

Übungsblatt 8

1. UDP - Prüfsumme

a) Berechnen Sie die UDP-Prüfsumme, welche sich über die folgenden drei 16Bit-Wörter ergibt:

- 1011 1011 0001 0000
- 1001 1001 0101 1001
- 0101 1011 0101 1001

b) Wie kann der Empfänger feststellen, dass im UDP-Paket ein Fehler aufgetreten ist?

c) Wie werden fehlerhafte Pakete auf der Empfängerseite behandelt?

2. UDP – Latenz

Beachten Sie das folgende Szenario:



Der Link hat eine Bandbreite von 1KByte/s . Die RTT zwischen Client und Server sei konstant 200ms. Der Client fordert vom Server eine Datei an, die anschließend an den Client übertragen wird. Verarbeitungsverzögerungen (Processing Delays) können vernachlässigt werden und es treten keine Übertragungsfehler auf. Deshalb muss nur die Übertragungs- und Ausbreitungsverzögerung beachtet werden.

Die Größe der zu übertragenden Datei beträgt 9720 Byte. Die Größe des UDP Headers beträgt 8 Byte und die des IP Headers 20 Bytes. Es wird angenommen, dass jedes UDP-Datagramm maximal 972 Byte an Nutzdaten aufnehmen kann. Die Anfrage des Clients an den Server nach der Datei ist (ohneHeader) 72 Byte groß.

Bitte beantworten Sie die folgenden Fragen:

- a) Wie lange dauert es, bis die Anfrage komplett vom Client zum Server übertragen ist?
- b) Wie viele UDP-Datagramme muss der Server an den Client schicken, um die komplette Datei zu übertragen?
- c) Wie viele Bytes muss der Server insgesamt an den Client schicken, um die Datei komplett zu übertragen?
- d) Wie lange dauert es insgesamt vom Stellen der Anfrage durch den Client bis zur Ankunft der vollständigen Datei am Client?

3. Wireshark

a) Analyse eines Webseiten-Aufrufs mit Wireshark

Rufen Sie eine beliebige Webseite auf, z.B.:

<https://www.th-deg.de>

Analysieren Sie den Aufruf mit Wireshark und stellen Sie fest, welche Protokolle beteiligt sind. Legen Sie dazu einen Filter fest, der nur Informationen über Ihre eigene IP zulässt. Ihre IP-Adresse finden sie mit dem Befehl ipconfig auf der Komandozeile (cmd).

b) Analyse von Video-Streams

Wir wollen das Verhalten eines typischen Video-Streams analysieren. Rufen Sie eine Internet-Seite mit einem Video als Inhalt (z.B. Youtube) auf und scannen Sie den Verkehr eine Zeit lang.

Zur Trafficanalyse bietet Wireshark eine Übersicht über den aktuellen Netzwerkverkehr. Hilfreich an dieser Stelle ist ein Blick den Wireshark **I/O-Graph** (im Menü Statistiken).

**Welches ist die maximale Netzwerkauslastung des Streams?
Wie viele Fehler sind aufgetreten?**

Es bestätigt sich die Vermutung wiederkehrender Netzwerkpeaks, die das Netz jeweils nahezu vollständig auslasten. In der Protokollübersicht zeigt sich außerdem, dass dieser Verkehr überwiegend von einer IP-Adresse ausgeht bzw. dahin führt.

Um weiter nach den Ursachen forschen zu können, lässt sich nun ein Filter auf diesen Rechner setzen. Aufschlussreich sind auch die Statistiken, die Wireshark bietet. Unter dem gleichnamigen Menü finden sich unter anderem eine Statistik die mit „**Endpunkte**“, umschrieben ist. Hier finden sie eine Liste der Kommunikation nach IP-Endgeräten. In dieser Liste ist ersichtlich, dass der Großteil des Datenvolumens von einer IP-Adresse ausgeht bzw. dahin führt. Anhand der IP-Adresse lässt sich nun auch das Gerät ausfindig machen.

c) Auslesen von Zugangsdaten mittels Wireshark

Im Internet gibt es viele Dienste, bei denen der Datenverkehr unverschlüsselt abläuft und somit Benutzerdaten in fremde Hände kommen können. Hier einige Beispiele:

- E-Mail-Abruf über POP3
- Webformulare auf Internet-Seiten
- FTP-Zugang zur Homepage

Deshalb sollten für kritische Daten nur verschlüsselte Protokolle z.B. HTTPS, SFTP usw. verwendet werden.

Zugangsdaten eines FTP-Servers auslesen:

Melden Sie sich an einem FTP-Server an und versuchen Sie die Benutzerdaten auszulesen. Als Beispiel können Sie den Belwue FTP-Server verwenden.

<ftp.belwue.de>

Geben Sie einen Fantasienamen und Passwort ein. Die Anmeldung wird natürlich fehlschlagen.

Beobachten und analysieren Sie den Netzwerkverkehr der Anmeldung mit Wireshark. Können Sie die Anmeldedaten direkt aus den Datenpaketen ablesen? Verwenden Sie einen Filter für das ftp-Protokoll.

Weitere Informationen zu Wireshark

Wenn Sie sich weiter für Wireshark interessieren, schauen Sie sich die You-Tube-Videos „Introduction to Wireshark (1 bis 3)“ an.

Viel Erfolg !!!

Viel Erfolg !!!