
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 13. Dezember 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

Vorwort	i
Diplomandenvorstellung	ii
Danksagungen	iii
Zusammenfassung	iv
Abstract	v
Inhaltsverzeichnis	vi
1 Übersicht	1
1.1 Was ist Steganographie	1
1.2 Einsatzgebiete	2
1.3 Vor- und Nachteile	2
1.4 Abgrenzung zur Kryptographie	2
1.5 Steganographie als "Wicked Problem"	4
Anhang	5
Tabellenverzeichnis	6
Verzeichnis der Listings	7
Literaturverzeichnis	8

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 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 Substitution 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).

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

A Deus	A clemens
B Creator	B clementissimus
C Conditor	C pius
D Opifex	D piissimus
E Dominus	E magnus
F Dominator	F excelsus
G Consolator	G maximus
H Arbitrator	H optimus
I Iudex	I sapientissimus
K Illuminator	K inuisibilis
L Illustrator	L immortalis
M Rector	M aeternus
N Rex	N sempiternus
O Imperator	O gloriosus
P Gubernator	P fortissimus
Q Factor	Q sanctissimus
R Fabricator	R incomprehensibilis
S Conservator	S omnipotens
T Redemptor	T pacificus
V Auctor	V misericors
X Princeps	X misericordissimus
Y Pastor	Y cunctipotens
Z Moderator	Z magnificus
W Saluator	W excellentissimus

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

1.2 Einsatzgebiete

Steganographie schützt Daten nicht vor Missbrauch, warum sollte man sie dann überhaupt verwenden, wenn Kryptographie viel sicherer ist?

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 Ta-

ble 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 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 Bei dem Erfolg eines computergestützten Verfahrens kommt es aber sehr stark auf die verwendete Technik und die verfügbare Rechenleistung an.

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 es nach der Erstellung des Steganogramm gelöscht/vernichtet werden.

Steganographie	Kryptographie
stegano = verdeckt graphie = schreiben	krypte = geheim graphie = 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]

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

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

1.5 Steganographie als "Wicked Problem"

Abbildungsverzeichnis

1.1	Buchstaben-Wort-Substitutionstabelle von Buch I der Polygraphia von Johannes Trithemius, Quelle: http://daten.digital-e-sammlungen.de/bsb00026190/image_71	2
-----	--	---

Tabellenverzeichnis

1.1	Vergleich zwischen Steganographie und Kryptographie, Quelle: [L: Stego VS Crypto]	3
-----	---	---

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 Schuster⁴
20.11.2016

[L:] <http://www.tecchannel.de/a/vertrauliche-daten-perfekt-versteckt,2024281>

⁴TODO 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