Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag Magdeburg

Dieser Artikel erscheint in der Serie „Informationstechnik und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?“ Herausgegeben von Jörg Sambleben und Stefan Schumacher

Anonymität im Internet

Jens Kubieziel

Der Artikel stellt verschiedene Möglichkeiten der Anonymisierung im Internet vor und zeigt deren historische Entwicklung.

Schlüsselwörter:Anonymität, Überwachung, Internet, Remailer, Cypherpunks, Tor, Mixmaster

---

Zitationsvorschlag: Kubieziel, Jens (2012). Anonymität im Internet. Magdeburger Journal zur Sicherheitsforschung, Band 1, 2012, S. 168–178.

http://www.wissens-werk.de/index.php/mjs/article/viewFile/116/114

Überwachung und Kontrolle im Internet

Überwachung und Kontrolle im Internet beschäftigen von Jahr zu Jahr mehr Menschen. Zum einen arbeiten immer mehr Menschen auf diesem Gebiet und zum anderen machen sich andere Gedanken, wie Kontrolle und Überwachung umgangen werden können. Die Liste der Feinde des Internet der Nichtregierungsorganisation Reporter ohne Grenzen wächst seit ihrer Erstausgabe. Dort finden sich bekannte Länder wie China oder Iran. Aber in der Ausgabe des Jahres 2011 sind auch Australien und Frankreich zu finden.

Anonymität im Internet

Im folgenden soll die Entwicklung der Anonymität im Internet anhand einiger charakteristischer Beispiele nachgezeichnet werden. Die Entwicklung so genannter Remailer war sehr wichtig. Dort wurden praktische Erfahrungen gesammelt und wichtige Erkenntnisse für spätere Weiterentwicklungen gewonnen. Die dort eingesetzten Grundprinzipien finden sich in aktuellen Projekten wieder. Neben den Remailern wird im folgenden insbesondere Tor betrachtet. Dies ist ein Forschungsprojekt, welches mittlerweile im Praxiseinsatz etabliert ist und weltweit die wohl meistgenutzte Anonymisierungssoftware darstellt.

Chaumsche Mixe

Die ersten Schritte für Anonymität im Internet wurden theoretisch vollzogen. Gegen Ende der 1970er Jahre wurde Forschern bewusst, dass eine Verschlüsselung vom Anfang bis zum Ende der Verbindung (Ende-zu-Ende-Verschlüsselung) nicht ausreichend ist. Karger (1977) diskutierte erstmals den Einfluss der Verkehrsdatenanalyse (sog. Traffic Analysis), er nutzte die durch ihn und seine Kollegen Padlispky und Snow gefundenen Ergebnisse (Padlipsky, Snow und Karger 1978).

Die Autoren gingen davon aus, dass jedes Paket, welches ein Computer absendet, verschlüsselt ist. Dennoch entstehen beim Versand Informationen, die für einen Angreifer ersichtlich sind. Dazu gehören die Größe des Pakets, die Sendezeit und die Empfangsadresse. Ein Angreifer verfolgt, wer mit wem kommuniziert, wie oft dies passiert und versucht, daraus Schlüsse zu ziehen. Diese Technik ist als Verkehrsdatenanalyse, abgeleitet vom englischen Wort »Traffic analysis«, bekannt und wird seit langem im Rahmen militärischer Aufklärung eingesetzt. Beispielsweise wird der Funkverkehr vom Gegner überwacht. Ein starker Funkverkehr zusammen mit anderen Indizien deutet auf einen bevorstehenden Angriff hin. Sehr oft wird der Kommandostützpunkt des Gegners überwacht. Kommt es dort zu auffällig vielen parkenden Fahrzeugen oder zu stärkeren Lieferungen von Fertiggerichten, so wird daraus geschlussfolgert, dass mehr Personal vor Ort ist und demzufolge größere Aktionen bevorstehen. Ähnliches kann auf die Verkehrsdaten von Internetverbindungen angewendet werden, um Kommunikationsbeziehungen aufzuzeigen.

Die Autoren der obigen Veröffentlichung entwickelten einige Ansätze, um die Verkehrsdatenanalyse zu erschweren. Doch erst Davon Chaum gelang es 1981 eine vollständige Lösung zu dem Problem zu finden. In Chaum (1981) diskutierte er den Einsatz so genannter Mixe. Seine Idee bezog sich zunächst auf E-Mails. Sie lässt sich jedoch gut auf andere Gebiete erweitern.

Ein Mix ist eine Software, welche ei-

ne E-Mail entgegennimmt und in gewissem Sinne bearbeitet, bevor diese weitergegeben wird. Dabei ist es das Ziel, dass die Beziehung zwischen Absender und Empfänger einer E-Mail verschleiert wird. Padlipsky, Snow und Karger (1978) hatten in ihrer Arbeit drei Probleme erkannt:

1. Größe der zu sendenden Objekte
2. Sende- bzw. Empfangszeiten
3. Adressen der Empfänger

Das erste Problem lässt sich durch gleichbleibende Größe der E-Mails recht einfach beheben. Das heißt, jede E-Mail wird in immer gleich große Abschnitte geteilt. Sollte eine E-Mail oder ein Teil davon zu klein sein, wird einfach »Müll« an das Ende angefügt (sog. Padding). Der Mix oder Mailserver, der die E-Mail schließlich zum Empfänger ausliefert, setzt alle Teile korrekt zusammen und verwirft das Padding. Damit ist die E-Mail nicht mehr anhand der Größe nachverfolgbar. Dies wurde bereits in Padlipsky, Snow und Karger (1978) diskutiert.

Das zweite Problem umgeht Chaum, indem jeder Mix die E-Mails zunächst zwischenspeichert und dann stapelweise weitersendet (Batch processing). Ein Angreifer kann somit sehen, dass E-Mails an den Mix gesendet werden. Er sieht nicht, was innerhalb des Mixes passiert und schließlich sieht er, dass E-Mails den Mix verlassen. Aber die Zeitpunkte des Empfangs und des Versands einer E-Mail entkoppelt der Mix.

Schließlich bleibt das Problem der Empfängeradressen. Jede E-Mail trägt die Adresse des Empfängers mit sich. Sonst wäre es den Zwischenstationen unklar, wohin die E-Mail zu senden ist. Chaum schlägt dazu Kaskaden von Mixen vor. Eine E-Mail wird dann nicht mehr direkt an den Empfänger geschickt. Vielmehr legt der Absender fest, welche Mixe die E-Mail zunächst passieren muss, bevor sie den Empfänger erreicht. Chaum spricht nun davon, dass die E-Mail stückweise versiegelt wird. Das heißt, der Sender bereitet die Nachricht zum Versand vor, fügt die Empfängeradresse hinzu und versiegelt diese E-Mail. Danach bekommt die Nachricht eine Information für den letzten Mix, dass er diese E-Mail bitte an den Empfänger weiterleiten möchte. Die E-Mail wird wiederum versiegelt und eine Nachricht an den vorhergehenden Mix eingebaut. Dieser erhält die Information, die Nachricht an den letzten Mix zu senden. So erhält man eine E-Mail die schichtweise versiegelt ist. In der Literatur ziehen die Autoren häufig den Vergleich zu einer Zwiebel. Diese ist ebenso schichtweise aufgebaut, wie die oben beschriebene E-Mail. Für das Prinzip ist daher »Onion Routing« ein häufig genutzter Begriff. Abbildung 1 illustriert dieses Zwiebelprinzip.

Die Versiegelung der E-Mail geschieht in der Praxis durch den Einsatz von Verschlüsselung. Das heißt, jeder Mix trägt einen Schlüssel und die E-Mail wird damit entsprechend verschlüsselt. Damit ist sichergestellt, dass nur der jeweilige Mix die E-Mail mit den zugehörigen Versandinformationen lesen kann.

Das Prinzip der Chaumschen Mixe hat einen wesentlichen Vorteil. Bisher wurde immer von einem Angreifer ausgegangen, der den Verkehr mitliest. Aber was ist, wenn ein Angreifer selbst aktiv wird und einen Mix betreibt? Das Prinzip bietet Schutz, sobald ein ehrlicher Mix-Betreiber in der Kette ist. Denn dann ist für den Angreifer keinerlei Zuordnung mehr möglich.

Die Arbeit Chaums ist noch heute Grundlage vieler Forschungsarbeiten im Bereich der Anonymität. Viele aktuell eingesetzte Lösungen nutzen Chaumsche Mixe oder eine Abwandlung dieser als Baustein in deren Design.

In den Folgejahren forschten viele Wis-

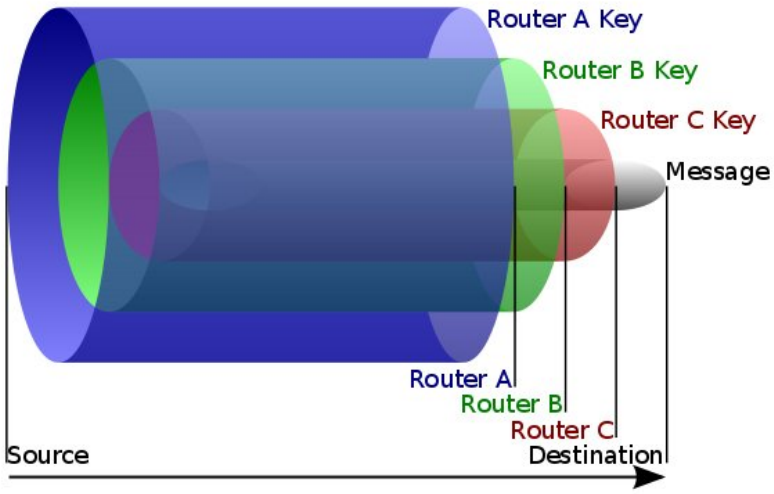

Abbildung 1: Das schichtweise Zwiebelprinzip des Onion Routing
Urheber: Harrison Neal, `http://de.wikipedia.org/wiki/Onion_Routing`

senschaftler an Verbesserungen des Konzepts bzw. versuchten die Ergebnisse in die Praxis zu übertragen. Besonders zu nennen ist der deutsche Informatiker Prof. Dr. Andreas Pfitzmann. Insbesondere Pfitzmann, Pfitzmann und Waidner (1991) diskutierte den Einsatz von Mixen im ISDN-Netz. Pfitzmann startete 2000 das Projekt »AN.ON – Anonymität.Online« als Zusammenarbeit der Technischen Universität Dresden und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Später stiess die Universität Regensburg als weiterer Projektpartner hinzu. Der Java Anon Proxy JAP, der mittlerweile unter JonDonym firmiert, ist eines der sehr aktiv genutzten Anonymitätsprogramme.

Entwicklung bei Remailern

Der Mailserver anon.penet.fi

Trotz vielfältiger Forschung auf dem Gebiet dauerte es recht lange, bis es erste praxistaugliche Lösungen gab. Gegen Ende der achtziger Jahre gab es mit dem E-Mail-Server `anon.penet.fi` den ersten Schritt in der Richtung. Der finnische Netzwerkadministrator Johan »Julf« Helsingius betrieb verschiedene Server. Einer davon gewährte den Zugang zum Usenet. Dies waren Diskussionsräume, die entfernt mit heutigen Webforen vergleichbar sind. Der Zugriff erfolgte textbasiert und mehr oder weniger zentral wurden Diskussionräume zur Verfügung gestellt. Diese sind meist thematisch in Hierarchien sortiert. So findet sich noch heute ein Zweig für deutschsprachige Diskussionen (Abkürzung de). Innerhalb des Zweiges

sind dann wieder Zweige, die sich mit Wissenschafts- (Abkürzung sci), Computer- (Abkürzung comp) und vielen anderen Themen beschäftigen. Unterhalb des Zweiges Wissenschaft existieren dann einzelne Räume für einzelne Richtungen (Mathematik, Geschichte etc.) und unterhalb des Zweiges Computer gibt es wiederum Zweige für Hard- und Software. Eine Ebene weiter sind dann schließlich Räume zu einzelnen Themen. Das gesamte Usenet ist in dieser hierarchischen Struktur aufgebaut. Bis Anfang des neuen Jahrtausends war das Usenet hoch frequentiert. Es fanden viele Diskussionen zu verschiedenen Themen statt. Unter anderem wurde das freie Betriebssystem GNU/Linux hier angekündigt und diskutiert. Mittlerweile lässt sich eine Abkehr von diesem Medium zugunsten von Webforen und anderen Diskussionsplattformen erkennen.

Eine Regel für das Usenet war, dass Nutzer mit ihrem Realnamen Beiträge veröffentlichten. Weiterhin machten es verschiedene Eigenschaften des Mediums einfach Nutzer zu erkennen oder zurückzuverfolgen. Die Diskussionen blieben nicht auf rein technische Sachverhalte beschränkt. Recht häufig wurden politische Ansichten diskutiert. Einige der Teilnehmer wollten nicht, dass ihre Ansichten mit ihrer Person verbunden sind. Daher sannen sie auf eine Lösung.

Helsingius argumentierte, dass es für Nutzer Möglichkeiten gibt, ihre wahre Identität zu verschleiern. Den Beweis trat er schließlich mit einer kleinen Software an, die er selbst entwickelt hatte und auf einem seiner Server installierte. Er ermöglichte Nutzern damit pseudonymen Zugang zum Usenet sowie auch für E-Mails.

Sein Programm bestand aus einer Datenbank. Darin war eine Zuordnung zwischen einem Pseudonym und einer E-Mail-Adresse vermerkt. Ein neuer Nutzer musste nun eine E-Mail an den Dienst schreiben und seine E-Mail-Adresse anmelden. Die Software wies dem Nutzer ein Pseudonym der Form `anXXXX` zu. Die `XXXX` waren dabei Zahlen. Nach der Anmeldung verfasste der Anwender eine E-Mail an die Adresse `anon@anon.penet.fi`. Die Software entfernte die wahre E-Mail-Adresse und ersetzte diese durch das `anXXXX`-Pseudonym. Der Empfänger der E-Mail oder des Beitrages konnte nun wieder antworten. Die Software ersetzte dann das Pseudonym und stellte die E-Mail dem Empfänger zu.

Dem System fehlten sämtliche Eigenschaften, die Chaum ausgearbeitet hatte. Die Schwachstelle war die Datenbank mit den Nutzerkennungen. Im Februar 1995 drohten finnische Strafverfolgungsbehörden damit, den Server zu beschlagnahmen (Helsingius 1996b). Denn vorher hatte einer der Nutzer Interna von Scientology veröffentlicht und die Organisation wollte wissen, wer hinter dieser Aktion steckt. Helsingius hatte die Wahl, entweder alle Kennungen preiszugeben oder die eine, nach der die Behörden verlangten. Er gab die eine preis. Jedoch kam es in der Folge immer wieder zu Versuchen, an Nutzerkennungen zu kommen. Schließlich eskalierte die Situation im Jahr 1996. Er wurde von der Zeitschrift »The Observer« auf der Titelseite beschuldigt, für die Weiterleitung von 90 % aller Kinderpornographie im Internet schuldig zu sein (Newton 2004). Später kamen Ermittlungsbehörden zu dem Schluss, dass es mit dem Dienst technisch unmöglich ist, Bild- oder andere Anhänge zu versenden. Die Attacken gegen Helsingius rissen nicht ab und im August 1996 schaltete er den Dienst ab (Helsingius 1996a).

Cypherpunk-Remailer

Mittlerweile war vielen Nutzern klar geworden, dass Anonymität im Internet ein wichtiger Bestandteil zur Erhaltung der Redefreiheit ist. So versuchten einige ähnlich gelagerte Systeme, wie das von Helsingius zu betreiben. Andere gingen einen Schritt weiter. Insbesondere eine Gruppierung, die unter dem Namen Cypherpunks bekannt war und ist, versuchte die Entwicklung voran zu treiben.

Unter dem Namen Cypherpunk-Remailer griffen sie die Ideen David Chaums wieder auf. Die Aktivisten testeten zunächst einige Designs und entschieden sich dann für eine Variante die zum Teil noch heute aktiv ist. Die wichtigste Eigenschaft ist die schichtweise Verschlüsselung. Der Anwender muss zunächst von allen Remailern die kryptographischen Schlüssel erfragen. Nachdem er diese hat, verschlüsselt er diese schichtweise wie es bereits bei den Chaumschen Mixen der Fall ist und sendet seine E-Mail schließlich auf den Weg. Bei der Aufbereitung der E-Mail ist dabei ein spezielles Format zu beachten. Dies machte die Benutzung des Dienstes recht kompliziert und fehleranfällig.

Lance Cottrell analysierte die Schwächen der Cypherpunk-Remailer und veröffentlichte seine Ergebnisse in Cottrell (*Mixmaster & Remailer Attacks*). Das Modell der Cypherpunks sendet die E-Mails *sofort* an die nächste Stelle weiter und verschickt alle E-Mails immer als Ganzes. Damit kann ein Angreifer eine Zuordnung anhand des Zeitpunktes des Versands einer Nachricht sowie anhand der Größe vornehmen. Cottrell gelang noch eine weitere Entdeckung. Die Cypherpunk-Remailer sind gegen so genannte Replay-Angriffe anfällig. Dabei wird eine Nachricht abgefangen und zwischengespeichert. Im folgenden sendet der Angreifer die E-Mail immer wieder. Der Weg der Nachricht ist fest vorgegeben, d.h. bei jedem Sendeversuch wird diese denselben Weg nehmen. Nun vergleicht der Angreifer Zeitpunkt und Größe der beobachteten Nachrichten. Mit jedem Versand derselben einmal abgefangenen Nachricht wird er sicherer sein, welchen Weg die E-Mail durch das Remailer-Netzwerk nimmt. Gegebenenfalls kann er so die Anonymität des Absenders aufheben.

Mixmaster-Remailer

Dies gab den Anstoss zur Entwicklung einer neuen Remailer-Generation, dem so genannten Mixmaster-Remailer (Möller, Cottrell, Palfrader u. a. 2003). Dieser behob die Schwächen der Cypherpunk-Remailer und setzte auf eine benutzerfreundlichere Oberfläche.

E-Mails, die über das Mixmaster-System verschickt werden, teilt die Software in Teile mit fester Größe auf. Die Mixmaster-Server sammeln die eingehenden E-Mails und senden diese in zufälliger Reihenfolge weiter. Der Benutzer wählt die einzelnen Server in einem Programm aus. Dieses verschlüsselt und formatiert die E-Mail entsprechend. Damit entfällt auch der schwierige Schritt.

Neben den eigentlichen vom Nutzer versandten E-Mails setzt Mixmaster so genannte Dummy-Nachrichten ein. Das sind von der Software selbst generierte Nachrichten. Diese werden durch das Netzwerk verschickt und vom letzten Remailer in der Kette gelöscht. Dies soll es einem Angreifer weiter erschweren, die Anonymität der Benutzer aufzuheben. In den Folgejahren ergab sich bezüglich Dummy-Nachrichten jedoch kein einheitliches Bild in der Forschung. Derzeit geht man davon aus, dass Dummy-Nachrichten durch den Einsatz statistischer Verfahren erkennbar

ist und somit keinen Mehrwert bringt.

Mixmaster hat sich als resistent gegen die meisten der Angriffe erwiesen. Lediglich ein theoretischer Angriff ist möglich. Dabei wird von einem global agierenden Angreifer ausgegangen. Dieser hält wie bei dem oben beschriebenen Replay-Angriff eine bestimmte E-Mail zurück. Danach flutet er das Mixmaster-Netzwerk mit eigenen Nachrichten. Dies geschieht solange, bis er sicher sein kann, dass im gesamten Netzwerk nur eigene Nachrichten vorhanden sind. Schließlich versendet er die zurückgehaltene Nachricht. Von allen eigenen Nachrichten kennt der Angreifer Sender und Empfänger sowie den Weg durch das Netzwerk. Eine einzige Nachricht nimmt einen anderen, unbekannten Weg. Der Angreifer kann die Nachricht verfolgen und schließlich den Empfänger bestimmen. Der Angriff ist jedoch eher theoretischer Natur. Denn zum einen leiten die Server mehr Dummy-Nachrichten in das Netzwerk, wenn von außen mehr Nachrichten in das Netzwerk kommen und zum anderen senden auch andere Nutzer minütlich Nachrichten.

Mixmaster ist noch heute eines der meistbenutzten Programme zur Anonymisierung von E-Mails oder Usenet-Nachrichten. Es gibt einige Erweiterungen für E-Mail-Programme. Damit lassen sich einfach E-Mails an das Mixmaster-Netzwerk schicken. Weiterhin ermöglicht die Seite Anonymouse[1] die einfache Bedienung über den Browser.

Mit Mixminion gibt es eine theoretische Weiterentwicklung von Mixmaster (Danezis, Dingledine und Mathewson 2003). Dies ist die dritte Generation von Remailern. Die Entwicklung der Software und damit auch der Aufbau eines funktionierenden Netzwerks wurde eingestellt. Die beiden Hauptentwickler wechselten zum Tor-Projekt und sind bis heute dort fest angestellt. In jüngerer Zeit versucht das Projekt crypto.is Mixminion und andere Software zum Schutz der Privatsphäre wiederzubeleben. Es ist jedoch noch zu früh, um hier eine Tendenz abzuschätzen.

Im Laufe der Jahre wurden weitere Arbeiten zu Anonymisierungsdiensten mit hohen Antwortzeiten vorgestellt. Bislang konnte keine das Forschungsstadium verlassen und eine größere Nutzerbasis aufbauen. Doch wie Dingledine und Mathewson (2006) schrieben ist eine große und diversifizierte Nutzerbasis wichtig, um einen hohen Grad an Anonymität zu bieten. Daher sind Mixmaster und mit Einschränkung auch Mixminion momentan die besten Werkzeuge, um anonym per E-Mail zu kommunizieren.

Der Austausch von E-Mails ist nun nicht der einzige Kommunikationsweg im Internet. Für viele Benutzer gehört der Besuch von Webseiten, Chatten und vieles mehr dazu. Die Antwortzeiten der Mixmaster-Remailer liegen derzeit zwischen 10 Minuten und 58 Stunden. Das heißt unter Umständen benötigt eine E-Mail sehr lange, um das Netzwerk zu passieren. Also eignet sich dieses Verfahren nicht für Zwecke, in denen der Nutzer eine schnelle Antwort wünscht. Hierfür wurden andere Verfahren entwickelt. Oben wurde bereits JAP bzw. JonDonym beschrieben, im folgenden soll Tor genauer vorgestellt werden.

Tor

Tor gilt derzeit als das am meisten eingesetzte Werkzeug zur Anonymisierung von Verbindungen mit kurzen Antwortzeiten (Besuch von Webseiten, Chatten etc.). Daneben wird Tor vielfältig wissen-

1 http://anonymouse.org/anonemail_de.html

schaftlich untersucht und hat eine aktive Entwicklergemeinde.

Die Wurzeln des Projekts liegen bei Überlegungen zur Absicherung der elektronischen Kriegsführung. Das Office of Naval Research (ONR) gehört zur United States Navy und ist für die Koordination sowie Ausführung wissenschaftlicher Forschung zuständig. Im Jahr 1995 startete das ONR die Finanzierung für ein Projekt zur Erforschung des Onion Routing. Dabei sollte eine Technik entstehen, die den Streitkräften eine weitgehend unbeobachtbare Kommunikation ermöglicht. Goldschlag, Reed und Syverson (1996) stellten das Prinzip genauer vor. Das U.S. Naval Research Laboratory (NRL), eine Abteilung des ONR, betrieb danach einige Server als Prototyp. Später wurde das Design verbessert und als eine neue Generation betrieben. Im Jahr 1998 gab es verschiedene Installationen innerhalb der USA sowie einen Server im kanadischen Verteidigungsministerium. Jedoch lief die Finanzierung 1999 aus und einige der Entwickler wandten sich anderen Aufgaben zu. Erst später trafen Paul Syverson und Roger Dingledine aufeinander und konnten die Defense Advanced Research Projects Agency (DARPA) überzeugen, Gelder für eine Weiterentwicklung bereitzustellen. Im Oktober 2003 gingen neue Server unter dem Namen Tor online. Später übernahm die amerikanische Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) die Finanzierung und seit 2005 steht das Projekt auf eigenen Beinen. Das heißt, die Entwicklung wird durch Spenden finanziert.

Tor wird als die zweite Generation des Onion Routing bezeichnet. Die Funktionsweise unterscheidet sich dabei grundlegend von der der ersten Generationen (Dingledine, Mathewson und Syverson 2004). Für das anonyme Abrufen von Webseiten kommen drei verschiedene Komponenten des Netzwerks zum Einsatz. Zunächst hat der Benutzer auf seinem lokalen Rechner einen so genannten Proxy installiert. Der Browser des Benutzers kommuniziert mit dem Proxy und teilt diesem mit, welche Webseiten besucht werden sollen. Der Proxy nimmt in regelmäßigen Abständen Kontakt zu Verzeichnisservern auf und befragt diese nach eine Liste von Tor-Relays, der dritten Komponente. Die Tor-Relays leiten die Verbindungen weiter, fragen in dem Beispiel die Webseite ab und geben die Antwort zurück.

Wenn nun eine Webseite besucht werden soll, sucht sich der Proxy drei Relays aus der Liste aus. Dort ist die IP-Adresse der Relays vermerkt sowie wie schnell deren Internetverbindung ist, welche Aktivitäten diese erlauben, die Schlüssel zur Verschlüsselung und einiges mehr. Nachdem die drei Relays gewählt wurden, nimmt der Proxy eine Verbindung zu ersten Relay auf und handelt einen gemeinsamen Schlüssel aus. Dieser Schlüssel ist nur für die Zeit der Verbindung aktiv und wird danach gelöscht. Damit kann ein Angreifer nachträglich nicht mehr die Daten entschlüsseln. Wenn der Schlüssel ausgehandelt ist, nutzt der Proxy die bestehende Verbindung mit dem ersten Relay und handelt darüber einen Schlüssel mit dem zweiten Relay aus. Schließlich handelt er einen dritten Schlüssel mit dem letzten Relay aus. Man kann sich den Verbindungsaufbau wie eine Teleskopstange vorstellen, deren Elemente stückweise ausgefahren werden.

Wenn die Verbindungsstrecke durch die Relays aufgebaut wurde, verschlüsselt der Proxy die Anfrage mit den ausgehandelten Schlüsseln und schickt diese auf den Weg. Jeder Relay kann eine Schicht mit dem ihm bekannten Schlüssel entziffern und gibt die Nachricht weiter. Der letzte leitet die Nachricht an das Ziel weiter, empfängt die Anfrage und

schickt diese rückwärts wieder auf den Weg. Das heißt, er verschlüsselt das Ergebnis mit seinem Schlüssel. Die beiden folgenden Relays verschlüsseln die Nachricht ebenfalls und der Proxy kennt alle Schlüssel der Kette. Er kann somit die Nachricht entpacken und den Inhalt lesen. Dieser wird an den Browser gegeben, welcher den Inhalt schließlich anzeigt.

Tor ist so aufgebaut, dass die Verbindungsstrecke mehrmals genutzt werden kann. Der Abruf von mehreren, auch verschiedenen Seiten kann durch denselben Kanal erfolgen. Nach ca. zehn Minuten wird die Verbindungsstrecke beendet. Das heißt, der Proxy baut die Verbindungen ab und alle Beteiligten verwerfen ihre ausgehandelten Schlüssel.

Im Verlauf der Zeit wurden diverse Angriffe gefunden oder es traten Schwierigkeiten im Einsatz auf. Daher gab es Anpassungen beim Design von Tor.

Die Spezifikation der Verzeichnisdaten wurde mehrfach verändert (*Tor directory protocol, version 3*). Dies war unter anderem der Tatsache geschuldet, dass das Netzwerk stark anwuchs. Daher umfasste die Liste aller Relays mehrere Megabyte. Die Verzeichnisserver mussten entsprechend viele und große Anfragen bearbeiten. Mittlerweile verteilen auch Relays Verzeichnisdaten. Diese sind von den Verzeichnisservern digital unterschrieben, daher kann die Integrität geprüft werden. Weiterhin findet eine Abstimmung über die Relays von seiten der Verzeichnisserver statt. Nur wenn die Mehrzahl der existierenden Verzeichnisserver ein Relay für gut befindet, wird das von einem Proxy eingesetzt.

Im Allgemeinen sind die Verzeichnisserver ein möglicher Schwachpunkt im Netzwerk. Wenn es einem Angreifer gelingt, Verzeichnisserver unter seine Kontrolle zu bringen, kann er unter Umständen falsche Daten verteilen und somit die Proxys über eigene Relays leiten. Dem versucht das Tor-Projekt zu begegnen, indem nur vertrauenswürdige Personen einen Verzeichnisserver betreiben dürfen und diese Verzeichnisserver speziell abgesicht sein müssen. Im aktuellen Design müsste ein Angreifer die Mehrzahl der Verzeichnisserver unter seine Kontrolle bringen, um tatsächlichen Schaden anrichten zu können.

Mittels so genannter Hidden Services lassen sich auch Informationen anonym anbieten. Das heißt, jemand könnte beispielsweise eine Webseite betreiben und durch die Hilfe von Hidden Services bleibt die Identität des Anbieters unklar. Das Design soll an dieser Stelle nicht erklärt werden, es ist jedoch Gegenstand vielfältiger Forschung. Nach dem derzeitigen Stand scheint es immer Möglichkeiten zu geben, den Anbieter zu identifizieren oder auf eine kleine Menge potenzieller Anbieter zu reduzieren. Øverlier und Syverson (2006) zeigten eine Möglichkeit auf. Infolgedessen wurden so genannte Eintrittswächter (Guard Nodes) eingeführt. Diese sind Relays, die an ersten Stelle in der Verbindungsstrecke stehen und über einen längeren Zeitraum immer wieder vom Proxy genutzt werden. Dadurch ist der beschriebene Angriff nicht mehr wirksam. Murdoch (2006) zeigte, wie der geografische Standort mittels Uhrzeitverschiebungen gemessen werden kann.

Einer der einfachsten und wahrscheinlich sehr häufig eingesetzten Angriffe gegen die Benutzer des Netzwerks liegt in der Tatsache begründet, dass jeder ein Relay betreiben kann. In der Vergangenheit wurden immer wieder Fälle bekannt, in denen jemand ein Relay betrieb und Verbindungen beobachtete, welche das Netzwerk verlassen. Verbindungen, die das Netzwerk verlassen, sind nicht notwendigerweise verschlüsselt. Wenn sich ein Nutzer auf einer Webseite bei-

spielsweise einloggt, kann der Betreiber des letzten Relays die Logindaten mitschneiden. Schutz gegen diese Angriffe besteht in der konsequenten Verschlüsselung der kompletten Verbindung. Das heißt, bei Webseiten ist darauf zu achten, dass HTTPS benutzt wird.

Im Allgemeinen gibt es gerade beim Besuch von Webseiten diverse Gefahren, die die Anonymität des Benutzers aufheben können. Die Webseite des Tor-Projekts listet einige auf. Weiterhin versuchen die Entwickler durch spezielle Pakete (Tor-Browser), diese Risiken für den Endanwender weitestgehend zu eliminieren.

Literaturverzeichnis

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24* (2).

Cottrell, L. (ohne datum). Mixmaster & Remailer Attacks. `http://web.archive.org/web/19981201070355/http://www.obscura.com/~loki/remailer-essay.html`.

Danezis, G., Dingledine, R. & Mathewson, N. (2003). Mixminion: Design of a Type III Anonymous Remailer Protocol. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy* (Seiten 2–15).

Dingledine, R. & Mathewson, N. (2006). Anonymity Loves Company: Usability and the Network Effect. In R. Anderson (Herausgeber), *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*. Cambridge, UK.

Dingledine, R., Mathewson, N. & Syverson, P. (2004). Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium*.

Goldschlag, D. M., Reed, M. G. & Syverson, P. F. (1996). Hiding Routing Information. In R. Anderson (Herausgeber), *Proceedings of Information Hiding: First International Workshop* (Seiten 137–150). Springer-Verlag, LNCS 1174.

Helsingius, J. (1996a). Johan Helsingius closes his Internet remailer. `http://preterhuman.net/texts/underground/Anonymity/PenetClosureAnnounce.txt`.

Helsingius, J. (1996b). Johan Helsingius gets injunktion in Scientology case. `https://w2.eff.org/Privacy/Anonymity/960923_penet_injunction.announce`.

Karger, P. A. (1977). *Non-Discretionary Access Control for Decentralized Computing Systems* (S.M. & E.E. thesis Nummer MIT/LCS/TR-179). Cambridge, MA.

Möller, U., Cottrell, L., Palfrader, P. (2003). Mixmaster Protocol — Version 2. IETF Internet Draft.

Murdoch, S. J. (2006). Hot or Not: Revealing Hidden Services by their Clock Skew. In *Proceedings of CCS 2006*.

Newton, M. (2004). *The encyclopedia of high-tech crime and crime-fighting*. Facts on File crime library. Facts On File. Zugriff am unter `http://books.google.com/books?id=sAK6\_W7lLkoC`

Øverlier, L. & Syverson, P. (2006). Locating Hidden Servers. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE CS.

Padlipsky, M. A., Snow, D. W. & Karger, P. A. (1978). *Limitations of End-to-End Encryption in Secure Computer Networks* (Technischer Bericht Nummer ESD-TR-78-158). Hanscom AFB, MA.

Pfitzmann, A., Pfitzmann, B. & Waidner, M. (1991). ISDN-mixes: Untraceable communication with ve-

ry small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems* (Seiten 451–463).

Tor directory protocol, version 3. (ohne datum). The Tor Project. https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=dir-spec.txt.