



Laborübung TCP

21.05. - 28.05.2019

Im Normalfall besteht der Ablauf einer TCP-Verbindung aus den drei Phasen Verbindungsaufbau, Datenübertragung und Verbindungsabbau. Ziel der praktischen Übung ist es, diese drei Phasen hinsichtlich ihrer Kommunikationsverläufe und -parameter zu analysieren.

Starten Sie den Rechner und booten Sie Ubuntu 14.04. Loggen Sie sich mit dem Benutzer „netlab“ und dem Passwort „netlab“ ein. Starten Sie anschließend das Programm Wireshark. Stellen Sie sicher, dass bei den Einstellungen zu TCP („Edit, Preferences, Protocols, TCP“) die beiden Optionen „Relative sequence numbers...“ und „... to reassemble TCP streams“ deaktiviert sind.

Starten Sie die Capture-Funktion. Initiieren Sie eine Verbindung zu dem HTTP-Server <http://www2.inf.h-bonn-rhein-sieg.de> (da hier sehr einfache Seiten vorliegen, so dass nur eine übersichtliche Anzahl von TCP-Segmenten übertragen wird). Schließen Sie den Browser und beenden Sie anschließend die Capture-Funktion.

- (a) Beschreiben Sie den Ablauf der DNS-Auflösung über IPv6 als auch über IPv4 für oben benannte Server-URL.
- (b) Die von Ihnen aufgezeichneten TCP-Segmente lassen sich den drei Phasen einer TCP-Verbindung zuordnen. Skizzieren Sie (per Hand oder mit Hilfe eines UML-Tools, wie z.B. <http://www.websequencediagrams.com/>) für jede der drei Phasen ein eigenes Sequenzdiagramm. Tragen Sie für jedes gesendete und empfangene TCP-Segment die Sequence-Number und Acknowledgement-Number sowie die in der jeweiligen Phase typischerweise gesetzten Flags ein. Vollziehen Sie an Hand dieser Parameter die Protokollabläufe in jeder der Phasen der TCP-Verbindung nach.

Hinweis: Um sich die TCP-Analyse zu Beginn etwas zu vereinfachen, markieren Sie das erste TCP-Segment der Verbindung und wählen Sie den Menüpunkt „Analyse“, dann „Follow TCP-Stream“ und schließen Sie das sich öffnende Fenster wieder. Danach hat Wireshark einen Stream-Filter, der nur die Pakete zu einer Verbindung im „Normalfall“ anzeigt.

- (c) Wie wird das dritte TCP-Segment (in diesem Fall vom Client) während der Verbindungsaufbauphase durch den Server bestätigt?
- (d) Was bedeutet ein gesetztes PSH-Flag?
- (e) Erläutern Sie im Detail den bei TCP eingesetzten Bestätigungsmechanismus. Gehen Sie hierbei auf folgende Fragestellungen ein:
 - Wie bestätigt der Empfänger ein einzelnes Segment?
 - Wie bestätigt der Empfänger zwei unmittelbar, aufeinander folgende Segmente in Reihe, z.B. Segment 1 und Segment 2?
 - Wie bestätigt der Empfänger zwei unmittelbare, jedoch nicht in Reihe aufeinander folgende Segmente, wie z. B. Segment 1 und Segment 3?
 - Wie bestätigt der Empfänger drei unmittelbar, aufeinander folgende Segmente in Reihe, z.B. Segment 1, Segment 2 und Segment 3?



- (f) In RFC 2018 ist die TCP-Option „Selective Acknowledgment“ definiert.
- Verschaffen Sie sich einen Überblick, was das Ziel und die Funktion dieser TCP-Option ist.
 - Schauen Sie danach unter `/proc/sys/net/ipv4/` nach, wie Linux mit selektiven Bestätigungen umgeht. Als Hilfestellung nutzen Sie die Manpage
 - Prüfen Sie auch Ihr vorhin aufgezeichnetes Capture, ob hier die Selective Acknowledgment Option gesetzt ist. Warum ist das so?
 - Wie sind die Fragestellungen aus Aufgabe (g) bei gesetzter Selective Acknowledgment Option zu beantworten?

Viel Spaß und Erfolg!