme from Google's paper **"How it works: The novel HTTP/2 'Rapid Reset' DDoS attack"** :



HTTP/1.1 and HTTP/2 request and response pattern

Flow monitoring should be able to capture this attack. It should be able to detect HTTP/2 traffic spikes and `RST_STREAM` anomalies using deep-packet inspection and mitigation tools like scrubbing or the blockhole mentioned in the paper.

Network telescopes cannot capture it. They monitor darknet from randomly spoofed attacks, but Rapid Reset's non-spoofed and application layer attacks shouldn't generate backscatter.

Honeypots are unlikely to capture it as well. Designed for reflection-amplification attack, they only detect direct attacks if configured to act as HTTP/2 servers, making them irrelevant here as well as they are not usually used this way.