TKN Telecommunication Networks Group

Praktikum
Rechnernetze und Verteilte Systeme

Block 7

— Packet-Trace-Analyse —

Termin: 21.-25.1.2019 & 28.1.-1.2.2019

Hinweis

Leider ist nicht auf allen im Praktikum genutzten Rechnern das Tool Wireshark installiert. Es gibt folgende Möglichkeiten das Tool dennoch zu benutzen:

- Wir empfehlen, dass Sie Wireshark auf Ihrem eigenen Rechner installieren und diesen zur Vorstellung mitbringen. Wireshark ist unter vielen Linux-Distributionen und Windows sowie Mac OSX verfügbar.
- Auf den Rechnern in den Pool-Räumen können Sie unter Windows die auf der Wireshark-Webseite verfügbare portable Version nutzen.

1 Theoretische Vorbereitungsaufgaben

Die folgenden Aufgaben sollen Ihnen helfen, sich auf den Vorbereitungstest vorzubereiten. Klären Sie bitte mögliche Fragen oder Unklarheiten unbedingt vor den ISIS-Testaten!

Da die Vorlesung die relevanten Themen für den Test noch nicht ausreichend behandelt hat (insbesondere Network Layer) wird der ISIS-Test dieses mal in der zweiten Woche stattfinden.[1] Nutzen Sie den ersten Termin daher für die Bearbeitung der praktischen Aufgaben und um sich mit dem Netzwerkanalyse-Tool *Wireshark* vertraut zu machen.

Aufgabe 1:
Sie haben in der Vorlesung wichtige Komponenten, aus denen das Internet zusammengesetzt ist, kennengelernt. Beantworten Sie in diesem Kontext die folgenden Fragen und machen Sie Sich klar, wo die Technologien jeweils verwendet werden:

a) Grenzen Sie die folgenden Begriffe gegeneinander ab. Auf welchem Ebene des ISO/OSI Modells arbeiten die jeweiligen Elemente?
   a) Repeater
   b) Hub
   c) Bridge
   d) Switch
   e) Router

[1] Es handelt sich hierbei um einen organisatorischen Fehler unsererseits, da die VL letztes Jahr früher endete und zum Ausgleich Zusatztermine hatte.

b) Was ist eine IP-Adresse, was eine MAC-Adresse?

c) Welches sind die speziellen IPv4-Adressen für Loopback und (limited) Broadcast?

d) Wie funktioniert ARP?

e) Nennen und erklären Sie die 4 Arten von Delay in einem Netz mit Paket-Vermittlung.

f) Was ist ein Autonomes System (AS)?

g) Was ist der Unterschied zwischen Peering und Transit?

h) Was ist der Unterschied zwischen Routing und Forwarding?

Aufgabe 2:
Beantworten Sie im Kontext von IP die folgenden Fragen:

a) Was sind Class A, B und C Netze? Welcher Teil der Adresse gehört jeweils zu Host bzw. Netzwerk?

b) Überprüfen Sie, ob die IPv4-Adresse `149.77.115.54` im Netzwerk `149.77.112.0` mit der Netzwerkmaske `255.255.252.0` liegt.

c) Nennen Sie zwei Ansätze, mit dem Problem der knappen Internet-Adressen umzugehen.

d) Wie hilft das heute verwendete Classless Inter-Domain Routing (CIDR), das Problem zu lösen?

Aufgabe 3:
Angenommen Sie greifen auf das Internet über einen "Router" zu. Beantworten Sie die folgenden Fragen:

a) Sie schalten Ihren Rechner an und erhalten automatisch eine IP-Adresse. Die dafür benutzte Technologie nennt sich DHCP. Wie sieht die initiale Anfrage nach einer Adresse aus?

b) Sie haben eine Adresse zugewiesen bekommen. Wie lange ist diese gültig?

c) Was macht Ihr Rechner, damit die Adresse länger gültig bleibt? Wann tut er dies?

d) Ihr "Router" stellt das Internet über NAT bereit. Was bedeutet das?

2 Präsenzaufgaben

Die folgenden Aufgaben werden im Termin unter Anleitung des Tutors durchgeführt.

Aufgabe 4:
Gegeben sei das Generatorpolynom $x^5+x^4+x^1+x^0$. Sie wollen den Bitstring 10010101011 verschicken. Welche CRC-Checksumme müssen Sie an den Bitstring anhängen? Wie wird auf Empfängerseite ein empfangenes Paket überprüft?

3 Praktische Aufgaben

Sie haben für diesen Block 2 Wochen Zeit die Aufgaben zu bearbeiten. Aufgrund des verschobenen ISIS-Test wird **keine** Rücksprache stattfinden.

Aufgabe 5:
*(Abgeleitet aus der Forensics Challenge 14 des Honeynet Project erstellt von Thomas Chopitea and Maximilian Hils)*Damit in einem Netzwerk unterschiedliche Systeme miteinander kommunizieren können, müssen mehrere Herausforderungen gelöst werden. Dazu gehört z.B. der Zugriff auf das physikalische Medium oder die Wegewahl durch ein komplexes Netzwerk. Die Lösung dieser Probleme wird durch entsprechende Protokolle realisiert.
Damit ein neues Protokoll nicht jedes Mal alle Aufgaben vollständig neu lösen muss, sind die Aufgaben in einem Netzwerk auf mehrere Schichten verteilt. In der Regel umfasst jedes Protokoll die Aufgaben einer Schicht und bietet über definierte Schnittstellen seine Dienste an die darüberliegende Schicht an. Daneben gibt es natürlich auch einige Ausnahmen, bei denen mehrere Schichten abdeckt werden.
In vorhergehenden Terminen haben Sie bereits das TCP und UDP benutzt, um den Transport von Daten zwischen zwei Prozessen über ein Netzwerk zu ermöglichen. Die einzelnen Datagramme der Transportprotokolle werden im Internet mit dem Internet Protocol (IP) transportiert. Beim Senden von TCP oder UDP Daten wird daher vor die UDP oder TCP-Steuerinformationen noch ein IP Header mit IP Steuerinformationen vorangestellt. Erst beim Empfänger werden diese Informationen in der jeweiligen Schicht wieder vollständig entfernt und ausgewertet, und die Daten werden an die nächste Schicht weitergegeben. Prinzipiell geschieht dies bei jedem einzelnen verwendeten Protokoll.
In diesem Termin soll das Verständnis für die einzelnen Protokolle und deren Funktionsweise vertieft werden. Dazu werden vorgegebene Mitschnitte von Paketübertragungen mit Hilfe von entsprechender Software analysiert. Nutzen Sie dafür den freien Network-Analyzer Wireshark[2]. Das Programm decodiert die Datenpakete von geläufigen Protokollen und stellt den Netzwerkverkehr in einem für Menschen lesbaren Format dar. Die einzelnen Funktionen der Software sind auf der zugehörigen Webseite dokumentiert.
Untersuchen Sie den auf der ISIS-Seite bereitgestellten Packet-Trace mit Wireshark.

a) Wie viele Pakete umfasst der Trace?

b) Wie groß sind die Pakete im Durchschnitt?

c) Notieren Sie alle im Trace auftauchenden MAC-Adressen.

d) Wie viele IP-Adressen tauchen im Trace auf?

e) Einige der auftauchenden MAC-Adressen sind mit IP-Adressen verknüpft. Notieren sie diese Verknüpfungen.

f) Bei welchem Anteil der Pakete wird das Internet Protocol (IP) auf der Vermittlungs/Netzwerkschicht (ISO/OSI Modell) verwendet?

g) Bei welchem Anteil der Pakete wird das Transmission Control Protocol (TCP) auf der Transportschicht verwendet?

h) Notieren Sie alle Protokolle der Applikationsschicht die TCP nutzen.

i) Notieren Sie alle Protokolle der Applikationsschicht die das User Datagram Protocol (UDP) nutzen.

j) Notieren sie alle auftauchenden Protokolle der Vermittlungs/Netzwerkschicht.

[2]Für gängige Betriebssysteme verfügbar unter `http://www.wireshark.org` oder unter Linux in der Regel über die Paketverwaltung

k) Notieren sie alle auftauchenden Protokolle der Sicherungsschicht.

l) Wie viele Domain Name System (DNS)-Abfragen fanden statt?

m) Wie viele IP-Pakete haben einen "Time-To-Live" (TTL) Wert größer als 200, mit genau 128 und mit genau 64? Versuchen sie, eine Erklärung für die gefundene Verteilung zu finden.

n) Untersuchen Sie das 16. Paket im Trace genauer:
   1. Wie groß ist der Ethernet-Header?
   2. Wie groß ist der IP-Header?
   3. Wie groß ist das IP-Datagram?
   4. Wie groß ist der TCP-Header?
   5. Wie groß ist das TCP-Segment?

o) Erstellen Sie ein Histogramm über die Länge der IP-Datagramme. Interpretieren Sie das Ergebnis.

p) Zwischen welchen IP-Adressen werden die meisten Bytes ausgetauscht? Erstellen Sie ein Histogramm über die Länge dieser IP-Datagramme. Interpretieren Sie das Ergebnis.

q) Zwischen welchen IP-Adressen werden die meisten Pakete ausgetauscht?

r) Bestand eine verschlüsselte Verbindung? Notieren Sie ggf. die beteiligten Hosts.

s) Wurde ein Web-Browser benutzt? Wenn ja, welche?

Tragen Sie Ihre Antworten in einen PDF-Dokument zusammen und reichen Sie dieses in einer Datei mit dem Namen **Block7a.TXXGYY.tar.gz** bis Sonntag nach dem zweiten Termin 23:55 Uhr auf ISIS ein.[3]

[3] Kleine Eselsbrücke für alle die immer noch unkomprimierte Tar-Archive abgeben: `tar -czvf` == "tar compress ze vu**ing files"

4 Vertiefungsaufgaben

Aufgabe 6:
Angenommen, Ihr Rechner befindet sich in einem Zustand, in dem er – bis auf seine eigene MAC-Adresse – über keine weiteren Information über das Netzwerk zu dem er sich gerade verbunden hat, verfügt.
Nun soll untersucht werden, welche Schritte nötig sind, bevor Ihr Rechner eine Verbindung zum Standardgateway und somit zum Internet aufbauen kann. Wir haben Ihnen dazu eine *weitere Trace-File* auf ISIS bereitgestellt.

a) Welches Protokoll ist dafür verantwortlich, dass Ihr Rechner eine IP-Adresse bekommt? Welche Pakete dieses Protokolls finden Sie in dem Trace-File? Was ist in diesen Paketen als Source- und Destination IP-Adresse eingetragen und warum? Welche Adresse möchte der Rechner gerne bekommen? Wird diesem Wunsch entsprochen? Wie lange ist die Adresse gültig? Was ist der zuständige DNS-Server?

b) Was sind die Pakete 1 und 4-7 und wozu dienen sie?

c) Nun verfügt der Rechner über alle nötigen Information, um Daten ins Internet zu schicken. Er ruft jetzt eine Webseite über eine URL auf. Nach welchem Hostnamen wird zunächst per DNS gefragt? Was ist die entsprechende Antwort des DNS-Servers?

d) Nun wird der HTTP-Server kontaktiert. Welche vollständige URL wird angefragt? Welcher Browser wird genutzt? Welche Server-Software antwortet? Handelt es sich um eine persistente Verbindung?

e) Nun wird eine zweite Verbindung aufgebaut. Welcher DNS-Name wird diesmal aufgelöst? Auf welchen Ports (Client/Server) wird die Verbindung aufgebaut? Welchem Protokoll entspricht das standardmäßig? Schauen Sie sich den Datenaustausch zwischen Server und Client an. Warum können Sie keine Sinnvollen Daten erkennen?

f) Mit dem Hintergrund, dass nicht nur Sie Ihren eigenen Netzwerkverkehr mitschneiden können, sondern auch jeder andere, der sich in Ihrem Netzwerk befindet, bzw. in Reichweite ihrer WLAN Karte aufhält, welche potentiellen Sicherheitsrisiken fallen Ihnen bei der Verwendung von Protokollen wie z.B. HTTP, FTP, SMTP, etc. ein?

Aufgabe 7:
Das Verfahren CSMA/CD erkennt Kollisionen und stoppt die Übertragung. Beschreiben Sie die Vorgehensweise Exponential Binary Backoff, mit der der nächste Sendeversuch für die kollidierten Partner festgelegt wird.

Aufgabe 8:
Wie groß ist in einem Ethernet-Netzwerk die Wahrscheinlichkeit, dass sich zwei Stationen erst nach der dritten Kollision nicht mehr gegenseitig bei der Übertragung stören, wenn sie anfangs gleichzeitig mit dem Senden beginnen wollen?

Aufgabe 9:
In der Vorlesung haben Sie Half-Duplexing und Full-Duplexing kennengelernt. Beantworten Sie die folgenden Fragen:

a) Erläutern Sie den Unterschied zwischen Half-Duplexing und Full-Duplexing.

b) Nennen Sie zwei Ansätze, Full-Duplex Kommunikation zu ermöglichen.

Aufgabe 10:
Nennen und erklären Sie 3 Aufgaben des Link-Layers.

Aufgabe 11:
Nennen und erklären Sie die 3 Klassen von MAC Protokollen.