Hochschule
Ravensburg-Weingarten

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 : 24. 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, 24. 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 ist 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 keine sensiblen Daten vermutet werden.
So wäre beispielsweise eine Anwendung denkbar, bei der ein Polizeipräsidium mit ihren verdeckten Ermittlern kommunizieren will. Da die Polizei davon ausgehen muss, dass die Kommunikation abgehört wird, würde einen Verschlüsselte Kommunikation zu viel Aufsehen erregen. Zudem kann es sein, dass die Verschlüsselung auch schon geknackt wurde.
Hier kommt dann die Steganographie ins Spiel, die es möglich macht einen legitimen und unauffälligen Kanal für die Datenübertagung zu verwenden. So ein Kanal könnte der Stream beim Schauen eines Videos oder die Nachrichten einer Webseite sein.
Die Steganographie bietet gerade deswegen, da sie oft hinter den großen Verschlüsselungsverfahren in Vergessenheit gerät, eine sehr gut Methode um hoch sensible Daten zu versenden.

1.2 Aufgabenstellung und Zielsetzung

Ziel der Bachelorarbeit ist es, bei dem in der Motivation bereit beschriebenen Szenario, der Polizei eine Kommunikationsmöglichkeit zu schaffen. Dabei soll es möglich sein, dass Anweisungen, Treffpunkte aber auch Bilder an den verdeckten Ermittler übertragen werden können. Dabei soll die Kommunikation über ein Netzwerk stattfinden und steganografisch verschlüsselt werden.
Die entstehende Anwendung soll als ein „Proof of Concept" dienen und die Möglichkeiten der Steganografie veranschaulichen.
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. 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.

1.3 Aufbau

Als erstes folgt die Einführung in die Grundlagen. Danach beschäftigt sich die Arbeit mit der Findung nach einem optimalen steganographischen Verfahren, mit dem die Daten übertragen werden sollen. Anschließend wird dieses Verfahren in einer realen Anwendung übertragen. Als letztes wird die Anwendung bewertet und ein Fazit gezogen.

1.4 Eigene Leistung

Es werden steganografische Verfahren bewertet und das Optimum ausfindig gemacht. Aus dem gefundenen Ergebnis wird einen Anwendung als „Proof of Concept" implementiert

die passend zur Zielsetzung die Datenkommunikation übernimmt. Das Programm wird danach evaluiert und auf mögliche Anwendungsgebiete getestet.

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.

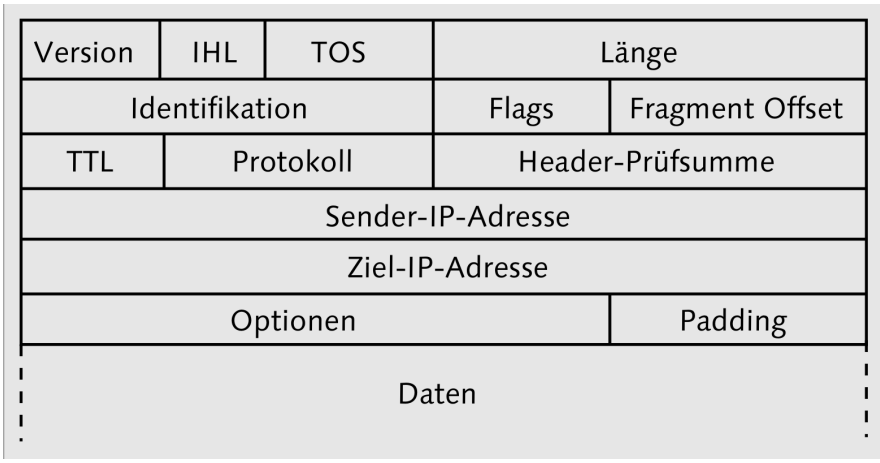

Bild 2.2: IPv4 Header [Zis13]

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.

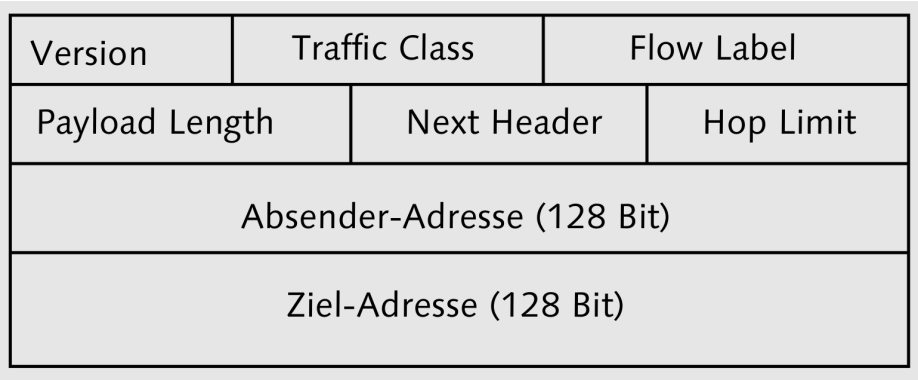

Bild 2.3: IPv6 Header [Zis13]

2.7.3 Transportschicht/ Transport Layer (Schicht 4)

2.7.4 Kommunikationsschicht/Session Layer (Schicht 5)

3 Was ist ein Covert-Channel?

3.1 Definition

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

Hierbei kann ein Kanal eine beliebige Methode sein Informationen zischen zwei Geräten über ein Netzwerk auszutauschen. Bei Covert-Channels wird sich die größtmöglich Mühe gegeben, diesen Informationskanal vor Dritten unbemerkt zu halten.
Bei steganografischen Covert-Channels werden Methoden aus der Steganografie verwendet um diesen Kanal zu verbergen.

In dieser Arbeit handelt es sich bei Covert-Channel immer um Kanäle, die mit einem steganografischem Verfahren verschlüsselt werden.

3.2 Was zeichnend einen guten Covert-Channel aus?

Bei den weit verbreiteten mathematischen Verschlüsselungen muss sich meistens keine sorgen gemachen werden, ob der Datenaustausch von Dritten entdeckt werden kann, da hier die Daten ohne richtigen Key nutzlos sind.
Bei den Covert-Chanels ist dies problematischer, da ein entdeckter Kanal in der Regel direkt interpretiert werden kann. Ein Covert-Channel lebt, wie der Name auch schon verrät, davon wie gut dieser versteckt ist.
Dabei besitzt die Steganografie einen großen Vorteil: Ist das Verfahren zum Verstecken der Daten nicht bekannt, so ist es nahezu unmöglich den Covert-Channel zu finden, da

nicht klar ist wo und nach was gesucht werden muss (Security by Obscurity).
Ist hingegen klar, um welches Verfahren es sich handelt und besteht die Vermutung, dass eine Kommunikation über einen versteckten Kanal stattfindet so kommt man leicht an die Informationen.
Um einen Covert-Channel zu Bewerten müssen folgende Aspekte betrachtet werden:

Der erste ist die Fähigkeit, wie einfach sich ein Kanal verstecken lässt. Hier fließt die allgemeine Unauffälligkeit des Covert-Channels ein, aber auch die Eigenschaften des bereits herrschenden Netzwerkverkehrs, in den der Channel eingebettet werden soll.
Der zweite Aspekt ist die Unbekanntheit des Verfahrens, sodass nicht nach einem möglichen versteckten Kanal gesucht werden kann. Hier kann einen Methode zur individuellen Gestaltung des Channels eine Verbesserung bringen.
Natürlich muss auch die Datenübertragungsrate betrachtet. Diese ist meistens sehr gering aber hier gibt es auch große Unterschiede zwischen den einzelnen Verfahren.
Die Integrität der Daten müssen die Channels ebenfalls gewährleisten.

3.3 Wozu sind Covert-Channels nicht geeignet?

Hohe Datenübertragung

4 Mögliche steganografische Covert-Channel

4.1 Klassische textbasierende Verfahren

Botschaften in Texten teilweise einzubetten ist mit der Steganographie möglich.
Gängig unter Textmanipulatoren ist die gezielte Wahl des ersten Buchstaben des Wortes, wobei die Aneinanderreihung dieser Buchstaben ein neues Wort ergibt.
Bei einem wissenschaftlich erarbeiteten Rückblick treten einige, nicht zu unterschätzende, Sicherheitslücken auf, wenn diese Art der Verschlüsselung angewendet wird.

Eine weitere Methode ist die Satzzeichen zu verwenden um Informationen zu kodieren. So kann zum Beispiel ein Punkt 00, ein Komma 01, ein Fragezeichen 10 und ein Ausrufezeichen 11 bedeuten. [LC17]

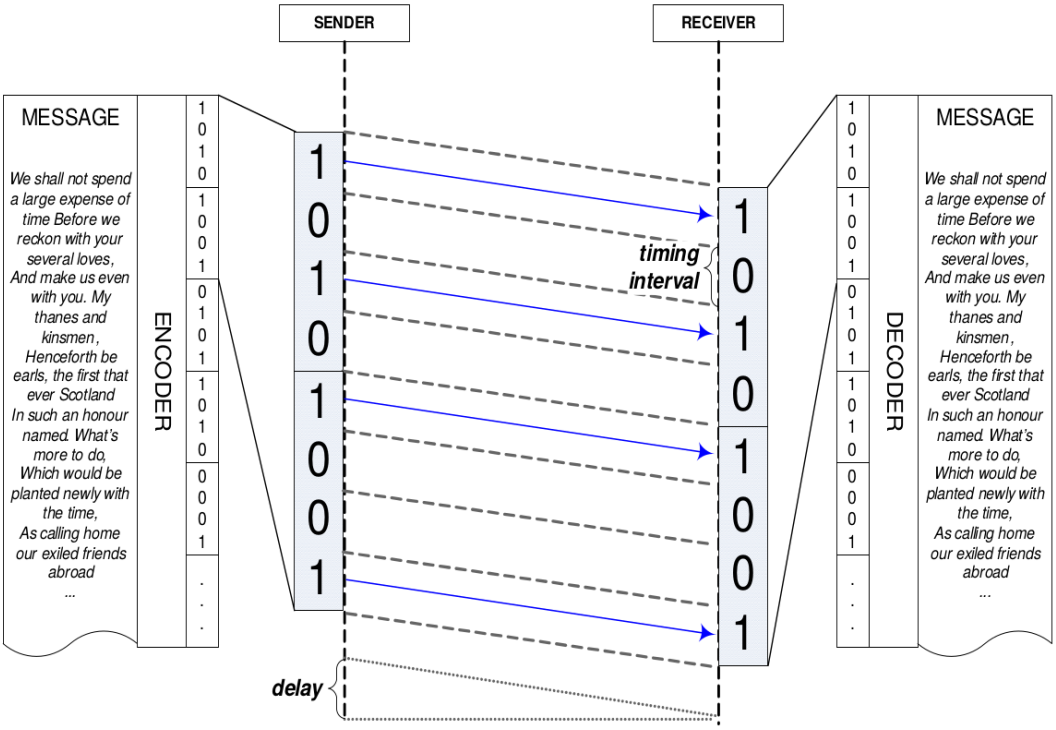

Bild 4.1: Kommunikation über einen Zeitabhängigen Kanal [CBS04]

4.2 Zeitabhängiger Covert-Chanel

4.3 Benutzung verschiedener Protokolle Reihenfolge

4.4 Benutzung verschiedener Ports

4.5 Benutzung von unbenutzten Bits in Protokoll-Headern

traffic normalizers

4.6 Verwendung der Paketgröße

4.7 Verstecken der Informationen in den Nutzdaten

4.7.1 Verwenung von Bilddateien

RGB Basierende Formate

Bildformate die auf die RGB Formate basieren sind zum Beispiel BMP (Windows Bitmap) oder auch GIF (Graphics Interchange Format). Diese Formate geben die Pixelfarbe basierend auf dem **R**ot-, **G**rün- und **B**lauwert. In diesen Werten können Daten versteckt werden. [KP00] So können beispielsweise die letzten beiden Bits manipuliert werden. Diese Veränderung ist für das menschliche Auge nicht zu erkennen, da die letzten Bits kaum eine Auswirkung auf die Höhe der Zahl haben.
Bei einer Farbtiefe von 24 Bit beträgt die maximale Änderung der Farbwerte nur 3 Farbstufen von insgesamt 256 möglichen.

00000000 (0) -> 00000011 (3)
11111111 (255) -> 11111100 (252)

Auf diese Weise lassen sich 6 Bit pro Pixel übertragen. In einem unkomprimierten HD Bild mit einer Auflösung von 1280x720 Pixeln (ca. 22 MByte) lassen sich 0,6912 Mbyte Daten übertragen.

In Abbildung **??** wird dieses System veranschaulicht:

Bildformate mit Alpha Kanal

Bildformate wie PNG (Portable Network Graphics) können zusätzlich zu den RGB Kanälen auch auch einen Alpha Kanal besitzen. Dies ist ein zusätzlicher Wert der die Transparenz des jeweiligen Pixel angibt. Bei einem Wert von 0 ist der Pixel „unsichtbar" und bei 255 ist der Pixel komplett sichtbar. Hier könnte man die Daten wie oben in den letzten beiden Werten speichern.

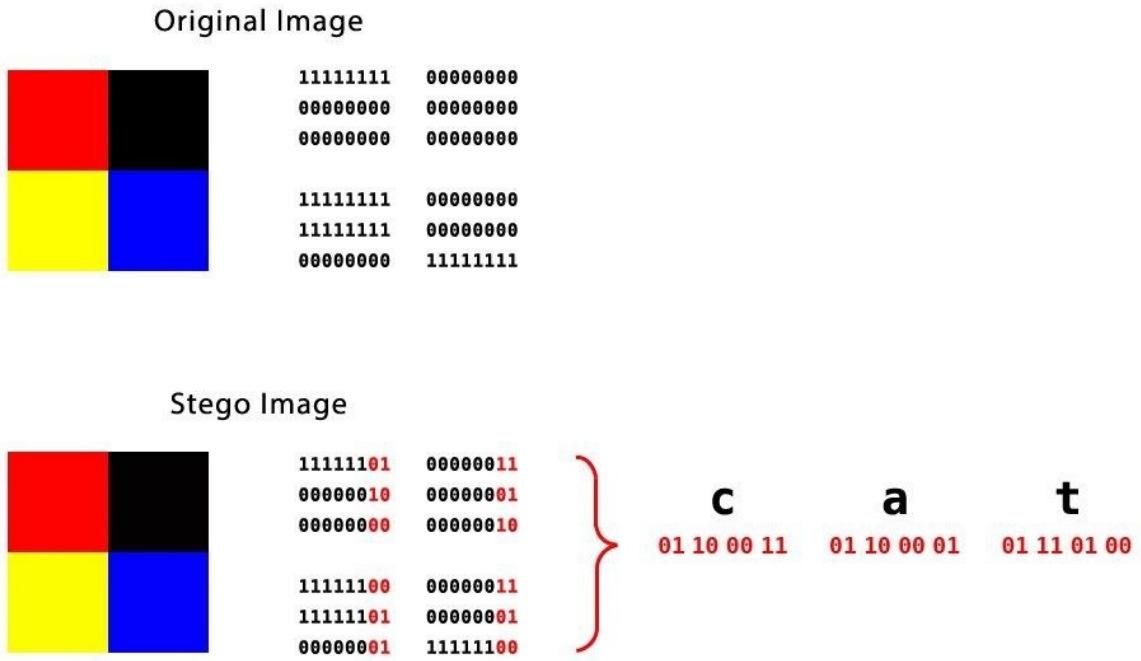

Bild 4.2: Codierung in den 2 letzten Bits [Use18]

Da die Transparenz keine direkte Auswirkung auf die Farbe der Pixel hat, kann man jedoch auch mehr Daten speichern.

Verwendung von „Shamir's Secret Sharing" Methode

Die Shamir's Secret Sharing Methode ist ein mathematisches Verfahren, das es möglich macht, ein Geheimnis auf mehrere Instanzen aufzuteilen. Dabei sind das Geheimnis und die dabei einstehenden „Shares" Integer-Werte.
Die einzelnen Instanzen können dabei keine Rückschlüsse auf das Geheimnis schließen. Allein wenn man den Großteil der „Shares" besitzt kann man das Geheimnis rekonstruieren.

Der folgende Abschnitt basiert auf dieser Literatur: [LT10]

Verschlüsseln:
Verwendet wird ein Geheimnis d, eine Anzahl von n Instanzen und eine Schwelle k < n.

1. Es wird eine Primzahl p zufällig gewählt.

2. Es werden k-1 Werte $c_1, c_2...., c_{k-1}$ mit den Werten zwischen 0 und p-1 vergeben.

3. Für $x_1, x_2.., x_n$ jeweils eine eindeutige reale Zahl wählen.

4. Mit Hilfe einer Polynomgleichung mit dem Grad k-1 werden nun n Gleichungen und somit auch Werte berechnet. $i = 1, 2, ..., n$

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + ... + c_{k-1} x_i^{k-1}) mod(p)$$

5. Nun können die n Shares erstellt werden. Diese sind wie folgt Aufgebaut $(x_i, F(x_i))$

Das Geheimnis ist nun in einer Funktion „abgespeichert". Die Shares sind Punkte, die auf dieser Funktion liegen. Damit die Funktion wieder rekonstruiert werden kann, müssen mindestens k der n Shares vorhanden.

Entschlüsseln:

Um die Nachrichten zu entschlüsseln müssen k Shares in die Formel oben eingesetzt werden.
Das hierdurch entstandene Gleichungssystem mit den Unbekannten d und c_1 bis c_{k-1}, kann zum Beispiel mit dem Gaußsches Eliminationsverfahren oder durch die Lagrangesche Interpolationsformel gelöst werden.

Dieses Verfahren kann man dazu verwenden, um Nachrichten unauffällig in den alpha Kanal eines PNG Bildes zu integrieren.
Die zu übertragende Nachricht M wird hierzu in Segmente von t Bit, mit $t = 3$ unterteilt. Bei der Umwandlung der Segmente in Dezimalzahlen entsteht so ein neues Array $M' = d_1, d_2...$ bei dem die Werte zwischen 0 und 7 liegen.

Im Gegensatz zu dem original Algorithmus greift man hier zusätzlich auf die Werte c_1, c_2 und c_3 zurück um hier Ebenfalls ein „Geheimnis" einzubetten. Zusammen mit d können nun k Werte integriert werden.

So ergibt sich:

$d = m_1, c_1 = m_2, c_2 = m_3, c_3 = m_4$

Folgende Werte werden definiert:

$p = 11$
$x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$

x kann hier eine beliebige Zahl annehmen und so als eine Art Verschlüsselung dienen. Fraglich ist, ob es sich dann noch um reine Steganografie handelt.

Die Werte von q_1 bis q_4 erben sich dann durch Einsetzten in sie Polynomgleichung.

$q_1 = F(x_1) = (m_1 + m_2x_1 + m_3{x_1}^2 + m_4{x_1}^3)mod(p)$
$q_2 = F(x_2) = (m_1 + m_2x_2 + m_3{x_2}^2 + m_4{x_2}^3)mod(p)$
$q_3 = F(x_3) = (m_1 + m_2x_3 + m_3{x_3}^2 + m_4{x_3}^3)mod(p)$
$q_4 = F(x_4) = (m_1 + m_2x_4 + m_3{x_4}^2 + m_4{x_4}^3)mod(p)$

Die Werte q_1 bis q_4 können nun beispielsweise in den alpha Kanal eines PNG Bildes eingefügt werden. Durch die modulo Funktion entstehen so entstehen Werte zwischen 0 und 10. Damit das Bild eine möglichst niedrige Transparenz bekommt muss der alpha Wert so groß wie möglich sein. Deshalb wird zu q jeweils der Wert 245 addiert, um so nah wie möglich an 255 zu kommen.
Die neu entstandenen Werte q'_1 bis q'_4 kann man nun in den alpha Kanal einfügen und über eine sensible Datenverbindung übertragen.

Zum Entschlüsseln muss man nun wieder 245 von den Werten des alpha Chanel subtrahieren. Durch das Erstellen und Lösen des Gleichungssystems, mit den oben gezeigten Formeln, können die Wert m_1 bis m_4 wieder berechnet werden.

5 Bewertung der Methoden

6 Welcher Kanal ist geeignet

7 Projekt Umsetzung

]

8 Etische Aspekte

9 Schlussbemerkungen und Ausblick

A Ein Kapitel des Anhangs

Literatur

[CBS04] Cabuk, Serdar, Carla E Brodley Clay Shields: *IP covert timing channels: design and detection. Proceedings of the 11th ACM conference on Computer and communications security*, 178–187. ACM, 2004.

[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.

[KP00] Katzenbeisser, Stefan Fabien Petitcolas: *Information hiding techniques for steganography and digital watermarking.* Artech house, 2000.

[LC17] Lockwood, Robert Kevin Curran: *Text based steganography.* International Journal of Information Privacy, Security and Integrity, 3(2):134–153, 2017.

[LT10] Lee, Che-Wei Wen-Hsiang Tsai: *A new steganographic method based on information sharing via PNG images. 2nd International Conference on Computer and Automation Engineering (ICCAE)*, 2010.

[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.

[Use18] User: Black Slash: *How to Hide Secret Data Inside an Image or Audio File in Seconds.* https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/, 2018. Abrufdatum: 22.01.2019.

[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.