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 20. November 2016

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 Wörter ”stegano” und ”graphein”, was übersetzt ”bedeckt schreiben” bedeutet [?]. 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, das 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 zu unterschreiten, dass niemand 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: Wir verstecken 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 von Johannes Trithemius (Siehe: Figure 1.1).

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

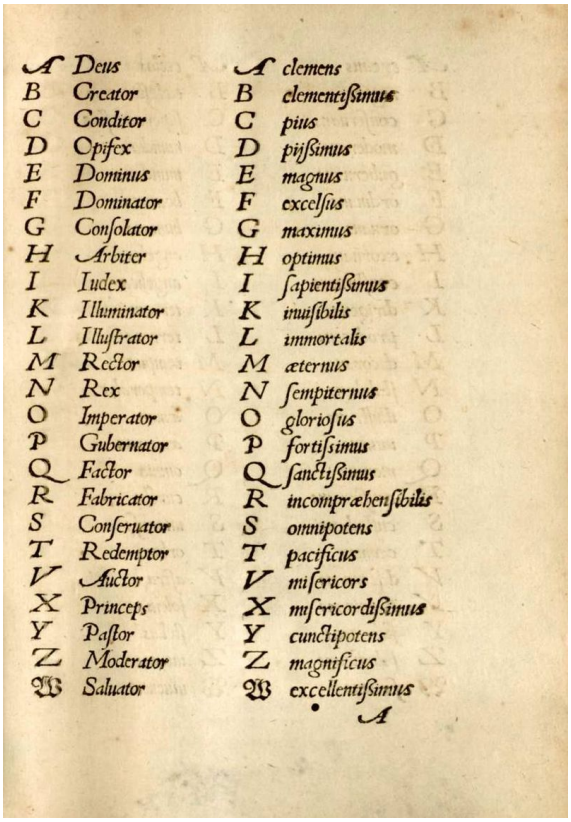

Abbildung 1.1: Buchstaben-Wort-Substitutionstabelle von Buch I der Polygraphia von Johannes Trithemius, Quelle: `http://daten.digitale-sammlungen.de/bsb00026190/image_71`

Zum Beispiel wenn ein Spion eine Nachricht an seinen Auftraggeber sendet kann er diese nicht einfach nur verschlüsseln, denn ganz nach dem Satz ”Wer nichts zu verbergen hat braucht auch nicht verschlüsseln” könnte jemand auf die Idee kommen das hier verbotene Informationen weitergegeben werden. Das ist der Moment wo man von Steganographie Gebrauch machen kann. Dabei wird nämlich die eigentliche Nachricht, ob jetzt verschlüsselt oder nicht, in einer weiteren unauffälligen Nachricht versteckt. Für einen dritten ist nun nicht mehr ersichtlich ob sich Tatsächlich weitere Informationen in dem unauffälligen Trägertext vorhanden sind. Er schöpft somit keinen Verdacht mehr das hier ein verbotener Informationsaustausch stattfindet.

1.2 Einsatzgebiete

1.3 Vor- und Nachteile

1.4 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 sich sicher sind, das in den Informationen 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 durch Analysen und Vergleiche eine versteckte Nachricht sichtbar gemacht werden kann. [3] Dabei kommt es wieder sehr stark auf die verwendete Technik an.

Am sichersten ist man wenn man beide Verfahren kombiniert. Dadurch hat man nicht nur die Vorteile der Kryptographie, nämlich 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, das er keine statistischen Merkmale des ursprünglichen Text mehr aufweist. Der Geheimtext ist dann nicht mehr von Rauschen zu unterscheiden. 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 das Steganogramm mit dem originalen Trägermaterial zu vergleichen, hier fallen dann Unterschiede auf. Das ist aber selten machbar, denn die originalen Trägermaterialien können gleich nach der Erzeugung des Steganogramm vernichtet werden.

1.5 Steganographie als ”Wicked Problem”

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

[3] TODO Dazu mehr in den Punkten XYZ (z.B:) Wicked Problem

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]

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 [4]
20.11.2016

[4] 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