IBN Übungsblatt 10 Tutor: Denitsa Ilieva

Lyubomira Dimitrova, Dung Nguyen, Maryna Charniuk

Aufgabe 1

a) Mit dem vorgeschlagenem Test wurde die Internetanbindung (eduroam Universität Heidelberg IPv4-Adresse: 129.206.136.122) mit den folgenden Leistungsmerkmalen gemessen:

- Übertragungsgeschwindigkeit **R** bzw. Durchsatz:
  - für das Herunterladen der Daten: 18,7 Mbps - wichtig für "normale" Internet-Nutzung.
  - für das Hochladen der Daten: 17,6 Mbps - wichtig, wenn man irgendwelche Information hochzuladen braucht, wie z.B., Nutzung den Cloud-Diensten.
- Reaktionsverzögerung (Ende-zu-Ende-Verzögerung?): 5 ms - wichtig für Internet-Benutzer, für denen simultane Datenübertragung in beiden Richtungen (Hochladen-Herunterladen) benötigt wird, wie z.B., Skype-Konferenzen, Online-Gaming.

b) Ja, es ist wichtig. Je näher ein Host von dem Server sich befindet, desto kleiner ist die **Ausbreitungsverzögerung**, die als (Länge der physischen Leitung)/Ausbreitungsgeschwindigkeit gemessen wird.

Auf die Messungen können noch folgende Punkte beeinflussen:

- Wenn Daten ziemlich groß sind und können in einem Paket nicht übertragen werden, kann Wartezeit im Puffer entstehen.
- Wenn es mehrere Daten gleichzeitig übertragen werden müssen, entsteht eine Warteschlange.

Aufgabe 2

a) Die gekapselte Nachrichten, nachdem der Header jeder Schicht hinzugefügt wurde, nennt man:

- in der Anwendungsschicht: Nachricht
- in der Transportschicht: Segment
- in der Netzwerkschicht: Datagramm
- in der Sicherungsschicht: Rahmen

b) Die Endpunkte für jede Schicht:

- in der Anwendungsschicht: Client-Server-Architektur, Anwendung "Web" - Server und Browser; Peer-to-Peer-Architektur, Anwendung "Skype" - zwei Hosts (Peers) - Browser und Browser.
- in der Transportschicht: Prozesse (bzw. zugehörige Sockets - APIs des BS)

- in der Netzwerkschicht: Start- und End-Hosts
- in der Sicherungsschicht: direkt verbundene Geräte (z.B., Host, Router, Switch, WiFi-Zugangspunkte) an beiden Enden einer Teilstrecke.

c) Dadurch kann das Ziel eines Pakets eindeutig adressiert werden:

- in der Anwendungsschicht: IP-Adresse
- in der Transportschicht: Zielportnummer
- in der Netzwerkschicht: Header-Wert in der Weiterleitungstabelle
- in der Sicherungsschicht: MAC-Adresse

Aufgabe 3

Web-Clients verwenden das HTTP Protokoll, um auf das eigene 'Mailbox'/Account auf einem Server zuzugreifen und somit eine E-Mail zu verfassen oder zu lesen. Die eigentliche E-Mail-Kommunikation wird, genauso wie bei den Mail-Clients, durch andere Protokolle gesteuert - z.B. SMTP (für das Verschicken von E-Mails) und POP3/IMAP (für das Empfangen/Aufrufen). Also benutzen Mail-Clients für den Zugriff zum 'Mailbox' meistens die POP3 und IMAP Protokolle.

Vorteile der Web-Clients:

- Einfachkeit: keine Installation und Einrichten nötig.
- Portabilität: ein Web-Client erlaubt es, das Account/Mailbox auf alle möglichen Geräten mit Internetzugriff aufzurufen, und nicht nur auf einem einzigen.

Vorteile der Mail-Clients:

- Lokalität: E-Mails werden auch auf dem eigenen (lokalen) Host gespeichert (POP3), was die Geschwindigkeit des Zugriffs erhöht, sowie das offline Lesen und Schreiben von E-Mails ermöglicht.
- Sicherheit: E-Mails befinden sich nicht nur auf einem Server, sondern auch lokal, was die Wahrscheinlichkeit, sie zu verlieren, erniedrigt. → Back-up

Aufgabe 4

Warteschlangenverzögerung hängt stark von Länge der Schlange ab, *Übertragungsverzögerung* hängt von seiner Geschwindigkeit und Paketlänge ab, *Ausarbeitungsverzögerung* hängt auch von seiner Geschwindigkeit und der Länge der physischen Leitung ab. Nur **Verarbeitungsverzögerung** kann sich verbessert werden. Algorithmus zur Verarbeitung kann mann immer weiter entwickeln um Zeitdauer zu optimieren.

Aufgabe 5

a) Welcher Host im Netzwerk wird durch diesen Angriff gestört oder sogar zum Absturz gebracht?

- (P stammt aus der) Transportschicht: Der Empfänger/End-Host, da erst bei ihm die Entkapselung passiert.
- Netzwerkschicht: Ebenfalls der Empfänger.
- Sicherungsschicht: Der erste Router auf dem Weg zum End-Host. Router entkapseln das Paket indem sie erstmal das Sicherungsschicht-Header des Senders entfernen und einen neuen hinzufügen. So würde das entkapselte Payload wiederum wie das ursprüngliche Paket aussehen, und der Router wird alles wiederholen, ohne irgendwas weiterleiten zu können.

Von welchem Host aus muss der Angreifer sein Paket verschicken, wenn er ein bestimmtes Ziel im Sinn hat?

- (P stammt aus der) Transportschicht: Von einem Sender, wenn das Ziel der Empfänger ist.
- Netzwerkschicht: Von einem Sender, wenn das Ziel der Empfänger ist.
- Sicherungsschicht: Von einem Sender, wenn das Ziel ein Router ist.

Aufgabe 6

Diese Antworten benutzen die Daten von Autoren (Fußnote 2, Seite 2 von `Wireshark_HTTP_v7.0.pdf`).

a) (File `http-ethereal-trace-1`) Frage:

4. *Status code* ist `200`.
5. Das HTML File ist zuletzt am `Dienstag, September 2003 05:29:00` modifiziert.
6. `73` Bytes wurden an Browser zurückgegeben.

b) (File `http-ethereal-trace-2`) Frage:

8. Nein, es gibt keine "IF-MODIFIED-SINCE" Zeile in der GET-Anfrage.
9. Es wird doch Inhalt des Files gegeben. Das sieht man bei der Zeile "Line-based text data..."

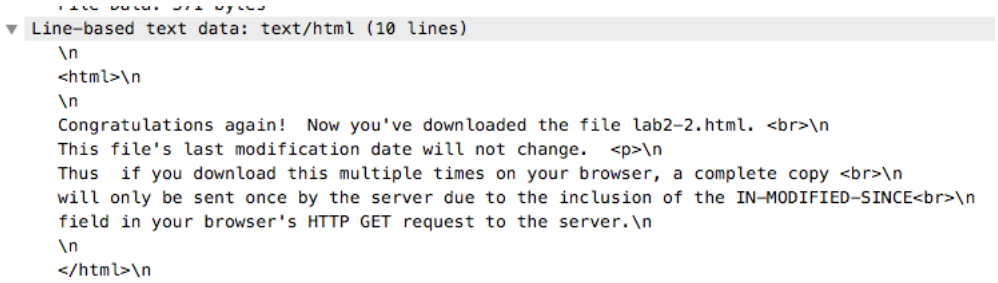

Figure 1: Inhalt

10. Es gibt die Zeile "IF-MODIFIED-SINCE", da steht der Datum, an dem das File zuletzt modifiziert wurde: `Tue, 23 Sep 2003 05:35:00 \r\n` . Dieser Datum steht auch bei der Zeile "Last-Modified" von der ersten HTTP Antwort des Servers (siehe 9.).

11. *Status Code* ist `304 Not Modified`. Der Server gibt keinen Inhalt des Files zurück, da der Browser schon den Inhalt hatte (Inhalt in Frage 9).

c) (File `http-ethereal-trace-3`) Frage:

15. Es gibt 4 Daten enthaltenen TCP-Segmenten, die gebraucht werden, zum Transport der einzigen HTTP Antwort und dem Text **Bill of Rights**.

- Anzahl der Payload-Bytes:
  - `0-1459`: 1460 Bytes
  - `1460-2919`: 1460 Bytes
  - `2920-4379`: 1460 Bytes
  - `4380-4815`: 436 Bytes

d)(File `http-ethereal-trace-4`) Frage:

16. Der Browser hat `3` HTTP GET Anfragen geschickt. Und zwar zu den folgenden Internet-Adressen:
  - /ethereal-labs/lab2-4.html HTTP 1.1
  - /catalog/images/pearson-logo-footer.gif HTTP 1.1
  - / kurose/cover.jpg HTTP 1.1

17. Die Images wurden aufeinanderfolgend heruntergeladen. Betrachten wir im Fenster bei der Spalte "Time", sehen wir dass die Zeitpünkte für die 2 Images nicht gleich sind. d.h. Sie könnten nicht parallel heruntergeladen werden (siehe No. 25 und 54).

Aufgabe 7

- Beschrieben wird eine Funktion zur Implementierung des *HTTP keep-alive* ohne Modifikation des Backend-Webservers. Dies wird zu *Anwendungsschicht* hinzugefügt.
- Diese Funktion wird dadurch implementiert, dass eine Zeile "Connection: Keep-Alive" zu dem HTTP-Header hinzugefügt wird und die Zeile "Connection: close" im existierenden Webserver hinzugefügt wird. Das Problem liegt daran, dass der TCP Proxy hier vor dem weiteren Transport des ganzen Textes verzögert werden muss, um eine TCP-Prüfsumme des Pakets wieder zu rechnen. Dies bringt Latenz zum Transport des Pakets. Um das zu lösen, wird es versucht die TCP-Prüfsumme unverändert zu halten, durch die Neuordnung des Wortes `Connection` zu *Cneonction*. Diese Neuordnung behaltet die Paketsgröße und auch die TCP-Prüfsumme, da `sum(ord(i) for i in "Connection") - sum(ord(i) for i in "Cneonction") = 0`.