Part 2: DDoS Discovery: Industry and Academic perspective

Q1

The monitoring technologies mentioned in the paper are:

- **Network Telescopes** – Systems that monitor traffic to unused IP addresses to detect malicious activity.

- **Flow Monitoring** – which collects data from different internet exchange points (IXP) and DDos control systems.

- **Honey Pots** – Decoy systems with intentional vulnerabilities to lure and trap attackers.
- **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 is different for each method:

  - Network telescopes can only detect data reaching "dark" areas, meaning that they will only cover areas that have been spoofed (therefore will not target real services).
  - Honeypots only capture attacks that were directed to specific services, and thus have a limited effect.
  - Flow Monitoring captures data from different addresses but still cannot capture the full scale of the DDos attack.

- Detection Methods

  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, and each method is sensitive to different attacks:

  Telescopes target spoofed direct-path attacks, missing reflection attacks.

Flow Monitoring, on the other hand, broadly captures attacks at IXPs, but is path-limited (as it captures only specific ones).

Honey Pots, as mentioned before, are limited to specific services, and mainly address reflection-amplification attacks.

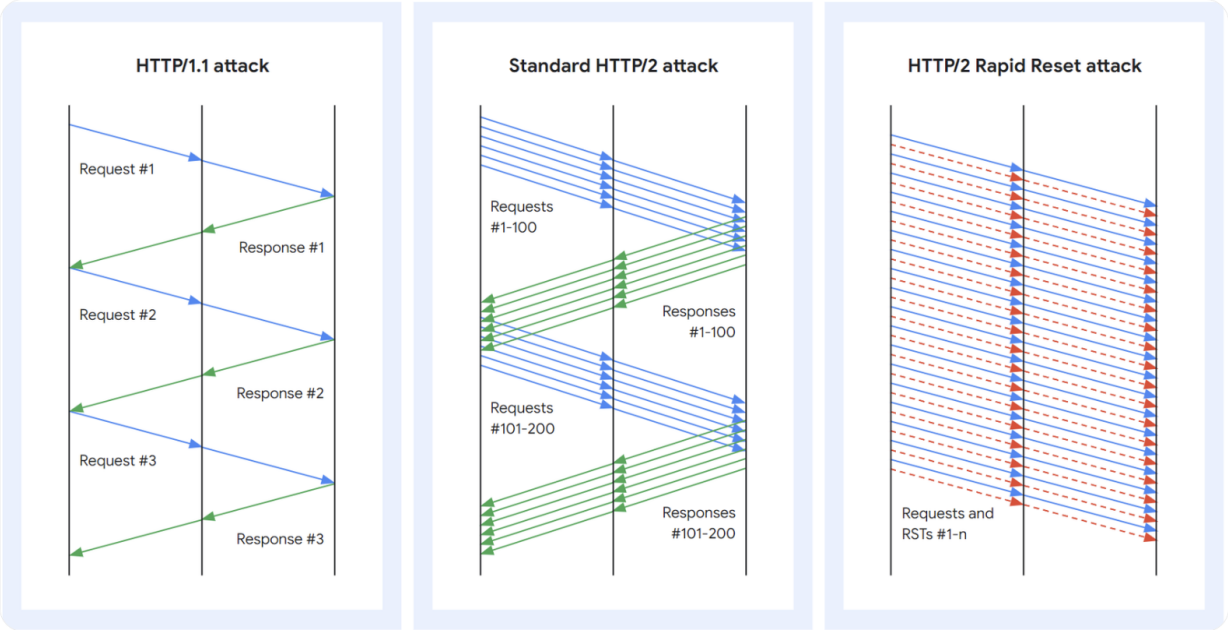
- Data Access

  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 an application layer DDoS attack exploiting HTTP/2's stream multiplexing. An Attacker sends and cancels 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. The system will detect the unusual pattern of the flow of data (repeated opening and resetting) and therefore sense the attack.

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.