HTBLuVA St. Pölten
Höhere Abteilung für Informatik

DIPLOMARBEIT

Einsatz von Steganographie

im Projekt GeocachingTools

Ausgeführt im Schuljahr 2016/17 von:

Simon Lehner-Dittenberger, 5AHIF-10

Betreuer/Betreuerin:

OSTR Mag. Otto Reichel

St.Pölten, am 16. Februar 2017

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche erkenntlich gemacht habe.

Simon Lehner-Dittenberger

St.Pölten, am 24.04.20XX

Diplomandenvorstellung

Max MUSTERMANN

Geburtsdaten:
06.02.1996 in Musterort

Wohnhaft in:
Musterstraße 13/1
3100 Musterstadt

Werdegang:
2010 - 2015:
HTBLuVA St.Pölten, Abteilung für Informatik
2006 - 2010:
Bundesrealgymnasium Wieselburg a. d. Erlauf

Kontakt:
max.mustermann@gmx.at

Danksagungen

Danke

Zusammenfassung

Abstract

Inhaltsverzeichnis

Kapitel 1

Übersicht

1.1 Was ist Steganographie

Die Steganographie ist eine Methode, die sich mit dem Verstecken von zu übermittelnden Nachrichten beschäftigt und kam schon in der Antike zum Einsatz. Das Wort kommt aus den griechischen Wörtern ”stegano” und ”graphein”, was übersetzt ”bedeckt schreiben” bedeutet [L: StegoGeschichte]. Dabei wird meist ein Text, aber auch andere Arten von Informationen, in einem Trägermedium versteckt. Diese Kombination wird als Steganogramm bezeichnet. Das Medium sollte so gewählt sein, dass sich die einzubettenden Daten leicht integrieren lassen. Außerdem benötigt es ein gewisses Maß an Entropie, damit Unregelmäßigkeiten nicht so stark auffallen, denn eine Blume ist in einer bunten Blumenwiese schwerer zu finden, als auf einem asphaltierten Parkplatz. Ziel ist es immer, die Wahrnehmungsschwelle eines Menschen so weit zu unterschreiten, dass man gar nicht auf die Idee kommt überhaupt nach einer versteckten Nachricht zu suchen. [1]

Die Möglichkeiten für Steganogramme haben sich mit der Entwicklung von Computer und elektronischer Datenverarbeitung sehr stark verändert, die Idee dahinter ist jedoch die Gleiche: Man versteckt Informationen. Früher hat man noch Beispielsweise mit unsichtbarer Tinte geschrieben, welche erst mit Hitze sichtbar wird (z.B. Zitronensaft). Auch wurden Techniken wie etwa die monoalphabetische Substituion benutzt, bei welcher Buchstaben des zu versteckenden Wortes über eine Tabelle durch Wörter ersetzt werden. Diese Wortfolge wird dann mit weiteren nicht in der Tabelle vorkommenden Worten ergänzt um vollständige, grammatikalisch korrekte Sätze bilden zu können. Eine solche Tabelle findet man zum Beispiel in dem Buch 1 der Polygraphia

[1] TODO Welche Techniken wofür gut sind und welche Trägermaterialen man braucht wird in den späteren abschnitten behandelt

von Johannes Trithemius (Siehe: Figure 1.1). Heute werden vor allem Verfahren eingesetzt, die Bilder und Videos nutzen, denn man kann die große Menge an Daten verwenden, welche jeden Tag millionenfach versendet werden. Diese können mit den richtigen Programmen auch sehr leicht manipuliert und bearbeitet werden, um sie als Steganogramme einzusetzen.

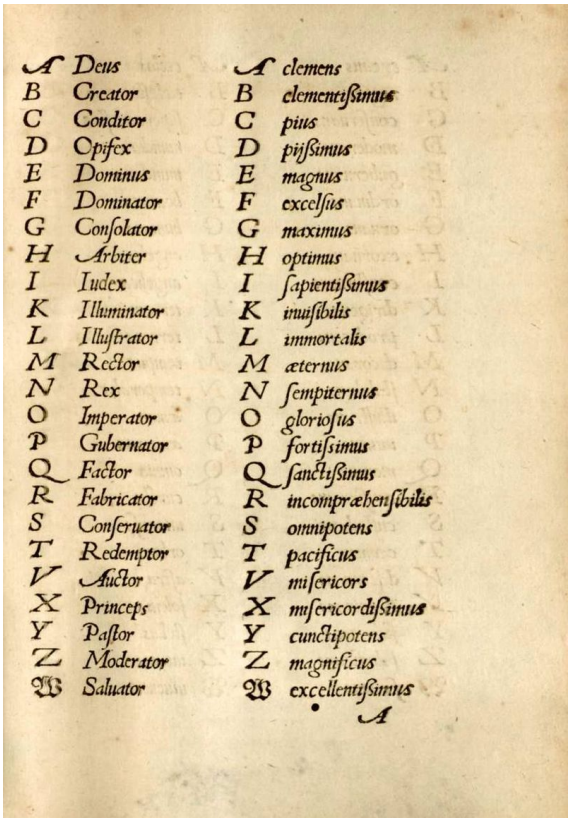

Abbildung 1.1: Buchstaben-Wort-Substitutionstabelle von Buch I der Polygraphia von Johannes Trithemius, Quelle: `http://daten.digitale-sammlungen.de/bsb00026190/image_71`

1.2 Abgrenzung zur Kryptographie

Kryptographie und Steganographie werden oft gemeinsam verwendet, wodurch meist nicht genau zwischen diesen beiden Verfahren unterschieden wird. Wie man in Table 1.1 [2] sehen kann, wirken beide Techniken auf den ersten Blick sehr ähnlich, sind aber bei genauerer Betrachtung zwei komplett unterschiedliche Verfahren. Wichtig ist hier vor allem zu beachten: Steganographie schützt Daten nicht vor Dritten, wenn diese gezielt danach Suchen und wenn sie sich sicher sind, dass in den Informationen,

[2] TODO Wie bekommt man die richtige Bezeichnung hier in den Text(unterschied zwischen label und caption)

die Ihnen vorliegen weitere Nachrichten versteckt wurden. Des Weiteren haben Steganogramme die Eigenschaft zwar von Menschen schlecht erkannt werden zu können, von Computern jedoch meist relativ schnell eine versteckte Nachricht sichtbar gemacht werden kann. Bei dem Erfolg eines computergestützten Verfahren kommt es aber sehr stark auf die verwendete Technik und die verfügbare Rechenleistung an.

Steganographie	**Kryptographie**
stegano = verdeckt graphein = scrheiben	krypte = geheim graphein = schreiben
Die Nachricht wird verborgen, nicht verschlüsselt	Die Nachricht wird verschlüsselt nicht verborgen
Scheinbar existiert gar keine Nachricht	Die Nachricht existiert, kann aber nicht gelesen werden

Tabelle 1.1: Vergleich zwischen Steganographie und Kryptographie, Quelle: [L: Stego VS Crypto]

Am sichersten ist es, wenn man beide Verfahren kombiniert. Dadurch hat man nicht nur die Vorteile der Kryptographie (Vertraulichkeit, Integrität und Authentizität), sondern auch die der Steganographie. Interessant ist hier vor allem die Eigenschaft von Verschlüsselungen: Diese gelten dann als sicher, wenn sie den Klartext derart verändern, dass er keine statistischen Merkmale des ursprünglichen Text mehr aufweist. Der Geheimtext kann also bei guten Verschlüsselungsverfahren statistisch nicht mehr von Rauschen unterschieden werden. Wenn man dieses ”Rauschen” dann mit Hilfe von Steganographie in ein unauffälliges Trägermedium einbettet, ist es selbst mit elektronischer Datenverarbeitung nicht mehr möglich, eine Nachricht im Steganogramm zu entdecken. Die einzige Möglichkeit für Dritte hier noch etwas herauszufinden, ist es das Steganogramm mit dem originalen Trägermaterial zu vergleichen. Hier fallen dann Unterschiede auf. Diese Technik ist aber in der Praxis selten anwendbar, denn einzigartige Trägermaterialien können sehr leicht hergestellt werden (z.B. Digitalfotografie) und weil das Trägermedium nicht zum Dekodieren benötigt wird, kann das Original nach der Erstellung des Steganogramm gelöscht werden.

1.3 Einsatzgebiete

Steganographie schützt Daten nicht vor Missbrauch, warum sollte man sie dann überhaupt verwenden, wenn Kryptographie viel sicherer ist? In der westlichen Welt ist Verschlüsselung durch das Internet so weit verbreitet, dass es als selbstverständlich erscheint, seine Daten und Konversationen verschlüsselt zu speichern. Doch in vielen Ländern ist es auch heute noch illegal solche Techniken einzusetzen. Selbst in den Vereinigten Staaten von Amerika gab es noch bis in das Jahr 2000 sehr restriktive

Gesetze was Verschlüsselung anbelangt. Das führte soweit, dass sogar ein T-Shirt auf welches der Source-Code für RSA-Encryption gedruckt wurde, unter das Waffengesetz fiel, als "export-restricted munition" deklariert und für den Export verboten wurde.

Hier kommt Steganographie zum Einsatz. Sie bietet eine Möglichkeit seine Daten und sich selber trotz der lokal geltenden Gesetze zu schützen. Nicht nur dass es schwer zu erkennen ist, ob sich überhaupt versteckte Daten auf einem Laufwerk befinden, steganographische Verfahren werden meist gar nicht von den Gesetzten verboten. Man befindet sich meist in einer Grauzone, was einem einen gewissen Verhandlungsspielraum verschafft.

Sie bietet auch Schutz vor potentiellen Hackern. Denn während bei verschlüsselten Daten ein sich lohnendes Ziel auf den Angreifer wartet, ist es bei Steganographie sehr unwahrscheinlich etwas Verwertbares zu finden, falls überhaupt etwas vorhanden ist. Dadurch macht man sich als Opfer sehr unattraktiv.

[L: StegoVersteck]

1.4 Steganographie als "Wicked Problem"

Die Steganographie besitzt viele Eigenschaften von sogenannten "Wicked Problems".

- Es gibt keine genaue Definition des Problems
- Sie haben keine Stopp-Regel ("Hat man auch wirklich nichts übersehen?")
- Es gibt keinen ultimativen und sofortigen Test für die Richtigkeit von Lösungen des Problems
- Wicked Problems haben weder eine abzählbare Lösungsmenge, noch gibt es eine gut beschriebene Gruppe an gültigen Operatoren

Diese Eigenschaften und die Tatsache das Kommunikation schwer zu definieren ist, führen dazu, dass paranoide oder phantasievolle Menschen glauben, Nachrichten zu empfangen, obwohl keine vorhanden sind. Da können selbst kleine unbedeutende Handlungen von Mitmenschen als geheime Nachrichtenübertragung interpretiert werden, was unter anderem zu Problemen führen kann, wo eigentlich keine sind.

Doch auch in der Verbrechensaufklärung kann die Wicked-Problem Eigenschaft von Steganographie zum Problem werden. Wird hier denn wirklich neben der offensichtlich

übertragenen Information noch eine versteckte Nachricht mitgesendet? Eine verdächtige Person kauft jeden Tag einen Kaffee auf dem Weg zur Arbeit. Die Verkäuferin ist die Freundin von dem Steuerberater des Chefs des Verdächtigen. Plötzlich kauft er aber einen Kräutertee. Hat er jetzt den Steuerberater vor irgendetwas gewarnt oder hat er heute nur Halsweh und möchte seinen Hals schonen? Das ist eben die Natur von Wicked Problems. Man kann sich nie sicher sein, denn es gibt weder eine genaue Fragestellung, noch ein eindeutiges Erfolgskriterium oder eine klar definierte Ausgangslage.

Kapitel 2

Moderne Steganographie

Mit moderner Steganographie sind Verfahren gemeint, welche nur mit Hilfsmittel der elektronischen Datenverarbeitung funktionieren. Sie verlassen sich meist darauf das in riesigen Zahlenmengen kleine Hinweise versteckt sind. Solch große Datenmengen lassen sich per Hand nicht mehr berechnen, wie etwa die vielen Millionen Bildpunkte auf einer digital Fotografie.

In dem nachfolgendem Kapitel werden einige dieser Verfahren erklärt und etwaige Fehler und Schwierigkeiten die damit verbunden sind aufgezeigt. Außerdem werden einige Implementierungen gezeigt, verglichen und auf die Verwendbarkeit im Alltag getestet.

2.1 Verstecken von Dateien

[1] Die Dateisysteme der Betriebssysteme bieten zahlreiche Möglichkeiten um seine Daten für dritte schwer auffindbar zu machen. In der folgenden Tabelle werden einige Verfahren verglichen und anschließend genauer erläutert. Es ist jedoch zu Bemerken, dass es sich hier um sehr einfache Verfahren handelt die höchstens Schutz gegen Computeranfänger bietet und für jeden Forensiker keine Herausforderung darstellen.

Beschreibung	Anwendbarkeit	Human Attack	Computer Attack
Alternativer Datenstream	ext. Programm wird benötigt	mittel	einfach
Dateien Verketten	überall unterstützt	mittel	einfach
Versteckte Datei	überall unterstützt	einfach	einfach
Dateiendung verändern	nur auf windows und osx [2]	einfach	sehr einfach

[1] TODO Ist das wirklich Steganographie?

2.1.1 Alternativer Datenstream

Die alternativen Dateistreams wurden von Windows bei ihrem Dateisystem NTFS deshalb eingefügt, da sie auch das Dateisystem von Apple HFS unterstützen wollten. Dort werden sogenannte Resource Forks verwendet um weitere Informationen wie Icons für Dateien zu speichern. Diese Dateistreams sind mit dem normalen Datei Explorer von Windows nicht direkt sichtbar, können aber erahnt werden wenn man die in den Eigenschaften angezeigte Größe mit der tatsächlichen Größe vergleicht. Vor allem für große versteckte Dateien wie Bilder oder Videos können hier leicht große Unterschiede erkannt werden.

Erstellen von ADS unter Windows

Alternative Dateistreams können nicht einfach mit dem Windows Explorer erstellt werden. Die einfachste Möglichkeit unter Windows alternative Dateistreams zu erstellen ist über die Kommandozeile. Angesprochen werden die einzelnen Streams über den Dateinamen der sichtbaren Trägerdatei und einem mit Doppelpunkt getrennten Namen für den Stream. Über diesen Bezeichner kann nun jedes Programm auf den alternativen Stream zugreifen.

Als Trägerdatei kann jede beliebige Datei verwendet werden. Je größer die gewählte Trägerdatei ist, desto unwahrscheinlicher ist es das jemanden der zusätzliche Datenstream auffällt. In dem folgenden Beispiel wird die Datei ”unscheinbare_textdatei.txt” über die Windows-Kommandozeile erstellt und mit einem unbedeutenden Text befüllt.

```
1 echo "Hallo Welt, hier ist nichts." > unscheinbare_textdatei.txt
```

Nun kann man mit dem gleichen Befehl und einem angepassten Dateinamen auf gleiche Weise alternative Datenstreams befüllen.

```
1 echo "Geheim" > unscheinbare_textdatei.txt:geheimer_stream.txt
```

Sowohl die Trägerdatei als auch der alternative Stream können mit jedem beliebigen Programm jederzeit bearbeitet werden. Zu beachten ist nur wieder das der Explorer und alle ”Datei öffnen” Dialoge die geheimen Streams nicht anzeigt. Dazu muss man wieder auf die Kommandozeile zurückgreifen. Zum Beispiel kann man den Stream mit dem Programm Notepad von Windows öffnen.

```
1 notepad unscheinbare_textdatei.txt:geheimer_stream.txt
```

Wie man sehen kann können diese alternativen Streams von jedem Programm ohne viel Mehraufwand geöffnet werden. Sie stellen also keinen ausreichenden Schutz vor ungewollten Zugriff auf den Inhalt da.
Um sich eine Übersicht über alle Dateien und ihre Streams machen zu können gibt es zahlreiche fertige Tools, welche ohne viel Aufwand das gesamte Dateisystem nach solchen Strukturen durchsuchen. Bei einem konkreten Verdacht kann jedoch auch das bei Windows mitgelieferte Programm dir verwendet werden. Man navigiert über die Kommandozeile in den jeweiligen Ordner und dort ruft man den dir Befehl mit dem Parameter $/r$ auf.

```
C:\stuff>dir /r
Datenträger in Laufwerk C: ist Windows
Volumeseriennummer: F8D1-CAC1

Verzeichnis von C:\stuff

16.02.2017  17:37    <DIR>          .
16.02.2017  17:37    <DIR>          ..
16.02.2017  17:44                28 unscheinbare_textdatei.txt
                                 11 unscheinbare_textdatei.txt:geheimer_stream
                                    .txt:$DATA
```

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Literaturverzeichnis

[L: StegoGeschichte] https://igw.tuwien.ac.at/designlehren/steganographie.pdf
Eine kurze Geschichte der Steganographie
Peter Purgathofer
12.11.2016

[L: Stego VS Crypto] http://digilib.happy-security.de/files/Steganographie.pdf
Kryptographie und Informationstheorie: Steganographie
Prof. Dr. Richard Eier, Institut für Computertechnik TU Wien
Michaela Schuster [3]
20.11.2016

[L: StegoVersteck] http://www.tecchannel.de/a/vertrauliche-daten-perfekt-ver
2024281
Vertrauliche Daten perfekt versteckt, Artikel vom 30.11.2009
pte pte
13.12.2016

[1] https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States

[3] TODO Ist Schuster der Autor oder Dr. Richard Eier? Außerdem - Ist das so richtig als Quelle drinnen?

[Kopka1] Helmut Kopka: *Latex Band 1, Einführung*
Addison-Wesley, 2000
ISBN: 3-8273-7038-8

[Demmig 1] Demmig, Thomas:
jetzt lerne ich Latex 2
Markt+Technik, 2004
ISBN 3-8272-6517-7

[Web 1] http://www.meta-x.de/faq/LaTeX-Einfuehrung.html
Latex-Einführung
28.September 2012

[JavaDoc05] http://docs.oracle.com/cd/E12839_01/core.1111/e10043/introjps.htm
Oracle Security Guide über das Java Sicherheits Model
13.11.2014