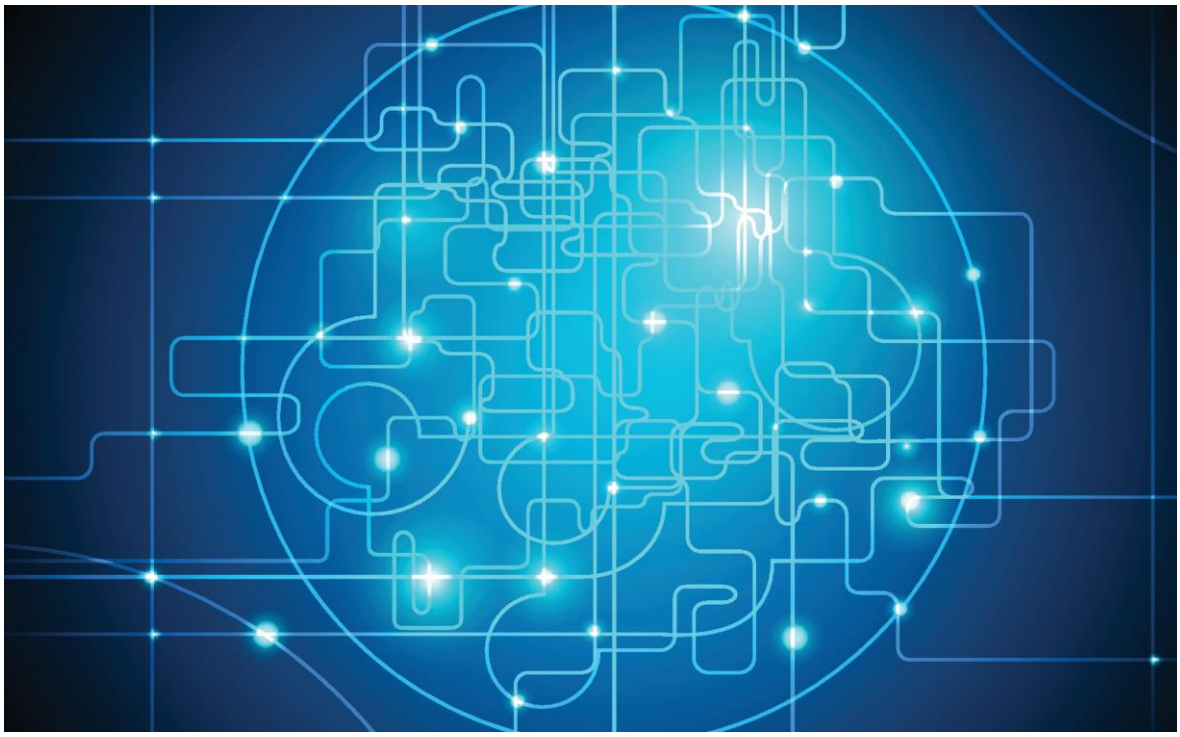
Erklärung und Analyse von WLAN – Sicherheitsverfahren
u.a. mit dem Tool Wireshark



Quelle: https://www.uibk.ac.at/newsroom/images/2016/vernetzung_1800x1080.jpg

Geschrieben von: Yannik Meier

Betreuer: Michel Liesegang, Felix Lauenroth

Lehrer: Herr Faßbender

Datum: 12.04.2018

Inhaltsverzeichnis

1. Abkürzungsverzeichnis

Virtuale Private Network	VPN
File Transfer Protocol	FTP
Network Attached Storage	NAS
Transmission Control Protocol	TCP
Internet Protocol	IP
Media Access Control	MAC
Local Area Network	LAN
Wide Area Network	WAN
Source-Adress-Table	SAT
Wireless Personal Area Network	WPAN
Wireless Wide Area Network	WWAN
Wireless Metropolitan Area Network	WMAN
Wireless Local Area Network	WLAN
Institute of Electrical and Electronics Engineers	IEEE
Wireless Ethernet Compatibility Alliance	WECA
Wired Equivalent Privacy	WEP
Wi-Fi Protected Access	WPA
Wi-Fi Protected Access 2	WPA2
Rivest Cipher 4	RC4
Familiennamen: Rivest, Shamir, Adleman	RSA
Advanced Encryption Standard	AES
Uniform Resource Locator	URL
Hypertext Transfer Protocol	http
Hypertext Transfer Protocol Secure	https
Domain Name System	DNS

2. Einleitung

Meine Facharbeit wollte ich in einem Fach schreiben, in dem ich Spaß am Unterricht habe und mich die Themen, die behandelt werden ansprechen. In meiner Freizeit bin ich ein sehr technikbegeisterter Mensch und probiere alles aus, was in irgendeiner Form mit Technik in Verbindung zu bringen ist. Vor einigen Jahren haben wir zu Hause einen neuen Router, eine FRITZ!Box, bekommen und einen schnelleren Internetanschluss. Nachdem ich mir angesehen habe was dieses Gerät alles an Möglichkeiten hat, weckte dies mein Interesse. Am Anfang habe ich mich durch das Menü geklickt und Berechtigungen verteilt, zum Beispiel wer das Internet nutzen darf. Danach habe ich mich mit Virtuale Private Network-Verbindungen (VPN - Verbindungen) beschäftigt, damit man immer eine sichere verschlüsselte Verbindung zu seinem Heimnetzwerk hat und auf den heimischen Router oder Drucker zugreifen kann. Mit den Diensten der FRITZ!Box war dies alles relativ leicht aufzubauen und zu nutzen. Als ich eine sichere Verbindung zu meinem Heimnetzwerk hatte und auf die Geräte in diesem zugreifen konnte, wollte ich mir zu Hause eine Festplatte einrichten, auf die ich von überall aus, mittels VPN und File Transfer Protocol (FTP) zugreifen kann. Ich nahm meine Festplatte und schloss diese an den Router, welcher die Festplatte als Network Attached Storage-Server (=NAS) einrichtete. Nun habe ich Benutzer hinzugefügt und Ordner verteilt, auf die ich aus dem Heimnetzwerk oder über VPN aus der ganzen Welt zugreifen konnte. Mein Interesse für Netzwerke ist seither sehr stark.

Mein zweiwöchiges Praktikum, welches ich in der Jahrgangsstufe 10 hatte und bei der Telekom in Bereich TeraStream (in der Entwicklung) absolvierte, verstärkte mein Interesse. Dort wurde ein neues Netz entwickelt, welches die Komplexität in Netzen deutlich senken soll. In dieser Zeit habe ich viel gelernt, zum Beispiel einiges über Netzwerkadressen und über den Vorgang, der während des Aufrufens einer Webseite geschieht. Bis zu diesem Zeitpunkt war mir gar nicht bewusst, was alles in dieser Sekunde passiert, wenn man eine Adresse eintippt und eine Webseite daraufhin angezeigt wird.

Diese zwei Ereignisse weckten mein Interesse für die Netzwerktechnik sehr und ich fand es faszinierend, was alles dahintersteckt. Schlussendlich wollte ich noch wissen wie man sich schützen kann, damit kein Dritter sehen kann, was man als Privatperson in seinem Netz macht. Aus diesem Grund habe ich mich für diesen Themenkomplex entschlossen.

Auf die Kooperation, zwischen dem Städtischen Gymnasium Rheinbach und der BWI GmbH mit Sitz in Meckenheim, hat mich mein Informatiklehrer Herr Faßbender aufmerksam gemacht

und den Kontakt hergestellt. Die Fachkenntnisse von Herr Liesegang und Herr Lauenroth, die für die BWI arbeiten, konnten ich für meine Facharbeit nutzen.

3. OSI-Schichtenmodell

Das OSI -Schichtenmodell (Open Systems Interconnection Model) ist ein Modell, welches die Kommunikation unter Rechner veranschaulichen und vereinfacht darstellen soll (siehe Anhang 8, Abbildung 1). Dieses Modell ist eine Veranschaulichung die nicht 1:1 dem entspricht, wie es in der Realität vorzufinden ist. Modelle sind immer gut, um ein Problem oder ein Verfahren vereinfacht zu erklären, jedoch sind sie nicht immer richtig anwendbar und genauso ist es bei diesem Modell auch.

Das OSI - Schichtenmodell besteht aus 7 Schichten (= Layer), die man sich anhand dieser Merksätze gut merken kann:

„Please Do Not Throw Sausage Pizza Away“[1] --> Layer 1 bis Layer 7 oder auch

„Alle Priester Saufen Trollinger Nach Der Predigt“[2] --> Layer 7 bis 1.

Nun beginne ich mit dem siebten Layer und arbeite mich bis auf den ersten herunter.

Der Layer sieben wird auch Application Layer (Anwendungsschicht) genannt. Hier kommunizieren zwei Applikationen miteinander und dabei werden die Dienste der unteren Schichten in Anspruch genommen. Dies wäre die Benutzeroberfläche, die der Endbenutzer sieht und in den jeweiligen Feldern seine Texte eingeben oder Knöpfe anklicken kann. In dem Layer sechs oder auch Presentation Layer (Darstellungsschicht) genannt, geht es, wie der Name schon sagt, um die Darstellung der Daten, also wie die Daten in den unterschiedlichen Betriebssystemen abgelegt werden. Es werden Kodierungsformen und Syntaxfestlegungen vereinbar, wenn zum Beispiel die vorhandenen, festgelegten Formate aus dem Betriebssystem nicht mit den ankommenden Formaten oder den Zeichensätzen (z.B.: ö,ó,ò,ø) übereinstimmen. Außerdem werden auf diesem Layer auch die Daten verschlüsselt. Der Sitzungslayer (Session Layer; Layer fünf) ist dafür verantwortlich, dass eine Session (= Sitzung) aufgebaut wird und diese auch während der ganzen Kommunikation bestehen bleibt. Diese Schicht kann man mit einem Telefonat vergleichen. Am Anfang wird überprüft, ob man überhaupt mit dem richtigen Partner verbunden ist. Danach werden ein paar Redewendungen ausgetauscht, damit man weiß mit wem überhaupt gesprochen wird. Sollten die ersten beiden Punkte positiv verlaufen sein und der richtige Partner ist auf der anderen Seite, so kann das Gespräch beginnen. Ist das Gespräch beendet, dann wird sich verabschiedet und der Hörer wird aufgelegt. Nun ist das

[1] siehe Fachwissen Netzwerktechnik von Berhard Hauser, Seite 77
[2] siehe Fachwissen Netzwerktechnik von Berhard Hauser, Seite 77

Gespräch (= Sitzung) beendet. Während des gesamten Gespräches bleibt die Verbindung die ganze Zeit bestehen. Genau so ist dies auch mit der Session. Der Layer vier ist die Transportschicht (Transport Layer). Diese Schicht transportiert die Daten und kontrolliert, ob diese auch richtig angekommen sind. Falls dies nicht der Fall ist werden die Daten erneut geschickt. Sind die Datenpakete zu groß und können nicht an einem Stück versendet werden, dann werden diese in kleinere Daten-Segmente aufgeteilt und durchnummeriert. Die Nummerierung ist sehr wichtig, weil der Empfänger die einzelnen Segmente wieder zu einem großen Datenpaket zusammensetzen muss. Des Weiteren werden auf dieser Schicht auch die Applikation und der Zielrechner adressiert. Port (=Schnittstelle) -Nummern werden hier auch vergeben. Der Layer drei ist die Netzwerkschicht (Network Layer), es wird die Adressierung der Daten-Segmente in das richtige Netzwerk übernommen und auch die Adressierung für den entsprechenden Zielrechner. Bei der Adressierung in einem Netzwerk gibt es zwei verschiedene Arten von Adressen. Zum einen sind dies die symbolischen und zum anderen sind dies die logischen Adressen. Diese werden entweder von dem Netzwerk automatisch zugeteilt oder von dem Administrator manuell vergeben. In den heutigen Transmission Control Protocol (=TCP) / Internet Protocol (=IP) Netzwerken werden die IP-Adressen (Internet-Protocol-Adressen) vergeben. In den alten IPX/SPX Netzwerken von Novell waren dies noch die IPX-Adressen. In dem vorletzten Layer zwei, der Datensicherungsschicht (Datalink Layer), wird die physikalische Adressierung (Media Access Control-Adressen), der einzelnen Rechner übernommen. Diese Media Access Control-Adressen (MAC-Adressen) wurden von dem Hersteller einprogrammiert und weltweit nur einmal vergeben. Die Datenpakete werden aus der darüberliegenden Schicht verpackt. Die Pakete werden in ein Frame (=Rahmen) gepackt, indem ein Header davorgesetzt wird. Ein Frame besteht aus einer Präambel, einer Ziel-MAC-Adresse, Quell-MAC-Adresse, einem Typ, Nutzdaten und einer FCS (Prüfsumme). Die Präambel ist zur Synchronisation der Empfänger und Sender verantwortlich und sie kündigt das Frame an. Die Prüfsumme wird aus dem gesamten Frame gebildet (ausgeschlossen der Präambel) und dient zur Überprüfung. Zu dem Frame hängt die Schicht noch einen Trailer (=Anhänger) hinter dran, der aus der Prüfsumme besteht. Zum Schluss werden die Daten noch zum Versenden aufbereitet. In Layer eins oder auch der Bitübertragungsschicht (Physical Layer) werden die vorbereiteten Daten aus Layer zwei über das jeweilige Medium versendet. Dabei werden bei Kupferleitungen elektrische Impulse übertragen und bei Lichtwellenleitern Lichtimpulse.

(Hauser 2013, Seite 77 - 79)

4. Netzwerkbestandteile

Ein Netzwerk besteht aus vielen verschiedenen Bestandteilen. Diese lassen sich in vier Komponenten gliedern: die Netzwerkendeinrichtung, die Netzwerkschnittstelle, das Übertragungsmedium und die Kopplungselemente. Auf die Netzwerkschnittstellen (zum Beispiel: Netzwerkkarten) und die Netzwerkendeinrichtungen (zum Beispiel: Computer, Drucker und Netzwerkfestplatten) werde ich nicht weiter fokussieren.
(Lüders und Sausel 2009, Seite 55)

4.1. Kopplungselemente

Möchte man zwei Geräte miteinander verbinden, kann dies sehr einfach mit einem Kabel erfolgen. Auf der einen Seite ist der Sender und auf der anderen Seite ist der Empfänger. Für eine Verbindung zwischen beiden müssen die Sender- und Empfängerleitungen gekreuzt werden, damit beide Geräte gleichzeitig senden und empfangen können. Diese Art von Kabel nennt man Crossover-Kabel.

Möchte man jedoch mehrere Endgeräte miteinander verbinden und dafür müssen größere Strecken zurückgelegt werden, dann benötigt man Kopplungsgeräte. In einem Netz sind Kopplungselemente keine passiven Komponenten, wie es zum Beispiel Kabel sind, sondern aktive. Sie sind elektronische Systeme und haben neben dem Aufbau der Verbindung auch noch weitere Aufgaben, wie zum Beispiel die Umsetzung, Verstärkung, Steuerung und Weiterleitung der Datenpakete.

Für die Verstärkung einer Verbindung werden Repeater genutzt, für die Steuerung zum Beispiel ein Router oder ein Switch, für die Umsetzung eine Bridge oder ein Medienkonverter und für die Weiterleitung ein Hub, ein Switch, ein Router oder auch eine Bridge. Im Folgenden werden lediglich die Kopplungselemente beschrieben, welche im Fokus der Facharbeit liegen.

(Lüders und Sausel 2009, Seite 74)

4.1.1. Router

Ein Router ist ein Wegfinder. Er sucht Wege und schickt Pakete über diese. Ein Router leitet seine Datenpakete mittels einer Adresse weiter und diese heißen in den meisten Fällen IP-

Adressen. Dem Router liegt eine sogenannte Routingtabelle vor, mit der er sehen kann über welchen Anschluss welches Netzwerk erreichbar ist. Zusätzlich ermitteln Router Metriken. Dies sind Daten über die Entfernung, die Kapazität der Übertragung, die Auslastung und die Fehlerrate. Er arbeitet auf dem Physical, dem Datalink und dem Network Layer. Dabei werden Datenpakete von dem Router auf dem dritten Layer überprüft und das hat zur Folge, dass Pakete ohne eine Adresse nicht weitergeleitet werden können. Einem Switch oder einer Bridge würde dies nichts ausmachen, da sie nur auf den ersten beiden Layern arbeiten. Router besitzen eine Netzwerkschnittstelle mit einer MAC-Adresse und sind dadurch nicht transparent. Außerdem haben sie auch zwei Schnittstellen, bei der mindestens eine für das Local Area Network (LAN) und eine für das Wide Area Network (WAN) zuständig sind. Beide sind voneinander abgeschirmt. Es gibt auch noch andere Netzwerktypen, die anhand dieser Grafik leicht zu verstehen sind (siehe Anhang 8, Abbildung 2).

(Lüders und Sausel 2009, Seite 80)

4.1.2. Hub

Ein Hub ist dafür da, um aus einem Anschluss mehrere zu machen. Hat man nur einen Netzwerkanschluss, aber mehrere Geräte, die man anschließen möchte, so kann man sich einen Hub nehmen, welcher ganz vereinfacht gesagt eine Mehrfachsteckdose ist. Natürlich ist das nicht ganz richtig, aber das Prinzip ist gleich. Die Mehrfachsteckdose ermöglicht es aus einer Steckdose mehrere zu machen und somit auch mehr Endgeräte anzuschließen. Beim Hub ist dies auch so. Er verteilt die eingehenden Signale an seine Anschlüsse (Ports) und die Netzwerkkarten des Endgerätes filtern die Daten letztendlich heraus. Ein Hub kann auch als Multi-Port-Repeater bezeichnet werden. Zusätzlich verstärkt ein Hub die Signale. Somit arbeitet er genau wie ein Repeater auf dem Physical Layer des OSI-Modells. Der Nachteil an einem Hub sind die Kollisionsdomänen.

Die Signale werden bei einem Hub direkt über einen Bus geleitet und dadurch entsteht die Gefahr von Kollisionen. Wenn zum Beispiel an Port 3 und Port 5 zwei Geräte gleichzeitig etwas senden besteht die Gefahr, dass diese Datenpakete kollidieren. Dabei gehen diese gegebenenfalls verloren. Umso mehr Geräte angeschlossen sind, desto höher ist die Wahrscheinlichkeit, dass Kollisionen auftreten können. Der Bereich in einem Netz, wo dies passieren kann nennt man Kollisionsdomäne. Es kann auch passieren, dass die Signallaufzeiten so lang sind, dass die Kollisionen nicht erkannt werden. Dies führt zu großen Problemen in der Datenübertragung. Wegen der großen Gefahr von Kollisionen bei Hubs werden diese

heutzutage kaum noch verwendet und sind nur noch in alten Netzen oder bei der Netzanalyse auffindbar. Aus diesem Grund werden dafür beispielsweise Switches verwendet.

(Lüders und Sausel 2009, Seite 75)

4.1.3. Switch

Zu den Kopplungselementen gehört auch ein Switch und dieser ist in sehr vielen Netzwerken aufzufinden. Sie arbeiten meistens in dem OSI-Modell auf der ersten Schicht, aber einige auch auf der zweiten. Genau wie ein Hub macht auch der Switch aus einem Anschluss mehrere. Das Lenkungsprinzip ist bei einem Switch komplexer und sicherer als bei einem Hub. Wird eine Netzwerkkomponente (PC oder Laptop), über ein entsprechendes Kabel, an einen Port (=Anschluss, Steckplatz) angeschlossen, so erkennt das der Switch und stellt einen Zusammenhang zwischen dem Port und der MAC-Adresse her. Diese Daten werden in eine Weiterleitungstabelle (Source-Adress-Table = SAT) eingetragen. Der große Vorteil eines Switches, gegenüber einem Hub ist, dass auch parallel Verbindungen aufgebaut werden können. Dies wird dadurch ermöglicht, weil für jeden Port ein eigenes Segment im Netz (umgangssprachlich: Teilnetz) erstellt wird und durch die Zuordnung von MAC-Adresse und Port, für jeden Port eine eigene Kollisionsdomäne erstellt wird. Die Datenkollision innerhalb eines Segmentes ist nun unmöglich. Des Weiteren gibt es in Switches zwei verschiedene Arten der Datenweiterleitung. Das eine heißt Store-and-Forward und das andere Cut-Through Verfahren, auf die ich nicht detailliert eingehen werde.

(Lüders und Sausel 2009, Seite 77 - 79)

Zusammenfassend lässt sich sagen, dass das Store-and-Forward Verfahren das sichere der beiden ist, aber etwas langsamer arbeitet. Das Cut-Through Verfahren ist viel schneller, dafür nicht so sicher und kann auch beschädigte Dateien weiterleiten.

(Hauser 2013, Seite 137-138)

4.2. Übertragungsmedium

4.2.1. Funknetze

In Netzwerken gibt es verschiedene Techniken für die leitungsungebundenen Übertragungen. Es gibt die ungerichtete Ausbreitung, die gerichtete Ausbreitung, welche eine Punkt zu Punkt

Verbindung ist und eine optische Übertragung, die meistens Infrarotlicht verwendet, aber auch aus elektromagnetischen Signalen bestehen kann. Im Folgenden werde ich die einzelnen Technologien erklären.

Zu den Wireless Personal Area Networks (=WPAN) Technologien gehören, die die sich auf den kleinsten, räumlichen Bereich beschränken. Zu WPAN gehört ZigBee, dass zum Beispiel bei Haushaltsgeräten verwendet wird und in einem Umkreis von 10 - 100 Metern empfangen werden kann. Die Vorteile dieser Verbindung ist, dass sie eine sehr geringe Reaktionszeit hat und dadurch Echtzeitanwendungen ermöglicht. Die Datenübertragungsgeschwindigkeit beträgt dabei lediglich 250 kbit/s. Eine weitere WPAN Technologie ist Bluetooth. Dieses ist heute in nahezu jedem Smartphone enthalten. Es gibt noch mehr WPAN Übertragungstechnologien, jedoch werden diese hier nicht weiter ausgeführt.

Eine andere Technologie ist Wireless Wide Area Network (=WWAN). Diese Technologie wird für Weitverkehrsnetze verwendet. Die Wi-Max-Technologie ist für den ungerichteten Betrieb entwickelt worden und wird in Mobilfunknetzen verwendet. Wireless Metropolitan Area Network (=WMAN) ist, neben WWAN ein anders Verfahren, für die Verbindung von Netzknoten innerhalb einer Stadt oder einer Region.

Die vierte und letzte Technologie ist Wireless Local Area Network (=WLAN). Dies ist ein lokales Netzwerk, dass über Funkübertragung kommuniziert. WLAN wird häufig mit Wi-Fi gleichgesetzt, aber die Standards von der Wi-Fi Alliance wurden basierend auf dem IEEE-802.11 Standards durchgesetzt. Das Institute of Electrical and Electronics Engineers (=IEEE) ist ein Verband, der Standards (≈Regeln) für bestimmte Technologien setzt. Also darf man die zwei Begriffe nicht gleichsetzten. 1999 wurde die Wi-Fi Alliance unter dem Namen Wireless Ethernet Compatibility Allaince (=WECA) gegründet. Wi-Fi hat eigentlich keine Bedeutung, wird aber oft mit Wireless Fidelity in Verbindung gebracht. Einige Merkmale des IEEE-802.11 Standards sind zum Beispiel, dass die Reichweite bis zu 100 Meter ist. Es gibt zwei Frequenzbereiche. Frequenzbereich 1 ist von 2,4 GHz bis 2,4835 GHz und Frequenzbereich 2 ist von 5,15 GHz bis 5,725 GHz. Die Anzahl der überlappungsfreien Kanäle ist auch festgelegt. Im Frequenzbereich 1 liegt diese bei 3 und im Frequenzbereich 2 liegt diese bei 19. Die maximale Strahlungsleistung liegt im Frequenzbereich 1 bei 100mW und in FB2 bei 500mW, diese dürfen auch unter keinen Umständen überschritten werden. Meistens liegt diese, aber nur zwischen 20 - 40mW. Die Bandbreite eines WLAN -Kanals ist 20 MHz, die Datenübertragungsgeschwindigkeit liegt bei 54 Mbit/s und in einer weiterentwickelten Form bei 300 Mbit/s. Man muss aber dazu sagen, dass die tatsächliche Übertragungsgeschwindigkeit

geringer ausfällt, weil sich alle Geräte den Up- und den Downstream teilen müssen. Zu dem Upstream gehören die Daten, die aus dem heimischen Netzwerk herausgeschickt werden und zu dem Downstream die, die empfangen werden. Die Verschlüsselung ist durch Wired Equivalent Privacy (=WEP), Wi-Fi Protected Access (=WPA) und Wi-Fi Protected Access 2 (=WPA2) gewährleistet. Die sicherste Verschlüsselung ist WPA2, denn die anderen beiden Verschlüsselungstypen besitzen Schwachstellen (siehe Kapitel 5.3). Die Vorteile dieses Standards sind, dass der Frequenzbereich des WLANs für jedermann frei nutzbar und dies ohne Lizenz möglich ist. Außerdem werden in einem WLAN die gleichen Adressierungen verwendet, wie es auch bei LAN der Fall ist. Obwohl eine andere Übertragungstechnik eingesetzt wird, ist die Interkonnektivität nicht eingeschränkt, also die Verbindung von einem Rechner und einem Netzwerk. Unabhängig von dem Standard ist ein WLAN in zwei verschiedenen Betriebsarten möglich. Einmal ist das der Ad-hoc-Modus, bei dem die einzelnen Stationen direkt miteinander kommunizieren. Dies ist nur bei einer sehr geringen Anzahl von Stationen geeignet und die Weiterleitung von Datenpaketen ist nicht problemlos möglich. Im Infrastrukturmodus hingegen kommunizieren alle Stationen über einen zentralen Accesspoint, welcher die Kommunikation der einzelnen Clients (=Endgeräte) koordiniert. Der Accesspoint wird per LAN Kabel angeschlossen und somit können WLAN und LAN problemlos miteinander verbunden werden. Es gibt aber auch einige negative Kritikpunkte am WLAN. Die Frequenzen des WLANs liegen im Mikrowellenbereich und eine Erwärmung des Gewebes ist nicht auszuschließen und damit auch nicht die gesundheitlichen Gefahren. Durch die maximalen Strahlungsleistungen der Funkstellen werden die WLANs nicht als gesundheitsschädlich angesehen, denn die gesetzlichen Grenzwerte werden eingehalten. Die Auswirkungen auf den Körper sind jedoch noch nicht vollständig erforscht.

(Lüders und Sausel 2009, Seite 71-73)

5. Absicherungsmaßnahmen WLAN

5.1. Allgemeine Absicherungsmaßnahmen

In einem WLAN ist es immer wichtig, dass man von außen nicht auf die interne Kommunikation zugreifen kann. Würde der Angreifer Zugriff auf den Router erhalten, über den alles gesteuert wird, dann kann er große Schäden anrichten. Zum Beispiel kann er Einstellungen ändern und der Internetzugang ausschalten. Außerdem kann er den Internetanschluss für DoS (Denial-of Service) -Attacken missbrauchen. DoS-Attacken sind Angriffe, bei denen das Netzwerk überlastet wird. Bei zu vielen Anfragen kann dies der Fall sein. Die Telefonleitung kann auch verwendet werden, um Unmengen an Kosten zu verursachen. Es gibt einfache Maßnahmen, die die Sicherheit des Netzwerkes verbessern können. Der Router hat eine Bedienoberfläche, die durch ein Passwort geschützt ist. Dieses sollte man, nach dem ersten anmelden, austauschen und durch ein neues, sichereres Passwort ersetzen. Wie das funktioniert wird in Kapitel 4.2.1 beschrieben. Die Verwendung von https, anstatt http im Browser ist stets zu empfehlen. Warum dies so ist, wird in Kapitel 5.3 erklärt. Ein anderer sehr wichtiger Punkt ist, dass die Firmware des Routers stets aktuell gehalten werden muss, um die maximale Sicherheit zu garantieren. Über diese Firmwareupdates werden unter anderem Sicherheitslücken geschlossen, denn eine lückenhafte Software möchte man nicht auf dem Router betreiben. Bei der Anmeldung auf den Router erscheint zuerst immer eine Seite, auf der man das Passwort eingeben muss. Sollte auf dieser Seite ein Bild angezeigt werden, auf dem Informationen jeglicher Art zu dem benutzten Router stehen, dann ist es ratsam dieses Bild auszutauschen. Man möchte dem Angreifer den Angriff schließlich nicht erleichtern. Dienste, die der Router bietet, welche aber nicht genutzt werden, sollte man deaktivieren. Darunter fällt auch das WLAN, denn dieses ist im aktivierten Zustand leichter anzugreifen, als wenn es deaktiviert ist. Es gibt Router, die eine Funktion besitzen, ihr Heimnetzwerk von außerhalb zu konfigurieren. Diese Funktion nennt man Fernzugriff und sollte generell ausgestellt werden.

(BSIFB - Sicherheitstipps)

Sollte es sich bei ihrem Router auch über einen WLAN Router handeln, dann sollten zusätzlich folgende Hinweise beachtet werden. Wenn zu anfangs der Access Point konfiguriert wird, sollte man diesen nicht über eine drahtlose Verbindung einrichten, sondern über ein Kabel. Dadurch

wird das Risiko vermindert, dass andere Personen Zugriff zu dem Netzwerk bekommen. Die SSID (Service Set Identifier) sollte auch geändert werden und mit dieser sollte nicht der Wohnort oder der eigene Name in Verbindung gebracht werden können. Im Idealfall vergibt man den Namen so, dass man nicht darauf kommt würden, wem das Netz gehört. Die SSID ist nichts anders als der Name, der angezeigt wird, wenn man das WLAN sucht. Ein sehr wichtiger Punkt bei einen WLAN ist, dass man auch für die richtige Verschlüsselung sorgt. Die aktuellste und sicherste Verschlüsselung ist WPA2, trotzdem muss ein sicheres Passwort gewählt werden. Sollte man es nicht für nötig halten sein WLAN zu verschlüsseln, dann kann ein Angreifer auf alle Daten zugreifen und große Schäden und Kosten verursachen. Es gibt auch noch andere Verschlüsselungen, jedoch haben diese einige Schwachstellen oder bieten nicht die gleichstarke Sicherheit, wie WPA2. Zusätzlich gibt es an vielen Routern eine WPS (Wi-Fi Protected Setup) Taste, die es ermöglicht eine Verbindung zum WLAN aufzubauen. Es muss ein Code aus Zahlen eingegeben werden, doch es lässt sich berechnen, wie die Reihenfolge der Zahlen ist und somit wird dem Einbrecher ermöglicht einzudringen.

(BSIFB - Sicherheitstipps - Sicherheitstipps zum privaten WLAN-Einsatz)

5.2. Sicheres Passwort

Immer wenn es um Verschlüsselungen geht braucht man ein Passwort, mit dem die verschlüsselten Dateien entschlüsselt werden können oder wenn man sich auf einer Website ein Konto angelegt hat, braucht man auch dort ein Passwort, mit dem man nur selbst Einsicht auf die Inhalte hat. Man möchte ja verhindern, dass sich jemand anderes Zugriff verschafft und somit an Inhalte gelangt, die ihn eigentlich nichts angehen. Immer nur der Benutzer, der das Konto oder eine Verschlüsselung auf bestimmte Inhalte (Netzwerke, Dateien) erstellt hat, soll auch als einziger mit seinem Passwort die Möglichkeit haben, diese freizugeben oder zu bearbeiten. Also ist es immer sehr wichtig sich mit der Auswahl eines Passwortes Zeit zu nehmen und nicht zu einfache Passwörter zu wählen, damit es für den Angreifer nicht zu leicht ist, Zugriff zu erlangen. Eine sehr beliebte Methode, um den Zugriff zu erlangen, ist der Brute-Force-Angriff. Hierbei generiert der Angreifer alle möglichen Passwörter und versucht so über diesen Rateprozess an das richtige Passwort zu gelangen. Je nach Komplexität des Passwortes kann dies viel zu lange dauern und die Methode ist nicht mehr sehr effizient. Es gibt viele

Eselsbrücken, mit denen man sich auf eine sehr einfache Art und Weise leicht zu merkende, aber schwierige Passwörter erstellen kann.

Nun folgen einige Tricks, wie man sich ein gutes Passwort erstellen und merken kann:

Bei Passwörtern sollte man immer darauf achten, dass sie nicht zu kurz sind und mindestens aus acht Buchstaben und Ziffern bestehen. Wenn das Passwort länger ist, ist es auch sicherer. (Bei den Verschlüsselungstypen von einen WLAN Netzwerk ist dies nicht der Fall dort sollte ein Kennwort von mindestens zwanzig Zeichen verwendet werden.) Außerdem ist es sehr schlecht, wenn auf unterschiedlichen Websites (Anwendungen, Diensten) das gleiche Passwort verwendet wird, denn hat der Angreifer das eine Passwort herausgefunden, probiert er dies zuerst auf anderen Webseiten aus. Bei dem Benutzernamen wird oft die E-Mail-Adresse verwendet und diese ist häufig dieselbe und somit leicht herauszufinden. Zu Anfangs sei schon einmal gesagt, dass bei der Auswahl der Passwörter der Fantasie keine gesetzt sind. Je kreativer und einfallsreicher ein Passwort gestaltet ist, desto schwieriger ist es zu knacken. Eine Methode, die man für ein gutes Passwort nehmen könnte wäre zum Beispiel folgende:

1. Man denkt sich einen beliebigen Satz aus, der nicht einmal einen Sinn ergeben muss. Die einzige Voraussetzung ist, dass man sich den Satz gut merken kann. Zum Beispiel: Meine Mutter backt heute drei tolle Computer und einen großen Fernsehturm.

2. Nun würde man sich immer den ersten Buchstaben des Wortes nehmen und daraus ein Passwort zusammensetzen: MMbhdtCuegF

3. Befinden sich in einem Kennwort mehrere Sonderzeichen, so ist dieses wieder ein Stück komplizierter. Also könnte man zum Beispiel aus dem ´und´ im Ausgangssatz ein & machen und aus dem Wort drei eine Zahl: MMbh3tC&egF

Das wäre zum Beispiel eine sehr einfachere Methode um ein schwieriges Passwort zu entwickeln. Man kann die Vorgehensweise der Methode auch noch weiterführen, um ein noch schwierigeres Passwort zu erstellen. Die Vorteile bei der Generierung sind, dass bei Passwörtern meistens alle möglichen Zeichen der Tastatur zur Verfügung stehen. Dadurch hat man sehr viele Variationsmöglichkeiten zum Beispiel zwischen Groß- und Kleinschreibung, Zahlen, Leerzeichen, Sonderzeichen (Klammern, Operatoren) und vielen mehr. Ist man jedoch eine Person, die sehr viel durch unterschiedliche Länder reist und immer andere PC oder Endgeräte verwendet, sollte darauf achten, dass die Zeichen, die verwendet werden, auch in der anderen Sprache auf der Tastatur verfügbar sind. Einige Kennwörter, die man niemals verwenden sollte, wären zum Beispiel Namen von Eltern, Freunden oder Haustieren, sowie den Geburtstag oder irgendwelche persönlichen Sachen, die andere über einen wissen könnten.

(BSIFB - Passwörter 2018)

Neben der Erstellung eines sicheren Passwortes sollte man auch die Passwörter regelmäßig ändern, um eine höhere Sicherheit zu gewährleisten.

(BSIFB - Umgang mit Passwörtern 2018)

5.3. Verschlüsselungstypen

In Funknetzen ist Sicherheit eines der obersten Gebote. Sie ist bei Funknetzen noch ein bisschen Wichtiger, denn es wird keinen physikalischen Kontakt zur Hardware benötigt. Zum Beispiel muss nicht in ein Haus oder Gebäude eingebrochen werden. Um Unbefugten den Eintritt zu verweigern, gibt es viele verschiedene Möglichkeiten. Es gibt ein EAP-Verfahren (Extensible Authentication Protocol), dass nur authentisierten (=bekannten) Nutzern den Zugriff gewährt. Auf dieses Prinzip werde ich aber nicht weiter eingehen. Andere Methoden sind die Verschlüsselungstypen, wie WEP, WPA und WPA2. Sie verwenden die Verschlüsselungsmechanismen River Cipher 4 (=RC4), RSA (= Rivest, Shamir, Adleman) und Advanced Encryption Standard (=AES), die ich aber nicht im mitsamt ihrem Algorithmus erklärt werden. Bei ihnen werden die Daten verschlüsselt und können nicht von unbefugten Personen mitgelesen werden. Jedoch gelten WEP und WPA als unsicher und WPA2 ist derzeit der sicherste Verschlüsselungstyp. Also sollte in jedem Router immer WPA2 eingestellt sein, um die maximale, momentan mögliche Sicherheit zu gewährleisten.

(Spitz et al. 2011, Seite 194)

5.3.1. WEP

WEP ist die Abkürzung für Wired Equivalent Privacy und der Vorgänger von WPA und WPA2. Die WEP - Verschlüsselung wurde für die Absicherung von einem WLAN verwendet. Bei WEP wird der RC4-Algorithmus eingesetzt.

In der WEP Verschlüsselung befinden sich einige Schwachstellen, die sich sehr leicht ausnutzen lassen. Auf YouTube bekommt man schon in einem sechs minütigen Video gezeigt, wie man mit einer bestimmten Anwendung eine WEP Verschlüsselung innerhalb von zehn Minuten oder weniger umgehen kann und das Passwort herausfindet. Der eingesetzte RC4-Algorithmus wurde von Ronals L. Rivest entwickelt und 1994 anonym veröffentlicht. Er entwickelte des Algorithmus für die RSA Security. Der RC4 Algorithmus arbeitet auf dem

Physical Layer und liefert einen Strom an Zahlen, deshalb wird der RC4-Algorithmus auch Stromchiffre genannt. Standardisiert wird er nicht, aber RC4 wurde in vielen standardisierten Protokollen verwendet, wie zum Beispiel in SSH (=secure shell), SSL (=secure socket layer) und halt auch WEP. Zusätzlich besteht die WEP-Verschlüsselung noch aus ein Initialisierungsvektor (=IV), einem geheimen Schlüssel K und einer weiteren Verschlüsselung namens XOR, die alle zusammen den verschlüsselten Text ergeben. Jedoch werde ich nicht im Detail darauf eingehen.

Es machte sich schnell bewegbar, dass in der WEP-Verschlüsselung einige Schwachstellen enthalten waren. Durch diese Schwachstellen war es relativ leicht Zugang zu dem geheimen Schlüssel zu erlangen. Ein Angriffspunkt wäre zum Beispiel, dass man den mit einem RC4 erzeugten, verschlüsselten Text nicht zweimal verschlüsseln darf, denn sonst kann man den Ursprungstext wiederherstellen.

Zusammenfassend kann man sagen, dass WEP anfangs ein einfallsreicher und guter Verschlüsselungsalgorithmus war, der schnell Schwachstellen aufwies. Diese wurden zwar versucht zu beheben, jedoch sind die Schwachstellen nicht verschwunden. WEP wurde trotzdem noch sehr lange verwendet.

(Spitz et al. 2011, Seite 68 bis 69, Seite 196 bis 198)

5.3.2. WPA/WPA2

Wie auch WEP sind auch WPA (Wireless fidelity Protected Access) und WPA 2 (Wireless fidelity Protected Access 2) Verschlüsselungstypen für WLAN Netze. WPA und WPA2 sind jedoch weiterentwickelte Verfahren von WEP. Auch WPA basiert, genau wie WEP, auf dem RC4 - Algorithmus, aber er enthält noch eine Erweiterung namens TKIP (Temporal Key Integrity Protocol), das durch einige Verfahren für mehr Sicherheit sorgen soll. Zum einen wird durch einen MIC (Message Integrity Code) verhindert, das falsche Nachrichten hinzugefügt werden können. Außerdem wird durch einen von TKIP „definierte Schlüsselmix verändert den Secret Key pro Paket und bezieht die MAC-Adresse des jeweiligen Geräts in den Secret Key mit ein“ (siehe Kryptographie und IT-Sicherheit von Stephan Spitz, Michael Pramateftakis und Joachim Swoboda, Seite 198). Dadurch verwenden alle Teilnehmer zu jedem Zeitpunkt andere Schlüssel. Ein erweiterter Initialisierungsvektor beseitigt das Problem, dass der öffentlich übermittelte Initialisierungsvektor doppelt mit einem Schlüssel verwendet wird. TKIP weist klare Verbesserungen gegenüber WEP auf. Jedoch beschränkt sich WPA vorerst nur auf Änderungen der Schlüsselerzeugung und der RC4 Algorithmus wird weiterhin als

Verschlüsselung verwendet. Ein Nachteil an TKIP war, dass es Performance Probleme hatte, weil die Netzwerkkarte den MIC berechnen musste und dies sehr viel Rechenleistung brauchte. Im Jahre 2004 wurde die Erweiterung von WPA auf WPA2 angekündigt und WPA2 wurde mit dem vollständigen IEEE 802.11i Standard vorgestellt. Zusätzlich hatte es auch noch AES (Advanced Encryption Standard) als Verschlüsselung mit dabei.

Bei allen Verschlüsselungstypen muss entweder ein PSK (Pre-Shared-Key) zu Beginn konfiguriert werden oder man nutzt zur Authentisierung das EAP-Verfahren. In kleineren Netzwerken wird dies meistens nicht verwendet, weil man dafür einen Authentisierungsserver braucht, um die Daten zu verwalten.

(Spitz et al. 2011, S. 198)

5.3.2.1. AES

AES ist die Abkürzung von Advanced Encryption Standard und wir in WPA2 verwendet. Die AES Verschlüsselung musste entwickelt werden, da 1997 schon vorhersehbar war, dass der Vorgänger DES (Data Encryption Standard) zu schwach wird. Durch die steigende Rechenpower der PCs konnte man einen 56 - Bit Schlüssel, der 1998 mit einem Brute-Force-Angriff innerhalb von 56 Stunden entschlüsselt werden konnte, 1999 in nur noch 22 Stunden entschlüsseln. 1997 suchte das NIST (National Institute of Standard and Technology) Vorschläge für den Advanced Encryption Standard. Ein Jahr später kamen 11 Vorschläge herein und diese mussten sich einer weltweiten Prüfung unterziehen. Im Jahr 2000 entschied man sich für den Rijndael - Algorithmus, der von Daemen und Rijmen aus Belgien eingereicht wurde.

Der AES ist eine symmetrische Block-Chiffre, beinhaltet einen Schlüssel K und hat eine Blocklänge von 128 Bit. Außerdem ist er ein sehr schneller Algorithmus.

(Spitz et al. 2011, Seite 81)

6. Analyse mit Wireshark

6.1. Was ist Wireshark

Wireshark ist ein kostenloses Programm mit dem man den Netzwerkverkehr auswerten kann.

(Wireshark · Go Deep. 2018)

In jedem Netzwerk, egal ob dies auf der Arbeit oder zu Hause im eigenem Netzwerk ist, müssen Geräte untereinander kommunizieren, um zum Beispiel Nachrichten auszutauschen oder Internetseiten aufzurufen. Mit Wireshark kann man die gesamte Netzwerkkommunikation bis ins kleinste Detail untersuchen und somit den ganzen Verkehr, der in einem Netzwerk passiert, auswerten. Dadurch kann man alles überwachen und kontrollieren, aber auch Fehleranalyse betreiben und das Netz verbessern oder wiederherstellen. Wireshark wird auch sehr häufig als Sniffer (=Schnüffler) bezeichnet, da es die Netzwerkkommunikation mitschneiden und analysieren kann. Das Programm ist besonders dafür geeignet, wenn man wissen möchte welche Protokolle in einem Netz verwendet werden, wie stark das eigene Netz ausgelastet ist oder welche Datenpakete von wem versendet und von wem empfangen wurden.

Bevor man Wireshark in einem Netz einsetzt, muss man sich darüber im Klaren sein, ob man in dem verbundenen Netzwerk überhaupt Datenpakete analysieren darf. Im heimischen Netzwerk sollte dies kein Problem sein, jedoch sieht die Verwendung von Wireshark im Netzwerk des Unternehmens anders aus. Bevor man hier mit der Analyse beginnt sollte man sich von der rechtlichen Seite her absichern, um nicht gegen bestimmte Auflagen zu verstoßen.

(Baumeister et al. 2016)

Nachdem man Wireshark gestartet hat wird man zuerst gefragt, über welche Schnittstelle man die Daten mitschneiden möchte. Einige Beispiele wären: Bluetooth, Ethernet oder WLAN. Neben den einzelnen Auswahlmöglichkeiten der Schnittstellen wird auch ein kleiner Graph angezeigt, der immer ausschlägt, wenn über die jeweilige Schnittstelle etwas gesendet oder empfangen wird. In meinem Fall war ich über das WLAN mit meinem Router verbunden, also habe ich die Schnittstelle für WLAN ausgewählt. Wäre man zum Beispiel über ein LAN-Kabel mit dem Router verbunden, dann würde man in diesem Fall Ethernet auswählen. Es sollte auch ein Ausschlag im Graphen sichtbar sein. Hat man die richtige Schnittstelle ausgewählt, wird sofort mit der Aufzeichnung des Datenverkehrs angefangen.

Im Folgenden stelle ich die wesentlichen Funktionen des Programmes vor, die ich hauptsächlich verwendet habe. Um die Datenaufzeichnung zu beenden, verwendet man in der oberen, linken Ecke einen roten Knopf. Danach hat man die Möglichkeit die Aufzeichnung abzuspeichern oder eine neue zu starten, indem man auf das blaue Symbol drückt, welches sich links neben dem roten Knopf befindet. Unter der Menüleiste befindet sich eine Zeile, in der man Filter eintragen kann, um unwichtige Dinge heraus zu sortieren. Zum Beispiel kann man nach bestimmten Schlagwörter, nach Protokollen, nach Adressen und nach vielem mehr suchen. Unter der Filterleiste kommt das wichtigste Feld, weil dort alle Datenverkehrsströme angezeigt werden. Es gibt mehrere Spalten, denen einzelne Kategorien zugeordnet sind.

Die Kategorien sind:

No. --> ist die Abkürzung für Nummer. Jedem Datenpaket, ab Beginn der Aufzeichnung, wird eine Nummer vergeben die zeitlich Sortiert sind.

Time --> ist die Zeit, die nach dem Start der Aufzeichnung mitläuft.

Source --> ist die Quelle, also das Gerät, welches das Paket absendet.

Destination --> ist das Ziel, also das Gerät innerhalb eines Netzes, an das das Paket gesendet werden soll.

Die Source und die Destination Adressen sind lokale Adressen, die von Router verteilt wurden.

Protocol --> ist das Protokoll, welches für den Inhalt des Datenpaketes verwendet wird.

Length --> ist die Länge des Datenpaketes.

Info --> sind die Informationen, die für das einzelne Datenpaket wichtig sind.

Um eine erweiterte Ansicht zu erhalten, kann man entweder das Datenpaket einmal anklicken und die Informationen werden im unteren des Fensters angezeigt oder man macht auf das Datenpaket ein Doppelklick und es wird ein neues Fenster geöffnet.

(siehe Anhang 8, Abbildung 3)

6.2. Versuch

Nachdem jetzt ungefähr klar geworden ist was Wireshark macht und welche wichtigen Funktionen es hat fange ich nur an meinen Versuch zu erklären.

Ziel:

Was ich in diesem Versuch darstellen möchte ist, dass jeder mit Wireshark Passwörter bei unverschlüsselter Datenübertragung Daten abfangen kann und somit sehr leicht an Benutzernamen und Passwörter kommt. Nachdem man eine Internetseite aufgerufen hat, steht man Anfang des Uniform Resource Locator (=URL) ein http (= Hypertext Transfer Protocol) oder ein https (= Hypertext Transfer Protocol Secure). Diese beiden Protokolle sind Internetprotokolle und werden im World Wide Web verwendet, um Daten zu übertragen. Der wichtigste Unterschied zwischen diesen beiden Protokollen ist, dass die http Daten unverschlüsselt und die https Daten verschlüsselt übertragen werden. Diesen Unterschied kann man schon im Namen an dem Wort Secure bei https erkennen. In meinem Versuch habe ich mir zwei Internetseiten herausgesucht, eine mit http und eine mit https. Die http Internetseite war "www.aavtrain.com", wie auch in Abbildung 4 zu erkennen. Die https Internetseite war "truck.cargo-fleet.com", wie in Abbildung 5 zu sehen ist.

Zuerst habe ich mich mit der http Internetseite verbunden, in Wireshark die Aufzeichnung gestartet und mich mit beliebigen Benutzernamen und Passwort angemeldet. Es kommt nicht darauf an, ob die Passwörter richtig oder falsch sind, sondern dass sie übertragen werden und wie sie übertragen werden. Direkt nachdem ich die Anfrage für den Login an den Server geschickt hatte, beendete ich die Aufzeichnung in Wireshark, damit nicht noch mehr unwichtige Datenpakete mit aufgezeichnet werden. Nun habe ich die relevanten Daten herausgefiltert und unter diesen das richtige http Protokoll herausgesucht. Nach ein paar weiteren Klicks öffnete sich ein ganz neues Informationsfenster und dort konnte ich alle relevanten Informationen zu der Übertragung einsehen (siehe Anhang 8, Abbildung 4). Im oberen Teil erhält man Informationen über den Host der Website, der URL, mit der man verbunden war und ob eine Verbindung vorhanden war. Direkt unter diesem Teil sieht man, was ich für meinen Usernamen und für mein Passwort für Daten eingegeben habe und das ich den Bestätigungsknopf gedrückt hatte. Darunter waren noch Informationen von der Länge des Inhaltes, dem Zeitpunkt des Aufrufs der Website und noch der HTML Code, der dazu benötigt wird, um die Website im Browser anzuzeigen.

Bei der verschlüsselten Übertragung sieht das ganz anders aus. Die Vorgehensweise, um die richtigen Informationen zu finden, ist bei der verschlüsselten Variante ähnlich. Nachdem das

richtige Datenpaket gefunden wurde, muss man dieses auswählen und sich das Informationsfenster anzeigen lassen. In diesem Fenster wird oben die Domain angezeigt. Im ganzen anderen Bereich wird zwar auch etwas angezeigt, jedoch nichts Verständliches (siehe Anhang 8, Abbildung 5). Daran kann man erkennen, dass die übertragenen Daten verschlüsselt sind und nicht mitgelesen werden können.

(Hacking mit Windows | Passwörter mitlesen mit Wireshark | Teil 1 - YouTube)

6.3. Auswertung

Wie man im Versuch gesehen hat, ist es für jemanden, der sich im selben Netzwerk befindet nicht sehr schwierig Anmeldedaten abzufangen. Anmeldedaten kann man abfangen, jedoch sind sie nur brauchbar, wenn sie unverschlüsselt sind, weil mit verschlüsselten Daten kann man nichts anfangen. Befindet man sich in einem Netzwerk, in dem sehr viel kommuniziert wird, ist es schwieriger die richtigen Daten herauszufiltern. Wenn jedoch die IP-Adresse, des zu analysierten Gerätes, und auch die zu überwachende Verbindung bekannt ist, kann man nach diesen Parametern filtern und alles Wichtige herausfinden. Ist die Kommunikation nicht verschlüsselt kann man die Anmeldeinformationen herausfinden und Schaden anrichten. Wenn der Sniffer (=Schnüffler /der Abhörende) einmal die Anmeldeinformationen hat kann er sich einfach auf der jeweiligen Website mit den Informationen anmelden und den Account parallel verwenden. Somit bleibt er unentdeckt und der eigentliche Benutzer bemerkt nicht, dass ein Angreifer mitliest.

Deshalb ist es sehr wichtig darauf zu achten, dass man seine Daten immer verschlüsselt überträgt. Möchte man seine Daten verschlüsselt übertragen, dann muss man im Webbrowser auf ein wichtiges Detail achten. Im oberen Teil des Browsers ist immer die URL, also das Fenster, in dem die Adresse steht, mit der man sich verbindet. Wenn vor der Adresse ein "http" steht weiß man, dass die Übertragung unverschlüsselt ist. Wenn jedoch vor der Adresse ein "https" steht, dann ist die Übertragung verschlüsselt. Der Vorteil an verschlüsselter Übertragung ist nicht, dass man die Datenpakete nicht einsehen kann, sondern dass man sie nicht lesen kann, wie bei dem Versuch zu erkennen ist. Man sollte nicht nur bei Internetverbindungen auf verschlüsselte Kommunikation achten, sondern bei egal welcher Art von Übertragungen. Um sicher im Internet unterwegs zu sein muss man kein Experte sein, es reicht schon, wenn man auf kleine Details achtet, wie zum Beispiel auf das „s“ bei https. Um auf die sicheren Internet-Verbindungen noch einmal zurück zu kommen, es gibt heutzutage

kaum noch Seiten, die nicht mehr über https laufen. Die meistens Dienste, die man nutzt (Amazon, Microsoft, Facebook, Twitter und Co.), laufen schon über das Protokoll https. Das soll nicht heißen, dass man nicht darauf achten sollte, es soll eher heißen, dass man auf Seiten, die nicht über https laufen, vorsichtig sein soll, was man dort macht, denn jeder kann die Datenpakete mitschneiden und auch lesen. Diese Seiten sind meistens nicht seriös und es gibt bestimmt noch andere Seiten, wo man das findet was man sucht.

(Hacking mit Windows | Passwörter mitlesen mit Wireshark | Teil 1 - YouTube)

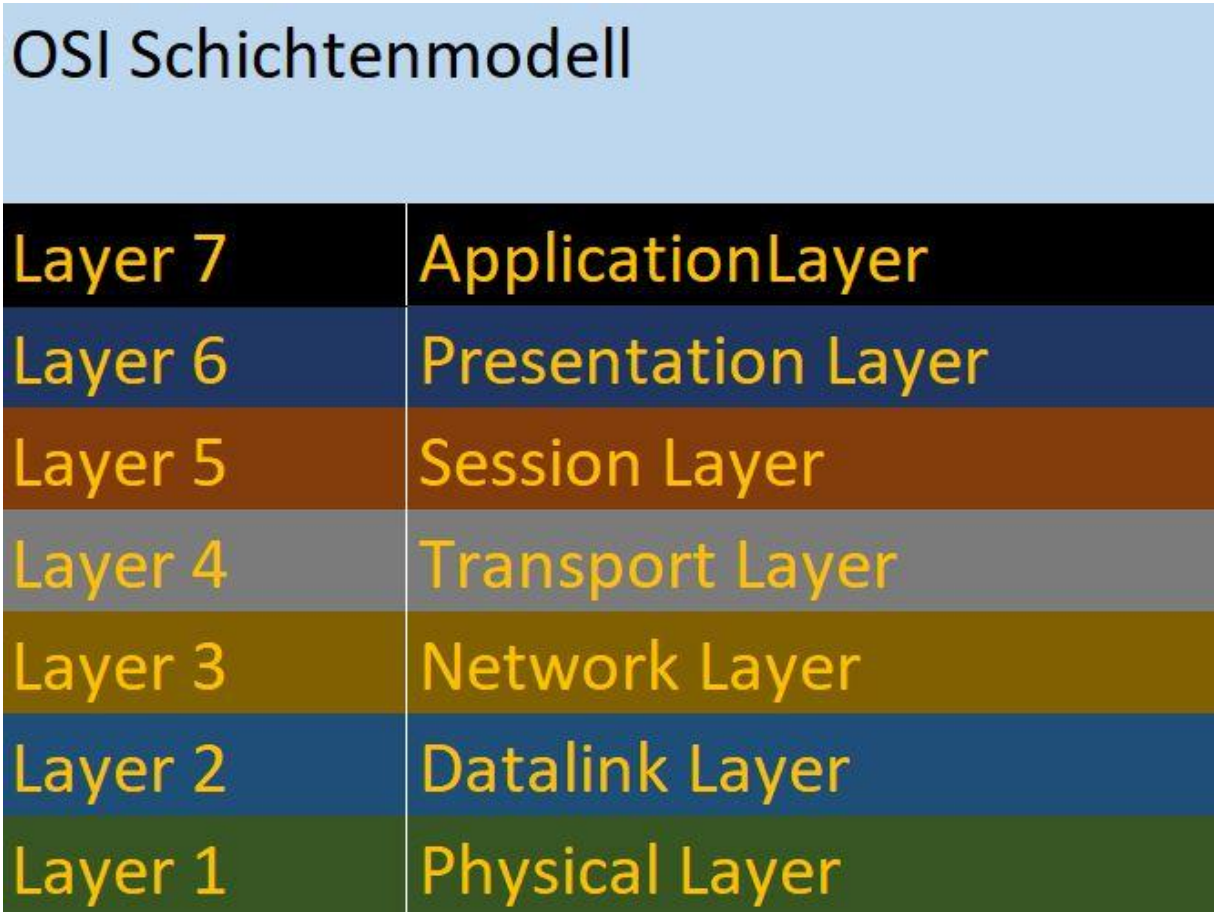
7. Fazit

In meiner Facharbeit wollte ich mich mit den einzelnen Netzwerkbestandteilen auseinandersetzen, um einen Überblick zu gewinnen, was in einem Netzwerk alles benötigt wird. Außerdem fand ich es wichtig zu wissen, wie man sich als Anwender mit kleinen Tipps absichern kann und gegen Angriffe in seinem heimischen WLAN geschützt ist. Die Wahl eines sicheren Passwortes nimmt dabei eine entscheidende Rolle ein und darf nicht unterschätzt werden. Ein wesentlicher Punkt bei der Absicherung in einem WLAN ist auch die Wahl der richtigen Verschlüsselung. Es gibt drei Verschlüsselungstypen, von denen aber nicht alle sicher sind. WPA2 ist die sicherste Variante und kann unter anderem mit dem Brute-Force-Angriff entschlüsselt werden. Zum Ende wollte ich noch einmal darstellen, was der Unterschied zwischen verschlüsselter und unverschlüsselter Datenübertragung ist. Dem Leser soll nicht nur gezeigt werden, was unverschlüsselte Kommunikation für Nachteile hat, sondern auch, wie leicht man sich schützen kann. In meinem Fall würde man https statt http verwenden.

Zusammenfassend kann gesagt werden, dass es in meiner Facharbeit darüber ging, wie ein Netzwerk grob aufgebaut ist und wie man sein WLAN schütz. Auf eine richtige und sichere Verschlüsselung sollte dabei immer geachtet werden.

8. Anhang

Abbildung 1:

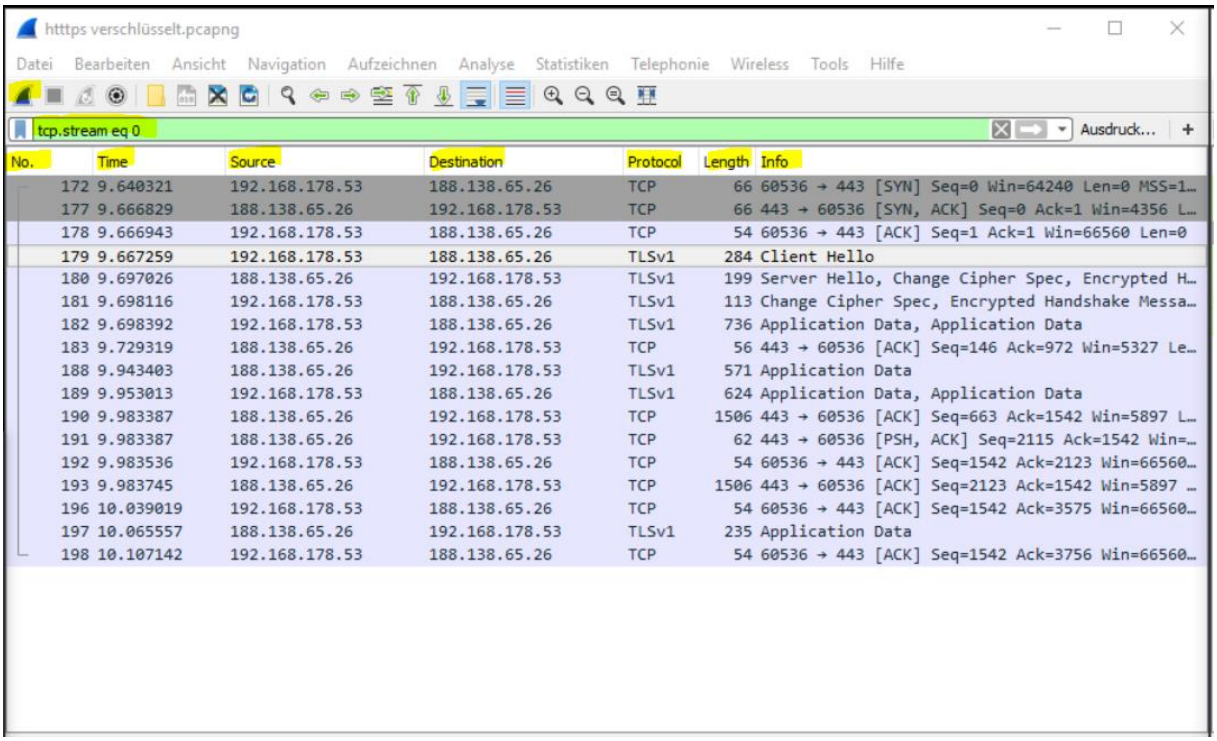


Quelle: Eigenes Bild, das in Excel gemacht wurde.

Abbildung 2:

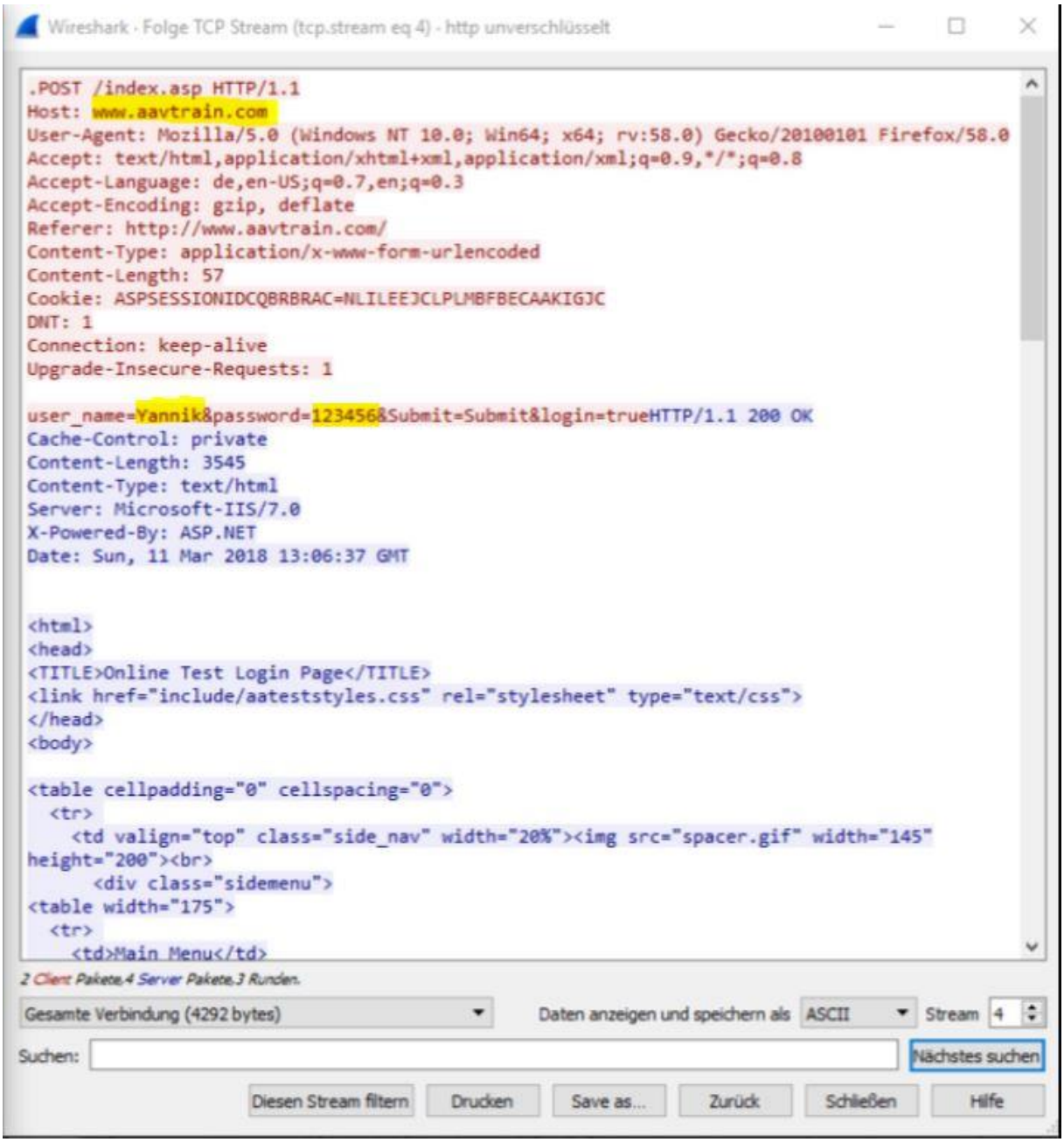
Quelle: http://slideplayer.org/slide/9824319/31/images/81/Einteilung+nach+Ausdehnung.jpg

Abbildung 3:



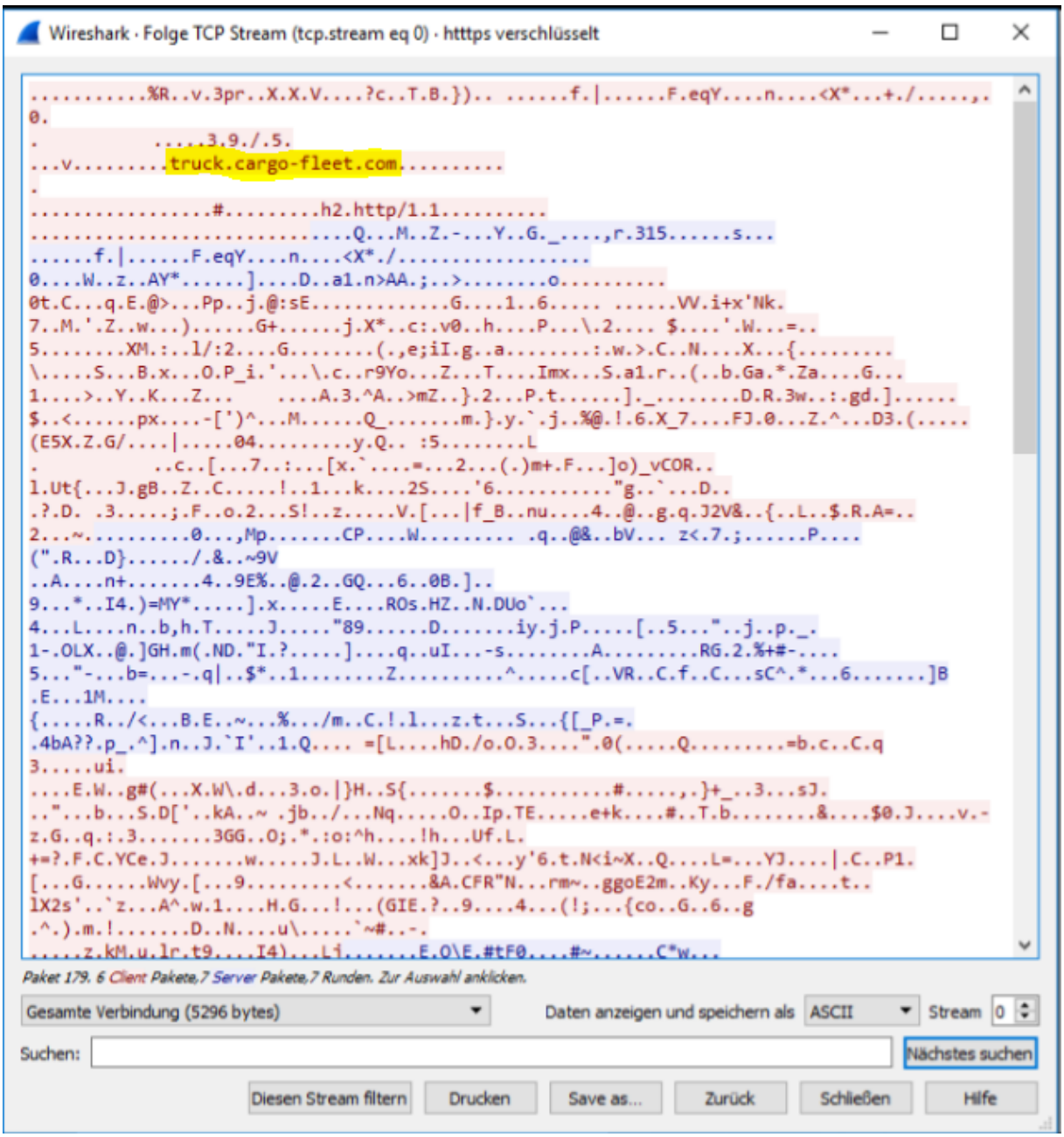
Quelle: Eigenes Bild, das in Wireshark gemacht wurde.

Abbildung 4:



Quelle: Eigenes Bild, das in Wireshark gemacht wurde.

Abbildung 5:



Quelle: Eigenes Bild, das in Wireshark gemacht wurde.

9. Literaturverzeichnis

Baumeister, Johann; Joos, Thomas; Dirscherl, Hans-Christian (2016): WireShark: Netzwerküberwachung für Profis mit Sniffer. PC Welt. IDG Tech Media GmbH. Online verfügbar unter https://www.pcwelt.de/ratgeber/Netzwerkanalyse-Mit-Wireshark-Netzwerk-Probleme-loesen-4731682.html, zuletzt aktualisiert am 03.02.2016, zuletzt geprüft am 12.03.2018.

BSIFB - Passwörter (2018). Online verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html;jsessionid=C6A470032A0A94E9ED837252A59AC985.1_cid351, zuletzt aktualisiert am 16.03.2018, zuletzt geprüft am 16.03.2018.

BSIFB - Sicherheitstipps. Online verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/Sicherheitstipps/sicherheitstipps_node.html, zuletzt geprüft am 17.03.2018.

BSIFB - Sicherheitstipps - Sicherheitstipps zum privaten WLAN-Einsatz. Online verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/WLAN/Sicherheitstipps/wlan_tipps.html, zuletzt geprüft am 17.03.2018.

BSIFB - Umgang mit Passwörtern (2018). Online verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang_node.html, zuletzt aktualisiert am 16.03.2018, zuletzt geprüft am 17.03.2018.

Hacking mit Windows | Passwörter mitlesen mit Wireshark | Teil 1 - YouTube. Online verfügbar unter https://www.youtube.com/watch?v=uloWEdikWYs, zuletzt geprüft am 12.03.2018.

Hauser, Bernhard (2013): Fachwissen Netzwerktechnik. Modelle - Geräte - Protokolle. 1. Aufl. Haan-Gruiten: Verl. Europa-Lehrmittel (Bibliothek des technischen Wissens).

Lüders, Martin; Sausel, Stephan (2009): Netzwerke. Lokale Netze analysieren, einrichten, und anbinden. 1. Aufl., Dr. 1. Braunschweig: Westermann (Angewandte Informatik).

Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim (2011): Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. 2., überarbeitete Auflage. Wiesbaden: Vieweg+Teubner Verlag / Springer Fachmedien Wiesbaden GmbH Wiesbaden.

Wireshark · Go Deep. (2018). Online verfügbar unter https://www.wireshark.org/#download, zuletzt aktualisiert am 03.04.2018, zuletzt geprüft am 11.04.2018.

10. Versicherung der selbständigen Erarbeitung

Ich versichere, dass ich die vorliegende Arbeit einschließlich evtl. beigefügter Zeichnungen, Kartenskizzen, Darstellungen u. ä. m. selbstständig angefertigt und keine anderen als die angegebenen Hilfsmittel benutzt habe. Alle Stellen, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, habe ich in jedem Fall unter genauer Angabe der Quelle deutlich als Entlehnung kenntlich gemacht.

_____, den _____

(Ort) (Datum)

_____

(Unterschrift)