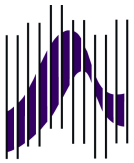
Hochschule
Ravensburg-Weingarten



Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

Messenger über einen verborgenen Netzwerkkanal

Bachelorarbeit

Wintersemester 2018/19

im Studiengang Angewandte Informatik

an der Hochschule Ravensburg - Weingarten

von

Maximilian Nestle Matr.-Nr.: 27427

Abgabedatum : 3. Januar 2019

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit mit dem Titel

Messenger über einen verborgenen Netzwerkkanal

selbständig angefertigt, nicht anderweitig zu Prüfungszwecken vorgelegt, keine anderen als die angegebenen Hilfsmittel benutzt und wörtliche sowie sinngemäße Zitate als solche gekennzeichnet habe.

Weingarten, 3. Januar 2019

Maximilian Nestle

_____

Inhaltsverzeichnis

Kurzfassung

Abstract

Danksagung

Vorwort

1 Einleitung

1.1 Motivation

In der heutigen Zeit wird die Datensicherheit immer wichtiger, da immer mehr personenbezogene Daten im Internet preisgegeben werden. Um die Datenübertragung zu sichern wird meistens ein asymetrisches Verschlüsselungsverfahren verwendet.
Dieses Verfahren bieten zwar ein hohes Maß an Sicherheit, hat aber auch Nachteile, wie zum Beispiel eine Erhöhung der Rechenzeit, die Verwaltung eines Key-Managers und die Bedrohung durch einen „Man-in-the-Middle" Angriff.
Eine Mögliche Alternative wäre beispielsweise die Steganographie. Dies ist die Kunst, Daten in legitimierten Datenkanälen zu verstecken ohne einen Verschlüsselung anzuwenden.
Steganographie ist zudem sehr unauffällig, da in unverschlüsselten Daten meistens keine sensiblen Daten vermutet werden.

1.2 Aufgabenstellung und Zielsetzung

Ziel der Bachelorarbeit ist die Erstellung eines Messengers, bei dem zwei Personen Daten empfangen und verschicken können. Dabei soll die Kommunikation über ein Netzwerk stattfinden und steganografisch verschlüsselt werden.
Die Daten sollen nicht mit einem mathematischen Verfahren verschlüsselt werden, sondern in ein oder mehreren Protokollen „versteckt" eingebettet und übertragen werden. Dazu soll ein optimales Verfahren zur Dateninfiltration und -exfiltration gefunden werden. Als Verfahren können hier zum Beispiel Covert- Channels eingesetzt werden. Das Verfahren sollte unauffällig, für Dritte schwer zu interpretieren und mit größt möglicher Übertragungsrate senden. Optimal wäre ein ähnliche Sicherheit zu gewährleisten, wie mit einer mathematischen Verschlüsselung.
Ziel ist es außerdem jedes Dateiformat übertragen zu können. Das resultierende Programm soll in der Lage sein, gleichzeitig Server und Client zu sein, was bedeutet, dass mit dem gleichen Programm gesendet und empfangen werden kann.

Eine einfache GUI soll dem Benutzter das Senden und Empfangen der Daten so einfach wie möglich machen.
Wünschenswert wäre ein möglichst einfacher Verbindungsaufbau, der ohne den direkten Austausch der IP- Adressen statt findet.

2 Grundlagen

2.1 Datenschutz

Der Datenschutz ist ein Überbegriff für das in Gesetzte festgelegten Recht, dass jede Person über die Preisgabe der personenbezogenen Daten bestimmen kann. Die Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI) definieren den Datenschutz wie folgt:

„Datenschutz garantiert jedem Bürger Schutz vor missbräuchlicher Datenverarbeitung, das Recht auf informationelle Selbstbestimmung und den Schutz der Privatsphäre" [Die18]

Das bedeutet, dass jeder der personenbezogene Daten, ohne Zustimmung des Betreffenden speichert oder weiterverarbeitet vor Gericht angeklagt werden kann. Damit dies nicht passiert haben die meisten Institute die mit personenbezogenen Daten umgehen einen Datenschutzbeauftragten, der die Einhaltung dieser Gesetzte überwacht.

2.2 Datensicherheit

Im Gegensatz zu dem Datenschutz bezieht sich die Datensicherheit nicht nur auf die personenbezogenen Daten, sondern auf alle Daten. Die Aufgabe der Datensicherheit werden durch das CIA-Prinzip beschreiben.
Zur Datensicherheit gehören nach diesem Prinzip alle Maßnahmen, die die **C**onfidentiality, **I**ntegrity und **A**vailability (Vertraulichkeit, Integrität, Verfügbarkeit) gewährleisten. [Nic18] Eine zusätzliche Aufgabe ist die Sicherstellung der Authentizität. Viele dieser Aufgaben werden mit Hilfe der Kryptographie realisiert und umgesetzt.

2.2.1 Vertraulichkeit

Die Vertraulichkeit ist dann gewährleistet, wenn die Daten nicht von unbefugten Personen eingesehen werden können. Es muss also ein System verwendet werden, bei dem sich befugte Benutzer legitimieren können und unbefugte beim Interpretieren gehindert werden.
In den meisten Fällen wird dies durch eine Verschlüsselung (symmetrisch oder asymmetrisch) umgesetzt. Alle legitimierten Benutzter erhalten den Schlüssel. Die Personen ohne Schlüssel können die Informationen nicht entschlüsseln - die Vertraulichkeit ist so garantiert.
Optimal wäre, wenn nicht legitime Benutzer, auch nicht an die verschlüsselten Daten kommen würde.

2.2.2 Integrität

Die Integrität beschäftigt sich damit, dass Daten nicht unbemerkt verändert oder abgefälscht werden. So soll zum Beispiel sichergestellt werden, dass eine Nachricht genau so beim Empfänger ankommt, wie sie abgesendet wurde.
Hierzu können Hash-Funktionen verwendet werden, die beim Verändern der Nachricht einen anderen Wert ergeben würden. Dabei müsste entweder die Hash-Funktion geheim sein oder der Hash-Wert verschlüsselt werden.

2.2.3 Verfügbarkeit

Der Dritte Punkt ist die Verfügbarkeit. Es soll immer sichergestellt wer, dass Daten aber auch Programm immer abrufbar sind. Hierzu gehören Mechanismen zur Vermeidung von DoS (Denial of Service) Angriffen. Diese Angriffe würden beispielsweise einen Server so überfordern, dass dieser keine Dateien mehr ausliefern kann - die Verfügbarkeit ist dann nicht mehr gewährleistet.

2.2.4 Authentizität

Die Authentizität bestätigt, dass Daten von der angegeben Informationsquelle stammen. Es ist ein Identitätsbeweis des Absenders gegenüber dem Empfängers.
Dies kann zum Beispiel mit einer Public-Key Verschlüsselung realisiert werden. So kann der Sender die Nachrichten mit seinem Public-Key verschlüsseln und jeder im Besitz des Public-Keys kann bestätigen, dass die Nachricht genau von dieser Person kommt.

2.3 Kryptographie

Kryptographie bedeutet „wörtlich: Die Lehre vom Geheimen schreiben" [Hel18] und beschäftigt sich mit der mathematischen Verschlüsselung von Informationen. Dabei gibt es zwei große Verschlüsselungsarten - die Symmetrischen und die Asymmetrischen Verschlüsselungen. Bei beiden Verfahren wird durch einen Schlüssel (meistens eine Zahl) und einem Algorithmus aus einer lesbaren Information eine Unlesbare. Um dies wieder Rückgängig zu machen wird ebenfalls ein Schlüssel und ein Algorithmus benötigt.
Eine der wichtigsten Grundprinzipien der Kryptographie wurde bereits im 19. Jahrhundert von A.Kerkhoffs aufgestellt. Eine der wichtigsten Ausagen hierbei ist, dass die Sicherheit einer Verschlüsselung nicht von dem Verschlüsselungsalgorithmus, sondern allein von dem Schlüssel abhängig sein soll. Das heißt, dass ein guter Verschlüsselungsalgorithmus öffentlich gemacht werden kann, ohne die Sicherheit zu gefährden. Ein Beispiel ist der RSA Algorithmus. Dies ist einer der heute verbreitetsten Algorithmen. Der Algorithmus ist für jeden öffentlich zugänglich, dies hat aber keine Auswirkung auf die Sicherheit, da die Sicherheit allein auf der Geheimhaltung des Passwortes basiert.
Dies hat zum Beispiel auch den Vorteil, dass bei einem Personalwechsel nicht der ganze Algorithmus ausgetauscht werden muss, sondern nur das Password.

2.4 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird zum Verschlüsseln und Entschlüsseln der gleiche Schlüssel verwendet.

$E_k(M) = C$
$D_k(C) = M$

[Ert01]

Der Schlüssel K wird dazu verwendet die Nachricht zu verschlüsseln und Entschlüsseln. Das Problem bei symmetrischen Verschlüsselungen ist die Schlüsselübertragung, die auf jeden Fall geheim stattfinden muss. Bekannte Beispiele sind der DES und AES.

2.5 Asymmetrische Verschlüsselung

Bei einer asymmetrisch Verschlüsselung hat man zum verschlüsseln einen anderen Schlüssel wie zum entschlüsseln. Dieses System wird „Public-Key-Kryptographie" genannt, da es einen öffentlichen (K1) und einen privaten Schlüssel (K2) gibt. Dabei wird der K1 zum Verschlüsseln verwendet und K2 zum Entschlüsseln.

$E_{k1}(M) = C$
$D_{k2}(C) = M$

[Ert01]

Dieses System löst das Problem der Schlüsselübergabe, da der öffentliche Schlüssel ohne Bedenke an den Kommunikationspartner übertragen werden kann. Bei einem Möglichen Angriff kann der Angreifer mit dem Schlüssel nichts anfangen, da er mit ihm nicht entschlüsseln kann. Nur der private Schlüssel, der geheim bleibt und nicht versendet wird, kann dann die Entschlüsselte Nachricht dechiffrieren.
Diese Art von Algorithmus kann so auch zur Authentifizierung eingesetzt werden. Bekannte Asymmetrische Verschlüsselungen sind der RSA-Algorithmus, der Algorithmus von Diffi und Hellmann oder Algorithmus von ElGamal.

2.6 Steganographie

Die Steganographie ist die Kunst vom verborgenem Schreiben. Je nachdem welche Literatur man verwendet wird die Steganographie als Unterpunkt der Kryptographie oder als einen eigene Disziplin gesehen. In dieser Arbeit wird die Steganographie eigenständig betrachtet und als alternative zur Kryptographie gesehen.
Beide, die Kryptographie und die Steganographie, sind Möglichkeiten Informationen geheim und von Dritten ungesehen zu übertragen. Wie bereits oben beschrieben beschäftigt sich die Kryptographie mit dem verschlüsseltem Schreiben. Die Steganographie hingegen benutzt keine Verschlüsselung, sondern versucht die geheime Information in einem unauffälligem oder legitimiertem Informationskanal zu verstecken.
Wie von Peter Purgathofer [Pur10] beschrieben hat die Steganographie eine große Bedeutung in der Geschichte, denn die Menschen waren gerade in Kriegszeiten schon immer auf der Suche nach einem sicher Weg Informationen zu übertragen.
So hat zum Beispiel der griechisch Spion Demaratos Wachstafeln dazu benutzt um Informationen zu verschicken. Nur hat er die nicht ins Wachs geschrieben sondern in das darunterliegende

Holz.
Ebenfalls soll Histiaeus, der Tyrann von Milet, seine geheimen Nachrichten auf die Schädel der Sklaven tätowiert haben. Die Haare wuchsen nach und die Nachricht war verborgen.
Es gibt noch viele andere Beispiel Angefangen von unsichtbarer Tinte bis hin zu Morsezeichen in Gemälden, aber vor allem Künstlern wurde oft vorgeworfen, mit Hilfe von Steganographie Geheime Nachrichten zu verbreiten. So wurde zu Beispiel Mozart immer wieder beschuldigt freibeuterische Nachrichten in der „Zauberflöte" versteckt zu haben.
Die Beispiele der Geschichte zeigen deutlich wie die Steganographie funktioniert: Es gibt immer eine unauffällige Trägernachricht (Wachstafel, Sklave, Gemälde, Musikstück...).
In diese Trägernachricht wie die geheime Nachricht versteckt (Unter Wach oder Haaren, Blickwinkel auf das Gemälde, Notenreihenfolge...)
Um die Nachricht zu entschlüsseln benötigt der Empfänger nur die Information wo sich die Nachricht befindet beziehungsweise wie sie versteckt wird. Das Schema von Gary C. Kessler [Kes15] macht dieses Prinzip sehr anschaulich:

Steganographisches Medium = Geheime Nachricht + Träger Nachricht + Steganografischer Schlüssel

Dabei darf der Steganografische Schlüssel nicht mit dem aus der Kryptographie verwechselt werden. Es handelt sich hier mehr um das Wissen wo und wie die geheime Nachricht verborgen ist.
Dabei bedient sich die Steganographie der „Security by Obscurity" (Sicherheit durch Unwissenheit), was bedeutet, dass die Sicherheit allein davon abhängt, ob das Geheimhaltungsverfahren unbekannt bleibt. Übrigens gehören kryptographische Verfahren die nicht unter Kerkhoffs Prinzip fallen auch zu „Security by Obscurity". Will man also ein solches System sicherer machen muss man dafür sorgen, dass das Verfahren so abwegig beziehungsweise obskur gestalten wird sodass nie jemand auf die Idee kommt nach einer geheimen Nachricht zu suchen

Die Steganographie hat in der Geschichte eine relativ einfache aber sichere Methode geboten Nachrichten zu übertragen. Aber auch heute mit dem Internet sind wir nahezu immer von Datenkanälen umgeben die sich für die steganographische Datenübertragung eignen. Der Vorteil hierbei ist, dass meistens unter den ganzen kryptographisch verschlüsselten Datenpaketen die Steganographie vergessen wird.

2.7 Internet Protokolle

Im den folgenden Kapiteln soll kurz das OSI-Schichtenmodell, auf welches das heutige Internet aufbaut, erklärt werden. Dabei repräsentiert jede Schicht eine Protokoll, das für die Kommunikation im Internet nötig ist.
Es werden nur die Protokolle betrachtet, die für dieses Projekt relevant sind.

2.7.1 Sicherungsschicht/Data Link Layer (Schicht 2)

Diese Schicht beinhaltet Protokolle, welche einen weitestgehend fehlerfreie Datenübertragung garantieren sollen. Außerdem wird der Zugriff auf das Übertragungsmedium ermöglicht. [Wik18]

Ethernet

Beim Ethernet-Protokoll werden die Daten in Pakete zerteilt. Diese können dann zwischen den Geräten im Netzwerk verschickt werden. Dabei ist das Ethernet-Protokoll immer nur im jeweiligen Netzwerksegment gültig. [Zis13] Die Adressierung wird mit Hilfe der MAC-Adressen realisiert. Diese Adresse ist einmalig und wird jedem netzwerkfähigem Gerät vom Hersteller zugeordnet.

7 Byte	1 Byte	6 Byte	6 Byte	4 Byte	2 Byte	bis 1500 Byte	max. 42 Byte	4 Byte
Präam-bel,	SFD	MAC-Adresse Ziel	MAC-Adresse Quelle	VLAN-Tag	Typ	Nutzdaten	PAD	FCS

Bild 2.1: Erweiterter Ethernet-Frame nach IEEE 802.1Q [Zis13]

2.7.2 Vermittlungsschicht/Network Layer (Schicht 3)

Die Protokolle dieser Schicht werden verwendet, um über Netzwerkgrenzen hinaus Nachrichten zu versenden. [Zis13] Dieses Protokoll liegt innerhalb der Nutzdaten des Ethernet-Pakets.

IPv4

Zur Adressierung werden IPv4 Adressen verwendet, die 32 bit (4 Byte) lang sind. Vergeben werden die Adressen von der IANA (Internet Assigned Numbers Authority). Jeder der aus dem Internet erreichbar sein will, muss sich bei der IANA oder einer untergeordneten Organisation eine IP-Adresse oder Adressbereich geben lassen.

Das Internet Protokoll wird wie in folgender Abbildung gezeigt in das Ethernet Paket eingebettet.

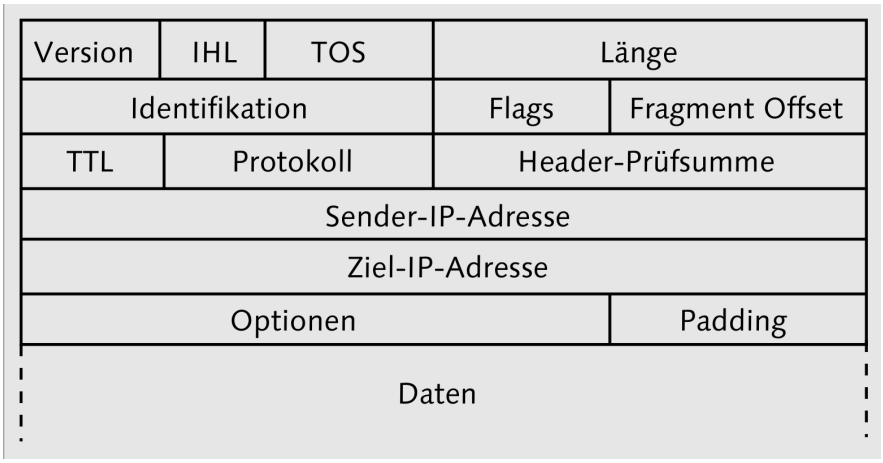


Bild 2.2: IPv4 Header [Zis13]

IPv6

Da die IPv4 langsam knapp werden, wurde das IPv6 Protokoll erstellt, welches über Adressen mit 6 Byte Länge verfügt. Dies bedeutet, dass deutlich mehr Adressen erstellt und vergen werden können. Die Funktion ist aber mehr oder weniger die gleiche.

Das IPv6 Internet Protokoll ist in folgender Abbildung gezeigt.

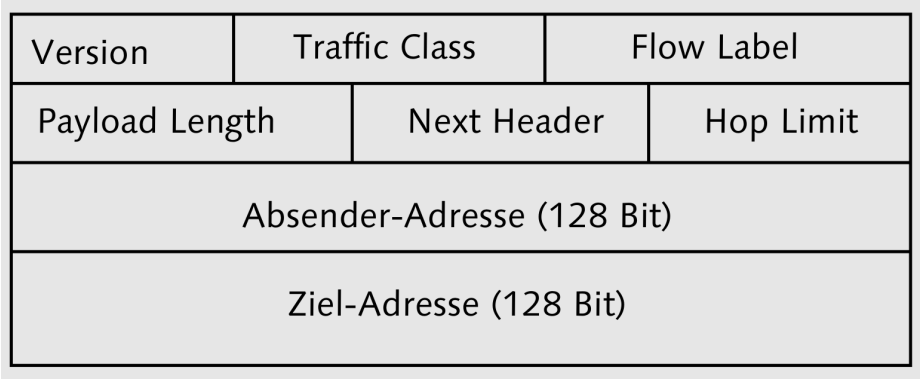


Bild 2.3: IPv6 Header [Zis13]

2.7.3 Transportschicht/ Transport Layer (Schicht 4)

2.7.4 Kommunikationsschicht/Session Layer (Schicht 5)

2.8 Covert-Channel

Covert-Channels sind Netzwerk Kanäle, die nicht offen praktiziert, erklärt, engagiert, angesammelt oder gezeigt werden. [Gol03]

3

3.1

3.1.1

4

4.1

4.1.1

5

5.1

5.1.1

6

6.1

6.1.1

7

7.1

7.1.1

8

8.1

8.1.1

9

9.1

9.1.1

10

10.1

10.1.1

11

11.1

11.1.1

12 Schlussbemerkungen und Ausblick

A Ein Kapitel des Anhangs

Literatur

[Die18] Die Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI): *Was ist Datenschutz?* https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/ueberblick-node.html, 2018. Abrufdatum: 16.10.2018.

[Ert01] Ertel, Wolfgang: *Angewandte Kryptographie. Fachbuchverlag Leipzig.* Carl Hanser Verlag), ISBN, 2001.

[Gol03] Goltz, James P.: *Under the radar:A look at three covert communications channels.* 2003.

[Hel18] Hellmann, Roland: *IT-Sicherheit: eine Einführung.* Walter de Gruyter GmbH & Co KG, 2018.

[Kes15] Kessler, Gary C.: *An Overview of Steganography for the Computer Forensics Examiner (Updated Version, February 2015)*, 2015.

[Nic18] Nico Grundmeier: *Sicherheitslücken im Internet.* http://www.informatik.uni-oldenburg.de/~iug10/sli/indexd917.html?q=node/19, 2018. Abrufdatum: 16.10.2018.

[Pur10] Purgathofer, Peter: *Eine kurze Geschichte der Steganographie.* Die Funktion verdeckter Kommunikation: Impulse für eine Technikfolgenabschätzung zur Steganographie, 9:65, 2010.

[Wik18] Wikipedia contributors: *OSI-Modell — Wikipedia, The Free Encyclopedia.* https://de.wikipedia.org/wiki/OSI-Modell, 2018. Abrufdatum: 03.01.2019.

[Zis13] Zisler, Harald: *Computer-Netzwerke*, 2013.