Denial-of-Service Vulnerability Discovery in next-generation HTTP using Protocol Reverse Engineering

Prof. Sven Dietrich
Department of Computer Science
City University of New York
Hunter College & The Graduate Center

To improve the data transmission speed of HTTP, HTTP/2 has extended features based on HTTP/1.1 such as stream multiplexing. Along with its wide deployment in popular web servers, numerous vulnerabilities are exposed. Denial of service (DoS), one of the most popular HTTP/2 vulnerabilities is attributed to the inappropriate implementations of flow control for stream multiplexing. To examine the potential flaws of stream multiplexing in various HTTP/2 implementations, modern HTTP/2 security analysis has heavily depended on manual analysis. However, each protocol implementation may exhibit different behaviors, which makes manual analysis somewhat challenging.

In this talk, we present PRETT2, a stateful fuzzing framework for discovering DoS flaws, which uses a Protocol Reverse Engineering technique with the help of network Traces and message Tokens. Based on the flow control process of a particular implementation inferred by protocol reverse engineering, PRETT2 performs stateful fuzzing to detect security flaws that may exhaust system resources. The experimental results on a variety of HTTP/2 implementations in browsers and servers show that PRETT2 successfully inferred multiple state machines and discovered security flaws that fall in the DoS domain, including a published CVE for Apache httpd. We also consider future work on HTTP/3, which is the latest HTTP protocol.