IETF123 HotRFC

Grounding High-level Intents to Low-level Network Configurations with LLM Agent

Mingzhe Xing
Beijing Zhongguancun Laboratory

Motivating Example

Threat Intelligence of HTTP 2.0 Rapid Reset DDoS Attack

Overview of HTTP/2 Rapid Reset Attack Mechanism:

- The attacker initiates a large number of requests using HTTP/2 , then immediately send RST_STREAM frames to terminate the connections.
- The server expends significant resources to process these requests and cancellations.

How to defend?

- Server operators should identify abuse based on connection patterns—e.g., a **TCP connection with >100 requests and >50% cancellations may be abusive**. Responses can vary from sending a GOAWAY frame to terminating the connection.

1. Which devices/software should I use for defense?
Router/WAF/Firewall/Nginx/Snort？
2. How should I configure these devices/software?

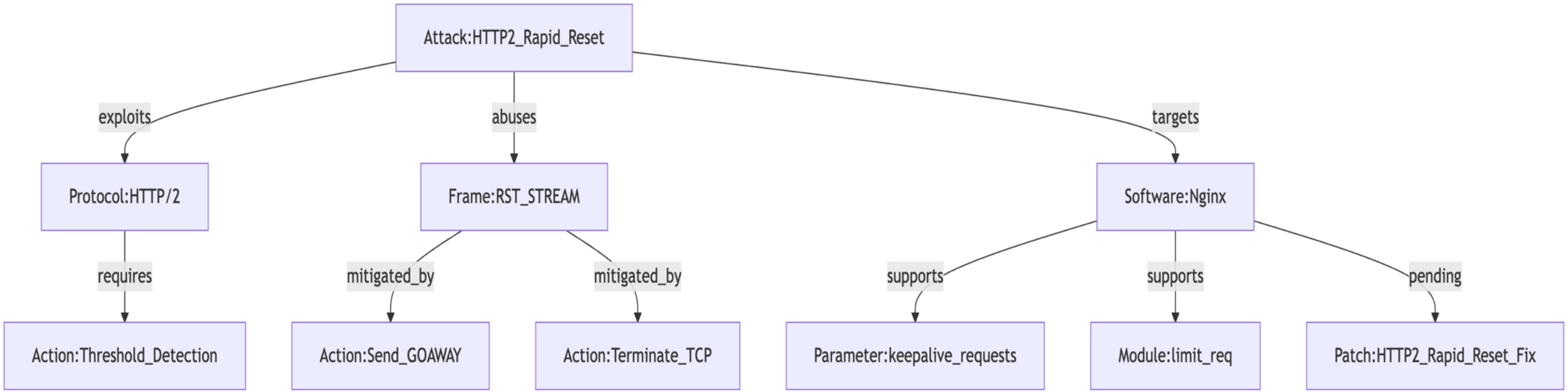
Problem Description

- Operators need to learn the intelligence and manually type commands to achieve specific intents
  - **A learning curve** to understand both the intelligence and network device configuration
  - **Expert Experience** in selecting the most appropriate solution
  - **Risks of typos or fat-finger** during practical operation

Methodology

- Using Large Language Model (LLM) Agent to understand high-level intents and generate low-level configurations
  - **Step 1**. Use LLM to parse the entities and relations in threat intelligence and device/software configuration manuals
  - **Step 2**. Connect these entities and relationships to a knowledge graph
  - **Step 3**. Use LLM to understand the **input intent** (*"**How to defense HTTP 2.0 rapid reset?**"*), and retrieve relevant subgraph
  - **Step 4**. Call the network-status API to fetch current topology, device models and configurations
  - **Step 5**. Generate low-level, executable network configurations by combining the intents with the subgraph and real-time network state

Methodology



For example, HTTP 2.0 rapid reset <--launch--> TCP connection >100 <--cancel--> Nginx <--config--> keepalive_requests 100;

Hackathon Project

Intel

Overview of HTTP/2 Rapid Reset Attack Mechanism:
The attacker initiates a large number of requests using HTTP/2, then immediately send RST_STREAM frames to terminate the connections.
The server expends significant resources to process these requests and cancellations.
How to defend?
Server operators should identify abuse based on connection patterns—e.g., a TCP connection with >100 requests and >50% cancellations may be abusive.
Responses can vary from sending a GOAWAY frame to terminating the connection.

Start Run

Input

nginx

```nginx
http {
    # Define rate limiting zone
    limit_req_zone $binary_remote_addr zone=req_limit:10m rate=30r/s;

    server {
        listen 443 ssl http2;

        # Limit requests per connection
        keepalive_requests 100;

        # Apply rate limiting to all requests
        limit_req zone=req_limit burst=50 nodelay;

        # Other server configurations...
    }
}
```

Output

What is the Goal?

- **New Draft**
  - Use LLM Agent to understand intents and intelligence, and ground them to low-level configurations
  - We welcome collaborations!
- Related Drafts
  - **A Framework for LLM-Assisted Network Management with Human-in-the-Loop**
    draft-cui-nmrg-llm-nm-00
  - **A Framework to Evaluate LLM Agents for Network Configuration,**
    draft-cui-nmrg-llm-benchmark

    draft-cui-nmrg-llm-benchmark
  - **Framework and Automation Levels for AI-Assisted Network Protocol Testing**
    draft-cui-nmrg-auto-test-00

Thanks