Hochschule Bonn-Rhein-Sieg

Internetkommunikation
SS19
Martina Kannen

Laborübung - HTTP 2.0

18.06. - 25.06.2019

Nachdem Sie sich in den voran gegangenen Laborübungen ausgiebig mit der Version 1 des HTTP-Protokolls auseinander gesetzt haben, sollen Sie heute die Kommunikation mit HTTP 2.0 analysieren.
Da HTTP 2.0 in der Praxis nur verschlüsselt vorzufinden ist, stoßen wir bei der Untersuchung des Protokolls auf zwei Problemstellungen:

- Wie können verschlüsselte Kommunikationen dekodiert werden, so dass sie hinreichend analysiert werden können?
- Welche Maßnahmen müssen ergriffen werden, damit ich alle relevanten Clients (auch mobile) in die Untersuchung mit einbeziehen kann?

Aufgabe 1 - Vorbereitung zur Decodierung der TLS-Kommunikation auf Clientseite

Zwar ist TLS nur als Option im HTTP 2.0 Standard vorgesehen, jedoch gibt es zurzeit keinen uns bekannten Browser der HTTP/2 ohne TLS unterstützt.
Im Falle von Mozilla und Chrome-Browser kann die Kommunikation Client-seitig dekodiert werden. Hierbei wird der Sessionkey der TLS-Kommunikation beim Client extrahiert und dem Wireshark zur Dekodierung übergeben.

Booten Sie Ubuntu und öffnen Sie ein Terminal. Bearbeiten Sie die folgende Schritte, um später die HTTP-2-Kommunikation zu dekodieren:

- Erstellen Sie zunächst (über den Befehl `touch`) die Datei sslkeylog.log im netlab HomeVerzeichnis.

- Legen Sie mit dem Befehl
  ```
  export SSLKEYLOGFILE=/home/netlab/sslkeylog.log
  ```
  die Umgebungsvariable SSLKEYLOGFILE an.

- Öffnen Sie Wireshark und geben Sie unter [Bearbeiten]->[Einstellungen]->[Protocols]->[SSL]->“(Pre)-Master-Secret log filename“ den Speicherort der oben angelegten Datei an.

- Starten Sie aus dem **selben** Terminal-Fenster den Firefox.

- Erläutern Sie, was genau der Befehl export in unserem konkreten Szenario bewirkt.

Aufgabe 2 - Analyse der HTTP 2.0 Kommunikation

Um die neuen Mechanismen in HTTP 2.0 besser verstehen zu können, haben wir eine etwas komplexere Webseite vorbereitet.

a) Starten Sie ein Capture im Wireshark. Rufen Sie die Webseite https://http2.netlab.inf.h-brs.de auf. Schließen Sie die Webseite und stoppen Sie das Capture.

b) Wie viele eingebettete Objekte beinhaltet die Webseite und um welche verschiedene Objekttypen handelt es sich hierbei?

c) Analysieren Sie die Kommunikation und beantworten Sie die folgenden Aufgaben:
   - Zeichnen Sie über ein Sequenzdiagramm den gesamten Kommunikationsablauf auf.
   - Wie viele Streams werden insgesamt geöffnet, wie viele vom Client, wie viele vom Server?
   - Welche Inhalte werden jeweils in einem Stream übertragen?

Viel Spaß und Erfolg!