Fingerprint your HTTP/2 Stack

A PoC by @Lapeluche (@Sekoia_fr)


Ory Segal
@orysegal
Abonné
HTTP/2 Client Fingerprinting - new research paper from Akamai's Threat Research Team: akamai.me/2qWlqON
À l'origine en anglais
RETWEETS
65
J'AIME
78
01:37 - 5 juin 2017
2
65
78

Passive


Ory Segal
@orysegal
Abonné
HTTP/2 Client Fingerprinting - new research paper from Akamai's Threat Research Team: akamai.me/2qWlqON
À l'origine en anglais
RETWEETS
65
J'AIME
78
01:37 - 5 juin 2017
2
65
78

1. SSTIC'16

Sequel « Comparaisons et attaques sur le protocole HTTP/2 »

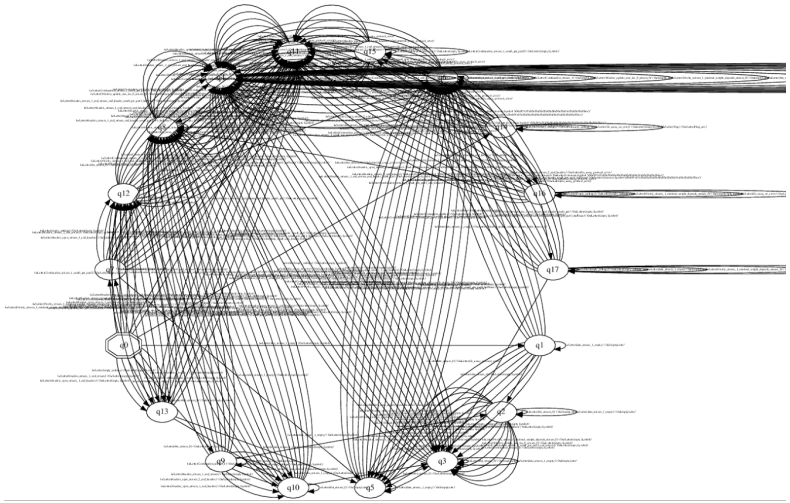
➔ **HTTP/2 is everywhere**
Most browsers, many servers.

➔ **HTTP/2 is complex**
Compressed binary protocol with a nice state machine.

➔ **HTTP/2 State Machine can be automatically reversed**
LSTAR algorithm can be use to actively infer the state machine of a targeted server

1. SSTIC'16

Sequel « Comparaisons et attaques sur le protocole HTTP/2 »



Applied to browsers

HowTo reverse state machine of browser's HTTP/2 stack

1. Create 2 servers : an HTTP + a fake HTTP/2
2. Connect to the HTTP server with your browser
3. The HTTP server exposes a JS that refreshes an image stored on our fake HTTP/2 server
    a. For every connection, the HTTP/2 « smart-fuzz » the browser (i.e. execute a testcase)
4. Once all testcases are computed → trace analysis

Testcase #1

« The server connection preface consists of a potentially empty SETTINGS frame (Section 6.5) that **MUST** be the first frame the server sends in the HTTP/2 connection. »

Testcase #4

« PING frames **MUST** contain 8 octets of opaque data in the payload. »

Testcase #9

« The PRIORITY frame can be sent for a stream in the "idle" or "closed" state. »

Applied to browsers

- Inferred browser state machines are all differents
  - *new/missing/different transitions in state machine*

- Each browser has its own way of implementing HTTP/2
  - Implementation strategies,
  - Initialization parameters,
  - Error handling strategies…

- **PoC with Edge, Chrome, Chromium, Safari and Firefox**

PoC - http2.lol

http2.lol - Fingerprint your HTTP/2 Stack

PoC for sstic.org by @Lapeluche

10%

---

http2.lol - Fingerprint your HTTP/2 Stack

PoC for sstic.org by @Lapeluche

firefox (85.71%)

```
{
    classification : { ... },
    test_plan : { ... }
}
```

http2.lol - Fingerprint your HTTP/2 Stack

PoC for sstic.org by @Lapeluche

firefox (85.71%)


```
{
    classification : { ... },
    test_plan : {
        test_case19 : [
            [
                [
                    "SETTINGS",
                    {
                        SETTINGS_MAX_FRAME_SIZE : 16384,
                        Payload : "b'\x00\x04\x00\x02\x00\x00\x00\x05\x00\x00@\x00'",
                        SETTINGS_INITIAL_WINDOW_SIZE : 131072
                    }
                ],
                [
                    "WINDOW_UPDATE",
                    {
                        Window Size Increment : 12517377
```