WebTransport Protocol Fuzzing

Bakalárska práca

Autor: Vladyslav Havriuk
Školiteľ: doc. RNDr. Martin Stanek, PhD.

https://github.com/qbitroot/webtransport-fuzzer

Čo je WebTransport?

- Moderný protokol pre obojsmernú komunikáciu klient-server.
- Postavený na **HTTP/3** a **QUIC**.
- Kombinuje nízku latenciu (ako UDP) s bezpečnosťou a spoľahlivosťou (TLS 1.3, Congestion Control).
- **Cieľ práce:** Testovanie bezpečnosti tohto protokolu.

Architektúra protokolov

Protokol	Rola	Vrstva
QUIC	Cesta (The Road)	Transport (L4)
HTTP/3	Dopravné predpisy	Application (L7)
WebTransport	Náklad (Cargo)	Application (L7+)

WebTransport využíva HTTP/3 na "setup", ale potom posiela dáta priamo cez QUIC streamy.

Fáza 1: Nadviazanie spojenia

Pred fuzzingom musíme prejsť striktným bezpečnostným procesom.

1. Handshake
QUIC + TLS 1.3

→

2. Settings
H3 Parameters
(Max Sessions)

→

3. Connect
HTTP Method:
CONNECT

Až po úspešnom kroku 3 sme v stave "OPEN" a môžeme fuzzovať.

Fáza 2: Fuzzing Loop

Sme v tuneli. Klame telom, že sme validný klient.

BooFuzz

Generuje invalidné
VarInts, Payloady...

STATE: OPEN

- Inject: Malformed Capsules
- Inject: Invalid Stream IDs
- Inject: Overflowed Datagrams

Metodika: Blackbox Fuzzing

> ### Prečo Blackbox?
>
> Náš fuzzer **nemá prístup k internému stavu** ani zdrojovému kódu servera.

Language Agnostic
Keďže komunikujeme výhradne cez sieťové rozhranie (network packets), nezáleží nám na tom, v akom jazyku je server napísaný.

Real-world scenár
Simulujeme útok reálneho útočníka, ktorý tiež vidí iba verejný port, nie kód aplikácie.

Ciele testovania (Targets)

Testujeme rôzne implementácie WebTransport Echo Serverov:

Python (aioquic) Rust (quinn / h3) Go (quic-go) C++ (mvfst)

Implementácia

Technológia: Python + BooFuzz + aioquic

- **Shim Architektúra:** Bridge medzi fuzzerom a šifrovaným spojením.
- **State Machine:** BooFuzz kontroluje logickú postupnosť (Connect -> Open Stream -> Send Data).

Záver: Vytvárame univerzálny nástroj na overenie robustnosti WebTransport implementácií.

Speaker notes