Eine kurze Geschichte der Steganographie

Peter Purgathofer

Das Bedürfnis nach geheimer Kommunikation ist vermutlich so alt wie unsere Fähigkeit zu kommunizieren. Steganographie ist aber mehr als geheime Kommunikation. »Ins-Ohr-flüstern« ist keine Steganographie, ebenso wenig wie die Verwendung von Geheimcodes und Verschlüsselungen, gemeinhin als »Kryptographie« bezeichnet. Steganographie ist die Kunst (oder auch die Wissenschaft), auf dem Rücken einer Kommunikation huckepack noch eine zweite, hoffentlich unentdeckte Informationsübertragung geschehen zu lassen. Dabei ist es irrelevant, ob die zur verdeckten Kommunikation missbrauchte originale Datenübertragung eigenständige Bedeutung hat, oder ob sie vollkommen irrelevant ist und nur zum Verschleiern der versteckten Information initiiert wurde.

Bevor ich Steganographie historisch und technisch etwas näher diskutieren möchte, ist es notwenig, einige Eigenschaften technisch-kryptographischer Verschlüsselung zu erklären, was ich im folgenden kurz tun möchte.

Kryptographie

Kryptographie ist die Wissenschaft der Verschlüsselung von Information, also der methodischen Umwandlung von »lesbarer« Information in unverständliche Daten. Verschlüsselungsverfahren gelten aus heutiger Sicht als sicher, wenn die aus der Verschlüsselung hervorgehenden Daten keinerlei statistische Auffälligkeiten mehr aufweisen. Jedes Muster, das im verschlüsselten Text zu finden ist, wäre nämlich Ansatzpunkt für einen »Angriff« auf die Verschlüsselung mit dem Ziel, den Text zu entschlüsseln. Idealerweise erzeugt ein gutes Verschlüsselungsverfahren also Daten, die statistisch von Rauschen nicht zu unterscheiden sind.

Ein zweites Prinzip moderner technischer Kryptographie ist, dass das die Sicherheit der Verschlüsselung zwar vom verwendete Veschlüsselungsverfahren abhängig ist, nicht aber von dessen Geheimhaltung. Diese als Kerckhoffs' Prinzip bezeichnete Eigenschaft besagt, dass gute Verschlüsselungsalgorithmen auch dann sicher sind, wenn bekannt ist, wie sie funktionieren, da die Sicherheit ausschliesslich von der Geheimhaltung des verwendeten Schlüssels abhängt. Verschlüsselungsverfahren, die geheim gehalten werden müssen, damit sie vor Angriffen sicher sind, gelten als schwache kryptographische Verfahren.

Kerckhoffs' Prinzip kann in der Steganographie nicht angewendet werden. Verdeckte Kommunikation kann nur funktionieren, wenn das verwendete Verfahren geheim bleibt. Im Gegensatz zu kryptographischen Verfahren verlässt man sich beim Verstecken von Nachrichten auf »Security by Obscurity«, sodass Kreativität und Originalität der verwendeten Verfahren von besonderer Bedeutung sind. Das Knacken von Verschlüsselung ist ein mathematisches Problem, das Entdecken steganographischer Kommunikation hingegen ist ein Problem, das nur mit systematischer Suche und detektivischem Spürsinn, eventuell unterstützt von statistischen Analysen, gelöst werden kann.

Kryptographie - ein Beispiel

Mit dem Verschlüsselungsgerät »Enigma«, das in Deutschland im Gefolge des Ersten Weltkriegs entwickelt wurde, stand den Nationalsozialisten ein Verfahren zur Verfügung, dass ihnen im sich anbahnenden Zweiten Weltkrieg einen entscheidenden Vorteil geben würde. Es ist Alan Turing zu verdanken, dass dieser Vorteil sich schliesslich in einen Nachteil verwandelte: der britische Mathematiker konnte, aufbauend auf den Vorarbeiten polnischer Hacker, ein Gerät entwickeln, mit dem eine Entschlüsselung von mit der Enigma verschlüsselten Texten möglich war, ohne dass die Schlüssel bekannt sein mussten. Späte Versionen der »Turing-Bombe« knackten Nachrichten in etwa sechs Minuten.

Wesentlich ist hier wiederum, dass mit der Enigma verschlüsselte Texte klar und deutlich als solche erkennbar waren. Das »Problem« war damit klar definiert: entschlüssele diese verschlüsselte Nachricht, knacke den Code der Enigma. Entscheidend bei der Kryptoanalyse der Nachrichten war die Tatsache, dass bekannt war, dass bestimmte Teile der Nachrichten wiederholend ident waren. So wurde beispielsweise jede Nachricht mit dem Gruß »Heil Hitler« unterzeichnet, was in der Analyse zum »Brechen« der Verschlüsselung von wesentlichem Vorteil ist. Man könnte sagen, dass die autoritäre Struktur der Wehrmacht ihr hier das Rückgrat gebrochen hat.

Aus heutiger Sicht kann die Tatsache, dass die verschlüsselte Kommunikation der Deutschen gelesen werden konnte, als kriegsentscheidend angesehen werden. Es ist interessant anzumerken, dass es den Alliierten lange Zeit gelungen ist zu verbergen, dass man mit der Enigma verschlüsselte Nachrichten lesen konnte. Neal Stephenson beschreibt in seinem historischem Roman »Cryptonomicon« auch die Bemühungen, diesen Vorsprung aktiv vor deutschen Mathematikern zu verbergen.

Steganographie in der Geschichte

Historische Beispiele für steganographische Kommunikation gehen mehrere tausend Jahre zurück. Aus der Antike ist bekannt, dass der in Persien lebende Grieche Demaratos die Spartaner vor Xerxes' bevorstehender Invasion warnte, indem er die Information nicht in das Wachs einer Wachstafel ritzte, sondern auf die darunterliegende Holztafel schrieb. Mit Wachs überzogen konnte er die leere Tafel so problemlos nach Hause schicken. Die Griechen konnten sich daraufhin auf den Überraschungsangriff vorbereiten und die Armee der Perser in einer griechischen Bucht schlagen.

Heradot schilderte einen Vorfall, bei dem Histiaeus, der Tyrann von Milet, eine Nachricht an Aristagoras übermittelte, indem er sie auf den rasierten Kopf eines Sklaven tätowierte. Nachdem dessen Haare dicht genug nachgewachsen waren, konnte die Nachricht nicht mehr entdeckt werden, der Sklave wurde ohne Verdacht zu erregen durchgelassen, nur um sich beim »Empfänger« den Kopf zu rasieren und so die Nachricht zu offenbaren.

Während kriegerischer Auseinandersetzungen gibt es sozusagen naturgemäß ein gesteigertes Bedürfnis nach versteckter Kommunikation. Damals war es üblich, geheime Nachrichten in Form von Morsezeichen in Bildern, beispielsweise Modezeichnungen, zu verstecken. 2006 hat das britische Nationalarchiv in einer Ausstellung entsprechende Dokumente gezeigt. Die Kreativität dieser Beispiele zeigt deutlich den starken Bedarf nach versteckter Kommunikation. Darüber hinaus hat die

Anwendung von Steganographie eine enorme Anziehungskraft für Romanautor/innen, zu sehen beispielsweise in Dan Browns jüngstem Werk »The Lost Symbol«.

Bildsteganographie

Eine gängige und in der Presse immer wieder diskutierte Form der Steganographie ist die technische Bildsteganographie. Dabei wird Information in dem Datenstrom versteckt, der in einem Computer ein Bild repräsentiert. Ich möchte im folgenden eine Form der Bildsteganographie kurz und nachvollziehbar beschreiben.

Bilder sind im Computer als Matrix von Bildpunkten, genannt »Pixel« (von »picture elements«), repräsentiert. Jedes solche Pixel eines Farbbildes wird in der Regel durch drei Werte definiert, die für die Intensität von drei Farbwerten in diesem Pixel stehen: Rot, Grün und Blau, die Farben der additiven Farbkomposition. Mit diesen drei Farbwerten wird das Bild am Monitor dargestellt, indem das dort befindliche Anzeigenelement mit diesen Werten gefüttert wird. Das geschieht mit allen Pixel des Bildes, sodass es schliesslich am Bildschirm sichtbar wird.

Die drei Farbwerte sind üblicherweise jeweils durch ein Byte repräsentiert. Ein Byte ist die Darstellung eines Wertes zwischen 0 und 255 im Binärsystem in Form von 8 Bit. Genauso, wie im 10er-Zahlensystem die »Einerstelle« einer Zahl wesentlich weniger Einfluss auf den Wert einer Zahl hat als zB. die Hunderterstelle, so hat auch das »Einerbit« nur einen sehr geringen Wert, noch viel weniger als die »Einerstelle« unserer Zahlen. Eine Veränderung dieses »Least significant Bit« eines Bytes ändert den Wert eines Bytes höchstens um 1. Ein solcher Unterschied im Farbwert fällt in einem Bild mit freiem Auge nicht auf.

Mit den »Least significant Bits« der Farbwerte (insbesondere des Blauwerts) steht uns in einem Bild ein Informationskanal zur Verfügung, der verwendet werden kann um Nachrichten zu verstecken. Ein/e Absender/in muss also nur die bildsteganographisch zu übertragende Information mit einem geeigneten Verfahren in eine Kette aus Bits, eine Bitfolge, verwandeln und diese Bits in die »Least significant Bits« der Farbwerte des Bildes zu übertragen. Das Bild verändert sich damit nicht sichtbar, trägt aber dennoch eine versteckte Information. [1]

Es sieht so als, als könnte jetzt nur ein/e wissende/r Empfänger/in die Information mit einem geeigneten Umkehrverfahren aus dem Bild extrahieren und damit wieder lesbar machen. Tatsächlich stimmt das aber so nicht.

Die aus sinnvoller Information generierte Bitfolgen weisen Muster auf, die mit dem mehr oder weniger zufälligen Rauschen eines Bildes nicht übereinstimmen. Mittels geeigneter statistischer Analysen ist es also möglich, Bilder zu isolieren, die offenbar eine steganographisch eingebettete Information enthalten. Damit verwandelt sich das Problem in ein Entschlüsselungsproblem, das steganographische Verfahren ist plötzlich »nur« noch ein Verschlüsselungsverfahren, denn das Bild ist effektiv nur noch »Träger« einer irgendwie codierten Nachricht.

---

[1] Ein solcher bildsteganographischer En-/Decoder steht beispielsweise unter http://futureboy.us/stegano/ zur freien Verwendung im Internet.

An dieser Stelle ist es hilfreich, sich an die weiter oben beschriebene Eigenschaft von technischen Verschlüsselungsverfahren zu erinnern, dass nämlich gute Kryptographie aus einer Nachricht statistisches »Rauschen« erzeugt. Nehmen wir also einen geeigneten (im technischen Sinne) guten Verschlüsselungsalgorithmus zu Hilfe, können wir unsere Bitfolge vor der Einbettung in das Bild in statistisches Rauschen verwandeln. Wir ersetzen damit das in nahezu jedem digitalen Bild vorhandene Bildrauschen im »Least significant Bit« gegen ein anderes, nämlich das Rauschen der verschlüsselten Bitfolge.

Damit wird einer systematischen Untersuchung aller im Internet übertragenen Bilder jegliche Aussicht auf systematischen Erfolg verwehrt. Wir haben es mit einem technischen Artefakt – das die verschlüsselte Nachricht tragende Bild – zu tun, bei dem nicht mehr nachgewiesen werden kann, ob tatsächlich eine geheime Datenübertragung vorliegt. Jedes Bild könnte Informationsträger sein, auch wenn unter Umständen keines tatsächlich eine »Huckepack«-Nachricht trägt.

Dieses Verstecken von Information im »Rauschen« digitaler Medien ist auch in Video, Audio, sogar in Webseiten und neuerdings auch in automatisierten Übersetzungen möglich. Denkbar wäre zB. auch die Übermittlung von Information im Hintergrundrauschen eines harmlosen Gesprächs via Internet-Telefonie.

Kriminelle Anwendungen von Steganographie

Jeder gesellschaftlichen oder politischen Gruppierung, die nicht einwandfrei und immer im legitimierten Bereich operiert, wird früher oder später unterstellt, mit Hilfe steganographischer Mittel zu kommunizieren. Terroristen, Pädophile, militante Tierschützer, organisierte Kriminelle, Wirtschaftsverbrecher – sie alle wurden irgendwann in einschlägigen Medien bereits mit dieser Form der verdeckten Kommunikation in Verbindung gebracht. So berichtet USA Today beispielsweise 2001: »Lately, al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com«.

Diese durchaus glaubwürdigen Unterstellungen geistern seit vielen Jahren durch die Medien, ohne dass bis heute irgendein Beweis dafür aufgetaucht wäre Das ist nicht weiter verwunderlich, findet man in einem Report des SANS Institute (»An Analysis of Terrorist Groups Potential Use of Electronic Steganography«) folgendes Zitat: »Although there have not been any steganographic imagery located on the Internet, it is quite conceivable that steganography is being used to covertly transmit information between different parties given the historic use of steganography.«[2]

Durch die eben beschriebenen Eigenschaften der technischen Bildsteganographie wird das aber auch nahezu unmöglich gemacht. Verstärkt wird das noch durch die flüchtige Natur technisch vermittelter Kommunikation.

Eine der wenigen bekannten und bewiesenen kriminellen Anwendungen von Steganographie ist die Verwendung im Rahmen des »GhostNet«. GhostNet ist ein von kanadischen Computersicherheits-Experten entdecktes und so benanntes System aus Software, Hardware und kriminellen Betreiber/innen, das im Wesentlichen zur politischen Spionage verwendet wird.

---

[2] Quelle: http://www.sans.org/reading_room/whitepapers/stenganography/an_analysis_of_terrorist_groups_potential_use_of_electronic_steganography_554

Mitte 2008 wandten sich Mitglieder der tibetischen Exil-Regierung des Dalai Lama am Computersicherheits-Experten der Universität Toronto mit der Bitte, ihre Computer auf Schadsoftware zu untersuchen. Die Forscher fanden prompt ein System, mit dem es Hackern möglich war, die über die Rechner abgewickelte Kommunikation abzuhören und sogar zu manipulieren. Das System schien von China aus gesteuert zu sein (was angesichts der komplexen politischen Situation jetzt nicht unbedingt überraschend ist).

Eine detaillierte Darstellung des Ghostnet und seiner Arbeitsweise findet sich in Folge 191 des »Security Now«-Podcast (http://grc.com/securitynow).

Für uns relevant ist die bei der Analyse der Schadsoftware entdeckte Verwendung von bildsteganographischer Kommunikation zur Übermittlung von Anweisungen an die Schadsoftware. GhostNet verbindet sich regelmässig mit Rechnern, indem es diese Server wie Web-Server behandelt und dort gespeicherte Bilder abruft. In diesen Bildern sind steganographisch versteckt Anweisungen enthalten, die von der Schadsoftware extrahiert und ausgeführt werden. Dieses Vorgehen ist als Strategie zur Tarnung der Kommunikation zu sehen: Jede Form von Nutzung des WWW erzeugt genau diese Art von Datenströmen: Bilder, die von Web-Servern heruntergeladen werden.

»...the client makes an outbound web connection to this web server, which is the command-and-control web server. It does it to a PHP page, asking for a PHP page or in some cases running a CGI script, which is very common for any kind of automated pages. So it's just a standard port 80 HTTP connection. The commands are sent back encoded in JPEG images. So even if you were watching the traffic, you'd just see web activity with an image being retrieved in response to a PHP query, which happens all the time every day.«[3]

Frühere Formen von Schadsoftware haben spezifisch dafür eingerichtete Kommunikationskanäle verwendet, die nur dann entdeckt werden, wenn tief gehende Analysen des Netzwerkverkehrs durchgeführt werden. Durch die Verwendung eines offenen und ungeschützten Übertragungskanals versteckt sich die Kommunikation des Ghostnet im offensichtlichen und fällt genau deshalb nicht auf.

Steganographie in der Kunst

Künstler greifen immer wieder auf Methoden der Steganographie zurück, um weitere Inhalte und Nachrichten in ihren Werken zu verstecken. Eine recht verbreitete und bekannte Methode dazu ist die anamorphische Verzerrung. Das wohl bekannteste Beispiel für diese Vorgehensweise ist das Bild »Die Gesandten« von Hans Holbein dem Jüngeren, in dem ein Totenschädel erst dann erkennbar wird, wenn man von rechts oben in einem Winkel von etwa 27° auf das Bild schauen kann. Es ist nicht bekannt, warum Holbein den Schädel so verzerrt ins Bild gesetzt hat; verschiedene Theorien verweisen auf eine mögliche ursprünglichen Platzierung des Bildes in einem Stiegenhaus, wo der Schädel dann von einer bestimmten Stelle aus deutlich sichtbar sein würde, oder auch auf das Verlangen des Künstlers, hier seine technischen Fertigkeiten zu demonstrieren.

Komponisten und Musikern wurde immer wieder unterstellt, geheime Botschaften in ihren Werken zu verstecken. Schon Mozart wurde unterstellt, freimaurerische Symbole, Gedankengut und Botschaften

---

[3] Quelle: Security now Podcast, Episode 191, http://grc.com/securitynow

in die Zauberflöte eingearbeitet zu haben. Ravel soll den Namen einer Freundin, Misia Sert, mehrmals in seinen Werken in musikalischer Form repräsentiert haben.

In der Zeit derSchallkonserve und der technischen Produktion von Musik zum späteren Genuss kamen neue Formen der Musiksteganographie auf: »Backward Masking« bezeichnet eine Methode, bei rückwärts laufendem Band Nachrichten aufzunehmen, die wiederum nur durch verkehrtes Abspielen der Musik zu hören ist. In dem im Verlag und Schriftenmission der Evangelischen Gesellschaft für Deutschland 1984 erschienenen Buch »Wir wollen nur deine Seele« wird von vielen populären Rock-Musikern behauptet, sie würden geheime Botschaften satanistischer und antichristlicher Natur in ihrer Musik zu vermitteln. So wäre beispielsweise in Led Zeppelins wohl bekanntestem Stück »Stairway to heaven« bei verkehrtem Abspielen die Zeile »Oh, here's to my sweet satan, the one whose little path would make me sad, whose power is satan« zu hören.

Nicht nur Hardrock und Heavy Metal Bands wurden zu dieser Zeit solcher steganographischer Attacken auf die geistige Gesundheit der Jugend bezichtigt, auch ABBA wurde bezichtigt, solche Nachrichten zu verbreiten. So soll sich in ihrem Hit »Waterloo« die Zeile »get the gun, get the gun, shoot shoot shoot« finden, wenn man die Platte in der richtigen Geschwindigkeit rückwärts abspielt.

Solche Interpretationen sind wohl in den meisten Fällen der Tendenz unseres Wahrnehmungsapparats zuzuschreiben, auch noch verstümmelte Reste von gesprochener Kommunikation verstehen zu wollen. Wie bei geschriebenem Text können wir auch bei gesprochenem Text den Verlust von etwa die Hälfte der Information in der Übertragung verkraften. So können wir auch neben Lärmquellen noch verstehen, was uns gesagt wird, und auch undeutliche Sprecher/innen oder solche mit entsprechend starkem Akzent können noch richtig interpretiert werden. Jenseits der 50 % helfen uns der (angenommene) Kontext und auch unsere Wunschvorstellungen im Verstehen von gesprochener (oder gesungener) Sprache. Rückwärts abgespielte Musik stellt in diesem Sinne einen geradezu idealen Nährboden für die Projektion von Ängsten und Vorurteilen dar.

Mythos Steganographie

Gerade hier zeigt sich, dass »Kommunikation« ein Begriff ist, der sehr oft einseitig und aus der Interpretation eines möglichen Empfängers definiert ist. In vielen dieser Fälle liegt keinerlei versteckte Nachricht vor, phantasievolle oder neurotische Hörer/innen betrachten sich aber als Empfänger einer solchen. Erklärbar wird solches Verhalten durch eine wesentliche Eigenschaft steganographischer Kommunikation: sie stellt ein »wicked Problem« dar.

Verschlüsselte Nachrichten sind meist als solche erkennbar, so dass das wesentliche Problem im Umgang mit kryptograpisch gesicherter Kommunikation in der Entschlüsselung zu suchen ist. Steganographische Kommunikation hingegen erzeugt ein Mysterium: ist denn hier tatsächlich etwas versteckt? Gibt es neben der unmittelbar wahrnehmbaren und (mehr oder weniger) verständlichen »sichtbaren« Information auch einen unsichtbare? Im Gegensatz zum überschaubaren, klar definierten Problem der Entschlüsselung einer vorliegenden verschlüsselten Nachricht ist das Entdecken steganographischer Kommunikation ein nur schlecht definiertes Problem mit unklaren Grenzen. Solche Probleme werden auch als »wicked problems« bezeichnet – hinterhältige Probleme,

die kleine klar definierte Ausgangslage haben, keine eindeutigen Fragestellungen und kein eindeutiges Erfolgskriterium

Dadurch können Nachrichten entstehen, wo keine sind, und es findet Kommunikation statt, wo keine ist. Auch das ist eine der Eigenschaften steganographischer Kommunikation: oft gibt es sie gar nicht. Das macht es um so schwerer, an sie zu glauben, wenn man sie findet.

Epilog: Druckersteganographie

2005 wurde bekannt, dass seit etwa 15 Jahren (mehr oder weniger) alle Hersteller von Laser-Farbdruckern jedes gedruckte Blatt mittels eines verborgenen Muster aus mit freiem Auge nicht erkennbaren gelben Punkten identifizierbar machen. Mit entsprechenden Hilfsmitteln sichtbar gemacht offenbaren die verräterischen Farbspuren zumindest die Seriennummer des Druckers und den Zeitpunkt des Ausdrucks. Eingeführt wurde diese Markierung auf Regierungsdruck, angeblich um Dokumenten- und Geldfälschern effektiver Verfolgen zu können. Sie erlaubt natürlich auch die (zumindest grobe) Identifikation des Ursprungs von Flugblättern, kritischen Werken und politischen Schriften.

Mit diesem Beispiel wird eine weitere Eigenschaft steganographischer Kommunikation deutlich: während in den Medien die Anwendung solcher Methoden durch »kriminelle Elemente« angeprangert wird, werden dieselben Mittel auch seitens des Staates ohne unser Wissen oder unsere Zustimmung (zumindest potentiell) gegen uns eingesetzt.