

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 : 27. Oktober 2018

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, 27. Oktober 2018

Maximilian Nestle

Inhaltsverzeichnis

Kurzfassung	II
Abstract	III
Danksagung	IV
Vorwort	V
1 Einleitung	1
1.1 Motivation	1
1.2 Aufgabenstellung und Zielsetzung	1
2 Grundlagen	3
2.1 Datenschutz	3
2.2 Datensicherheit	3
2.2.1 Vertraulichkeit	4
2.2.2 Integrität	4
2.2.3 Verfügbarkeit	4
2.2.4 Authentizität	4
2.3 Kryptographie	5
2.4 Symmetrische Verschlüsselung	5
2.5 Asymmetrische Verschlüsselung	6
2.6 Steganographie	6
2.7 Internet Protokolle	6
12 Schlussbemerkungen und Ausblick	16
A Ein Kapitel des Anhangs	17
Literatur	19
Stichwortverzeichnis	19

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 asymmetrisches 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 legitimierte Datenkanälen zu verstecken ohne eine 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 eine 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 Benutzer 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 Betroffenen 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 Confidentiality, Integrity und Availability (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 legitimen Benutzer 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 werden, dass Daten aber auch Programme 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 angegebenen Informationsquelle stammen. Es ist ein Identitätsbeweis des Absenders gegenüber dem Empfänger.

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 Aussagen 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 Passwort.

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.

$$E_{k_1}(M) = C$$

$$D_{k_2}(C) = M$$

[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

2.7 Internet Protokolle

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*, 2001.
- [Hel18] HELLMANN, ROLAND: *IT-Sicherheit: eine Einführung*. Walter de Gruyter GmbH & Co KG, 2018.
- [Nic18] NICO GRUNDMEIER: *Sicherheitslücken im Internet*. <http://www.informatik.uni-oldenburg.de/~iug10/sli/indexd917.html?q=node/19>, 2018. Abrufdatum: 16.10.2018.