Hacking mit Franzis

Ohne Vorkenntnisse

Schritt für Schritt zum sicheren Linux auf dem USB-Stick

Peter Loshin

Anonym im Internet mit Tor und Tails

Nutze die Methoden von Snowden und hinterlasse keine Spuren im Internet.

- Tor-Browser-Bundle (TBB) und Tails installieren und nutzen
- Wenn Tor nicht ausreicht: Tor-Relays, Bridges und Obfsproxy
- Verborgene Tor-Dienste und anonyme E-Mail-Kommunikation

FRANZIS

Peter Loshin ist unabhängiger Berater zu Internetprotokollen und Open-Source-Netzwerktechnologien. Er schreibt auch zu diesen Themen. Seine Arbeiten erscheinen regelmäßig in führenden Fachzeitschriften und auf Webseiten. Dazu gehören CPU, Computerworld, PC Magazine, EarthWeb, Internet.com und CNN.

Peter Loshin

Anonym im Internet mit Tor und Tails

Nutze die Methoden von Snowden und hinterlasse keine Spuren im Internet.

- Tor-Browser-Bundle (TBB) und Tails installieren und nutzen
- Wenn Tor nicht ausreicht: Tor-Relays, Bridges und Obfsproxy
- Verborgene Tor-Dienste und anonyme E-Mail-Kommunikation

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

This edition of **Practical Anonymity** by **Pete Loshin** is published by arrangement with **ELSEVIER INC.**, a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA

ISBN der englischen Originalausgabe: 978-0124104044

Programmleitung: Dr. Markus Stäuble
Satz und Übersetzung: G&U Language & Publishing Services GmbH
art & design: www.ideehoch2.de
Druck: C.H. Beck, Nördlingen
Printed in Germany

ISBN 978-3-645-60416-1

Inhaltsverzeichnis

Vorwort

Der Google-CEO Eric Schmidt löste 2009 einen Proteststurm aus, als er erklärte: »Datenschutz ist tot!« Er sagte:

> *Wenn Sie etwas tun, von dem niemand etwas wissen sollte, dann sollten Sie es am besten erst gar nicht tun. Wenn Sie aber wirklich einen Datenschutz brauchen, dann ist es in Wirklichkeit so, dass Suchmaschinen einschließlich Google diese Informationen eine Zeit lang aufbewahren, und es ist beispielsweise wichtig, dass wir in den Vereinigten Staaten alle dem Patriot Act unterliegen. Es ist möglich, dass diese Informationen den Behörden zugänglich gemacht werden.*

Für diejenigen, die legitime Gründe haben, das Internet anonym zu nutzen – Diplomaten, Angehörige des Militärs und anderer staatlicher Organisationen, Journalisten, politische Aktivisten, IT-Profis, Strafverfolgungsbeamte, politisch Verfolgte und andere –, bilden Anonymisierungsnetzwerke ein wertvolles Instrument. Es gibt viele gute Zwecke, für die Anonymität sehr wichtig sein kann.

Die anonyme Nutzung des Internets wird durch die vielen Websites, die alles über uns wissen, durch Cookies und Werbenetzwerke und durch die Protokollierung von IP-Adressen bei den Providern erschwert, und auch neugierige Beamte können eine Rolle spielen. Es reicht nicht mehr aus, die Cookies im Browser auszuschalten, um online allein gelassen zu werden.

Für viele mag die Verwendung eines Open-Source-Werkzeugs zur Verbindung mit dem Internet über ein Anonymisierungsnetzwerk zu kompliziert sein (oder scheinen), da die meisten Informationen über Werkzeuge mit Beschreibungen ihrer Funktionsweise und Erörterungen darüber überfrachtet sind, wie sie die Sicherheit maximieren. Selbst für technisch versierte Benutzer ist das manchmal zu viel des Guten. Die Verwendung dieser Werkzeuge kann jedoch in Wirklichkeit ganz einfach sein.

Für viele Benutzer kann die Möglichkeit, das Internet anonym zu nutzen, im wahrsten Sinne des Wortes über Leben und Tod entscheiden. Niemand sollte daher durch übermäßige Kompliziertheit daran gehindert werden, Anonymisierungswerkzeuge zu verwenden, insbesondere dann, wenn ein wirklich dringender Bedarf vorliegt. Dieses Buch bietet das Know-how, mit dem gefährdete Benutzer so schnell und sicher wie möglich anonym online gehen können.

Auf den folgenden Seiten erfahren Sie, wie Sie das wirkungsvollste und am häufigsten genutzte dieser Anonymisierungswerkzeuge einsetzen. Es schützt Diplomaten, Angehörige des Militärs und anderer staatlicher Organisationen, Journalisten, politische Aktivisten, Strafverfolgungsbeamte, politisch Verfolgte und andere. Diese praktische Anleitung lässt die theoretischen Grundlagen und die technischen Einzelheiten außen vor. Der Schwerpunkt liegt stattdessen darauf, wie Sie so schnell wie möglich »von null auf anonym« kommen können.

Danksagungen

Ich möchte all denen, die zum Tor-Projekt beigetragen haben, für ihre Beteiligung an diesem wichtigen Unternehmen danken. Insbesondere möchte ich den Personen meinen Dank aussprechen, die mit dem Tor-Projekt verbunden sind und mir freundlicherweise geholfen haben, dieses Buch zu vollenden:

Karsten Loesing, Forscher und Leiter des Tor-Metrics-Projekts, der trotz seines vollen Terminkalenders freundlicherweise die Zeit fand, das Buch auf technische Richtigkeit durchzusehen.

Runa A. Sandvik, Entwicklerin, Sicherheitsforscherin und Übersetzungskoordinatorin, die meine nervtötenden Fragen über Tor großzügig und hilfreich beantwortet und mir einige Einsichten in die Schwierigkeiten gegeben hat, über Tor zu schreiben.

Roger Dingledine, Projektleiter und einer der ursprünglichen Tor-Entwickler, der mir sehr geduldig fast eine Stunde seiner Zeit geschenkt hat, um mir auf dem Tor Project Hack Day 2013 in Boston zu erklären, wie Tor funktioniert.

Andrew Lewman, geschäftsführender Direktor, ohne dessen Hilfe ich dieses Buch nicht hätte abschließen können.

Wie immer danke ich auch den erfahrenen Fachleuten bei Elsevier, angefangen bei Syngress-Herausgeber Steve Elliot, der mich dazu überredet hat, wieder mit dem Schreiben von Büchern anzufangen, Ben Rearick, dem redaktionellen Projektmanager, sowie Mohana Natarajan, Produktmanagerin, die das gesamte Projekt bis zum Abschluss geleitet hat.

Anonymität und Umgehung der Zensur

Obwohl es so aussehen mag, ist das Internet kein anonymes Medium (und ist es auch nie gewesen). Die Leute verhalten sich jedoch, als ob es anonym wäre, indem sie etwa auf Websites widerliche Kommentare veröffentlichen oder im »Inkognito«- oder »Privat-Modus« ihres Browsers nach fragwürdigen Inhalten suchen.

Sobald Sie jedoch Verbindung mit dem Internet haben, geben Sie Ihre Identität über die IP-Adresse Ihres Computers bekannt. Damit lässt sich über Ihr Konto bei Ihrem Provider Ihre Anschrift ermitteln bzw. über Ihr Firmennetzwerk Ihr Arbeitsplatzrechner.

Selbst wenn Sie über eine fremde IP-Adresse auf das Internet zugreifen (z. B. über das WLAN in einem Hotel, in einem Internetcafé oder auf einem geborgten PC), können Sie von jedem, der die Sitzung überwacht, identifiziert werden, sobald Sie sich an Social-Networking-Websites anmelden oder nach Ihren E-Mails sehen.

Immer wieder zeigt es sich, dass die Nutzung des Internets Spuren hinterlässt – Spuren, die jemand, der daran interessiert ist, sammeln und mit Ihrer Person in Verbindung bringen kann. Angesichts des PRISM-Programms, das im Juni 2013 ruchbar wurde – eine Zusammenarbeit der NSA (National Security Agency) mit neun der größten Anbieter von Internetdiensten, darunter Google, Microsoft, Apple und Facebook, um Daten zu erfassen und zu speichern –, sind Bedenken über Datenschutz alles andere als paranoide Vorstellungen.

Das wurde im Jahr 2012 auf eindrucksvolle Weise veranschaulicht, als die E-Mails des ehemaliges CIA-Direktors David Petraeus (& Co.) an die Öffentlichkeit gerieten. Wenn schon der Direktor der CIA nicht in der Lage ist, die digitalen Spuren seiner außerehelichen Affären zu verwischen, welche Hoffnung besteht dann für andere? (Siehe »Don‘t be a Petraeus: A Tutorial on Anonymous Email Accounts« auf *https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts*.)

Das Beispiel von Petraeus zeigt, dass der typische Benutzer selbst bei der Verwendung geliehener Netzwerkverbindungen an unterschiedlichen Standorten so viel persönliche Informationen offenlegt, dass jegliche Vorspiegelung von Anonymität online zu einer Farce wird.

Alles, was Sie online unternehmen, kann auf verschiedenen Wegen ausspioniert werden, aber mit entsprechender Sorgfalt ist es möglich, die offensichtlichsten Spuren zu verwischen. Darum geht es in diesem Buch: wie Sie Kontakt mit dem Internet aufnehmen und dabei sicher sein können, dass jemand, der die Verbindung abhört, nicht herausfinden kann, was Sie tun (oder dass Sie es dieser Person zumindest sehr schwer machen).

Der zweite wichtige Aspekt der Anonymität im Internet betrifft die Umgehung der Zensur. In Ländern wie China und dem Iran verhindern staatliche Firewalls den Zugriff auf Websites, die von der Regierung als inakzeptabel eingestuft werden. Benutzer in solchen Ländern würden wahrscheinlich gern die Belästigung durch zielgerichtetes Marketing ertragen (was in liberalen Ländern ein Grund für die Verwendung von Tor ist), wenn sie dafür

die Möglichkeit hätten, die staatliche Zensur zu umgehen. Aber sie müssen nicht einmal diesen Kompromiss eingehen, denn wenn sie in der Lage sind, anonym Verbindung zum Internet aufzunehmen, können sie gewöhnlich auch die Zensur umgehen.

Wie können Bürger in Diktaturen unzensierte Nachrichten lesen, wenn die Regierung den gesamten Internetzugang filtert? Wie können Diplomaten, Spione, Geschäftsleute oder Journalisten die Wahrheit an Orten verbreiten, an denen der Internetzugriff aus politischen oder wirtschaftlichen Gründen zensiert wird oder unerwünschte Inhalte gefiltert werden? Wie können Informanten über Missetaten berichten, ohne sich selbst Gefahr auszusetzen?

Für viele besteht die Antwort darin, Tor zu verwenden (*https://www.torproject.org*), ein Open-Source-Projekt, das Benutzern überall die anonyme und durch keinerlei Zensur eingeschränkte Nutzung des Internets erlauben soll. Tor sorgt für Anonymität, indem es die Möglichkeiten der Gegner einschränkt, durch Analyse des Netzwerkdatenverkehrs personenbezogene Informationen zu gewinnen.

Mit »Gegner« meine ich hier jeden, der versucht, Ihre Identität und Ihren Standort herauszufinden, und zwar unabhängig davon, ob es eine Regierungsbehörde, ein korrupter Beamter, ein Manager oder ein Stalker ist. Was es mit der »Analyse des Netzwerkdatenverkehrs« auf sich hat, wird im Abschnitt »Why we need Tor« (»Warum wir Tor brauchen«) des Überblicks über das Tor-Projekt (*http:s//www.torproject.org/about/overview.html*) erklärt:

> *Die Verwendung von Tor schützt Sie vor einer gängigen Form der Internetüberwachung, die als »Analyse des Netzwerkdatenverkehrs« bezeichnet wird. Mithilfe einer solchen Analyse kann ermittelt werden, wer über ein öffentliches Netzwerk mit wem spricht. Wer die Quelle und das Ziel Ihres Internet-Datenverkehrs kennt, kann Ihr Verhalten und Ihre Interessen herausfinden. Das kann Auswirkungen auf Ihren Kontostand haben, wenn beispielsweise eine E-Commerce-Website die Preise auf der Grundlage des Landes oder Ihrer Organisation festlegt. Es kann sogar Ihren Arbeitsplatz und Ihre körperliche Unversehrtheit gefährden, wenn offengelegt wird, wer Sie sind und wo Sie sich befinden. Wenn Sie sich*

beispielsweise im Ausland befinden und Kontakt mit den Computern Ihres Arbeitsgebers aufnehmen, um E-Mails einzusehen oder zu lesen, können Sie dabei versehentlich Ihre Nationalität und Ihren Arbeitgeber gegenüber jedem aufdecken, der das Netzwerk beobachtet, selbst wenn die Verbindung verschlüsselt ist.

Wie funktioniert diese Analyse? Internet-Datenpakete bestehen aus zwei Teilen: den Nutzdaten und einem Header für die Weiterleitung. Bei den Nutzdaten handelt es sich um das, was gesendet wird, also z. B. eine E-Mail-Nachricht, eine Webseite oder eine Audiodatei. Selbst wenn Sie die Nutzdaten bei der Kommunikation verschlüsseln, kann die Analyse des Datenverkehrs eine Menge darüber zeigen, was Sie tun, und möglicherweise sogar, was Sie sagen. Das liegt daran, dass sich diese Analyse auf den Header konzentriert, der die Quelle, das Ziel, die Größe, die Zeit usw. angibt.

Ein grundlegendes Problem für den Datenschutz besteht darin, dass der Empfänger schon durch einen Blick auf den Header erkennen kann, dass die Nachricht von Ihnen stammt. Das können aber auch autorisierte Zwischenstationen wie die Provider und manchmal auch nicht autorisierte Zwischenstationen. Eine einfache Form der Datenverkehrsanalyse kann darin bestehen, sich irgendwo zwischen Sender und Empfänger zu platzieren und die Header einzusehen.

Es gibt aber noch leistungsfähigere Arten der Analyse. Manche Angreifer spionieren in mehreren Teilen des Internets und verwenden anspruchsvolle statistische Techniken, um die Kommunikationsmuster vieler verschiedener Organisationen zu verfolgen. Dagegen hilft keine Verschlüsselung, da sie nur den Inhalt des Internetdatenverkehrs unlesbar bar, nicht aber die Header.

Mehr über Tor: Wer steht hinter dem Tor-Projekt?
»Gebührende Vorsicht« ist eine etwas geschwollene Formulierung für: »Mach deine Hausaufgaben, bevor du ein Risiko eingehst.« Immer, wenn Sie eine Software einsetzen, um Ihre Privatsphäre zu schützen oder Sicherheitsmaßnahmen zu ergreifen, vertrauen Sie den Autoren und Herausgebern dieser Software. Sie müssen überzeugt sein, dass die Personen, die die Software zur Verfügung stellen, sowohl fähig als auch vertrauenswürdig sind:

Fähig, damit Sie sich keine Sorgen darüber machen müssen, dass die Produktionssoftware mit erheblichen Fehlern durchsetzt ist oder dass einfach zu behebende Fehler lange Zeit nicht behoben werden.

Vertrauenswürdig, damit Sie nicht befürchten müssen, dass die Entwickler dem Druck von anderen Stellen nachgeben und die Software auf eine Weise ändern, die die Sicherheit verringert.

Vertrauen in Menschen, die Sie nicht persönlich kennen, entspringt gewöhnlich dem Ruf dieser Personen. Das Tor-Projekt hat einen Ruf von Offenheit und Transparenz: Ein Großteil ihrer Tätigkeiten, von der Fehlersuche über die langfristige Projektentwicklung bis zur Diskussion darüber, wie die Funktionen am besten erfüllt werden können, erfolgt öffentlich, auf der Wiki-Seite, in den Diskussionslisten und auf der Website des Projekts. Der gesamte Quellcode der Software sowie der Quellcode der Website sind zur Untersuchung und Kommentierung zugänglich.

Wenn Sie sich zum Schutz Ihrer Anonymität auf Tor verlassen wollen, sollten Sie mehr über die Personen erfahren, die hinter Tor stehen. Das ist fast noch wichtiger, als zu lernen, wie das Tor-Protokoll funktioniert. Links zu Informationen über die Personen, die das Tor-Projekt tragen – finanziell sowie technisch – finden Sie in Anhang C, Abschnitt C.2. Ich möchte Ihnen jedoch ans Herz legen, auch eigene Nachforschungen anzustellen.

1.1 Was bedeutet Anonymität?

Computer machen es viel schwieriger und komplizierter, anonym zu bleiben. Bevor es Computer und das Internet gab, reichte es meistens aus, nicht aufzufallen – also so auszusehen und zu handeln wie alle anderen –, um unter dem Radar der Leute zu bleiben, die Ausschau nach Ihnen hielten, ob das nun »die Behörden« waren, jemand, der eine Rechnung eintreiben wollte, oder ein aufdringlicher Vertreter.

In der Welt der Computer gibt es jedoch viele verschiedene Möglichkeiten, Sie zu identifizieren – und sie alle können automatisiert werden, sodass nicht einmal die Möglichkeit besteht, an einem schlafenden Nachtwächter oder einer abgelenkten Sekretärin vorbeizuschlüpfen:

- IP-Adressen. Alle Geräte, die mit dem Internet verbunden sind, können anhand ihrer IP-Adresse identifiziert werden. Diese Adresse wird vom Provider zugewiesen, sodass dieser das Konto und den Standort des verwendeten Systems aus einer IP-Adresse ermitteln kann.
- Browsercookies. Webserver, insbesondere solche, die Dienste bereitstellen, legen auf Ihrem System »Cookies« mit identifizierenden Informationen ab, wenn Sie auf den Dienst zugreifen.
- Systemprofile. Informationen über Ihr System, z. B. den verwendeten Browser, das Betriebssystem, die installierten Schriftarten, Plug-Ins und sonstige Software (und mehr) können dazu herangezogen werden, ein Profil Ihres Systems zu erstellen. Mehr darüber erfahren Sie auf Panopticlick (*https://panopticlick.eff.org/*), einem Forschungsprojekt der EFF (Electronic Frontier Foundation, *https://www.eff.org/*).

Sie können nicht einfach zu einer Website surfen, ohne Ihre Identität preiszugeben, und wenn irgendjemand nach Ihnen sucht (oder nach Ihrem Computer), kann er Software einsetzen, die den Zugriff durch Sie sofort erkennt und meldet. Es ist nicht möglich, im Kielwasser einer Gruppe autorisierter Benutzer hereinzuschleichen, die Türsteher auf irgendeine Weise zu überreden oder auszutricksen oder sich in einer Wolke von IP-Adressen zu verstecken.

1.2 Was ist Tor?

Tor ist ein Werkzeug zur Wahrung der Anonymität und zur Umgehung der Zensur. Es handelt sich um eine Softwaresuite, die Anonymisierungsprotokolle für gewöhnliche IP-Adressen verwendet. Tor-Knoten (also Computer, auf denen die Tor-Netzwerksoftware läuft), bauen sichere Netzwerkverbindungen zwischen dem auf Anonymität bedachten Benutzer und den Websites auf, die er besuchen möchte. Tor-Clients nutzen Zwischensysteme, sogenannte »Relays«. Dabei handelt es sich um Computer, auf denen Tor-Software läuft und die so eingerichtet sind, dass sie diese Verbindungen für alle aufbauen, die sie benötigen.

Mehr über Tor: Einzelheiten über die Tor-Netzwerkprotokolle
Dieses Buch gibt nur eine sehr allgemeine Beschreibung der Funktionsweise von Tor, ohne auf die Einzelheiten der Protokollimplementierung einzugehen. Wenn ich sage, dass ein Tor-Client eine Verbindung herstellt, dann können Sie davon ausgehen, dass das ein gerüttelt Maß an kryptografischer Kommunikation umfasst, um die Identitäten der Systeme zu bestätigen, die Netzwerkdaten ordnungsgemäß zu verschlüsseln und alles zu vermeiden, was die Identität des Benutzers offenlegen könnte, sowie alles zu tun, was eine solche Offenlegung verhindert.

Um ein genaueres Verständnis des Tor-Projekts zu gewinnen, sollten Sie sich als Erstes das Dokument »Tor: The Second-Generation Onion Router« über das Design des Protokolls ansehen (*https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf*), das viele der Sicherheitsprobleme und Schwierigkeiten beschreibt, denen sich ein Anonymisierungsprotokoll stellen muss. Die Spezifikation des Protokolls ist als »Tor Protocol Specification« (von Roger Dingledine und Nick Mathewson) auf *https://gitweb.torproject.org/torspec.git?a5blob_plain;hb5HEAD;f5tor-spec.txt* erhältlich.

Tor beruht auf dem Grundprinzip eines Netzwerkproxys, also eines Mechanismus, durch den Sie Verbindung mit einem Netzwerk aufnehmen können. Das Proxysystem handelt dabei an Ihrer Stelle. Wenn Sie also über einen Proxy einen entfernten Server erreichen wollen, stellt der Proxy für Sie die Internetverbindung her und tut für diesen Zweck so, als sei er Sie. Der Server glaubt, dass Sie das Proxysystem wären. Woher Sie in Wirklichkeit ins Internet gehen, weiß er nicht.

Proxys sind eine großartige Möglichkeit, Regeln zu umgehen, mit denen Ihr Zugriff zum Internet eingeschränkt wird – sei es durch eine staatliche Firewall, eine Unternehmensfirewall oder Kindersicherungssoftware. Beispielsweise kann ein Unternehmen, das seinen Angestellten die Benutzung von Facebook verbietet, diese Regel durchsetzen, indem es alle Versuche blockiert, von einem System innerhalb des Firmennetzwerks aus eine Verbindung zur Domäne *facebook.com* oder zu IP-Adressen von Facebook-Servern herzustellen.

Durch die Nutzung eines Proxydienstes können Angestellte diese Sperre umgehen. Dabei nimmt ein anderer Server, der von der Unternehmensfirewall nicht blockiert wird, einen URL entgegen und leitet Inhalte von der verbotenen Website zu dem Benutzer weiter. Da dabei nicht versucht wird, direkt auf die verbotene Website zuzugreifen, wird der Vorgang von der Unternehmensfirewall auch nicht blockiert.

In der Praxis sind Proxys ein bisschen komplizierter, und es sind Gegenmaßnahmen möglich, um den Zugriff zu Proxys zu stören oder ganz zu unterbinden. Ein solcher Proxydienst lässt sich gewöhnlich leicht aushebeln, indem man seine Adresse zur Liste derjenigen hinzufügt, die von der Unternehmensfirewall blockiert werden. Wenn die IT-Mitarbeiter die erhöhte Nutzung von Bandbreite zur Verbindung mit einem Proxyserver feststellen, können sie diesen aufspüren und die Firewallregeln so ändern, dass auch der Zugriff darauf blockiert wird. Die Benutzer müssen dann einen anderen Proxyserver finden oder irgendeine andere Maßnahme ergreifen, um den Filter zu umgehen.

Einfache Proxys können das Problem, ohne Zensureinschränkungen auf beliebige Inhalte zuzugreifen, zwar für einige Benutzer lösen (z. B. für Kinder, die die Kindersicherung umgehen wollen), aber in manchen Fällen sind sie wirkungslos:

- Sie müssen Vertrauen darin haben, dass die Personen, die den Proxyserver betreiben, Ihre Privatsphäre respektieren, da der Proxyserver mitbekommt, welche Websites Sie aufrufen, und diese Informationen protokollieren kann. Wenn Ihr Gegner Zugriff auf den Proxyserver bekommt oder Ihre Netzwerksitzung über die Internetverbindung des Proxyservers beobachtet, dann ist diese Sitzung nicht länger geheim.
- Proxyserver lassen sich leicht blockieren, wenn sie erst einmal entdeckt sind – und sie lassen sich auch leicht entdecken, vor allem, wenn mehrere Personen denselben Proxy nutzen.

Tor ist eine ausgeklügeltere Form von Proxy: Es verschleiert Ihr tatsächliches Ziel vollständig und verwendet für anonymen Datenverkehr auch nicht immer dieselbe Zieladresse – wodurch es leichter erkennbar wäre und sich daher durch eine Firewall blockieren ließe. (Manche Gegner blockieren Tor-Relays, deren Adressen öffentlich zugänglich sind, wodurch es nötig wird, Bridge-Relays und andere Mechanismen zu verwenden. Mehr darüber erfahren Sie in Kapitel 4.)

Anstatt Verbindung zu einem Proxyserver aufzunehmen und ihm mitzuteilen, welchen Server im Internet Sie erreichen wollen, nehmen Sie Verbindung mit einem Tor-*Knoten* auf und lassen Ihren Datenverkehr davon an einen weiteren Tor-Knoten weiterleiten. Tor-Knoten, die Tor-Datenverkehr annehmen und zu anderen Knoten weiterleiten können, werden als *Relays* bezeichnet. Ein Tor-Knoten, der Datenverkehr von einem anderen Tor-Knoten annimmt, heißt *Transitknoten*.

Der Tor-Transitknoten, mit dem sich Ihr Tor-Client verbindet, hat keine Ahnung davon, wohin der Datenverkehr geht und womit Sie letzten Endes Verbindung aufzunehmen versuchen. Nur der Tor-*Austrittsknoten* – also

das Tor-Relay, das Datenverkehr aus dem Tor-Netzwerk ins öffentliche Internet weiterleitet – kennt Ihr eigentliches Ziel, aber dafür weiß er nicht, woher der Datenverkehr stammt.

Wenn Sie Verbindung mit dem Tor-Netzwerk aufnehmen, folgt der Computer darin einem zufälligen Pfad. Er wählt einen Transitknoten als Eingang in das Netzwerk aus, einen weiteren Transitknoten innerhalb des Netzwerks und einen Austrittsknoten, der den anonymisierten Datenverkehr ins öffentliche Internet weiterleitet. Der Eintrittsknoten kennt die IP-Adresse Ihres Computers und die IP-Adresse des von Ihrem Computer ausgewählten nächsten Knotens, aber das ist auch alles.

Der zweite Transitknoten kennt weder Sie noch das beabsichtigte Ziel, sondern nur den Eintritts- und den Austrittsknoten. Der Austrittsknoten schließlich weiß nichts über Ihr System oder über Sie, sondern lediglich, welches Ziel Sie zu erreichen versuchen.

Abbildung 1.1 gibt Ihnen einen groben Überblick über die Funktionsweise des Tor-Netzwerks: Der Client am linken Bildrand wählt drei Tor-Relays aus (innerhalb der Tor-Netzwerkwolke) und erstellt gestaffelt verschlüsselte Tunnel, von denen bei jedem Relay einer entfernt wird, bis beim Durchgang durch den Austrittsknoten die Websitzung geöffnet wird.

Mehr über Tor: Grafische Darstellung des Tor-Netzwerks
Die verschiedenen Aspekte des Anonymisierungsnetzwerks von Tor grafisch darzustellen ist nicht sehr einfach. In diesem Kapitel finden Sie einige Abbildungen (siehe Abbildung 1.1 bis 1.3) sowie Links zu anderen Illustrationen. Eine hervorragende Darstellung bietet die interaktive Grafik auf der EFF-Seite »Tor and HTTPS« (*https://www.eff.org/pages/tor-and-https*).

Eine Diskussion einiger der Probleme sowie Vorschläge für genauere bzw. ansprechendere grafische Darstellungen von Tor für technisch weniger versierte Personen finden Sie in »Visual overview of the Tor network« (*https://blog.torproject.org/blog/visual-overview-tor-network*).

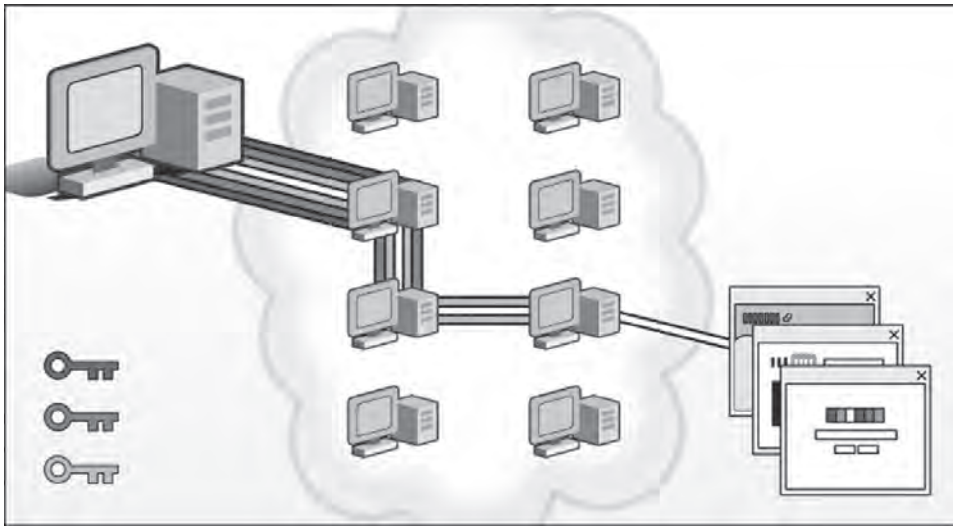

Abbildung 1.1: Tor verschlüsselt die Daten dreimal, einmal für jedes Relay auf dem Weg zum Ziel (Tor-Projekt, *https://archive.torproject.org/tor-package-archive/manual/short-user-manual_en.xhtml*).

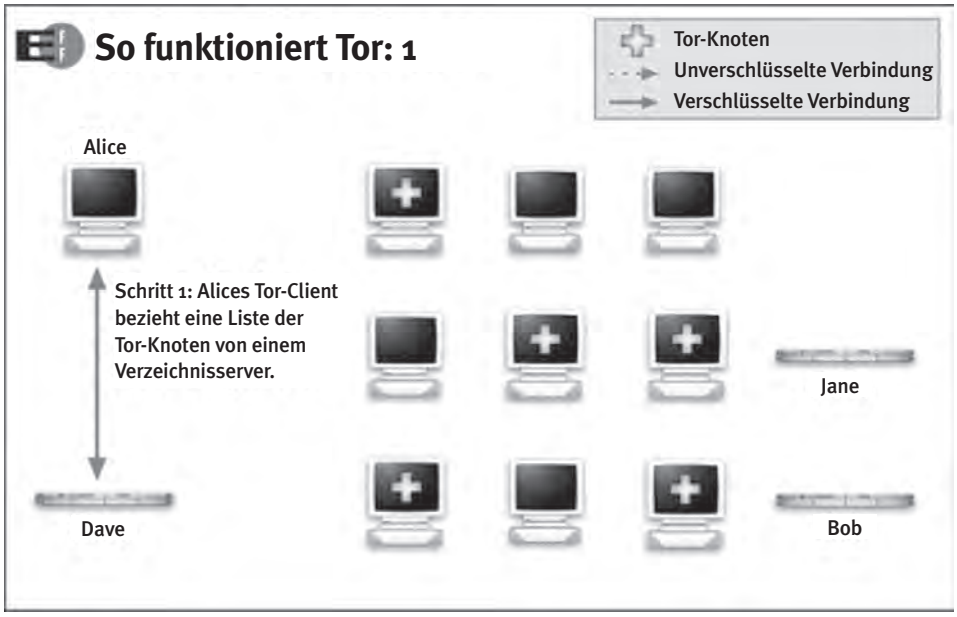

Abbildung 1.2: Alice nimmt über einen Tor-Client Verbindung zu einem Tor-Verzeichnisserver auf dem Computer Dave auf.

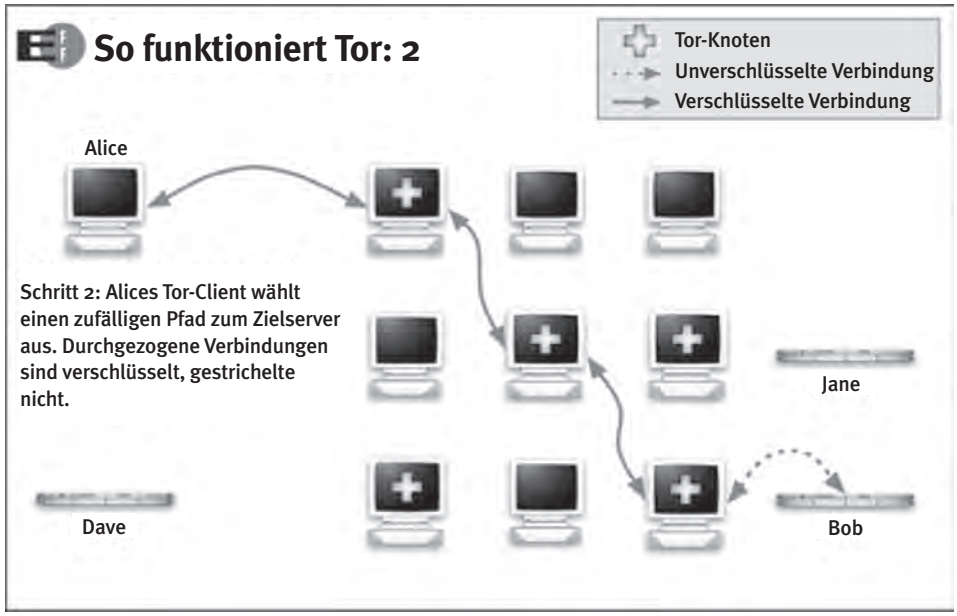

Abbildung 1.3: Verschlüsselte Verbindungen sind als durchgezogene Linien dargestellt, Klartextverbindungen gestrichelt.

1.3 Gründe für die Verwendung von Tor

Es gibt eine Menge guter Gründe für die Verwendung von Tor, und viele davon werden auf der Website des Tor-Projekts dargestellt. Warum *Sie* Tor verwenden, ist letzten Endes Ihre Sache. Lesen Sie weiter, wenn Sie nicht sicher sind, ob Tor etwas für Sie ist.

Die beiden Hauptgründe für die Verwendung von Tor bestehen darin, die Privatsphäre zu wahren und Zensurbestimmungen zu umgehen.

Es gibt viele gute Gründe, seine Privatsphäre wahren zu wollen. Insbesondere möchte man keine unerwünschte Aufmerksamkeit auf seine Interessen ziehen – sei es, um einer Flut von Werbung zu entgehen, die aufgrund

Ihrer Google-Suchvorgänge persönlich auf Sie abgestimmt wird, oder um nicht ins Fadenkreuz von Netzwerkadministratoren zu geraten, die den Datenverkehr nach »verbotenen« Inhalten absuchen.

Angesichts der Menge an Daten, die gesammelt werden können – und tatsächlich gesammelt werden! –, wenn Sie manche populäre Websites aufsuchen, ist es sinnvoll, keine persönlichen Daten durchsickern zu lassen. Um sich einmal anzusehen, welche persönliche Daten aufgedeckt werden können, probieren Sie Lightbeam aus (*http://www.mozilla.org/de/lightbeam/*), ein Firefox-Add-on, das grafisch darstellt, wie viele Informationen von verschiedenen Werbenetzwerken gesammelt werden.

Werfen Sie auch einen Blick auf Disconnect (*https://disconnect.me/tools*), eine Antitracking-Browsererweiterung für Chrome, die Google-, Twitter- und Facebook-Anmeldungen trennt, damit sie nicht aktiv bleiben und Informationen über Sie sammeln, nachdem Sie die betreffenden Websites verlassen haben. Im Coderepository dieses Programms heißt es: »Disconnect hindert Dritte und Suchmaschinen daran, nachzuspüren, welche Webseiten Sie aufsuchen und welche Suchvorgänge Sie durchführen.«

Eine vorgeschlagene Lösung zur Wahrung der Privatsphäre ist die »Do-not-track-Richtlinie« (*https://www.eff.org/issues/do-not-track*). Dabei soll ein neuer HTTP-Header – der DNT-Header (für »do not track«) – Webservern und Drittanbieter-Trackingeinrichtungen die Bitte vermitteln, die Aktivitäten des Benutzers nicht zu verfolgen. Das Problem bei dieser »Lösung« besteht darin, dass die Server diese Bitte auch erfüllen müssen. Tatsächlich handelt es sich dabei um nicht mehr als um eine Bitte, denn es gibt keine Möglichkeit, die Einhaltung sicherzustellen. Eine solche Möglichkeit würde dem Geschäftsmodell gerade der Unternehmen zuwider laufen, die das meiste Tracking durchführen. Der Artikel »Do Not Beg: Moving Beyond DNT through Privacy by Design« (*http://www.w3.org/2012/dnt-ws/position-papers/21.pdf*) erklärt, warum DNT eine nicht technische Nicht-Lösung für ein Problem ist, für das Tor eine echte Lösung bietet.

Die Nutzung eines Anonymisierungsnetzwerks wie Tor gibt den Benutzern die Kontrolle darüber, welche Informationen sie beim Surfen offenlegen.

Wenn ein Remoteserver oder ein Netzwerkprovider den tatsächlichen Standort oder die Organisation des anonym surfenden Benutzers nicht kennt, kann er auch keine maßgeschneiderten Antworten auf der Grundlage dieser Informationen geben.

Solche maßgeschneiderten Antworten sind eine Möglichkeit, mit der Regierungen große Firewalls unterhalten, um ihre Bürger von Nachrichtenquellen abzuschirmen, die als regimegefährdend gelten.

Firmenwebsites können besondere Angebote zusammenstellen, je nachdem, ob der Benutzer bereits Kunde ist oder nicht. Unternehmen können ihre Websites auch so einrichten, dass Mitbewerber darüber keine Informationen einholen können. Verdeckte Ermittler können sich versehentlich selbst verraten, wenn Kriminelle mit Netzwerkkenntnissen ihre Aktivitäten zu IP-Adressen zurückverfolgen, die zu Strafverfolgungsbehörden gehören. Diese Beispiele sind nicht nur theoretische Möglichkeiten, sondern dokumentierte Fakten.

Für die unterschiedlichen Bedürfnisse an Privatsphäre ist nicht immer dieselbe Lösung erforderlich. Wie bereits erwähnt, kann in manchen Fällen schon die Nutzung eines Proxydienstes ausreichen. Jemand, der nur seinen Browserverlauf vor seinem Lebenspartner verbergen möchte, kann einfach die Option für den privaten Modus (Firefox) oder den Inkognito-Modus (Chrome) einschalten – z. B. wenn es darum geht, eine besonderes Geschenk zu besorgen oder eine Überraschungsparty zu organisieren, weshalb der Lebenspartner besser nicht die besuchten Websites sehen sollte.

Der private Browsermodus bietet jedoch *keine* echte Anonymität: Jemand, der das Netzwerk beobachtet oder auf die Serverprotokolle der von Ihnen besuchten Websites zugreift, weiß trotzdem alles über Sie. Diese Optionen dienen lediglich dazu, Ihre Webaktivitäten vor Personen zu verbergen, die Zugriff auf Ihren Computer haben.

Es gibt jedoch einen erheblichen Unterschied zwischen den Bedürfnissen nach Privatsphäre und Anonymität einer Person, die ihren Lebenspartner überraschen möchte, und eines politischen Aktivisten, der hinter einer staatlichen Firewall arbeitet. Letzterer hat es mit einem Gegner zu tun, der jeden Aspekt der Arbeit in Computernetzwerken im Lande kontrolliert oder zumindest kontrollierten kann und der über ausreichend Personal und technische Mittel verfügt, um alles daranzusetzen, dem Aktivisten die erforderlichen Internetwerkzeuge für den organisierten Widerstand zu versagen.

Es ist äußerst wichtig, die Stärke der Bedrohung abzuschätzen. Für den wirkungsvollen Einsatz jeglicher Art von Sicherheitswerkzeugen für Computer oder Netzwerke ist dies unverzichtbar.

Tor kann für Personen hilfreich sein, die nach Informationen über eine peinliche Krankheit suchen, aber nicht von Google-Anzeigen für entsprechende Produkte zugeschüttet werden wollen. Es kann sogar lebensrettend sein. Doch je stärker Ihr Bedarf nach Datenschutz ist, umso sorgfältiger müssen Sie sich damit vertraut machen, wie Tor funktioniert, was es für Sie tun kann – und was nicht.

Es gibt verschiedene Möglichkeiten, die Stärke der Bedrohung abzuschätzen, insbesondere im Zusammenhang mit staatlichen Behörden und anderen Organisationen. Beispielsweise beschreibt der Artikel »How Do You Asses Your Organization's Cyber Threat Level?« (*http://www.mitre.org/work/tech_papers/2010/10_2914/10_2914.pdf*) systematisch Methoden, um auf der Grundlage dessen, was Sie über Ihre Gegner wissen, zu bestimmen, wie besorgt Sie um das Wohlergehen Ihrer Organisation sein sollten.

Tor kann Ihnen helfen, wenn Sie in einem Land, in dem Internetbenutzer für die Beschaffung (und Verbreitung) bestimmter Informationen bestraft werden, das Internet nutzen müssen.

Regierungsbehörden müssen Internetverbindungen nicht einmal selbst überwachen, sofern sie die Möglichkeit haben, auf Provider und Web-Publisher Druck auszuüben, sodass diese Protokolle aller Netzwerkaktivitäten führen.

In den allgemeinen Geschäftsbedingungen und Datenschutzerklärungen der meisten Provider und Websites steht ausdrücklich, dass sie legitimen Anforderungen von Regierungs- und Strafverfolgungsbehörden nachkommen, auch wenn das bedeutet, Ihre »privaten« Daten zu entschlüsseln.

Nicht alle großen Internetunternehmen behandeln das Recht ihrer Benutzer auf Privatsphäre mit demselben Respekt. Der EFF-Bericht »Who Has Your Back?« (*https://www.eff.org/who-has-your-back-2014*) gibt Ihnen eine Vorstellung davon, welche Unternehmen gewillt sind, dieses Recht hochzuhalten, und was sie dazu zu tun bereit (und nicht bereit) sind.

1.4 Was Tor nicht leisten kann

Wenn Sie annehmen müssen, dass Ihr gesamter Netzwerkdatenverkehr überwacht wird (oder überwacht werden kann) – was der Fall ist, wenn Sie von einem Unternehmen oder von einem Land mit einer staatlichen Firewall aus das Web aufzusuchen –, dann können Sie auch davon ausgehen, dass beim Zugriff auf eine verbotene Website die Alarmlämpchen auf dem Schreibtisch einer zuständigen Person aufleuchten.

Tor ist so konstruiert, dass es Ihnen in solchen Situationen helfen kann – aber es bietet keinen vollständigen Schutz.

Die Tor-Verbindungen verlaufen von der Verbindung zum Eintrittsknoten über ein Transitrelay durch das Netzwerk und zum Austrittsknoten. Alle »Hops« (Abschnitte) zwischen den Relays sind verschlüsselt. Die Verbindung vom Austrittsknoten zur Zielwebsite jedoch wird von Tor nicht verschlüsselt. Wenn jemand das Netzwerk der Zielwebsite überwacht, kann er an Ihre unverschlüsselten Websitzungen gelangen. Das können Sie in Abbildung 1.3 erkennen, wo die Verbindung zwischen dem Tor-Austrittsknoten und dem Server Bob als nicht verschlüsselt dargestellt ist. Im Idealfall ist auch dieser letzte Hop verschlüsselt, aber das ist nicht immer der Fall. Eine Teillösung für dieses Problem wird in dem Kasten »HTTPS und HTTPS Everywhere« weiter hinten in diesem Kapitel beschrieben.

Tor kann auch keine Sicherheit bieten, wenn Ihr Gegner Ihren Computer gehackt und beispielsweise Software oder Hardware installiert hat, die Tastenbetätigungen aufzeichnet und weiterleitet (*Keylogging*), den Zugriff auf bestimmte Netzwerkressourcen verhindert oder Ihre Tätigkeiten weitermeldet. Denken Sie daran: »Anonymität braucht Gesellschaft.«

Was es mit diesem Satz auf sich hat, erfahren Sie in dem Artikel »Anonymity Loves Company: Usability and the Network Effect« auf *http://freehaven.net/anonbib/cache/usability:weis2006.pdf*). Wenn Sie als einzige Person in einem Netzwerk hinter einer Firmen- oder einer staatlichen Firewall Tor benutzen, dann sind Sie nicht gerade besonders anonym.

Tor hindert Sie auch nicht daran, Ihre Anonymität durch Ihre Online-Aktivitäten selbst aufzugeben. Wenn Sie über Tor auf persönliche Konten zugreifen, Ihre persönlichen Daten auf Websites eingeben oder heruntergeladene Dateien öffnen, kann das Ihre Anonymität gefährden. (Weitere Einzelheiten erfahren Sie im Abschnitt »Öffnen Sie keine Dokumente«.)

Des Weiteren kann Sie Tor nicht vor *durchgängigen Timing-Angriffen* schützen, bei denen der Angreifer sowohl den (verschlüsselten) Netzwerkdatenverkehr überwacht, der Ihren Computer verlässt, als auch denjenigen, der am Zielserver ankommt. Ein solcher Angriff ist jedoch nur mit erheblichen Ressourcen und Zugriff auf viele verschiedene Netzwerke möglich. Bei den Angreifern handelt es sich um Staaten oder um ähnlich mächtige Organisationen.

Betrachten Sie zur Veranschaulichung das folgende Beispiel: Der Angreifer erkennt (durch die Überwachung Ihrer lokalen Netzwerkübertragungen), dass jemand irgendwo über Tor 100 KB verschlüsselte Daten gesendet hat, und bemerkt wenige Augenblicke später, dass 100 KB beim Blog eines politischen Aktivisten angekommen sind. Selbst wenn die Daten verschlüsselt sind, kann das Ärger für den Blogger bedeuten, da der Angreifer nachweisen kann, dass sein Computer die Quelle des verbotenen Inhalts war. Wenn unmittelbar nach der Ankunft der Daten auch noch ein umstürzlerischer Artikel auf der Website erscheint, wird die Sache noch schlimmer. In jedem Fall ist die Anonymität des Benutzers dahin, und der Benutzer kann erwarten, dass die Behörden ihn verstärkt überwachen.

Die Entwickler von Tor arbeiten weiterhin daran, die Verwundbarkeit gegenüber solchen Angriffen zu verringern, und um einen solchen Angriff ausführen zu können, sind erhebliche Ressourcen und Fähigkeiten erforderlich. Doch trotzdem müssen Sie sich darüber im Klaren sein, dass dies möglich ist, und entsprechende Vorsichtsmaßnahmen treffen. Der Artikel »Avoid risks and protect online identity« (*https://blog.torproject.org/blog/avoid-risk-and-protect-online-identity*) gibt unter anderem auch Hinweise für sicheres Bloggen.

1.5 So funktioniert Tor

Tor verwendet ein Protokoll mit »Zwiebelschalen-Routing« (»Onion Routing«), um den Benutzern einen Internetzugriff über ein Proxynetzwerk zu ermöglichen, und verhindert dadurch, dass der Zielserver (oder jemand, der diesen Server oder dessen Netzwerk überwacht) die IP-Adresse des Benutzercomputers ermittelt. Die Bezeichnung »Zwiebelschalen-Routing« geht darauf zurück, dass der Netzwerkdatenverkehr in mehrere Schichten verpackt wird, wobei die Systeme diese Schichten bei der Weiterleitung unterwegs eine nach der anderen abziehen – wie beim Häuten einer Zwiebel.

Die Wirksamkeit von Tor fußt darauf, dass es viele Benutzer gibt, zwischen denen Sie sich »verstecken« können. Der grundlegende Vorgang sieht wie folgt aus:

- Ein Tor-Client ruft eine Liste der verfügbaren Tor-Relays ab. Diese Liste wird als Konsensdokument bezeichnet, da sich alle Tor-Verzeichnisserver darüber einig sind, dass die darin verzeichneten Relays an das Netzwerk angeschlossen und zur Weiterleitung von Tor-Datenverkehr vertrauenswürdig sind (siehe Abbildung 1.2).
- Der Tor-Client legt seinen eigenen Pfad durch das Tor-Netzwerk fest. Diese Route besteht aus dem Eintrittshop zu einem Eintrittsknoten, dem zweiten Hop vom Eintrittsknoten zu einem weiteren Transitknoten und dem dritten Hop von dem internen Transitknoten zum Austrittsknoten.

- Der Austrittsknoten stellt die gewünschte Verbindung (gewöhnlich zu einem Webserver) für den ursprünglichen Tor-Client her und fungiert als dessen Proxy.

Wer den Netzwerkdatenverkehr vom und zum Tor-Client überwacht, kann erkennen, dass der Client Tor-Datenverkehr an einen Tor-Eintrittsknoten sendet. Dieser Datenverkehr ist verschlüsselt und wird technisch als geschützt angesehen (vorausgesetzt, dass Tor korrekt installiert, konfiguriert und verwendet wird).

Wird der Datenverkehr zwischen dem Tor-Client und dem Tor-Austrittsknoten untersucht, kann der Klartext der Websitzung gelesen werden (falls keine durchgängige Verschlüsselung mit HTTPS durchgeführt wird; siehe den Kasten über HTTPS). Es ist dann jedoch nicht möglich, den Standort (die IP-Adresse) des ursprünglichen Tor-Clients herauszufinden.

Eine grafische Darstellung der Art und Weise, in der der Netzwerkdatenverkehr geschützt wird, sehen Sie auf *https://www.eff.org/pages/tor-and-https*. Dort können Sie erkennen, welcher Datenverkehr angreifbar ist, je nachdem, ob Sie Tor, HTTPS Everywhere oder beides verwenden.

Zusätzliche Werkzeuge für Tor: HTTPS und HTTPS Everywhere
HTTPS steht für HTTP Secure. In einem URL teilt diese Angabe dem Browser mit, dass der Server ein zusätzliches Protokoll verwendet (Transport Layer Security, TLS), um die Daten zu verschlüsseln.

Wenn Sie eine Website aufsuchen, die HTTPS unterstützt, erhalten alle URLs das Präfix *https://* (statt *http://*). Alles, was dann vom oder zum Server gesendet wird, ist so verschlüsselt, dass nur der empfangende Computer es entschlüsseln kann.

Wenn HTTPS *nicht* verwendet wird, kann ein Gegner, der das lokale Netzwerk überwacht (WLAN oder Ethernet), erkennen, welche Websites und welche Seiten auf diesen Websites Sie aufsuchen und welche Informationen Sie senden und empfangen. Dazu gehören auch IDs und Passwörter.

Wird HTTPS verwendet, kann ein solcher Gegner zwar bestimmen, auf welche Website Sie zugreifen, aber nicht sehen, welche Seiten Sie sich dort ansehen und welche Informationen Sie senden und empfangen.

HTTPS reicht nicht aus, um anonym auf eine Website zugreifen zu können, ist aber eine wichtige Methode, um die Menge der Informationen zu verringern, die Sie online offenlegen.

Das Projekt HTTPS Everywhere (*https://www.eff.org/https-everywhere*) ist eine Zusammenarbeit zwischen der EFF (*https://www.eff.org/*) und dem Tor-Projekt. Es handelt sich dabei um eine Browsererweiterung für Firefox und Chrome, die die Verwendung von HTTPS auf Websites erleichtert, die das Protokoll unterstützen. HTTPS Everywhere ist in der Tor-Softwaredistrubution enthalten und wird allen Benutzern empfohlen, die eine Überwachung und Übernahme Ihrer Websitzungen verhindern möchten.

1.5.1 Bestandteile des Tor-Protokolls

Zu Tor gehören die folgenden Systeme:

- Der *Tor-Client*, eine Software, die auf einem Computer (PC, Netbook, Tablet, Smartphone usw.) läuft und die Verbindung zum Anonymisierungsnetzwerk von Tor aufnimmt. Auch das System, auf dem die Tor-Clientsoftware läuft, wird als Tor-Client bezeichnet.
- Der *Tor-Verzeichnisdienst*. Er besteht aus einer Reihe von Servern, die eine Datenbank der aktiveren Tor-Relays pflegen und Anforderungen nach Informationen darüber beantworten.
- Der *Tor-Eintrittsknoten*. Dieses System nimmt Netzwerkdatenverkehr von einem Tor-Client entgegen und leitet ihn an einen anderen Tor-Knoten weiter. Bei dem Eintrittsknoten kann es sich um einen beliebigen Typ von Tor-Relay handeln (Austritts-, Transit- oder Bridge-Knoten).

Da der Tor-Datenverkehr auf dem ersten Hop, also vom Client zum Eintrittsknoten, verschlüsselt wird, kennt der Eintrittsknoten nur die IP-Adresse des ursprünglichen Tor-Clients, aber nicht das Ziel, und kann auch nicht auf die gesendeten Inhalte zugreifen.

- Der *Tor-Transitknoten*. Dieser Computer nimmt Tor-Datenverkehr von einem Tor-Knoten entgegen und leitet ihn an einen weiteren Tor-Knoten. Transitknoten können für den ersten und den zweiten Hop in einer Tor-Verbindung verwendet werden. Sie haben keine Möglichkeit, zu erkennen, welchen Bestimmungsort der von ihnen weitergeleitete Datenverkehr hat und welchen Inhalt er umfasst.
- Der *Tor-Austrittsknoten*. Dieser Computer nimmt Tor-Datenverkehr von einem anderen Tor-Knoten an und leitet ihn an sein vorgesehenes Ziel im öffentlichen Datenverkehr. Tor-Austrittsknoten können als Quelle oder Ziel von unerwünschten oder verdächtigen Inhalten erscheinen und haben Zugriff auf jegliche unverschlüsselte Daten, die vom oder zum Ziel gesendet werden. Aus diesem Grund ist es wichtig, HTTPS Everywhere zu verwenden (siehe Kasten).

Tor-Netzwerkknoten (Systeme, die Tor-Datenverkehr weiterleiten) werden auch als *Relays* bezeichnet. Ein Tor-Relay, das als Austrittsknoten eingerichtet ist, kann auch als Transitknoten verwendet werden. Der Knotentyp hängt jeweils davon ab, wie das System in einer Verbindung genutzt wird. Die Betreiber von Tor-Relays können ihre Computer jedoch auch so einrichten, dass sie nur als Austritts- oder nur als reine Transitknoten funigeren.

Tor-Clients führen eine direkte Kommunikation nur mit dem Tor-Verzeichnisserver (zur Ermittlung der Tor-Relays) und dem Tor-Eintrittsknoten durch (zum Senden und Empfangen von Daten). Jegliche Kommunikation des Clients mit anderen Tor-Knoten (Transit- und Austrittsknoten) und dem Ziel erfolgt über den Eintrittsknoten und wird von einem Knoten zum anderen weitergeleitet.

Eine ausführliche Beschreibung des Tor-Protokolls finden Sie in der Spezifikation von Roger Dingledine und Nick Mathewson (*https://gitweb.torproject.org/torspec.git?a5blob_plain;hb5HEAD;f5tor-spec.txt*).

1.5.2 Sichere Tunnel mit den öffentlichen Schlüsseln der Tor-Knoten aufbauen

Der Tor-Client wählt einen Eintritts-, einen Transit- und einen Austrittsknoten und damit eine zufällige Route aus.

Anschließend verschlüsselt er die Daten, die er an das Ziel sendet, mithilfe des Schlüssels, der dem ausgewählten Austrittsknoten gehört. (Zur Erhöhung der Sicherheit sollten die Daten, die an den Zielserver gehen, mithilfe des Protokolls HTTPS verschlüsselt werden.)

Die so verschlüsselten Daten verschlüsselt der Client mit dem Schlüssel des Transitknotens, und diese zweifach verschlüsselten Daten dann noch einmal mit dem Schlüssel des Eintrittsknotens. Nun kann der Client Webdaten über einen sicheren Tunnel durch das Anonymisierungsnetzwerk von Tor senden und empfangen:

- Der Tor-Eintrittsknoten entschlüsselt ein Paket und sendet es an den Transitknoten im zweiten Hop.
- Der Tor-Transitknoten entschlüsselt wiederum dieses Paket und leitet es an den Austrittsknoten im dritten Hop.
- Der Tor-Austrittsknoten entschlüsselt das Paket und leitet es an das Ziel.

Tor-Transitknoten (oder Transit-Relays) können Pakete von beliebigen anderen Tor-Knoten empfangen und an beliebige andere Tor-Knoten (also andere Transit-Relays oder Austrittsknoten) weiterleiten. Befindet sich der Knoten im ersten Hop einer Tor-Verbindung, so fungiert er als Eintrittsknoten.

Da die Eintrittsknoten Datenverkehr von beliebigen Tor-Clients annehmen, weiß ein Gegner, der einen Tor-Client beobachtet, nur, dass dieser Client Tor benutzt, und kennt den Tor-Eintrittsknoten. Dieser Eintrittsknoten leitet den Datenverkehr des beobachteten Clients ebenso wie den Datenverkehr *anderer* Clients an Tor-Transitknoten weiter. Sofern also genügend Benutzer denselben Eintrittsknoten verwenden, kann der Gegner nicht bestimmen, welcher Datenverkehr zu welchem Transitknoten geht.

Der Transitknoten im zweiten Hop leitet den Datenverkehr zum Austrittsknoten weiter, ohne zu wissen, von welchem Tor-Client dieser Datenverkehr stammt. Das Gleiche gilt auch für den Austrittsknoten, sofern HTTPS verwendet wird. (Wenn das Ziel HTTPS nicht unterstützt, liegt der ausgehende Datenverkehr im Klartext vor und kann überwacht werden.)

Bei der Weiterleitung der Daten durch das Tor-Netzwerk werden die Verschlüsselungsschichten wie Zwiebelschalen abgezogen (daher die Bezeichnung »Onion Routing«).

Der einzige Tor-Knoten in der Verbindung, der mit dem Tor-Client in Verbindung gebracht werden kann, ist daher der Eintrittsknoten, und der einzige Knoten, der Rückschlüsse auf das Ziel zulässt, der Austrittsknoten. Vom internen Transitknoten (der im zweiten Hop) kann nur auf den Eintritts- und den Austrittsknoten gefolgert werden. Das Ergebnis ist eine Kommunikationsverbindung, die keinen Zusammenhang zwischen dem Tor-Client und dem angesprochenen Server im Internet mehr erkennen lässt.

1.5.3 Der Austrittsknoten als Vertreter des Tor-Clients

Der gesamte Netzwerkverkehr, der aus dem Tor-Netzwerk austritt, sieht so aus, als sei er von den Tor-Austrittsknoten in das Internet eingespeist worden – nicht von den ursprünglichen Clientknoten.

Daher fungiert das gesamte Tor-Netzwerk als Proxy: Sie geben Daten ein, die wiederholt verschlüsselt und verpackt werden, damit es so aussieht, als kämen sie von dem Austrittsknoten. Ebenso sieht auch der gesamte eingehende Datenverkehr so aus, als käme er vom gewählten Eintrittsknoten des Clients statt von dem tatsächlichen (und möglicherweise blockierten) Server.

Diese Eigenschaft macht Tor so wertvoll: Wenn eine staatliche Firewall z. B. den gesamten Datenverkehr zu YouTube blockiert, können Tor-Benutzer diese Sperre umgehen, indem sie Tor-Eintrittsknoten verwenden, die von dieser Firewall nicht blockiert werden.

Aus demselben Grund können Tor-Benutzer auch im Internet surfen, ohne persönliche Informationen preiszugeben (insbesondere ihre IP-Adresse, die fast immer direkt zu einem konkreten Standort zurückverfolgt werden kann).

1.6 Wer verwendet Tor?

Tor wird aus unterschiedlichsten Gründen genutzt. Manche mögen »falsch« wirken, weil es darum geht, Einschränkungen des Internetzugriffs zu umgehen, die von Autoritäten verschiedener Art aufgestellt wurden. Beispielsweise können Kinder, Angestellte oder Bürger Websites aufrufen, deren Besuch ihnen von den Eltern, der Geschäftsführung oder der Regierung verboten wurde.

Tor erlaubt es, ohne Freigabe durch die zuständigen Autoritäten auf Inhalte im Internet zuzugreifen und sie zu veröffentlichen – und das auf eine Weise, die eine Identifizierung verhindert. Für ein Kind mag das Risiko beim Besuch einer verbotenen Website nur in elterlicher Maßregelung bestehen (die in manchen Fällen durchaus verdient sein kann), für andere aber – z. B. für Informanten, die Unternehmensinterna verraten, oder für politische Aktivisten – kann die Gefahr viel größer sein. Und das betrifft nicht nur die Informanten, die mit Repressalien zu rechnen haben, sondern auch die Personen, denen der Zugriff auf die betreffenden Informationen verwehrt wird.

Solchen Benutzern gibt Tor ein Werkzeug an die Hand, um Gutes zu tun, z. B. um wichtige Informationen zu verbreiten oder um den Widerstand gegen ein diktatorisches Regime zu organisieren. Es gibt viele gute Gründe zur Nutzung von Tor, doch manche sehen es als eine Bedrohung an, die es Kriminellen erlaubt, ungestraft Verbrechen zu begehen.

Das Problem bei diesem Argument besteht darin, dass jeder, der in der Lage ist, ein Verbrechen *mit* Tor zu begehen, die gleiche Anonymität auch durch andere kriminelle Maßnahmen erreichen kann, indem er z. B. das

Smartphone oder den Computer einer anderen Person stiehlt oder Botnetze betreibt, um übernommene Computer zu steuern.

Außerdem unterstellt diese Argumentation, dass »falsch« und »illegal« das Gleiche ist, was aber eindeutig nicht der Fall ist. Die Personen, die Tor entwickeln und unterstützen, tun dies, weil sie an die Menschenrechte glauben und an die Notwendigkeit der Anonymität zur Verteidigung dieser Rechte, insbesondere in Situationen, in denen die Ausübung dieser Rechte ohne Anonymität Gefahr bedeutet.

Auf der Website des Tor-Projekts gibt es eine großartige Seite, die beschreibt, was für Personen Tor nutzen (*https://www.torproject.org/about/torusers.html.en*). Diese Liste ist nicht erschöpfend, aber es ist ganz gut zu sehen, dass ein gesetzestreuer Bürger immer dann, wenn er nicht von einer Regierungsbehörde oder einer anderen Stelle identifiziert werden möchte, auf Tor zurückgreifen kann.

Die folgende Aufstellung nennt einige Kategorien von Benutzern, die auf der Website des Tor-Projekts erwähnt werden und für die Tor hilfreich ist.

1.6.1 Normalbürger

Ihr Provider – und die Angestellten, die für Ihren Provider arbeiten – können alles sehen, was Sie im Internet tun. Zwar können sie nicht unbedingt alle Einzelheiten erkennen (wenn Sie über HTTPS auf Websites zugreifen), aber sie können immerhin jede Website und jede Webseite protokollieren, die Sie besuchen, und dabei festhalten, wann und wie lange Sie sich dort aufhalten. Auch Webwerbenetzwerke können einen Großteil Ihrer Webaktivitäten verfolgen, wenn nicht gar alle. Wenn Sie an Ihrem Arbeitsplatz auf das Internet zugreifen, kann sich auch Ihr Arbeitgeber (und dessen ISP) darüber informieren, welche Websites Sie besuchen.

Warum stellt das für »Menschen wie du und ich« ein Problem dar? Aus einer Reihe von Gründen:

- Es ist sehr einfach, aus Webaktivitäten falsche Schlüsse zu ziehen. Das kann einfach nur nervtötend sein, wenn irgendwelche Werbenetzwerke ständig Anzeigen für Produkte im Zusammenhang mit Ihren letzten Suchvorgängen einblenden, aber auch ernsthafte Konsequenzen haben, etwa wenn Sie Ihren Job verlieren, weil Ihr Arbeitgeber aufgrund Ihrer Suche nach »Chemotherapie« glaubt, dass Sie Krebs haben.
- Werbetreibende und andere Personen, die Zugriff auf Aufzeichnungen über das Surfen im Web haben, können eine IP-Adresse zu einer Straßenanschrift zurückverfolgen und mit anderen Informationen über Sie und Ihre Webaktivitäten verknüpfen.
- Eltern möchten verhindern, dass Ihre Kinder online zu viele Informationen preisgeben.
- Wenn jemand Themen recherchieren möchte, die in seinem Land als »sensibel« eingestuft werden (z. B. Alkohol in Saudi-Arabien oder Menschenrechte in China), kann es sein, dass diese Suchvorgänge entweder blockiert (gefiltert) werden oder unerwünschte Aufmerksamkeit oder Untersuchungen nach sich ziehen.

Wenn Sie über Tor auf Ihr Facebook- oder Google-Konto zugreifen, sind Sie zwar dagegen geschützt, dass jemand die Kommunikation abfängt. Beachten Sie aber, dass dies keinen Schutz vor Gegnern wie denen bietet, die im PRISM-Projekt der NSA beschrieben werden, wobei die NSA Zugriff auf die Server von Google und Facebook hat. Ihre persönlichen Daten sind auf diesen Servern gespeichert und unterliegen den Richtlinien der betreffenden Websites.

In der Regel sollten Sie es vermeiden, mit Tor auf irgendwelche Informationen zuzugreifen, die Sie als Person identifizieren können, wenn dies eine Gefahr für Sie darstellt.

1.6.2 Militär

Tor wurde ursprünglich mit Mitteln des US Naval Research Laboratory mit dem Ziel entwickelt, die Kommunikation von staatlichen Stellen zu schützen. Es gibt zahlreiche militärische Anwendungen für Tor:

- Verdeckte Ermittler und Agenten können Tor nutzen, um der Erkennung durch Gegner zu entgehen, die Netzwerkaktivitäten überwachen. Tor stellt für Agenten ein Werkzeug dar, um verdeckt Verbindung mit Systemen aufzunehmen, die bekanntermaßen zum Militär gehören. (Die IP-Adressregistrierung ist öffentlich, und das gilt auch für IP-Adressen für Regierungsstellen und Militäreinrichtungen.)
- Mithilfe verborgener Dienste (siehe Kapitel 6 und den Kasten »Verborgene Tor-Dienste«) können Informationen (für Führungs- und Lagedienste) erfasst und verbreitet werden, ohne den Standort der Dienste und die Standorte und Identitäten derjenigen preiszugeben, die sie nutzen.
- Aufklärung, insbesondere die Verbindung mit Ressourcen, die auch der Gegner verwenden kann. Mithilfe von Tor können Militärangehörige auf solche Ressourcen zugreifen (Webserver, Onlineforen usw.), ohne ihren Standort und ihre Identität preiszugeben (die sich aus der IP-Adresse ihres Netzwerkclients leicht ableiten ließe).

Hätte die US-Regierung versucht, Tor ausschließlich für die »offizielle« Verwendung zu reservieren, dann wäre Tor genau das Gegenteil von anonym geworden: Tor-Datenverkehr aufzuspüren wäre dann eine todsichere Möglichkeit geworden, Personen zu erkennen, die im Auftrag der Regierung unterwegs sind.

1.6.3 Journalisten und ihre Leser/Zuschauer

Journalisten – und das betrifft auch Blogger und andere Arten von »Privatjournalisten« – können Tor zu ihrem Schutz nutzen, wenn sie aus Teilen der Welt berichten, in denen es keinen sicheren Zugang zum Internet gibt. Außerdem können sie damit auch ihre Quellen schützen, die anonym bleiben möchten.

1.6.4 Strafverfolgungsbehörden

Strafverfolgungsbehörden und ihre Mitarbeiter können Tor für ihre Ermittlungsarbeit nutzen:

- Sie können damit Informationen von fragwürdigen Websites oder Netzwerkdiensten abrufen, die von illegalen Organisationen betrieben oder für illegale Zwecke verwendet werden.
- Sie können verdeckte Ermittlungen durchführen, ohne preiszugeben, dass die verwendeten Systeme IP-Adressen haben, die für Strafverfolgungsbehörden registriert sind.
- Sie können Informanten helfen, Hinweise zu geben, ohne ihre Identität preiszugeben.

1.6.5 Informanten und Aktivisten

Auf der Website des Tor-Projekts finden Sie viele Beispiele für Aktivisten und Informanten, die Tor nutzen, um sich für Menschenrechte und gegen Korruption einzusetzen (siehe *https://www.torproject.org/about/torusers.html.en#activists*).

1.6.6 Personen mit und ohne große Öffentlichkeitswirkung

Allen Personen, deren Aktivitäten in der Öffentlichkeit sehr stark wahrgenommen werden, kann Tor helfen, Meinungen zu verbreiten oder Sachverhalte zu recherchieren, die unbequem sind oder die nichts mit ihrem üblichen öffentlichen Auftreten zu tun haben.

Ebenso ist Tor für diejenigen geeignet, die nur über wenige Ressourcen und wenig Einfluss verfügen, um Meinungen auszudrücken und Dinge zu recherchieren, die leicht fehlinterpretiert werden oder unerwünschte Auf-

merksamkeit auf sich ziehen können. Mit Tor können sie ihre Meinungen ausdrücken, ohne Angst vor Repressalien aufgrund unbequemer Ansichten durch Arbeitgeber, Behörden oder andere Autoritäten zu haben.

1.6.7 Geschäftsleute und IT-Experten

Geschäftsleute nutzen Tor als wichtiges Werkzeug für eine Reihe von Zwecken:

- Anonymer Zugriff auf die Onlineressourcen von Mitbewerbern, insbesondere wenn diese Mitbewerber Filter einsetzen, um ihre Informationen vor Benutzern zu verbergen, die vom Netzwerk der Konkurrenz aus ihre Websites aufsuchen.
- Bereitstellung einer Möglichkeit für Angestellte, um auf wirklich anonyme Weise Missstände an die Geschäftsleitung zu melden.

Auch IT-Experten können Tor nutzen, insbesondere um Unternehmensfirewalls und andere Netzwerkressourcen zu testen. Da der Tor-Datenverkehr von außerhalb der Organisation zu kommen scheint, können damit Sicherheitseinrichtungen und Firewalls sowie Betriebsabläufe getestet werden. Es ist damit auch möglich, die Unternehmensfirewall zu umgehen, ohne sie umzukonfigurieren.

1.6.8 Weitere Personen

Jeder, der unerkannt bleiben und nicht auffallen möchte, kann Tor einsetzen. Tor hindert Verfolger daran, ihre Opfer zu finden – ganz gleich, ob Sie sich vor einem ausfälligen Familienangehörigen oder einem übereifrigen Inkassobüro verstecken wollen.

Tor ist insbesondere für Personen nützlich, die in einem ungleichmäßig verteilten Machtkampf liegen, die also nur in Ruhe gelassen werden wollen,

während ihr Gegner Zugang zu ausgefeilten Ressourcen hat. Beispielsweise sind Fälle bekannt, in denen korrupte Politiker, Regierungsangestellte und Beamte von Strafverfolgungsbehörden ihre Privilegien missbraucht haben.

1.6.9 Der Vorteil eines breiten Spektrums an Benutzern

Angehörige des Militärs und von Strafverfolgungsbehörden, die zum ersten Mal von Tor hören, äußern oft den Wunsch, dass Tor für ungesetzlich erklärt oder dass zumindest eine Hintertür eingebaut wird, über die die »richtigen Leute« in der Lage sind, Personen zu verfolgen, die Tor für kriminelle Aktivitäten missbrauchen.

Tor verdankt seine Nützlichkeit jedoch zu einem großen Teil der Tatsache, dass es keine Möglichkeit gibt, seine Benutzer als Kriminelle (oder Spione oder Verräter) zu erkennen. Ein Tor-Benutzer kann ein Verbrecher sein, aber auch das Opfer eines Verbrechens, ein verdeckter Ermittler, ein Diplomat, ein Aktivist usw.

Hätte die US Navy (oder das FBI oder irgendeine andere Regierungsbehörde) bei der Entwicklung von Tor entscheiden, dass das Projekt geheim gehalten und nur für autorisierte Benutzer von staatlichen Stellen zugänglich sein soll, wäre es zur Wahrung der Anonymität so gut wie wirkungslos geworden. Es wäre nämlich genau umgekehrt gewesen: Jeder Gegner, der ein Netzwerk überwacht und dabei Tor-Datenverkehr entdeckt, hätte dann sicher sein können, dass die betreffenden Systeme zur US Navy (oder einer anderen staatlichen Organisation) gehören.

Es gibt auch keine zuverlässige Möglichkeit, zwischen »Guten« und »Bösen« zu unterscheiden, was den Einbau einer Hintertür problematisch macht. Wie soll man Schurken davon abhalten, diese Hintertür aufzuspüren und zu verwenden? Erschwerend kommt hinzu, dass sich die »Guten« durchaus von den »Bösen« hereinlegen, erpressen und umdrehen lassen. Darum gibt es keine Hintertür in Tor.

Die Vielseitigkeit der Benutzer, die sicher sein können, dass es keine Hintertür gibt, ist das, was Tor nützlich macht, denn dadurch können sich alle Benutzer umso erfolgreicher verstecken.

Werkzeuge für Tor: Verborgene Tor-Dienste
Ein Nebenprodukt der Tor-Netzwerkarchitektur ist die Möglichkeit, *verborgene Dienste* bereitzustellen, also Web- oder andere Netzwerkserver, die nur über das Tor-Netzwerk zugänglich sind und deren Standort nicht ermittelt werden kann.

Das funktioniert wie folgt: Einzelne Computer (Knoten) können anonym Verbindung zum Tor-Netzwerk aufnehmen und alles tun, was auch reguläre Internetknoten tun können. Gewöhnlich greifen sie dabei als Clients auf Web- oder andere Internetdienste zu. Ein Tor-Knoten kann aber auch als anonymer Server dienen. Sein Dienst ist dann für jeden zugänglich, der Tor verwendet, wobei der Server jedoch verborgen bleibt (ebenso wie ein Tor-Client).

Verborgene Dienste werden über sogenannte *Pseudo-URLs* angesprochen, die wie reguläre URLs aussehen, aber die Pseudo-Top-Level-Domäne *.onion* aufweisen. Eine typische Ressource eines verborgenen Tor-Dienstes sieht wie folgt aus:

```
http://idnxcnkne4qt76tg.onion/
```

Dies ist der Pseudo-URL der offiziellen Website des Tor-Projekts, zugänglich nur als verborgener Dienst über Tor.

1.7 Wie wird Tor verwendet?

Um das Anonymisierungsnetzwerk von Tor zu verwenden, nutzen die meisten das Tor-Browserpaket (Tor Browser Bundle, TBB). Das geht ganz einfach:

- Laden Sie die passende Version des TBB für Ihr Betriebssystem herunter (von *https://www.torproject.org/*) und überprüfen Sie den Download (siehe Anhang A).
- Entpacken Sie TBB. Für die meisten Benutzer bedeutet das einfach, auf die herunterladene Datei zu klicken, um sie zu öffnen.
- Führen Sie den Tor-Browser aus. Dazu ist es in den meisten Fällen nur erforderlich, auf das entsprechende Anwendungssymbol zu klicken.

Das TBB führt die gesamte Tor-Software aus, die erforderlich ist, um mit der anonymen Internetnutzung zu beginnen. Das schließt die Initialisierung der Tor-Verbindung, das Öffnen des Tor-Browsers und die Verwaltung der Tor-Verbindung über die Vidalia-Systemsteuerung ein. (Sollte Vidalia in Ihrem TBB nicht enthalten sein, können Sie es separat herunterladen.)

In einigen Teilen der Welt wird die Website von Tor blockiert. In Anhang B werden andere Möglichkeiten beschrieben, um an die Software zu kommen.

Wenn Sie Tails verwenden wollen, müssen Sie ein wenig anderes vorgehen:

- Laden Sie die Tails-Distribution herunter (*https://tails.boum.org*) und überprüfen Sie sie (siehe Anhang A).
- Brennen Sie die Tails-Distribution auf eine bootfähige DVD.
- Starten Sie Tails von der DVD.

Die Verwendung von Tails erfordert eingehendere technische Kenntnisse als TBB, da Sie die Distribution erst als bootfähiges Image auf eine DVD brennen müssen. Außerdem muss das System, auf dem Tails laufen soll, so eingerichtet werden, dass es von einer DVD starten kann.

Nachdem Sie Tails gestartet haben, müssen Sie noch die Netzwerkeinstellungen für die Verbindung mit dem Internet konfigurieren. Nachdem Sie das erledigt haben, startet Tails automatisch den Tor-geeigneten Browser, sodass Sie genauso wie bei der Verwendung von TBB mit dem anonymen Surfen beginnen können. Weitere Einzelheiten erfahren Sie in Kapitel 2.

1.7.1 Vorausplanen und Tor jetzt kennenlernen

Nach den oben genannten drei Schritten – Herunterladen, Entpacken und Ausführen – sollten die meisten Benutzer loslegen können. Wenn Sie wissen wollen, wie der Tor-Browser und Vidalia (die Tor-Systemsteuerung) aussehen oder wenn Sie verschiedene Websites ausprobieren oder Verbindung zu einem verborgenen Tor-Dienst aufnehmen möchten, brauchen Sie nicht mehr zu wissen.

Für die Bedrohungen, denen sich viele Benutzer ausgesetzt sehen, reicht das aus. Wenn Sie lediglich neugierige Nachbarn davon abhalten wollen, Ihre Websitzungen auszuspionieren, müssen Sie nicht mehr tun.

Es kann jedoch immer etwas schiefgehen, und es gibt zahllose Möglichkeiten, durch die Sie selbst bei der Verwendung von Tor Ihre IP-Adresse oder andere personenbezogene Daten unbeabsichtigt preisgeben können. Unter bedrohlicheren Umständen, in denen Ihr Gegner hervorragenden Zugriff auf Einzelsysteme und Netzwerke hat und eine erheblich stärkere Überwachung erfolgt, ist mit der wirkungsvollen Nutzung von Tor natürlich mehr verbunden.

Es ist sinnvoll, sich mit Tor vertraut zu machen, bevor Sie dringenden Bedarf dafür haben. Fehler, die Ihnen beim Ausprobieren unterlaufen, ziehen weniger starke Konsequenzen nach sich als solche, die Sie unter gefährlicheren Umständen machen. Lernen Sie den Umgang mit Tor jetzt, damit Sie keine dummen Anfängerfehler machen, wenn Sie es wirklich brauchen.

1.7.2 TBB oder Tails?

Die Software des Tor-Projekts wird in zwei Formen ausgeliefert: als ausführbare Datei, die unter dem Betriebssystem Ihrer Wahl läuft, und als Gesamtpaket, das die TBB-Clientsoftware in einer abgespeckten, »sauberen« Linux-Version namens Tails enthält (*https://tails.boum.org*).

Tails enthält fast alle TBB-Komponenten, die auch unter jeder anderen Linux-Distribution laufen. Wenn Sie es auf eine bootfähige DVD brennen (oder auf einen USB-Stick laden), können Sie Tails jedoch auf jeglichem System ausführen, das einen Start direkt von DVD oder einem USB-Laufwerk ermöglicht.

Zwischen den beiden Möglichkeiten (Ausführung unter Ihrem üblichen Betriebssystem oder mit einem eigenen Betriebssystem) bestehen die folgenden grundlegenden Unterschiede:

- TBB lässt sich auf Ihrem üblichen Betriebssystem bequemer und einfacher verwenden.
- Tails kann sicherer gemacht werden und läuft auf jedem Computer (der von DVD oder einem USB-Stick gestarten werden kann).

Zurzeit kann es noch schwierig oder gar unmöglich sein, Tails auf OS X-Systemen zu starten. Wenn Sie also einen Mac haben, müssen Sie TBB verwenden.

1.7.3 Tor Browser Bundle

Das TBB enthält alles, was Sie benötigen, um sich anonym im Internet zu bewegen: die Tor-Netzwerksoftware sowie den Tor-Webbrowser (eine modifizierte Version von Firefox). Es gibt TBB-Versionen für Windows, OS X und Linux.

Mit TBB können Sie Tor von Ihrem normalen Desktop-Computer ausführen und gleichzeitig einen Internetzugriff haben, der nicht über Tor geschützt wird. Das ermöglicht auch den Einsatz auf einem Computer, der für die normale Internetnutzung verwendet wird. Dies stellt normalerweise kein Problem dar, allerdings sollte der Benutzer Sicherheitshygiene und empfohlene Vorgehensweisen für die Sicherheit beachten.

1.7.4 Tails

Im Gegensatz zu TBB handelt es sich bei Tails um ein komplettes Sicherheits-Betriebssystem (auf der Grundlage von Debian Linux), das von einer DVD oder einem USB-Stick gestartet wird. Dadurch können Sie Tor auf Computern in Internetcafés, geliehenen Computern und solchen ausführen, die auf der Ebene des Betriebssystems geknackt wurden (z. B. durch die Installation von Keyloggern unter Windows).

Bei korrekter Authentifizierung können sich die Benutzer sicher sein, dass das Betriebssystem keine beabsichtigten Hintertüren enthält, keine privaten Informationen aufzeichnet und anderen Websites nicht erlaubt, persönliche Daten zu lesen oder zu schreiben.

Tails ist mit Tor verzahnt und startet automatisch den Webbrowser Iceweasel und Tor (nachdem einmalig die Netzwerkverbindung konfiguriert wurde).

1.7.5 Vertrauen ist gut ...

Wenn Sie Tor oder irgendeine andere Sicherheitssoftware verwenden, müssen Sie ihr vertrauen können. Sind Sie zu dem Schluss gekommen, dass das Tor-Projekt eine renommierte und vertrauenswürdige Gruppe ist, dann können Sie auch der Software vertrauen. Gut und schön – aber wie können Sie sicher sein, dass die von Ihnen heruntergeladene Software auch wirklich diejenige ist, die die Mitarbeiter des Tor-Projekts veröffentlicht haben?

Eine vertrauensstärkende Maßnahme besteht darin, Tor direkt von der Website des Tor-Projekts herunterzuladen (oder von einem zuverlässigen Mirror). Die Projektwebsite verwendet HTTPS, weshalb es sinnvoll ist, den URL in der Adressleiste zu prüfen: Das Symbol mit dem Sicherheitsschloss muss geschlossen sein. Das ist ein gutes Indiz dafür, dass die Website nicht gehackt wurde und Sie die richtige Website erreicht haben.

Die beste Möglichkeit, sicherzustellen, dass die heruntergeladene Software tatsächlich diejenige ist, die vom Tor-Projekt angeboten wird, bietet die digitale Signatur, die alle Tor-Softwaredownloads aufweisen (sowohl TBB als auch Tails). Diese Signaturen werden auf derselben Seite veröffentlicht, auf der Sie auch die Downloads finden.

Um die Echtheit der heruntergeladenen Tor-Software zu prüfen, müssen Sie auch die Signaturdatei herunterladen und mit einer OpenPGP-kompatiblen Software validieren (siehe *http://www.openpgp.org/*), nachdem Sie die entsprechenden Signierschlüssel von einem PGP-Schlüsselserver importiert haben.

Die Signierschlüssel des Tor-Projekts sind auf der Projektwebsite erhältlich (*https://www.torproject.org/docs/signing-keys.html*). Dort finden Sie auch Anleitungen zur Validierung von Downloads (*https://www.torproject.org/docs/verifying-signatures.html.en*). Die Schlüssel und die Anleitungen stehen auch in Anhang A.

Wozu all dieser zusätzliche Aufwand? Eine Möglichkeit, Tor auszuhebeln, besteht darin, die Benutzer dazu zu verleiten, statt der echten eine gehackte Version der Tor-Software herunterzuladen. Eine solche Version erweckt den Anschein, wie beabsichtigt zu funktionieren, kann aber in Wirklichkeit Tor-Netzwerkakvititäten direkt an den Gegner melden. Das lässt sich mit einem *Man-in-the-middle-Angriff* bewerkstelligen, bei dem die Anforderung zum Herunterladen der Software abgefangen und stattdessen der gehackte Code zurückgegeben wird, anstatt die Lieferung der richtigen Software durch die Projektwebsite von Tor zu gestatten.

1.8 Sichere Verwendung von Tor

Es ist eine gute Idee, sich die Warnungen des Tor-Projekts zur sicheren Verwendung von Tor anzusehen (*https://www.torproject.org/download/download.html.en#warning*). Eine Zusammenfassung dieser Vorsichtsmaßnahmen finden Sie im Folgenden.

1.8.1 Verwenden Sie den Tor-Browser

Nehmen Sie keinen anderen Browser. Wenn Browserfunktionen hinzukommen oder geändert werden, können mehr Informationen über Sie preisgegeben werden, als Ihnen lieb ist. Anstatt alle Browser für Tor sicher zu gestalten, haben sich die Mitarbeiter des Tor-Projekts darauf konzentriert, den Tor-Browser so sicher wie möglich zu machen.

1.8.2 Öffnen Sie keine Dokumente

Öffnen Sie auf einem Computer, der mit dem Internet verbunden ist, keine Dokumente, die Sie über Tor heruntergeladen haben. Das ist sehr wichtig, gilt aber nur für die Verwendung von TBB. Unter Tails ist es ungefährlich, Dateien zu öffnen. Dokumentdateien wie *.doc*- und *.pdf*-Dateien können Probleme verursachen, wenn sie von einer Anwendung geöffnet werden, die »offen« arbeitet. Falls ein solches Dokument einen Weblink enthält, so wird der Webinhalt beim Öffnen der Datei (automatisch) heruntergeladen. Allerdings wird der Link dabei von der Anwendung geöffnet und nicht vom Tor-Browser! Das ist schlecht, denn dadurch erfährt der Besitzer des Links Ihre IP-Adresse. Und was noch schlimmer ist: Ein Gegner kann den URL in dem Dokument beim Herunterladen der Datei mit Ihrer Verbindung verknüpft haben. Damit werden Sie dann definitiv mit der nicht mehr anonymen Sitzung assoziiert, was Ihren Versuch, anonym zu bleiben, unterläuft.

1.8.3 Installieren und aktivieren Sie keine Browser-Plug-Ins

Gegner können manche Plug-Ins (z. B. Flash, RealPlayer oder Quicktime) dazu nutzen, ein System zu zwingen, seine IP-Adresse preiszugeben, was die Anonymität aufhebt. Andere Plug-Ins können Schwachstellen oder sogar Malware enthalten, weshalb es am besten ist, ganz darauf zu verzichten.

1.8.4 Vermeiden Sie Websites ohne HTTPS

Selbst mit HTTPS Everywhere (das in TBB enthalten ist) wird Ihre Sitzung im Klartext zum Tor-Austrittsknoten übertragen, wenn Sie eine HTTP-Website besuchen.

1.8.5 Verwenden Sie Bridges und suchen Sie Gesellschaft

Dies ist eher als Vorschlag gedacht, aber er ist nützlich, wenn Sie mehr Sicherheit brauchen. Da der Tor-Netzwerkverkehr auffällig ist und durch Netzwerküberwachungssoftware festgestellt werden kann, reicht die hier beschriebene grundlegende Tor-Einrichtung möglicherweise nicht aus, denn dabei können Sie als Benutzer des Tor-Netzwerks erkannt werden. Wo Tor legal ist, mag das keine Rolle spielen, aber in anderen Ländern kann das ein echtes Problem sein. Tor-Bridge-Relays sind besondere Relays, die nicht öffentlich aufgeführt und nicht leicht zu entdecken sind. Wenn staatliche Firewalls den Zugang zu den Tor-Eintrittsknoten aktiv blockieren, sind Bridges unverzichtbar.

Der Vorschlag, sich »Gesellschaft zu suchen«, bedeutet, Tor zusammen mit vielen anderen Tor-Benutzern zu verwenden, die unterschiedliche Interessen verfolgen, um Tor auf diese Weise »legitimer« zu machen, da es von vielen verschiedenen Arten von Menschen genutzt wird.

2

Das Tor Browser Bundle

Das Tor Browser Bundle (TBB) ist die Softwaresuite, mit der Sie Tor unter einem Desktop-Betriebssystem (Windows, OS X oder Linux) ausführen. Dazu müssen Sie die komprimierte Anwendung nach dem Herunterladen entpacken. Klicken Sie dann auf das Symbol für den Tor-Browser, um eine anonyme Internetsitzung zu öffnen.

2.1 Der Inhalt des TBB

Die drei Hauptbestandteile des TBB sind Tor, Vidalia und der Tor-Browser. Darüber hinaus enthält es einige zusätzliche Hilfsprogramme. In diesem Abschnitt werden die einzelnen Komponenten beschrieben.

Das TBB ist ein *Paket*, und die Software Torbutton ist als eigenständiges Programm darin enthalten, was historische Gründe hat: Früher musste man verschiedene Komponenten der Tor-Software herunterladen und

dann zusammen benutzen. Torbutton war ursprünglich nur dazu da, dem Benutzer eine einfache Schaltfläche zur Verfügung zu stellen, über die er Tor im Browser ein- und ausschalten konnte.

Tor funktioniert heutzutage aber anders. Torbutton sollten Sie möglichst gar nicht mehr für sich allein verwenden, auch wenn es immer noch als eigenständiges Programm im TBB enthalten ist.

2.1.1 Vidalia

Vidalia ist die Systemsteuerung von Tor. Sie stellt Steuer- und Konfigurationselemente zur Verfügung und bietet darüber hinaus Elemente wie eine Netzwerkkarte, die zeigt, welche Knoten sich im Tor-Netzwerk befinden und durch welche Länder die Tor-Verbindungen verlaufen, Diagramme der Netzwerknutzung, das Logbuch mit den Tor-Meldungen usw.

Sie können Tor auch nutzen, ohne jemals auf Vidalia zurückzugreifen, allerdings bietet diese Systemsteuerung manchmal die beste Möglichkeit, die Tor-Konfiguration zu ändern, um Ihren eigenen Knoten als Relay oder Bridge für andere Tor-Benutzer einzurichten oder einen verborgenen Tor-Dienst zu erstellen. Vidalia kann auch für Netzwerk- und für erweiterte Konfigurationsfunktionen wie die folgenden genutzt werden:

- Einrichten von Tor als Proxydienst. Manche Benutzer müssen Tor als Proxydienst einrichten, weil die Organisation, die den Netzwerkzugriff anbietet, einen Proxy erfordert, oder weil der Benutzer Beschränkungen beim externen Netzwerkzugriff überwinden muss. Tor kann so eingerichtet werden, dass es den Proxydienst vom Endbenutzer unbemerkt nutzt.
- Überwinden von Firewalls. Firewalls können den Netzwerkdatenverkehr auf der Grundlage des verwendeten *Ports* filtern, der angibt, welche Art von Netzwerkdienst verwendet wird. Webdatenverkehr wird gewöhnlich über die Ports 80, 443 oder 8080 abgespult. Tor lässt sich so einrichten, dass es diese Ports nutzt, um die Firewall zu überwinden.

Wenn Sie Tor starten, wird ein Vidalia-Fenster geöffnet, in dem Sie Tor einrichten, die laufende Tor-Sitzung steuern und auf grafische Darstellungen von Daten rund um Tor sowie auf das Tor-Logbuch zugreifen können (siehe Abbildung 2.1).

Sollte Vidalia in Ihrem TBB nicht mehr enthalten sein, können Sie es zusätzlich von einschlägigen Downloadseiten (z. B. Chip oder Computer-BILD) herunterladen.

Abbildung 2.1: Vidalia enthält eine Statuskonsole und Verknüpfungen zu Tor-Funktionen und Konfigurationseinstellungen.

Mehr über Tor: Die Zukunft von Vidalia
Vidalia wird zurzeit hauptsächlich im TBB verwendet (Tails enthält eine Version mit weniger Möglichkeiten), aber für die Zukunft des Tor-Projekts wird Vidalia als Sackgasse betrachtet. In Zukunft werden die meisten der von Vidalia übernommenen Funktionen zu anderen Bestandteilen des Pakets verlegt. Dazu wird Stem verwendet (*https://stem.torproject.org/*), ein Werkzeug zur Programmierung von Tor in Python.

2.1.2 Tor

Tor ist die Kernkomponente, die sich um die Tor-Netzwerkkommunikation kümmert. Das schließt die Abfrage des Tor-Netzwerks nach Informationen über Tor-Relays, die Wahl des Eintritts-, des Transit- und des Austrittsknotens, die Einrichtung der Tor-Verbindung und alle anderen Netzwerkaspekte von Tor ein. Diese Aufgaben werden aber gewöhnlich alle für den Benutzer unsichtbar erledigt.

Die Softwarekomponente Tor handhabt die Tor-Netzwerkkommunikation auf die gleiche Weise, wie sich die Netzwerksoftware auf Windows-, OS X- oder Linux-Systemen um Internetverbindungen mit Remotesystemen kümmert.

2.1.3 Mozilla Firefox ESR und Torbutton

Der Tor-Browser ist eine Firefox-Version namens Mozilla Firefox ESR (siehe *http://www.mozilla.org/en-US/firefox/organizations/*), ein beständigeres Release des Browsers für Gruppen oder Organisationen, die weniger häufige Aktualisierungen und dafür eine größere Stabilität benötigen (siehe Abbildung 2.2). (ESR steht für »Extended Support Release«, also »Release mit erweiterter Unterstützung«.)

Der Tor-Browser ist so eingerichtet, dass er eine Seite des Tor-Projekts öffnet (nämlich *https://check.torproject.org*), die die von Ihnen gesendeten Pakete untersucht und damit prüft, ob Ihr System korrekt an das Tor-Netzwerk angeschlossen ist. Angezeigt werden dann das Ergebnis und die IP-Adresse, die Sie scheinbar benutzen. Wenn Sie Tor korrekt eingerichtet haben, sehen Sie wie in Abbildung 2.2 den grünen Schriftzug: »Herzlichen Glückwunsch. Ihr Browser benutzt jetzt Tor.« Anderenfalls wird eine rote Fehlermeldung angezeigt (»Sie benutzen nicht Tor«).

Wie Sie in Abbildung 2.2 sehen, gibt die Seite *check.torproject.org* auch die IP-Adresse an, über die Sie scheinbar Verbindung aufnehmen. Die Prüfseite

untersucht, ob die Verbindung über Tor erfolgt, indem sie diese IP-Adresse mit der Liste aller gültigen Tor-Austrittsknoten vergleicht. Eine Übereinstimmung bedeutet, dass tatsächlich eine Tor-Verbindung vorliegt.

Innerhalb des Tor-Projekts gibt es das eigenständige Programm Torbutton (siehe *https://www.torproject.org/torbutton/*), das ursprünglich eine Schaltfläche zu einem normalen Webbrowser hinzufügte, über die Tor ein- und ausgeschaltet werden konnte. Der gesamte Funktionsumfang von Torbutton ist im aktuellen TBB enthalten, nur ist diese Schaltfläche nicht mehr vorhanden.

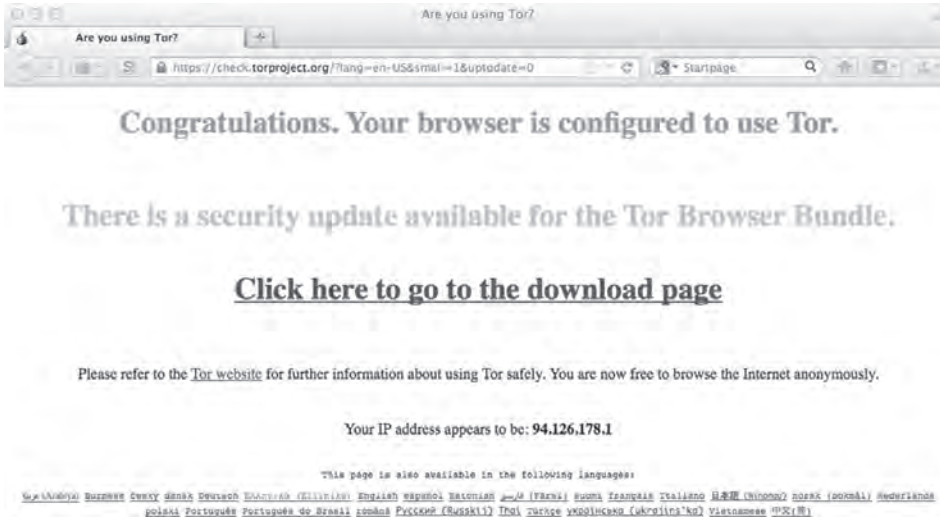

Abbildung 2.2: Die Startseite des Tor-Browsers informiert Sie über den Zustand Ihrer Tor-Netzwerkverbindung. Die hier gezeigte Meldung weist Sie auf eine gute Tor-Verbindung hin, allerdings sehen Sie auch (in der zweiten Zeile) den Warnhinweis, dass eine Aktualisierung des TBB vorhanden ist (und heruntergeladen werden sollte).

Torbutton ist zwar ein separates Programm, es ist aber im TBB enthalten. Allerdings wird den meisten Benutzern davon abgeraten, Torbutton getrennt vom Browser einzusetzen. Die Funktionen von Torbutton werden jetzt über Vidalia oder die Tor-Konfigurationsdatei verwaltet.

Wenn Sie den Tor-Browser starten, wird in der Standardkonfiguration alles eingeschaltet, was zur Nutzung von Tor erforderlich ist. Damit entfällt die Notwendigkeit für eine Schaltfläche zur Aktivierung und Deaktivierung.

2.1.4 Weitere Inhalte

Das TBB enthält besondere Firefox-Patches (siehe *https://www.torproject.org/projects/torbrowser/design/#firefox-patches*), um »Datenschutz und Sicherheit zu verbessern«. Außerdem gehören zu dem Paket zusätzliche Hilfsprogramme, mit denen Sie Daten von der dauerhaften Speicherung ausnehmen und festlegen können, welche Informationen über das Netzwerk externen Systemen zur Verfügung gestellt werden (siehe *https://www.torproject.org/projects/torbrowser/design/#components*).

Zu den weiteren Bestandteilen des Pakets gehören:

- HTTPS Everywhere (*https://www.eff.org/https-everywhere*). Diese bereits in Kapitel 1 erwähnte Komponente dient zum sicheren Surfen, indem sie die Websitzungen zwischen Client und Remoteserver verschlüsselt. Dadurch werden die Daten geschützt, die ansonsten vor dem Eintreffen am Tor-Eintrittsknoten und dem Absenden vom Tor-Austrittsknoten zum Zielserver im Klartext übermittelt würden.
- NoScript (*http://noscript.net*). Dieses Browser-Plug-In verhindert die Ausführung von nicht vertrauenswürdigen Skripten und Programmen, mit denen Gegner die Browser manipulieren und dazu bringen könnten, etwas über ihre Benutzer zu verraten.

2.2 Das TBB verwenden

Wenn Sie Tor zum ersten Mal verwenden, fällt Ihnen vielleicht auf, dass es langsam zu sein scheint. Das liegt an dem Zusatzaufwand durch die drei hinzugekommen Hops für jede Richtung. Außerdem wird die Leistung dadurch gesenkt, dass die Daten verschlüsselt und an jedem Tor-Knoten entschlüsselt werden müssen. Ein weiterer Faktor ist die Tatsache, dass die gesamte verfügbare Bandbreite für den Zugang zum Tor-Netzwerk begrenzt ist. In Zeiten großer Nachfrage müssen Sie diese Bandbreite möglicherweise mit vielen anderen Benutzern teilen.

Ob Sie nun Tails oder das TBB einsetzen, die Verwendung von Tor, Vidalia und des Tor-Browsers erfolgt in den Grundzügen sehr ähnlich – allerdings nicht völlig gleich.

Ein Unterschied tritt auf, wenn Sie Tails auf einem System in einem Netzwerk verwenden, das eine Authentifizierung erfordert (z. B. in einem WLAN, für das ein Passwort erforderlich ist). Da Tails nicht für das System und dessen Netzwerkverbindung eingerichtet ist, müssen Sie das manuell erledigen, insbesondere wenn ein Passwort benötigt wird. (Es ist auch möglich, die Tails-Konfiguration zu speichern, wenn Tails von einem USB-Laufwerk gestartet wird. Mehr darüber erfahren Sie in Kapitel 3 in dem-Abschnitt über *Datenpersistenz*.)

Ist das Tails-System mit einem verkabelten Netzwerk verbunden, für das keine Authentifizierung erforderlich ist, sollte es korrekt im Netzwerk hochgefahren werden und sich mit Tor verbinden.

Ein weiterer Unterschied zwischen dem TBB und Tails besteht darin, dass die Firefox-Version in Tails die Bezeichnung Iceweasel trägt. Allerdings gibt es keinen Funktionsunterschied zwischen den beiden Browsern. Wenn Sie sich im Hilfemenü den Punkt *Über Iceweasel* ansehen, finden Sie den Hinweis »designed by Mozilla«. Folgen Sie dem dort angegebenen Link, um weitere Informationen zu erhalten.

2.2.1 Erste Schritte

Das TBB können Sie auf Ihrer Festplatte installieren, aber das bedeutet, dass Sie das Programm und seine Konfigurationsdateien auf dem Clientsystem speichern. Viele Benutzer bevorzugen es dagegen, die Tor-Software auf einem Wechsellaufwerk vorzuhalten.

Nachdem Sie die für Ihr Betriebssystem geeignete Version heruntergeladen (und anschließend die digitale Signatur überprüft) haben, entpacken Sie die Software auf dem Speichergerät Ihrer Wahl.

Am einfachsten ist es, Tor direkt im Downloadordner auszupacken. Sie können aber auch ein anderes Verzeichnis oder ein Wechselmedium (wie einen USB-Stick, eine DVD oder eine Speicherkarte) angeben.

Tor von einem Wechselmedium aus zu verwenden macht es einfacher, die Nutzung zu leugnen. Haben Sie Tor auf Ihrem Computer installiert, ist das ein Indiz dafür, dass Sie es auch benutzen, was an manchen Orten schon als Schuldbeweis gilt. Wenn Sie Tor dagegen auf einem Wechselmedium unterbringen, können Sie es verstecken oder zerstören.

2.2.2 Das TBB starten: Windows

Der Windows-Download des TBB ist eine selbstentpackende ausführbare Datei. Wenn Sie darauf doppelklicken, werden alle TBB-Dateien in den Ordner *Tor Browser* entpackt. Um Tor zu starten, öffnen Sie diesen Ordner und doppelklicken auf die Datei *Start Tor Browser*. (Es kann sein, dass diese Datei als *Start Tor Browser.exe* angezeigt wird.) Daraufhin wird Vidalia und anschließend der Tor-Browser geöffnet.

Der Tor-Browser ruft die Seite *check.torproject.org* auf (siehe Abbildung 2.2) und sollte die Glückwunschmeldung und die IP-Adresse anzeigen, von der Ihre Tor-Verbindung auszugehen scheint (sowie ggf. andere wichtige Meldungen).

2.2.3 Das TBB starten: Mac OS X

Der Mac OS X-Download des TBB ist eine Zip-Datei. Wenn Sie darauf doppelklicken, werden die Tor-Programme in einen OX X-Programmordner mit einem Namen wie *TorBrowser_de.app* entpackt.

Je nachdem, welche Sprachversion von Tor Sie ausgewählt haben, sieht dieser Name anders aus. Klicken Sie nun auf das Symbol *TorBrowser*. Daraufhin wird Vidalia und anschließend der Tor-Browser geöffnet.

Der Tor-Browser ruft die Seite *check.torproject.org* auf (siehe Abbildung 2.2) und sollte die Glückwunschmeldung und die IP-Adresse anzeigen, von der Ihre Tor-Verbindung auszugehen scheint (sowie ggf. andere wichtige Meldungen).

2.2.4 Das TBB starten: Linux

Die folgenden Anleitungen gelten für Linux, Unix und BSD-Versionen.

Der Linux-Download des TBB ist eine *tar/gz*-Datei. In einer benutzerfreundlichen Linux-Version wie Ubuntu doppelklicken Sie auf die komprimierte Datei, um den Archivmanager zu öffnen, der komprimierte Dateien entpackt.

Nach dem Entpacken (entweder über die GUI oder über die Kommandozeile) doppelklicken Sie auf das Symbol *start-tor-browser*, um Tor auszuführen. Wenn die Software korrekt installiert wurde, sehen Sie eine Eingabeaufforderung, in der Sie auswählen können, ob der Dateiinhalt angezeigt oder die Datei ausgeführt werden soll. Klicken Sie auf *Run/Ausführen*, um Tor zu starten.

Weitere Einzelheiten über die Installation finden Sie in den folgenden Abschnitten.

Mehr über Tor: Verwenden Sie für Linux formatierte Medien!
Wenn Sie Schwierigkeiten haben, Tor auf einem Linux-System von einem USB-Laufwerk ans Laufen zu bekommen, kann das daran liegen, dass Linux nicht korrekt auf dieses Laufwerk zugreifen kann.

Wenn Sie eine Programmdatei von dem Wechselmedium aus ausführen wollen, auf dem Sie das TBB installiert haben, dann muss dieses Medium zur Verwendung durch Linux formatiert sein. Bei der Formatierung für ein anderes Betriebssystem kann es Probleme geben.

Um herauszufinden, ob Tor ausführbar ist, prüfen Sie die ersten zehn Zeichen für jeden Eintrag im Verzeichnislisting. Der erste Buchstabe ist `d` und bedeutet, dass es sich bei dem Eintrag um ein Verzeichnis (*directory*) handelt. Ein `x` bedeutet, dass das Element ausführbar (*eXecutable*) ist. Hat das Medium kein für Linux geeignetes Format, so wird in dem Listing kein `x` angezeigt, und Sie sind nicht in der Lage, Tor auszuführen.

Bei korrekter Installation sieht das Listing des Tor-Verzeichnisses in etwa wie folgt aus (beachten Sie das `x` für den Eintrag der Datei `start-tor-browser`):

```
$ ls -l
total 28
drwxr-xr-x 3 peter peter 4096 Apr 1 21:25 App
drwxr-xr-x 5 peter peter 4096 Apr 1 21:25 Data
drwxr-xr-x 5 peter peter 4096 Apr 1 21:25 Docs
drwxr-xr-x 3 peter peter 4096 Apr 1 21:25 Lib
-rwxr-xr-x 1 peter peter 7325 Apr 1 21:25 start-tor-browser
drwxr-xr-x 2 peter peter 4096 Apr 1 21:25 tmp
```

2.2.5 Installation auf Ubuntu: GUI

Kopieren oder verschieben Sie die TBB-Downloaddatei zum gewünschten Speicherort (also entweder zu einem Verzeichnis/Ordner auf dem Benutzer-Desktop, auf ein Wechsellaufwerk oder ein anderes Speichergerät).

Doppelklicken Sie auf die heruntergeladene Datei. Daraufhin wird ein Archivmanager-Fenster geöffnet. Klicken Sie auf die Schaltfläche zum Entpacken. Daraufhin wird das TBB im gewünschten Verzeichnis oder Gerät entpackt.

2.2.6 Installation auf Ubuntu: Kommandozeile

Wenn Sie Tor von einem Wechselmedium aus verwenden möchten, müssen Sie als Erstes die heruntergeladene komprimierte Datei auf dieses Gerät kopieren. (Das können Sie auch mit einem grafischen Dateimanager erledigen.) Schalten Sie dann zur Linux-Kommandozeile um, indem Sie das Programm Terminal öffnen.

Hier müssen Sie als Erstes das Verzeichnis wechseln, um zu dem gewünschten Wechselmedium zu gelangen. In Ubuntu werden Wechselmedien im Verzeichnis `/media` aufgeführt. (In anderen Linux-Distributionen kann es andere Verzeichnisse oder eine andere Benennung geben.) Wechseln Sie daher zu diesem Verzeichnis:

```
$ cd /media
```

Sehen Sie sich nun das Listing für das Verzeichnis `/media` an:

```
$ ls -l
total 36
drwx------ 12 peter peter 16384 Dec 31 1969 1E2C-46A0
drwx------  5 peter peter 4096  Apr 30 10:54 USB20FD
```

Um das TBB beispielsweise auf dem USB-Stick namens USB20FD zu speichern, wechseln Sie wie folgt dorthin:

```
$ cd USB20FD
```

Rufen Sie dann erneut ein Verzeichnislisting auf. Wenn Sie die komprimierte TBB-Datei bereits dorthin kopiert haben, erhalten Sie dabei folgende Ausgabe:

```
$ ls -l
total 42876
-rw-r--r-- 1 peter peter  1303378 Feb 21 17:31 checkin.pdf
-rw-r--r-- 1 peter peter  2607996 Jan 18 22:38 IMG_0536.JPG
-rw-r--r-- 1 peter peter  3152669 Jan 18 22:38 IMG_0537.JPG
-rw-r--r-- 1 peter peter 36834876 Apr 29 14:43 tor-browsergnu-
linux-i686-2.3.25-6-dev-de.tar.gz
$
```

Geben Sie nun den folgenden Befehl ein, um das TBB zu entpacken:

```
$ tar -xvzf tor-browser-gnu-linux-i686-2.3.25-6-dev-de.tar.gz
```

Daraufhin sehen Sie, wie die einzelnen Dateien entpackt werden. Anschließend kehren Sie wieder zur Eingabeaufforderung `$` zurück.

Befehle für Dateien können von Linux automatisch vervollständigt werden, sodass Sie nicht den gesamten Dateinamen eingeben müssen, sondern nur so viel, um die Datei im aktuellen Verzeichnis eindeutig zu bezeichnen. Anschließend können Sie einfach Tab drücken.

Prüfen Sie erneut das Verzeichnislisting:

```
$ ls -l
total 42880
-rw-r--r-- 1 peter peter  1303378 Feb 21 17:31 checkin.pdf
-rw-r--r-- 1 peter peter  2607996 Jan 18 22:38 IMG_0536.JPG
-rw-r--r-- 1 peter peter  3152669 Jan 18 22:38 IMG_0537.JPG
drwx------ 7 peter peter     4096 Apr  1 21:25 tor-browser_de
-rw-r--r-- 1 peter peter 36834876 Apr 29 14:43 tor-browser-
gnulinux-
i686-2.3.25-6-dev-de.tar.gz
```

Ein neues Verzeichnis namens `tor-browser_de-DE` erscheint. (Der genaue Name hängt von der gewählten Sprachversion ab.) Wechseln Sie dorthin:

```
$ cd tor-browser_de
```

Listen Sie die Dateien in diesem Verzeichnis auf:

```
$ ls -l
total 28
drwxr-xr-x 3 peter peter 4096 Apr 1 21:25 App
drwxr-xr-x 5 peter peter 4096 Apr 1 21:25 Data
drwxr-xr-x 5 peter peter 4096 Apr 1 21:25 Docs
drwxr-xr-x 3 peter peter 4096 Apr 1 21:25 Lib
-rwxr-xr-x 1 peter peter 7325 Apr 1 21:25 start-tor-browser
drwxr-xr-x 2 peter peter 4096 Apr 1 21:25 tmp
```

Die Datei *start-tor-browser* startet den Tor-Browser, wenn Sie sie wie folgt an der Kommandozeile ausführen:

```
$ ./start-tor-browser
```

2.2.7 Vidalia

Vidalia ist die Systemsteuerung von Tor. Sie stellt Werkzeuge zur Verfügung, mit denen die Benutzer ihre Tor-Sitzungen verwalten und sich ansehen können, wie Tor funktioniert. Wenn Sie ein Tor-Relay einrichten oder einen verborgenen Tor-Dienst hinzufügen möchten, können Sie das über Vidalia erledigen.

Mehr über Tor: Tails, Vidalia und dauerhafte Konfiguration
Die in Tails enthaltene Version von Vidalia hat weniger Optionen als die Version im TBB, da sich viele der Einstellungsmöglichkeiten in Vidalia auf die Einrichtung eines Computers als Tor-Relay oder als verborgener Tor-Server beziehen.

Tails ist dagegen für Endbenutzer gedacht, die Anonymität suchen und eine Möglichkeit brauchen, ein System zu starten, ohne Spuren zu hinterlassen. Tails kann zwar auch als Relay und als verborgener Dienst laufen, doch dazu sind Persistenz der Daten (siehe Kapitel 3) und eine Bearbeitung der Tor-Konfigurationsdatei erforderlich. Nur erfahrene Benutzer sollten versuchen, Tails auf diese Weise einzusetzen.

Um ein Tor-Relay oder einen verborgenen Server von einer bootfähigen Linux-Distribution (z. B. Linus) auf einem Wechselmedium aus zu betreiben, fahren Sie zunächst Linux hoch und starten dann den Tor-Browser von einem USB-Laufwerk (oder einer CD/DVD). Das Relay bzw. den verborgenen Dienst können Sie dann mit der TBB-Version von Vidalia konfigurieren.

In Abbildung 2.1 sehen Sie die grundlegende Oberfläche von Vidalia. Der Statusbereich zeigt an, ob Tor läuft oder nicht. Wenn Sie Tor starten, wird hier ein Fortschrittsbalken eingeblendet. Ist die Tor-Software auf dem neuesten Stand und die Verbindung in Ordnung, wird im Statusbereich eine grüne Zwiebel angezeigt. Umstände, die die Verwendung von Tor weniger sicher machen, werden entsprechend anhand einer »Warnskala« in Gelb und Rot farbig markiert.

2.2.8 Schnellzugriff

In diesem Bereich sind die Tor-Verknüpfungen angeordnet. *Hilfe*, *Über* und *Beenden* erklären sich von selbst. In Tails sind *Beenden* und *Tor stoppen* nicht verfügbar, da es unter Tails keine andere nutzbare Netzwerkverbindung gibt, sodass es nicht sinnvoll wäre, eine Option bereitzustellen, um die Tor-Anbindung ausdrücklich zu beenden.

Das Hilfesystem von Vidalia ist tatsächlich ziemlich hilfreich. In vielen Fällen geht es darüber hinaus, Ihnen einfach nur zu sagen, was Sie tun sollen, und erklärt außerdem, warum Sie es tun sollten oder müssen.

Was in der Tails-Version von Vidalia außerdem fehlt, sind die Verknüpfungen, um ein Tor-Relay einzurichten (*Weiterleitung einrichten*) und auf die Tor-Einstellungen zuzugreifen. Wie bereits erwähnt, ist Tails nicht zur Verwendung als Relay oder verborgener Server gedacht, sondern als mobile Möglichkeit für den anonymen Internetzugriff. Eine Änderung der Einstellungen ist möglich, allerdings sollten Sie das nur tun, wenn Sie sich damit genau auskennen. Wenn das Tails-Medium nicht beschreibbar ist (z. B. eine DVD-R), können Änderungen an der Konfiguration ohnehin nicht für die nächste Sitzung gespeichert werden.

Wenn Sie die Tor-Konfiguration bearbeiten müssen (in der Datei *torrc*), lesen Sie die Beschreibung im Artikel »Editing torrc from GUI« (*https://tails.boum.org/forum/Editing_torrc_from_GUI/*).

2.2.9 Logbuch

Wenn Sie die Tor-Konfiguration mit Vidalia (oder manuell) ändern wollen oder festlegen möchten, wie die aktuelle Verbindung ausgeführt werden soll, müssen Sie Ihre Maßnahmen mit dem Vidalia-Logbuch überprüfen.

Steuerschaltflächen für das Logbuch finden Sie am oberen Rand des Fensters. Sie können auswählen, ob Sie das Protokoll im einfachen oder im erweiterten Modus anzeigen lassen wollen.

Im einfachen Modus erhalten Sie einen Überblick über das, was gerade geschieht. Dazu werden Meldungen wie die folgende ausgegeben (sie zeigt den Status beim Start von Tor an):

```
The Tor Software is Running
You are currently running version „0.2.3.25
(git-17c24b3118224d65)“ of the Tor software.
```

Im erweiterten Modus erhalten Sie viel mehr Meldungen mit mehr Einzelheiten. Für die oben gezeigte Aktion – die Verbindung mit Tor – liefert der erweiterte Modus viel mehr Informationen, wie Sie in Abbildung 2.3 sehen.

Sie können auch die Einstellungen für das Logbuch ändern, um festzulegen, wie es gehandhabt wird, wo es gespeichert werden soll usw.

Bei der Betrachtung des Logbuchs in Vidalia ist nicht immer der gesamte Text einer Meldung sichtbar. Es kann daher bequemer ein, die Meldungen zu speichern oder zu kopieren und sie sich in einem Texteditor anzusehen.

2.2.10 Tor starten/stoppen

Diese Schaltfläche macht genau das, was die Beschriftung besagt: Wenn Tor läuft, heißt sie *Tor stoppen*, und ein Klick darauf beendet die Tor-Netzwerksoftware. Anderenfalls lautet die Bezeichnung der Schaltfläche *Tor starten*. Wenn Sie darauf klicken, starten Sie die Tor-Software und stellen die Tor-Anbindung wieder her.

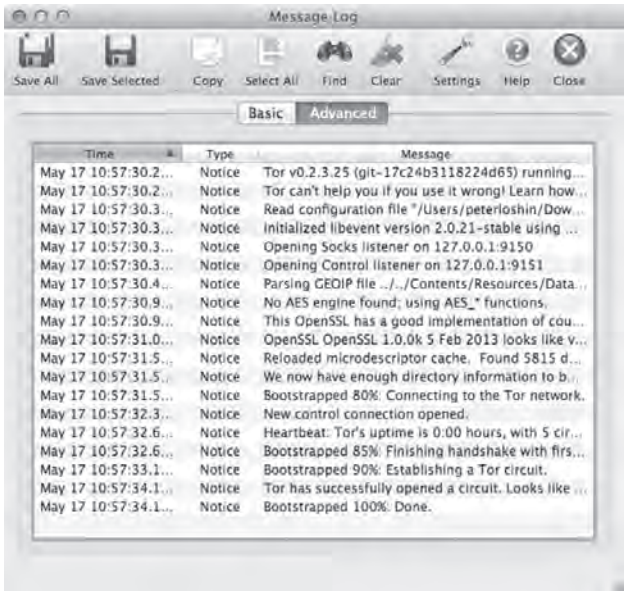

Abbildung 2.3: Erweiterte Ansicht des Tor-Logbuchs. Die Inhalte können durchsucht, gespeichert und kopiert werden.

Das können Sie in Abbildung 2.1 erkennen, wo als Status »Verbindung zum Tor-Netzwerk hergestellt!« angezeigt wird. Die erste Verknüpfung im Schnellzugriffsbereich ist mit »Tor stoppen« beschriftet.

2.2.11 Weiterleitung einrichten

Wenn Sie Tor starten, läuft es in der Standardeinstellung als Tor-Client. Das bedeutet, dass Sie damit über das Tor-Netzwerk Verbindung mit dem weltweiten (unzensierten) Internet und mit verborgenen Diensten aufnehmen können. Ihr System nutzt Tor dann für den vorgesehenen Zweck, nämlich um Filter, Überwachungseinrichtungen und Zensurmaßnahmen zu umgehen.

Die Nutzung von Tor auf diese Weise verbraucht Tor-Netzwerkressourcen, insbesondere Eintritts- und Austrittsknoten (da diese höhere Ansprüche an ihre Besitzer stellen). Je mehr Tor-Clients das Netzwerk nutzen, umso höher wird der Bedarf an Infrastruktur. Ein Großteil der Infrastruktur für das Tor-Netzwerk wird freiwillig von Benutzern bereitgestellt, die ein bisschen Bandbreite übrig haben und helfen möchten.

Wenn Sie anderen helfen wollen, die Tor verwenden möchten oder müssen, können Sie das zurzeit dadurch tun, dass Sie Ihr System auf drei verschiedene Weisen einrichten, um damit die Tor-Netzwerkinfrastruktur zu erweitern:

- als Nicht-Austrittsknoten
- als Austrittsknoten
- als Bridge-Relay

Was es bedeutet, ein Tor-Netzwerkrelay einzurichten, und wie Sie Ihr System dazu konfigurieren, wird ausführlich in Kapitel 5 besprochen.

Diejenigen, die die Konsequenzen verstehen und zu akzeptieren bereit sind, werden dazu ermutigt, ein Relay einzurichten, denn dies ist eine der einfachsten Möglichkeiten, durch die Tor-Benutzer zum Tor-Projekt beitragen können. Diese Maßnahme bringt jedoch auch gewisse Nacheile mit sich. Wenn Sie nicht bereit sind, sich den (gewöhnlich sehr geringen) Risiken auszusetzen, aber dennoch helfen wollen, können Sie sich mit Spenden an den Kosten für die Einrichtung von Relays beteiligen.

Wenn Sie selbst ein Relay einrichten, haben Sie die Kontrolle darüber, wie viel Netzwerkbandbreite Sie für Tor bereitstellen und wie viel Datenverkehr durch Ihr System läuft.

2.2.12 Netzwerk betrachten

Ein Klick auf *Netzwerk betrachten* öffnet ein Fenster mit vier Bereichen (siehe Abbildung 2.4). Von oben rechts gegen den Uhrzeigersinn sind das die folgenden:

- Weltkarte. Wenn eine Tor-Verbindung ausgewählt ist, zeigt die Karte, in welchen Ländern die Relays stehen, durch die diese Verbindung verläuft. Die Standorte werden anhand der Länderregistrierung der IP-Adressen dieser Tor-Relays bestimmt. Die Genauigkeit geht aber nicht über das Land hinaus, sodass Relays innerhalb eines Landes alle an demselben Punkt angezeigt werden.
- Eine Liste aller zurzeit aktiven Tor-Relays. Sie können nach der verfügbaren Bandbreite (angezeigt durch bis zu drei gelbe Balken), den Ländern oder dem Relaynamen sortiert werden. Um weitere Informationen über ein Relay zu gewinnen, klicken Sie darauf. Genauere Angaben zu dem Relay werden dann in der unteren rechten Ecke angezeigt.
- Verbindungen und ihr Status. Dieses Feld zeigt Informationen über die Tor-Relays in allen zurzeit bestehenden Tor-Verbindungen an. Wenn Sie auf eine Verbindung klicken, werden ausführliche Einzelheiten über die zugehörigen Relays in dem Bereich in der unteren rechten Ecke angezeigt.
- Angaben zu den Relays. Zeigt genauere Angaben über ein oder mehrere Relays an (die Sie in der Relay- oder der Verbindungsliste ausgeführt haben). Dazu gehören Standort (Land), IP-Adresse, verfügbare Bandbreite, Aktivitätsdauer des Systems sowie Datum und Uhrzeit der letzten Aktualisierung dieser Informationen.

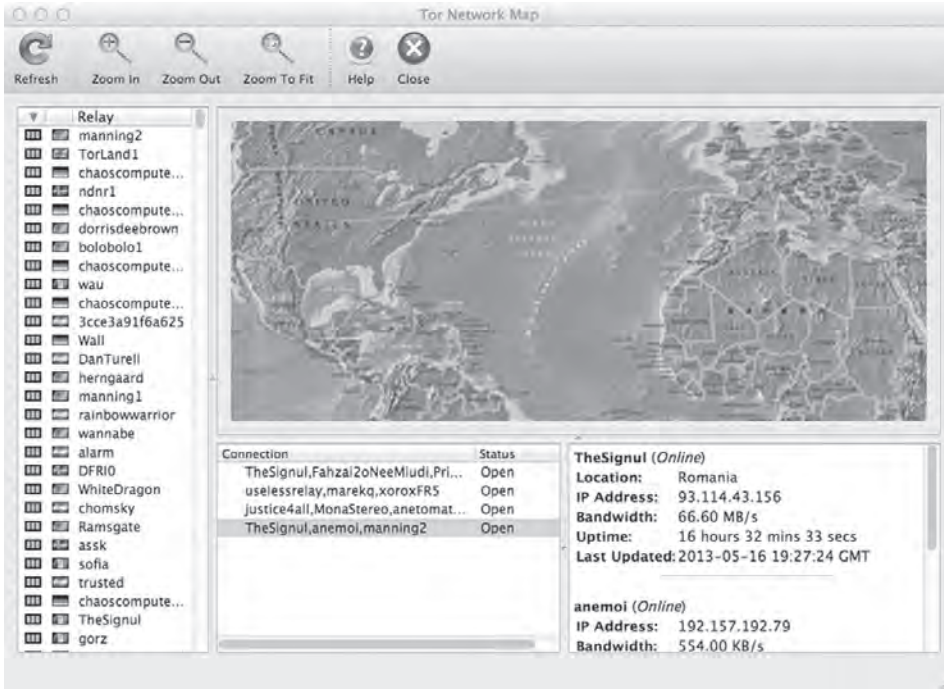

Abbildung 2.4: Die Tor-Netzwerkkarte

2.2.13 Eine neue Identität verwenden

»Identität« bedeutet in diesem Fall den Austrittsknoten Ihrer Tor-Verbindung, der direkt mit den gewünschten Remoteservern kommuniziert.

Welchen Grund kann es geben, sich eine »neue« Identität zu beschaffen? Nehmen wir an, Sie wollen anonym auf ein persönliches E-Mail-Konto zugreifen und gleichzeitig Inhalte in einem politischen Blog veröffentlichen. Ihr E-Mail-Konto ist zwar mit nichts anderem verbunden, aber wenn Sie über dieselbe Tor-Verbindung Ihr Blog bearbeiten, gehen Sie das Risiko ein, dass ein Gegner diesen Zusammenhang feststellt. Ihre Anonymität kann gefährdet sein, wenn der Gegner eine Verbindung zwischen diesen beiden Identitäten herstellt.

Dieses Problem lässt sich jedoch nicht einfach dadurch lösen, dass Sie eine neue Identität nutzen. Warum das so ist, erfahren Sie im Folgenden. (Sie können sich auch einfach merken, dass Sie Tor/Tails neu starten müssen, wenn Sie anonym eine Aufgabe beginnen wollen.)

Tor richtet Tor-Netzwerkverbindungen ein (gewöhnlich vier neue beim Start von Tor) und schaltet regelmäßig zwischen ihnen um. Zurzeit läuft eine Verbindung nach zehn Minuten ab. Alte Verbindungen werden verworfen. Der Aufbau neuer Verbindungen erfolgt häufig genug, um Schutz gegen Gegner zu bieten, die Tor-Protokolle blockieren.

Jede dieser Verbindungen ruft eine andere IP-Adresse hervor, die für Ihren Computer steht, mit anderen Worten, eine neue Identität. Wenn Sie auf *Eine neue Identität verwenden* klicken, schaltet Tor zu einer neuen Identität um (gewöhnlich zu einer, die bereits eingerichtet ist, aber noch nicht benutzt wurde).

Durch die Änderung der Tor-Konfigurationsdatei (*torrc*) können Sie festlegen, wie und wie oft Tor-Verbindungen verwendet und für ungültig erklärt werden und wann verwendete Verbindungen verworfen werden.

Der Klick auf *Eine neue Identität verwenden* weist Tor an, eine neue Identität für die *nächste* Verbindung zu nutzen. Tor verwirft die laufende Verbindung nicht sofort, um eine neue zu nutzen. Die Dokumentation von Tails weist darauf hin: »Diese Funktion von Vidalia ist keine Lösung, um verschiedene Kontextidentitäten wirklich zu trennen. Stattdessen müssen Sie Tails herunterfahren und neu starten.« (Siehe dazu *https://tails.boum.org/doc/anonymous_internet/vidalia/index.en.html*.)

Wie es in der Dokumentation heißt, sorgt Tails nicht dafür, dass »unterschiedliche Kontextidentitäten wie durch Zauberhand getrennt werden« (siehe *https://tails.boum.org/doc/about/warning/index.en.html#identities*), was bedeutet, dass diese Funktion nicht dazu geeignet ist, die Probleme zu lösen, für die sie scheinbar gedacht ist. Die empfohlene Vorgehensweise besteht darin, Tails bzw. Tor komplett neu zu starten.

2.2.14 Bandbreitengraph

Wenn Sie auf *Bandbreitengraph* klicken, erscheint ein Fenster, dass die Bandbreite des Tor-Netzwerks für gesendete und empfangene Daten im Zeitverlauf darstellt. Das ist praktisch, um zu prüfen, ob das System tatsächlich mit Tor verbunden ist und Tor zur Datenübertragung nutzt, und um festzustellen, wie viele Daten gesendet und empfangen werden.

Wenn Sie Ihr System als Tor-Netzwerkrelay eingerichtet haben, kann Ihnen die Beobachtung des Bandbreitendiagramms eine Vorstellung davon geben, wie stark (oder schwach) Ihr Relay genutzt wird.

2.3 Einstellungen

Die Einstellungskonsole von Vidalia enthält die folgenden Schaltflächen:

- Allgemein
- Netzwerk
- Beteiligung
- Dienste
- Aussehen
- Fortgeschritten
- Hilfe

Sie können Tor durchaus auch erfolgreich und produktiv einsetzen, ohne jemals irgendwelche Einstellungen zu ändern. Das gilt allerdings nicht in jedem Fall, insbesondere dann nicht, wenn Sie einen Proxy für den Zugang zum Internet verwenden oder wenn ein Gegner bestimmte Ports oder den Zugriff auf Tor blockiert.

Mehr über Tor: Fehlende Funktionen von Vidalia in Tails
Die Tails-Version von Vidalia enthält keine Einstellungskonsole, da sie dazu dient, eine Konfiguration für die dauerhafte Nutzung von Tor vorzunehmen (einschließlich der Konfiguration verborgener Dienste und Tor-Relays). Tails dagegen ist hauptsächlich dazu gedacht, sich auf einfache Weise als anonymer Benutzer mit dem Tor-Netzwerk in Verbindung zu setzen.

2.3.1 Allgemein

Unter *Allgemein* sind folgende Einstellungen zu finden:

- Eine Option, um die Tor-Netzwerksoftware automatisch zu starten, sobald Vidalia geöffnet wird. Dies ist zwar nicht unbedingt notwendig, aber empfehlenswert.
- Die Angabe des Speicherorts für die Tor-Software und die zugehörigen Dateien.
- Einstellungen für die Proxyanwendung. Dazu gehören die Angabe von Speicherort und Name der Proxyanwendung sowie jegliche Optionen und Argumente, die beim Start des Proxys zu verwenden sind, und ein Kontrollkästchen, um sie einzuschalten.

Wenn sie zur Verbindung mit dem Internet eine Proxyanwendung einsetzen, muss sie eingeschaltet sein, damit ein Internetzugang möglich ist. Der Tor-Netzwerkzugriff erfolgt über die Internetverbindung. Wenn Ihre Netzwerkanbindung eine Proxyanwendung erfordert, so gilt das daher auch für die Tor-Anbindung.

2.3.2 Netzwerk

Die Einstellungen unter *Netzwerk* betreffen drei Aspekte der Netzwerkanbindung:

- Die Verwendung eines Proxys für den Zugang zum Internet. Hier geben Sie die Netzwerkadresse und den Port des Proxys, Ihren Benutzernamen und Ihr Passwort und den Typ des verwendeten Proxys an (SOCKS4, SOCKS5 oder HTTP/HTTPS).
- Zugang über eine Internet-Firewall, die einige Ports blockiert. Netzwerkanwendungen (wie Web, E-Mail, Chat usw.) nutzen jeweils unterschiedliche Ports, um deutlich zu machen, welche Art von Datenverkehr übertragen wird. Viele Firewalls blockieren alle Ports außer denen für den HTTP-, also den Web-Datenverkehr (Ports 80 und 443). Wenn Tor nicht funktioniert und es nicht am Proxy liegt, kann die Firewall der Grund sein. Wenn ja, versuchen Sie hier nur die beiden HTTP-Ports anzugeben, sodass der gesamte Tor-Datenverkehr darüber geleitet wird.
- Zugang zum Internet über einen ISP, der die Tor-Anbindung blockiert. Manche Provider sperren Tor-Datenverkehr, indem sie Ihre Netzwerkdaten untersuchen und die IP-Adressen mit denen von Tor-Relays vergleichen (die öffentlich einsehbar sind). Diese Art der Filterung kann von einem Unternehmen oder einer Regierung durchgesetzt werden. In jedem Fall müssen Sie ein Bridge-Relay verwenden. (Mehr darüber erfahren Sie in Kapitel 4.)

Wenn Sie nicht sicher sind, ob ein Proxy verwendet wird, wie die Firewall funktioniert oder ob Ihr Provider Tor sperrt, sollten Sie sehr vorsichtig vorgehen, um sich die erforderlichen Informationen zu beschaffen.

Die IT-Mitarbeiter oder Netzwerkbeauftragten nach Proxys, Firewalls und insbesondere nach der Tor-Anbindung zu fragen kann bei denen, die für die Durchsetzung der Netzwerkrichtlinien der Organisation verantwortlich sind, Alarm auslösen.

Möglicherweise bemerken Sie erst dann, dass ein Proxy oder eine Firewall vorhanden ist, wenn Sie erfolglos versuchen, Verbindung zum Tor-Netzwerk aufzunehmen. Prüfen Sie die Konfiguration Ihres System nach Möglichkeit selbst, um herauszufinden, ob Ihr Betriebssystem als Proxy eingerichtet ist. Wenn es keinen Proxy gibt, Sie aber trotzdem Schwierigkeiten haben, zu Tor durchzukommen, kann eine Firewall den Zugriff auf die Tor-Relays blockieren. In diesem Fall können Sie eine Tor-Bridge verwenden (siehe Kapitel 4).

Wenn Sie mit dem technischen Personal sprechen müssen, ist es besser, den Anschein von Unwissenheit als von Verschlagenheit zu erwecken. Fragen wie »Warum komme ich mit meinem Smartphone nicht in das Firmen-WLAN?« oder »Wie kann ich von meinem privaten Laptop aus eine Verbindung zum Internetanschluss im Büro herstellen?« erregen weniger Verdacht als: »Wie muss ich Tor einrichten, um durch die Unternehmensfirewall zu kommen?«

2.3.3 Beteiligung

Es gibt vier Optionen, um Tor zu verwenden und Ihre Ressourcen im Tor-Netzwerk zur Verfügung zu stellen:

- Ausführung nur als Client
- Bridge-Relay
- Nicht-Ausgangsrelay (Transitrelay)
- Ausgangsrelay

Die meisten Benutzer bleiben bei der Standardeinstellung und führen Tor nur als Client aus. Das ist am sichersten, geht am einfachsten und fällt am wenigsten auf. Wenn Sie wissen, was Sie tun, und Netzwerkbandbreite übrig haben, können Sie Ihr System auch als Tor-Bridge oder als Tor-Relay einrichten.

Ein Bridge-Relay zu betreiben stellt dabei die erste Stufe dar und bildet die sicherste Möglichkeit, eigene Ressourcen im Tor-Netzwerk zur Verfügung zu stellen. Ein System als Tor-Bridge auszuführen ist sicher, da es dabei keinen Tor-Datenverkehr ins Internet weiterleitet. Die IP-Adresse des Bridge-Betreibers taucht daher nirgendwo in irgendwelchen Serverprotokollen auf. Da Bridges auch in keinen öffentlich geführten Listen auftauchen, kann die IP-Adresse Ihres Systems von Angreifern auch nicht leicht erkannt werden.

Die nächste Stufe besteht darin, ein reines Transit-Relay zu betreiben. Dabei sendet und empfängt Ihr System nur verschlüsselten Tor-Datenvekehr zwischen anderen Tor-Knoten und Tor-Clients. Ein solches Transit-Relay kann als Eintrittsknoten fungieren (der verschlüsselten Netzwerkdatenverkehr von einem Tor-Client entgegennimmt), aber auch Daten von einem Eintrittsknoten annehmen und an einen Austrittsknoten weiterleiten.

Beim Betreiben eines Transit-Relays besteht ein äußerst geringes Risiko, mit bestimmten (verbotenen oder illegalen) Inhalten in Verbindung gebracht zu werden. Ihr Provider kann in seinen Nutzungsbedingungen außerdem eine solche Teilnahme untersagen oder es bevorzugen, dass Sie Ihre Bandbreite nicht für solche Arten von Anwendungen zur Verfügung stellen.

Einen Austrittsknoten zu unterhalten stellt die nächste Stufe dar, und dies ist mit einem etwas größeren Risiko verbunden, da Ihr System dabei unverschlüsselte Daten handhabt (etwa wenn der Endbenutzer auf einen Webserver zugreift, der HTTPS nicht unterstützt; siehe den Kasten »HTTPS und HTTPS Everywhere in Kapitel 1). Wenn diese Daten auf verbotene Inhalte untersucht werden, laufen Sie Gefahr, (irrtümlicherweise) für diese Inhalte zur Verantwortung gezogen zu werden.

Das Tor-Netzwerk stützt sich auf Benutzer rund um die Welt, die ihre Ressourcen bereitstellen. Wenn Sie sich ebenfalls beteiligen wollen, aber technisch nicht versiert genug sind, können Sie die Betreiber von Tor-Austrittsknoten auch durch Spenden unterstützen. (Weitere Informationen

erhalten Sie in »Support the Tor Network: Donate to Exit Node Providers« auf *https://blog.torproject.org/blog/support-tor-network-donate-exit-node-providers*.)

Die Einrichtung eines Tor-Relays (siehe *https://www.torproject.org/docs/tor-doc-relay.html.en*) ist für Personen, die über gewisse Kenntnisse in Systemadministration verfügen und sich selbst um ihre Betriebssicherheit kümmern können (*https://trac.torproject.org/projects/tor/wiki/doc/OperationalSecurity*), nicht allzu schwer. Mehr über die Bereitstellung von Ressourcen im Tor-Netzwerk erfahren Sie in Kapitel 5.

2.3.4 Dienste

Diese Registerkarte ist dazu da, verborgene Tor-Dienste hinzuzufügen und einzurichten. Zurzeit ist die Unterstützung von Vidalia für verborgene Dienste noch relativ neu, und die Tor-Dokumentation enthält die Warnung, dass sich noch Bugs darin befinden können.

Es ist einfacher, verborgene Dienste über Vidalia als manuell zu konfigurieren, allerdings fehlen in Vidalia einige der erweiterten Funktionen, die bei der Verwaltung der verborgenen Dienste in der Tor-Konfigurationsdatei *torrc* zur Verfügung stehen.

Weitere Informationen über die Einrichtung und Verwendung verborgener Dienste erhalten Sie in Kapitel 6.

2.3.5 Aussehen

Hier können Sie die Sprache der Vidalia-Oberfläche ändern und eine andere Gestaltung auswählen. Außerdem können Sie entscheiden, ob die Tor-Symbole auf Ihrem Desktop angezeigt oder verborgen werden sollen.

2.3.6 Fortgeschritten

Diese Registerkarte ist in drei Bereiche unterteilt:

- *Tor Control*. Hier geben Sie an, wie die Tor-Netzwerkverbindung über den lokalen Host Verbindung mit dem Tor-Netzwerk aufnimmt. Außerdem richten Sie die Authentifizierung für die Verwendung von Tor ein.
- *Tor-Konfigurationsdatei*. Hier geben Sie den Speicherort der Tor-Konfigurationsdatei (*torrc*) an. Außerdem haben Sie die Möglichkeit, die zurzeit geladene Version dieser Datei zu bearbeiten. Die Änderungen, die Sie dabei vornehmen, können entweder nur auf die laufende Sitzung angewendet oder für die zukünftige Nutzung gespeichert werden.
- *Datenverzeichnis*. Hier geben Sie das Verzeichnis an, in dem Tor die erforderlichen Daten speichert, z. B. zwischengespeicherte Versionen des Tor-Konsensverzeichnisses (die Liste aller Tor-Relays, die von den Tor-Verzeichnisservern verbreitet wird) und kryptografische Schlüssel, die zur Kommunikation über das Tor-Netzwerk erforderlich sind.

2.4 Den Tor-Browser verwenden

Der Tor-Browser ist eine modifizierte Version von Firefox ESR. Auch Iceweasel, der in der Tails-Distribution enthaltene Browser, basiert auf dem Mozilla-Browserprojekt. Die beiden Tor-Browser sind funktional (fast) identisch und sollten jedem vertraut vorkommen, der schon einmal Firefox (oder verwandte Browser) verwendet hat.

Bei der Änderung von Einstellungen des Tor-Browsers sollten Sie äußerst vorsichtig sein, da die Standardwerte sorgfältig von den Entwicklern des Tor-Projekts ausgewählt wurden, um für maximale Sicherheit und Nützlichkeit zu sorgen. Die Änderung einiger Einstellungen beschwört offensichtlich Probleme für die Wahrung der Anonymität herauf, z. B. wenn Sie dem Browser erlauben, sich den Verlauf zu merken, oder Warnungen über

die Installation von Add-Ons durch Websites abschalten. Andere Einstellungen können Probleme verursachen, die nicht so auffällig sind, weshalb es im Allgemeinen am besten ist, die Browsereinstellungen nicht anzufassen.

2.5 Wenn Tor keine Verbindung herstellen kann

Ohne zusätzliche Konfiguration funktioniert Tor nicht immer auf Anhieb. Wenn Tor nicht funktioniert, probieren Sie die folgenden Richtlinien zur Störungssuche in Software allgemein und bei Tor im Besonderen aus.

2.5.1 Grundlegende Störungssuche

Wenn Sie nach der Ursache eines Netzwerkproblems suchen, sollten Sie als Erstes überprüfen, ob das System mit dem Netzwerk verbunden ist. Vergewissern Sie sich vor einem Start von Tor, dass die Internetverbindung funktioniert und alle Kabel (falls erforderlich) angeschlossen sind.

Häufig lässt sich das Problem lösen, indem Sie alle Stecker abziehen, hineinpusten und sie wieder anschließen.

Ein weiterer Trick, der oft die Lösung bringt, besteht darin, das System aus- und wieder einzuschalten.

2.5.2 Brauchen Sie einen Proxy?

Möglicherweise können Sie in der Netzwerkkonfiguration des Browsers oder des Systems erkennen, ob ein Proxy für den Internetzugriff erforderlich ist. Um sich die Browsereinstellungen anzusehen, wählen Sie im Browsermenü *Einstellungen*. (Die Proxyeinstellungen werden gewöhnlich unter den »erweiterten« Einstellungen angezeigt.)

Der Browser kann so eingerichtet sein, dass er die Proxykonfiguration des Systems verwendet. In diesem Fall müssen Sie das entsprechende Dienstprogramm zur Systemkonfiguration öffnen. (Manche Browser erledigen das auch für Sie.) Wenn ein Proxy vorhanden ist, sollte er in der Konfigurationsanzeige aufgeführt werden.

Um Tor zur Verwendung eines Proxys einzurichten, klicken Sie in Vidalia auf die Verknüpfung *Einstellungen* und öffnen dann die Registerkarte *Netzwerk*. Aktivieren Sie das Kontrollkästchen *Ich benutze einen Proxy, um ins Internet zu gelangen*. Daraufhin werden Sie aufgefordert, Angaben über den Proxy zu machen. (Zumindest einige dieser Angaben können Sie wahrscheinlich wie oben erwähnt aus der Systemkonfiguration beziehen.)

2.5.3 Das Logbuch einsehen

Wenn Sie das Tor-Logbuch im erweiterten Modus öffnen, können Sie viele Meldungen sehen, die einen Hinweis darauf geben, was nicht funktioniert. Wenn beispielsweise die Systemuhr nicht richtig eingestellt ist, kann Tor nicht arbeiten. (Ihr Computer wird mit einer IP-Adresse maskiert, die gewöhnlich zu einem Computer in einem anderen Land gehört, weshalb Tor das, was der Remoteserver für die lokale Uhrzeit Ihres Systems hält, und die tatsächliche Uhrzeit in Einklang bringen muss.)

Einige der Meldungen im Logbuch scheinen zwar nicht sehr hilfreich zu sein, allerdings sollen Sie trotzdem versuchen, sie zu lesen, da sie oft Hinweise auf das Problem geben, wenn auch in ziemlich kryptischer Form. Wenn Sie beispielsweise eine Meldung darüber sehen, dass ein Programm fehlt, besteht die Lösung darin, Tor neu zu installieren. Wird in einer Meldung davon gesprochen, dass eine Adresse bereits verwendet wird (oder unerreichbar ist), müssen Sie das System möglicherweise neu starten oder Tor zur Überwindung einer Firewall umkonfigurieren.

2.5.4 Tor für Firewalls einstellen

Wenn Sie sich hinter einer Firewall befinden, die nur den Zugriff auf Webserver erlaubt, können Sie Tor so einstellen, dass es keine unzulässigen Ports verwendet.

Ein *Port* ist so etwas wie eine Adresse für ein bestimmtes Programm auf einem Computer. Internetprotokolle senden Netzwerkdaten zu und von bestimmten Programmen, die auf Internetservern laufen, indem sie die IP-Adresse und die Portnummer des Programms angeben.

Eine Firewall kann den Datenverkehr auf Daten einschränken, die über Port 80 (für unverschlüsseltes HTTP) und 443 (für verschlüsseltes HTTPS) an Webserver gesendet werden.

Um Tor hinter einer Firewall zu verwenden, die eine solche strenge Portfilterung durchführt, öffnen Sie in Vidalia die Einstellungen und wechseln zur Registerkarte *Netzwerk*. Klicken Sie dort auf das Kontrollkästchen *Meine Firewall lässt nur Verbindungen zu bestimmten Ports zu*. Daraufhin werden Sie aufgefordert, die gültigen Ports anzugeben. (In der Standardeinstellung werden nur die Ports 80 und 443 verwendet, die Standardports für das Webprotokoll HTTP.)

Wenn Antivirussoftware Ihren Tor-Zugang blockiert, können Sie entweder Tails verwenden (das hochfährt, ohne irgendwelche Software zu starten, die auf den Festplatten des Systems installiert ist) oder das Antivirusprogramm deaktivieren oder deinstallieren.

2.5.5 Wenn Tor immer noch keine Verbindung herstellen will

Sollte Tor immer noch keine Verbindung aufnehmen, liegt es möglicherweise daran, dass Ihr Provider Tor ausdrücklich sperrt, indem er Tor-Relayadressen filtert und verhindert, dass Sie auf Tor-Relays zugreifen.

Manche Länder sperren Tor, aber auch einzelne Provider oder Organisationen, die eigene Firewalls betreiben. In einem solchen Fall sind Tor-Bridges nützlich, da sie nirgendwo vollständig und öffentlich zugänglich aufgeführt werden.

Tor so einzurichten, dass es eine Bridge verwendet, ist relativ einfach. Dazu müssen Sie zunächst die Adressen einiger Bridges herausfinden und dann in den Netzwerkeinstellungen von Vidalia das Kontrollkästchen *Mein Provider blockiert Verbindungen zum Tor-Netzwerk* aktivieren. Anschließend können Sie in dem daraufhin eingeblendeten Feld die Bridge-Adressen eingeben.

Sie sollten mehr als eine Bridge angeben, denn eine einzige reicht unter Umständen nicht aus. Sollte eine Bridge nicht mehr zur Verfügung stehen, besteht eine bessere Chance, dass die Tor-Verbindung beim Ausfall einer Bridge nicht unversehens zusammenbricht, wenn Sie noch einige andere in Reserve haben.

Ausführlichere Informationen darüber, wie Sie Tor-Bridges finden und verwenden, erhalten Sie in Kapitel 4.

3

Tails

Tails (siehe *https://tails.boum.org/*) ist eine angepasste und abgespeckte Linux-Distribution, die Tor sowie andere Komponenten enthält, um ein Betriebssystem bereitzustellen, das die Privatsphäre stärkt. Es handelt sich bei Tails um ein Teilprojekt von Tor. Manchmal wird es fälschlicherweise TAILS geschrieben, als Akronym für »The Amnesiac Incognito Live System«.

Es gibt zwar noch viele andere Linux-Distributionen, die im Hinblick auf Anonymität konzipiert wurden, doch viele Benutzer bevorzugen Tails wegen seiner Verbindung mit dem Tor-Projekt. Die Implementierer von Tails arbeiten mit den Entwicklern des Tor-Projekts zusammen, um Schwachstellen zu verringern und die Gesamtsicherheit zu verbessern.

Da es sich um eine Linux-Distribution handelt, enthält Tails eine Reihe von Anwendungen und Funktionen, die im TBB unter Windows oder OS X nicht unmittelbar bereitstehen. Da Tails das laufende Betriebssystem ist, stellen Dinge, die auf einem normalen Widnows- oder OS X-System die Anonymität gefährden könnten, hier kein Problem dar.

Mehr über Tor: Tails auf Apple-Computern
Es ist zwar möglich, Tails auf einem Apple-Computer zu starten, allerdings ist das alles andere als einfach. Tatsächlich kann der Vorgang ziemlich chaotisch sein. Wenn Sie eine andere sinnvolle Möglichkeit haben (z. B. die Verwendung von Tails auf einem »Wintel«-System oder die Nutzung von TBB), sollten Sie diese Vorgehensweise (zurzeit) tunlichst vermeiden.

Falls Sie Tails unbedingt auf einem Macintosh starten müssen, sollten Sie im Tails-Forum (*https://tails.boum.org/forum*) nach aktuellen Threads über die Verwendung von Tails auf OS X-Systemen suchen.

Beispielsweise kann Ihr Betriebssystem Ihre IP-Adresse preisgeben, wenn Sie eine Datei mit Webinhalten öffnen. Wenn Sie eine Datei über das Tor-Netzwerk herunterladen, geschieht das anonym: Die Betreiber des Servers, von dem Sie die Datei beziehen, können den Download nur mit dem von Ihnen benutzten Tor-Austrittsknoten in Verbindung bringen.

Wenn Sie nun aber die Datei öffnen und sie einen URL enthält, versucht Ihre Textverarbeitung, den entsprechenden Inhalt herunterzuladen. Jetzt können die Betreiber des Servers Ihre Kopie der heruntergeladenen Datei mit Ihrer echten IP-Adresse in Verbindung bringen.

Es spielt keine Rolle, ob der Autor der Datei den Link als Trick eingebaut hat, um den Empfänger zu identifizieren, oder als harmlose Möglichkeit, Inhalte zu liefern: Die Internetverbindung, die zum Herunterladen dieser Inhalte aufgebaut wird, gibt Ihre Identität preis.

Wenn Sie eine Anwendungsdatei in einem Programm öffnen, das nicht ausdrücklich zur Nutzung von Tor umkonfiguriert (und möglicherweise geändert) wurde, verwendet es das öffentliche Internet, und das bedeutet, dass der gesamte Inhalt im lokalen Netzwerk preisgegeben wird und die IP-Adresse des Benutzers für den Remotesever und jeden zugänglich ist, der ausreichend Zugriff auf das System hat. Sie ist dabei also nicht mehr durch eine Tor-Verbindung geschützt.

In Tails wurde der Netzwerkstack geändert, sodass sämtliche Internetverbindungen standardmäßig durch das Tor-Netzwerk geleitet werden. Steht das Tor-Netzwerk nicht zur Verfügung, so haben Sie auch keinen Zugang zum Internet.

Bei der Verwendung des TBB unter Windows, OS X oder einer normalen Linux-Distribution kann Ihr System Sie versehentlich verraten, wenn Sie Dateien mit Webinhalten öffnen, da in diesem Fall nur die TBB-Anwendungen (im Grunde genommen also der Tor-Browser) Tor verwenden, während gleichzeitig auch öffentliche Internetverbindungen ablaufen können.

Das bedeutet nicht, dass Tails nicht in der Lage ist, Netzwerkdatenverkehr außerhalb von Tor zu erledigen. Es ist lediglich so eingerichtet, dass es die öffentlichen Internetprotokolle nur zur Verbindung mit Remoteservern über Tor-Relays verwendet.

Es kann hin und wieder auch notwendig sein, einen »unsicheren« Browser für den Zugriff auf einen Dienst einzusetzen, z. B. in Netzwerken, die eine Anmeldung oder Registrierung zur Aktivierung der Verbindung erfordern. Darum ist die Option *Unsicherer Webbrowser* in Tails enthalten.

3.1 Der Umfang von Tails

Tails enthält genügend Software, um die meisten üblichen Aufgaben von Desktop-Computern zu erfüllen (z. B. E-Mail, Web, Erstellen und Bearbeiten von Dokumenten für alle wichtigen Anwendungen, vollständige Netzwerkfunktionen und Standardfunktionen des Betriebssystems, die auf allen Linux-Systemen zur Verfügung stehen). Jeder, der schon einmal mit Linux gearbeitet hat, sollte mit der in Tails enthaltenen Software vertraut sein. (Eine vollständige Liste finden Sie auf *https://tails.boum.org/doc/about/features/index.en.html*.) Zu den wichtigsten Softwarepaketen gehören die folgenden:

- *Firefox/Iceweasel*: Iceweasel (*http://wiki.debian.org/Iceweasel*) ist ein »Fork« (eine modifizierte Version) von Firefox, die einige Sicherheitsmerkmale enthält, aber keine der Grafiken, die von Mozilla, den Herausgebern von Firefox, als Warenzeichen geschützt sind. (Dies ist eine lange Geschichte, in der es hauptsächlich um Lizenzprobleme geht. Um sich eine Vorstellung von der Problematik zu machen, lesen Sie »Debian bug report on use of Mozilla Firefox trademark without permission« auf *http://bugs.debian.org/cgi-bin/bugreport.cgi?bug5354622* und »mozilla thunderbird trademark restrictions/still dfsg free?« auf *http://lists.debian.org/debian-legal/2004/12/msg00328.html*.)
- *Pidgin/OTR:* Pidgin (*http://www.pidgin.im*) ist ein Instant-Messaging-Client, OTR (Off-the-Record Messaging, siehe *http://www.cypherpunks.ca/otr/index.php*) ein Plug-In, das privates Instant Messaging erlaubt. Beide Programme sind in Tails vorinstalliert und konfiguriert.
- *Gnu Privacy Guard:* GnuPG, wie es kurz genannt wird (*http://gnupg.org*), ist der De-facto-Standard für die Verschlüsselung mit öffentlichen Schlüsseln (Ver- und Entschlüsselung von Daten und digitale Signaturen). Tails enthält auch GnuPG-Plug-Ins, sodass Daten mit Anwendungsprogrammen wie dem Texteditor gedit (*http://projects.gnome.org/gedit*) und OpenOffice (*http://openoffice.org*) verschlüsselt werden können.
- *OpenOffice.org:* Eine (für viele) ausreichende Bürosoftwaresuite. Verschlüsselungsmöglichkeiten sind darin zurzeit noch nicht enthalten. Um Textdokumente zu verschlüsseln, zu entschlüsseln, digital zu signieren oder um digitale Signaturen in solchen Dokumenten zu überprüfen, wird daher gedit bevorzugt, das GnuPG unterstützt.
- *Metadata Anonymization Toolkit (MAT):* Ein GUI-Werkzeugkasten (*https://mat.boum.org*), mit dem Metadaten von Textverarbeitungs-, Grafik-, Medien- oder anderen Arten von Datendateien entfernt werden können. Metadaten enthalten Informationen über den Benutzer und das System, die die Datei erstellt haben, und können auch Informationen über Bearbeiter oder Autoren der Datei preisgeben. Wenn Sie Datendateien senden oder empfangen und dabei Ihre Anonymität wahren wollen, sollten Sie dieses Werkzeug nutzen.

- *Unsicherer Webbrowser:* Dies ist eine weitere Version von Iceweasel, das selbst eine Variante von Firefox Mozilla ESR ist. Sie ist zum ungesicherten Surfen im Web eingerichtet (was erforderlich sein kann, um eine Webverbindung zu aktivieren). Auf der Startseite sehen Sie eine Menge in Rot hervorgehobener Warnungen sowie eine Erklären, wie und wann Sie diesen Browser verwenden sollten.

Dies ist nur eine Auswahl der Anwendungen, die über die grafische Oberfläche von Tails leicht zugänglich sind. Über die Tails-Menüs besteht darüber hinaus Zugriff auf weitere Programme, unter anderem die folgenden:

- GIMP (Bitmap-Grafik)
- Inkscape (Vektorgrafik)
- Scribus (Desktop-Publishing)
- Audacity (Audioaufnahme, -bearbeitung und -wiedergabe)

Diese Liste der enthaltenen Software ist alles andere als erschöpfend. Als Linux-Distribution umfasst Tails zahlreiche Kommandozeilenprogramme sowie ein Sortiment weiterer Anwendungen. Auf dem Desktop können Sie sich ansehen, welche Programme eingeschlossen sind (im Menü *Anwendungen*, das in der oberen linken Ecke des Desktops zugänglich ist).

Sie können auch das Synaptic-Paket verwenden (*http://www.nongnu.org/synaptic/*), um die installierte Software zu verwalten. Dazu müssen Sie Tails mit einem Administratorpasswort starten, um eine Änderung der Systemeinstellungen zu erlauben. Mit Synaptic können Sie sich ansehen, welche Pakete installiert sind. Es ist jedoch nicht möglich, Pakete zu installieren, die in der Tails-Distribution nicht enthalten sind. (Weitere Hinweise zur Installation von zusätzlicher Software unter Tails finden Sie weiter hinten.)

3.2 Tails einrichten

Das Schöne an Tails ist, dass Sie es auf (fast) jedem Computer von einem USB-Stick oder einer DVD starten können, ohne irgendwelche Spuren auf diesem Rechner zu hinterlassen. Tails muss nicht auf dem System installiert werden und legt auch keinerlei Anmeldungen, Cookies oder sonstige Informatoinen auf dem Systemlaufwerk ab, die als Beweis herangezogen werden könnten.

Dazu muss das System, auf dem Sie Tails ausführen, von einer DVD oder einem USB-Stick gestartet werden können, weshalb es (wie bereits erwähnt) am einfachsten ist, dies auf einem Computer zu tun, der für Windows oder Linux gedacht ist, und nicht auf einem modernen Apple-Computer.

3.2.1 Tails beziehen

Der erste Schritt besteht darin, das DVD-Image (die ISO-Datei) herunterzuladen (von *https://tails.boum.org/download/index.en.html*) und auf eine DVD zu brennen. Anstatt hier selbst zu beschreiben, wie Sie dazu vorgehen, verweise ich auf die Anleitung zum Brennen einer ISO-Datei von Ubuntu (siehe *https://help.ubuntu.com/community/Burnin gIsoHowto*). Wenn Sie eine bootfähige DVD haben, können Sie Tails ausführen, indem Sie die DVD in das Laufwerk einlegen und das System starten.

Die ISO-Datei mit Tails umfasst etwa 850 MB, was sich über eine Breitbandverbindung in wenigen Minuten herunterladen lässt. Laden Sie auch die digitale Signatur herunter und überprüfen Sie sie, bevor Sie weitermachen. Eine ausführliche Anleitung, wie Sie die Signatur prüfen, finden Sie in Anhang A.

3.2.2 Das System zum Starten von Tails einrichten

Die meisten Computer sind so eingerichtet, dass Sie mit dem Betriebssystem starten, das auf der Festplatte installiert ist. Sie können auch ein weiteres Betriebssystem installieren und dann beim Einschalten des Computers wählen, welches hochgefahren werden soll. Um Tails zu verwenden, müssen Sie dagegen die Systemhardware so konfigurieren, dass sie von einem angeschlossenen Gerät (USB-Laufwerk) oder dem DVD-Laufwerk startet, wenn sich darin eine startfähige DVD befindet.

Auf den meisten Systemen können Sie die Bootreihenfolge des Computers im BIOS ändern. Die Einzelheiten dieses Vorgangs unterscheiden sich von System zu System sehr stark. Allgemein sind folgende Schritte erforderlich:

- Schalten Sie den Computer aus und wieder ein und achten Sie dabei sorgfältig auf Meldungen wie »Press ESC to enter SETUP« oder »Press ALT-F12 to configure BIOS«.
- Drücken Sie die angegebene Taste, um das BIOS-Konfigurationsprogramm zu öffnen. Diese Programme werden fast immer in einfacher Textform dargestellt. Mit den Pfeiltasten, ESC, der Eingabetaste und einigen Funktionstasten können Sie die zu konfigurierenden Elemente auswählen und ändern.
- Ändern Sie die Konfiguration so, dass das System von Betriebssystemen auf Wechselmedien (DVD/CD-Laufwerk oder angeschlossenes USB-Gerät) starten kann. Am einfachsten ist es, alle Konfigurationsoptionen durchzugehen. Der Name des Eintrags, den Sie brauchen, enthält wahrscheinlich eine Bezeichnung wie »boot order« und wird oft unter den erweiterten Optionen (»advanced«) angeboten.

Da es viele verschiedene Arten von Computerhardware gibt und die Produkte im Laufe der Zeit geändert werden, kann es sich lohnen, online nach weiteren Einzelheiten über das vorliegende System zu suchen (falls Sie Probleme bei der Konfiguration haben). Ubuntu bietet einige besonders hilfreiche Informationsquellen dafür an, ein System für den Start von einer LiveCD-Linux-Distribution einzurichten, beispielsweise den

Artikel »BIOS is not set to boot from CD or DVD drive« auf *https://help.ubuntu.com/community/BootFromCD#BIOS_is_not_set_to_boot_from_CD_or_DVD_drive*.

3.3 Tails verwenden

Tails kann von DVD oder von einem USB-Stick gestartet werden. Beide Vorgehensweisen haben ihre Vor- und Nachteile.´

Wenn Sie Tails von einer DVD starten, hat das folgende Auswirkungen:

- Sie können sicherer sein, dass von Ihrer Tails-Sitzung keine Spuren zurückbleiben, denn weder auf den Festplattenspeicher des Systems, auf dem Sie Tails führen, noch auf die Tails-DVD werden irgendwelche Daten geschrieben.
- Sie können sicherer sein, dass Ihre Tails-Kopie nicht von einem Angreifer manipuliert wird. Wenn Sie Ihre Tails-Distribution auf eine DVD-R (eine schreibgeschützte DVD) brennen, kann niemand etwas hinzufügen oder die Tails-Software entfernen oder ändern.
- Jedes Mal, wenn eine neue Version von Tails veröffentlicht wird, müssen Sie sie herunterladen und eine neue DVD brennen (und die veraltete Version vernichten).
- Sie müssen eine DVD mit sich herumtragen (und schützen). Dabei müssen Sie entsprechende Vorsichtsmaßnahmen treffen, insbesondere, wenn Sie in weniger angenehme Gegenden reisen. Es wäre nicht sehr klug, auf die DVD »Tails: anonymes Internet« zu schreiben.

Führen Sie Tails von einem USB-Laufwerk aus, so bedeutet das Folgendes:

- Da das USB-Gerät ein beschreibbares Medium ist, können Sie darauf – sofern es groß genug ist – einen *persistenten Speicherbereich* anlegen. Der persistente Speicherbereich von Tails wird verschlüsselt und mit einem Passwort gesichert, sodass Sie darin persönliche Dateien und Arbeits-

unterlagen, zusätzliche Software für die Arbeit mit Tails, eigene Konfigurationen Ihres Tails-Systems und von Anwendungsprogrammen sowie Verschlüsselungsschlüssel auf geschützte Weise ablegen können.

- Da der USB-Stick ein beschreibbares Medium ist, kann ein Angreifer, der physischen Zugang dazu hat, wichtige Software darauf manipulieren oder entfernen oder Malware hinzufügen (Viren oder Keylogger).
- Eine Tails-Installation auf einer SD-Karte oder einem USB-Stick lässt sich leicht und ohne Verdacht zu erregen transportieren.
- Auf einem USB-Laufwerk lässt sich Tails auf einfache Weise aktualisieren, selbst wenn ein persistenter Speicherbereich vorhanden ist. Im Gegensatz zu DVDs kann das Laufwerk auch wiederverwendet werden. Es wird jedoch empfohlen, das USB-Laufwerk von der letzten veröffentlichten Tails-Version aus zu aktualisieren, was bedeutet, dass Sie Tails ohnehin auf eine DVD brennen müssen. (Das ist zwar nicht unbedingt erforderlich, aber einfacher und ratsam.)
- Nicht alle Computer können von USB-Geräten starten.

Ob Sie Tails von DVD oder von einem USB-Laufwerk ausführen, hängt davon ab, wie, wo und wozu Sie das System nutzen.

3.3.1 Tails starten

Zum Starten von einer DVD müssen Sie die DVD in das Laufwerk legen und den Computer einschalten. Wenn das NetBIOS des Systems so eingerichtet ist, dass es den Start von DVD erlaubt, und die DVD korrekt gebrannt wurde, fährt das System hoch und zeigt einen Startbildschirm mit den Optionen *Live* und *Live (failsafe)* an. Wählen Sie mit den Pfeiltasten *Live* aus und drücken Sie die Eingabetaste.

Wenn Tails dann nicht startet, versuchen Sie es erneut, wählen diesmal aber *Live (failsafe)* aus. Dadurch wird Tails ohne bestimmte Funktionen gestartet, die bekanntermaßen Probleme beim Start verursachen können.

Wenn der *Live*-Start von Tails gelingt, sehen Sie als nächstes ein Dialogfeld, in dem Sie gefragt werden: *Weitere Optionen?* Wird auf dem Gerät ein persistenter Speicherbereich erkannt, erscheint außerdem die Frage: *Use persistence?*

Die »weiteren Optionen« umfassen Folgendes:

- Sie können ein Administratorpasswort festlegen, um einem Superuser Zugriff auf das Betriebssystem zu gestatten. Ohne ein solches Passwort können Sie keine der »Systemfunktionen« nutzen. Dazu gehören Dinge wie z. B. die Anzeige von Protokolldateien. Im Allgemeinen müssen Sie keine Aufgaben zur Systemadministration vornehmen, allerdings kann die Einsichtnahme in die Protokolle bei der Ursachenforschung für System- und Netzwerkprobleme hilfreich sein. Das Passwort wird auch benötigt, um Zugriff auf die Laufwerke des Systems zu bekommen, auf dem Sie Tails von DVD oder einem USB-Gerät gestartet haben.
- Eine *Tarnoption*, bei der Tails mit der grafischen Benutzeroberfläche gestartet wird, die (zumindest bei flüchtiger Betrachtung) wie der Desktop von Windows XP aussieht. Das kann für manche Benutzer sinnvoll sein, um bei der Verwendung von Tails in der Öffentlichkeit nicht aufzufallen.

Wenn auf dem USB-Stick ein persistenter Speicherbereich vorhanden ist, gibt Tails Ihnen die Möglichkeit, während der Sitzung darauf zuzugreifen. Diese Möglichkeit sollten Sie sparsam und nur dann verwenden, wenn es wirklich notwendig ist.

3.3.2 Tails herunterfahren

Es kann notwendig sein, eine Tails-Sitzung so schnell wie möglich zu beenden. Wenn ein Angreifer Zugang zu Ihrem System bekommt, während es Tails ausführt, kann er aus dem Arbeitsspeicher eine Menge an Informationen über Sie und Ihre Netzwerkaktivitäten beziehen. Das unterläuft

die Anonymität und kann eine Katastrophe darstellen, wenn Sie Schlüssel und andere geheime Informationen in einem persistenten Speicherbereich abgelegt haben.

Eines der Ziele bei der Entwicklung von Tails bestand darin, dass das System so schnell und einfach heruntergefahren werden kann wie möglich.

Sie können das System vom System- oder Administrationsmenü (in der Nähe der oberen linken Ecke) herunterfahren (ausschalten) und neu starten. Sobald Sie »auf den Knopf gedrückt« haben, löscht das System den Arbeitsspeicher und hält unmittelbar an.

Eine weitere, noch schnellere Möglichkeit zum Herunterfahren bzw. Neustarten besteht darin, auf den roten Aus-Schalter in der oberen rechten Bildschirmecke zu klicken. Zur Auswahl stehen die beiden Optionen *Shut down immediately* und *Reboot immediately*. Wenn Sie auf eine davon klicken, wird die entsprechende Aktion sofort ausgeführt.

Die schnellste Möglichkeit, Tails auszuschalten, besteht darin, das Medium aus dem Computer zu entfernen, also die DVD oder (was noch besser geht) den USB-Stick oder die SD-Karte. Daraufhin werden alle Systemaktivitäten angehalten, und das System fährt herunter.

3.3.3 Tails auf einem USB-Laufwerk installieren

Tails enthält das Programm Tails LiveUSB Creator, mit dem Sie ein startfähiges USB-Laufwerk erstellen können. Zurzeit können USB-Geräte nur mit Zusatzprogrammen wie diesem startfähig gemacht werden.

Wenn Sie die in Tails enthaltene Version von LiveUSB Creator nicht ausführen können (wenn es Ihnen also nicht möglich sein sollte, Tails auf eine DVD zu brennen und von dort zu starten), verwenden Sie ein anderes Programm, das die gleiche Aufgabe verrichtet (siehe Abschnitt 3.3.4).

Dieser Vorgang funktioniert bei SD-Karten (einschließlich mini- und micro-SD) und für USB-Speichergeräte.

Um Tails auf ein startfähiges USB-Laufwerk zu bekommen, wird die Verwendung des Tails-Programms LiveUSB Creator empfohlen. Starten Sie das System mit Tails, klicken Sie oben links auf *Anwendungen* und zeigen Sie auf *Tails*, um sich die Werkzeuge zur Verwendung von Tails anzusehen, die zur Auswahl stehen.

Wählen Sie *Tails USB Installer*, um Tails LiveUSB Creator zu öffnen. Als Erstes wird ein Dialogfeld mit drei großen Schaltflächen angezeigt:

- *Clone & Install:* Hiermit kopieren Sie die zurzeit laufende Version von Tails auf ein USB-Gerät. Dabei werden alle Daten überschrieben, die sich auf dem Gerät befinden.
- *Clone & Upgrade:* Hiermit kopieren Sie die zurzeit laufende Version von Tails auf ein USB-Gerät, auf dem bereits eine ältere Tails-Version installiert ist. Die alte Installation wird dabei überschrieben. Andere Partitionen auf dem Gerät bleiben unberührt.
- *Upgrade from ISO:* Hiermit aktualisieren Sie ein USB-Gerät, auf dem zurzeit eine ältere Tails-Version läuft, von einer ISO-Datei mit einer jüngeren Version.

Die sicherste Vorgehensweise besteht darin, das System mit der neuesten Version von Tails von DVD zu starten und dann zu klonen. Dadurch übertragen Sie die neueste Version auf Ihr DVD-Laufwerk.

Bei *Clone & Install* wird das USB-Gerät gelöscht und die zurzeit laufende Tails-Version darauf installiert. Das bedeutet, dass jegliche Malware, die sich eventuell im Dateisystem des USB-Geräts befindet, entfernt wird. Allerdings gehen auch alle Daten verloren, die Sie darauf gespeichert haben.

Befinden sich bereits Daten auf dem Stick, können Sie die Option *Clone & Upgrade* wählen. Dadurch werden alle persistenten Speicherbereiche, die Sie auf dem Laufwerk angelegt haben, unverändert gelassen. Nur der Speicherbereich mit der älteren Tails-Installation wird gelöscht und mit der aktualisierten Software überschrieben.

Wenn Sie nicht in der Lage sind, Tails auf eine DVD zu brennen und von dort zu starten, aber über eine Tails-Version auf einem USB-Gerät verfügen, können Sie die aktuelle Tails-ISO-Datei herunterladen, Ihre Tails-Version starten und die letzte Option wählen, *Upgrade from ISO*.

Leider ist diese letzte Option mit einigen Risiken verbunden. Beispielsweise sollten Sie keine Verbindung zu einem Netzwerk aufnehmen, solange Sie die veraltete Tails-Version verwenden, denn wenn sie über eine Schwachstelle verfügt, laufen Sie sonst Gefahr, sich zu verraten.

Überprüfen Sie auch sehr sorgfältig die digitale Signatur der ISO-Datei, da Sie sie ungesehen auf dem USB-Gerät installieren. Bei den anderen Methoden ist es erforderlich, erst die aktuelle Version von Tails zu starten, sodass Sie mit Tor prüfen können, ob Sie in der Tat aktuell ist und korrekt läuft.

3.3.4 Tails manuell auf einem USB-Gerät installieren

Es ist möglich, Tails »per Hand« auf einem USB- oder SD-Gerät zu installieren (siehe »Manually Installing onto a USB Stick« auf *https://tails.boum.org/doc/first_steps/man ual_usb_installation/index.en.html*), aber dazu ist es erforderlich, ein Programm herunterzuladen und zu verwenden, das die gleichen Aufgaben erledigt wie LiveUSB Creator.

Wenn Sie auf diese Weise vorgehen, können Sie jedoch keinen dauerhaften Speicherbereich für Daten auf dem USB-Gerät einrichten.

Zurzeit werden die folgenden Programme für Windows, Mac OS X und Linux empfohlen :

- *Windows:* Von Pendrivelinux (*http://www.pendrivelinux.com*) gibt es das Programm Universal USB Installer (*http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3*), das eine startfähige Linux-Distribution auf ein USB-Gerät schreibt.
- *Mac OS X:* Zurzeit wird der EFI-Bootmanager (Extensive Firmware Interface) rEFInd (*http://sourceforge.net/projects/refind*) empfohlen.
- *Linux:* In gängigen Linux-Distributionen wie Ubuntu und Debian ist das Progarmm isohybrid enthalten.

Aktuelle Informationen zur Verwendung dieser Programme sind auf der Website des Tor-Projekts zu finden.

3.3.5 Tails aktualisieren (Clone & Upgrade)

Eine Tails-Installation auf einem beschreibbaren USB-Gerät können Sie aktualisieren, indem Sie im LiveUSB Creator (siehe Abschnitt 3.3.3) die Option *Clone & Upgrade* wählen.

Da der Creator die Version von Tails kopiert, die ausgeführt wird, müssen Sie die neueste Version herunterladen, installieren und auf DVD brennen und dann von dieser DVD starten, bevor Sie den Creator öffnen. *Clone & Upgrade* aktualisiert das USB-Gerät, lässt aber alle persistenten Speicherbereiche unberührt.

Merken Sie sich, dass Sie nicht von dem USB-Gerät starten dürfen, das Sie aktualisieren wollen, sondern von der neuesten Tails-Version auf DVD. Öffnen Sie den Creator erst, nachdem Sie das USB-Gerät eingesteckt haben. Um nicht durcheinanderzukommen, ist es für mich am einfachsten, das zu aktualisierende USB-Gerät erst von dem System abzuziehen, bevor ich die neueste Version von Tails starte.

3.3.6 Persistente Speicherbereiche auf dem Tails-Medium

Wenn Sie Tails von einem beschreibbaren Medium wie einem USB-Gerät starten, können Sie persistente Speicherbereiche verwenden. Dann können Sie eine verschlüsselte Partiton erstellen und Tails so einrichten, dass es dort möglich ist, Daten-, Anwendungs- und Konfigurationsdateien, Verzeichnisse, Webverlaufsdateien usw. zu speichern.

Bevor Sie persistente Speicherbereiche verwenden, sollten Sie sich jedoch über die möglichen Gefahren informieren. Lesen Sie dazu als Erstes den Artikel »Warnings About Persistence« (*https://tails.boum.org/doc/first_steps/persistence/warnings/index.en.html*), in dem einige der Probleme erklärt werden, die persistente Speicherbereiche für die Wahrung der Anonymität mit Tails bedeuten.

Es können unter anderem folgende Probleme auftreten:

- *Wenn Ihr Tails-Startlaufwerk mit persistentem Speicherbereich einem Gegner in die Hände fällt*, kann er es öffnen und findet dabei neben Tails auch den verschlüsselten Datenbereich. Wenn er bemerkt, dass geheime Informationen auf dem USB-Gerät gespeichert sind, wird er verschiedene Tricks anwenden, um sie zu entschlüsseln.
- *Wenn Sie den persistenten Speicherbereich nutzen*, können Sie die System- und die Anwendungskonfiguration ändern. Das kann zwar die Nutzung von Tails bequemer machen, wenn Sie beispielsweise die Netzwerkkonfiguration vereinfachen, oder den Einsatz eines Proxys erleichtern. Allerdings kann es auch zu Problemen führen, denn durch eine Änderung der Konfiguration können Sie versehentlich Informationen preisgeben oder die Anonymität unterlaufen, wenn Sie ein eindeutiges Systemprofil gestalten (siehe Panopticlick auf *https://panopticlick.eff.org*).

Durch die Nutzung von persistenten Speicherbereichen können Sie sogar versehentlich Konfigurationsdateien speichern, die Sie gar nicht aufbewahren wollen, indem Sie Dateien in einem Verzeichnis mit dem Benutzerordner verknüpfen oder ein benutzerdefiniertes Verzeichnis persistent machen (siehe Abschnitt 3.3.7).

- *In persistenten Speicherbereichen kann zusätzliche Software zur Verwendung mit Tails installiert werden.* Die neueste Version (0.18) enthält sogar eine experimentelle Funktion, die Zusatzsoftware Ihrer Wahl automatisch installiert – und bei Vorhandensein einer Netzwerkverbindung auch automatisch aktualisiert. (Eine kurze Erklärung finden Sie auf *https://tails.boum.org/doc/first_steps/persistence/configure/index.en.html#additional_packages*.)

Diese Funktion installiert auf Ihrem Tails-USB-Laufwerk anhand Ihrer Liste Software, sofern Sie mit dem APT-Installer von Debian installierbar ist. Das ist eine sehr vielseitige Möglichkeit, da Sie damit Ihren persönlichen Werkzeugkasten für die Verwendung mit Tails zusammenstellen können. Allerdings stellt dies auch ein großes Risiko dar.

Selbst die harmloseste Software kann Bugs (oder gar Malware) enthalten, die Ihre Anonymität gefährden oder zunichtemachen. Wenn Sie ein bestimmtes Programm benutzen müssen, das nicht in Tails enthalten ist, sollten Sie das besser nur tun, wenn Ihr System nicht mit dem Internet verbunden ist. Für Software, die eine Netzwerkverbindung erfordert, sollten Sie sich um Rat an das Tails- oder Tor-Projekt wenden.

- *Die Verwendung eines persistenten Speicherbereichs zur Installation nicht genehmigter Plug-Ins oder zum Umkonfigurieren der in Tails enthaltenen Plug-Ins kann Ihre Anonymität gefährden oder ganz aufheben.* Das gilt aus den gleichen Gründen, aus denen Sie vor der Installation von Browser-Plug-Ins in Tails gewarnt wurden.
- *Seien Sie bei der Verwendung eines persistenten Speicherbereichs vorsichtig.* Nutzen Sie ihn sparsam und nur dann, wenn Sie ihn wirklich brauchen. Schalten Sie die persistente Speicherung im Konfigurationsassistenten auch nur für die Elemente ein, die dauerhaft festgehalten werden müssen, und ändern Sie die Standardeinstellungen von Tails nur, wenn es absolut notwendig ist (und wenn Sie wissen, was Sie tun).
- *Greifen Sie nur auf den persistenten Speicherbereich zu, wenn es notwendig ist.* Wenn Sie eine persistente Partition auf Ihrem USB-Gerät installiert haben, können Sie beim Start von Tails auswählen, ob Sie darauf

zugreifen möchten oder nicht. Wenn nicht, wird die Partition nicht eingehängt und das Passwort für den Datenzugriff nicht eingegeben. Das kann die Nutzung Tor in Umgebungen sicherer machen, in denen Sie digital (durch Keylogger) oder optisch überwacht werden.

3.3.7 Persistente Speicherbereiche einrichten

Den Assistenten für die persistente Speicherung rufen Sie über *Anwendungen > Tails* oder *Anwendungen > Systemwerkzeuge* auf. Wählen Sie dort jeweils den Punkt *Configure persistent volume*.

Wenn Sie persistente Speicherbereiche verwenden möchten, bildet die Tails-Seite zu diesem Thema einen guten Ausgangspunkt (*https://tails.boum.org/doc/first_steps/persistence/index.en.html*). Hier finden Sie Links sowohl zu warnenden Hinweisen als auch zu Anleitungen für folgende Aufgaben:

- Erstellen und Einrichten eines persistenten Speicherbereichs (*https://tails.boum.org/doc/first_steps/persistence/configure/index.en.html*). Im Grunde genommen müssen Sie nur *Anwendungen > Tails > Configure persistent storage* wählen, den Eingabeaufforderungen folgen und die Anweisungen lesen. »Persistent Volume Features« (*https://tails.boum.org/doc/first_steps/persistence/configure/index.en.html#index3h1*) erklärt, welche Dateitypen und Konfigurationsdateien gespeichert werden können.
- Aktivieren und Nutzen des persistenten Speicherbereichs (*https://tails.boum.org/doc/first_steps/persistence/use/index.en.html*). Den persistenten Speicherbereich aktivieren Sie bei der Anmeldung, indem Sie ein Kontrollkästchen aktivieren und ein Passwort eingeben. Sie können auch einen schreibgeschützten Zugriff einrichten, sodass keine Änderungen auf das Medium geschrieben werden können. Nach dem Start können Sie im Ordner *Persistent* des Benutzerordners auf die Dateien zugreifen.

- Löschen des persistenten Speicherbereichs (*https://tails.boum.org/doc/first_steps/persistence/delete/index.en.html*). Wählen Sie *Anwendungen > Tails > Delete persistent storage* und klicken Sie auf die Schaltfläche *Delete*. Erstellen Sie dann eine verschlüsselte Partition (*https://tails.boum.org/doc/encryption_and_privacy/encrypted_volumes/index.en.html*), um das Laufwerk zu löschen. Dabei werden die alten Positionen für Tails und den persistenten Speicherbereich gelöscht. Als Nächstes müssen Sie den verfügbaren Speicherplatz auf sichere Weise bereinigen (*https://tails.boum.org/doc/encryption_and_privacy/secure_deletion/index.en.html#clean_disk_space*) und Tails dann neu installieren (*https://tails.boum.org/doc/first_steps/usb_installation/index.en.html*). Starten Sie das Gerät dann neu. Jetzt können Sie auch einen neuen persistenten Speicherbereich erstellen (*https://tails.boum.org/doc/first_steps/persistence/configure/index.en.html*).

3.3.8 Whisperback

Noch mehr als die meisten anderen Software-Projekte sind Tails (und Tor) auf genaue und aktuelle Informationen über Bugs im Code angewiesen. Da diese Software dazu dient, die persönliche Sicherheit und Freiheit zu gewährleisten, haben alle Benutzer ein eigennütziges Interesse daran, Bugs zu melden, damit sie so schnell wie möglich behoben werden.

Um das Melden von Fehlern zu vereinfachen – und sicher zu machen! – hat das Tails-Projekt das Programm Whisperback entwickelt. Wie in »Report a bug« beschrieben (*https://tails.boum.org/doc/first_steps/bug_reporting*), starten Sie Whisperback links oben auf dem Bildschirm über *Anwendungen > Systemwerkzeuge > Whisperback*.

3.3.9 KeePassX

Laut der eigenen Projektwebsite (*http://www.keepassx.org*) ist KeePassX »ein Open-Source-Passwortsafe, der Ihnen dabei hilft, Ihre Passwörter auf einfache und sichere Weise zu verwalten. Er nutzt eine stark verschlüsselte Datenbank, die mit einem Masterschlüssel gesichert ist.«

Zu den Funktionen gehören eine sichere (durch eine Passphrase geschützte) und durchsuchbare Datenbank für Benutzerpasswörter und ein Generator für starke Passwörter. Veröffentlicht wird das Programm als freie Software unter der GNU General Public Licence.

Wenn Sie Anmeldeinformationen im persistenten Speicherbereich ablegen, sollten Sie das mithilfe von KeePassX auf sichere Weise tun.

Im Artikel »Manage passwords with KeePassX« (*https://tails.boum.org/doc/encryption_and_privacy/manage_passwords/index.en .html*) finden Sie Anleitungen und eine Übersicht über die Vorteile der Verwendung von KeePassX:

- Mit KeePassX können Sie Ihre Passwörter in einer verschlüsselten Datenbank speichern, die durch eine einzelne Passphrase geschützt ist.
- Sie können gefahrlos auf alle passwortgeschützten Dienste zugreifen und müssen sich dafür nur eine einzige Passphrase merken.
- KeePassX generiert starke Passwörter, ohne dass es nötig ist, sie so zu gestalten, dass sie sich leicht merken lassen. Den Benutzern bietet sich der Vorteil der stärkstmöglichen Passwörter ohne die Schwierigkeit, sie sich merken zu müssen.

3.3.10 Metadata Anonymization Toolkit

Wenn eine Anwendungsdatei – ein Dokument einer Textverarbeitung, ein Foto, eine Audioaufnahme usw. – erstellt wird, schließt das dazu verwendete Programm oft *Metadaten* darin ein, also Daten über die Daten in der

Datei. Wenn Sie beispielsweise ein Word-Dokument öffnen, können Sie darin den Namen, die Telefonnummer und die E-Mail-Adresse der Person finden, auf deren Rechner das Dokument geschrieben wurde. Wenn Sie anonym bleiben wollen, möchten Sie natürlich nicht, dass Ihre Datendateien Ihre Identität preisgeben.

Das Metadata Anonymization Toolkit (MAT) ist eine Sammlung von Werkzeugen, um Metadaten aus Anwendungsdateien wie den folgenden zu entfernen:

- Portable Network Graphics (*.png*)
- JPEG (*.jpg*, *.jpeg* ...)
- Open Documents (*.odt*, *.odx*, *.ods* ...)
- Office OpenXml (*.docx*, *.pptx*, *.xlsx* ...)
- Portable Document Fileformat (*.pdf*)
- Tape Archives (*.tar*, *.tar.bz2*, *.tar.gz* ...)
- Zip (*.zip*)
- MPEG Audio (*.mp3*, *.mp2*, *.mp1* ...)
- Ogg Vorbis (*.ogg* ...)
- Free Lossless Audio Codec (*.flac*)
- Torrent (*.torrent*)

MAT ist offizieller Bestandteil des Tails-Projekts mit der Homepage *https://mat.boum .org/*.

Die Verwendung von MAT als GUI-Anwendung auf dem Tails-Desktop ist einfach, sofern Sie das Standardverhalten akzeptieren. Dabei erstellt MAT eine Kopie der zu bereinigenden Datei und nennt sie *<dateiname>.cleaned.<erweiterung>*. Die ursprüngliche Datei mit Metadaten ist also nach wie vor vorhanden, allerdings gibt es jetzt auch eine »saubere« Kopie.

MAT lässt sich auch an der Kommandozeile ausführen. Die verfügbaren Optionen können Sie sich ansehen, indem Sie das Programm wie folgt starten:

```
$ mat -d dateiname.erweiterung
```

Dieser Befehl gibt die in der Datei gespeicherten Metadaten zurück. Um die Datei zu bereinigen und eine Sicherungskopie zu speichern (das Standardverhalten der GUI-Anwendung), geben Sie folgenden Befehl ein:

```
$ mat -b dateiname.erweiterung
```

Der Befehl `mat` ohne Optionen gibt eine Hilfeanzeige mit einer Reihe weiterer Optionen zurück.

3.3.11 Claws Mail

Claws Mail (*http://www.claws-mail.org*) ist ein Open-Source-E-Mail-Client, der in Tails enthalten ist, um Ihnen anonymen Zugriff auf Ihr E-Mail-Konto zu geben.

Allerdings sollten Sie Claws nicht einsetzen, um über Tor auf Ihr persönliches E-Mail-Konto zuzugreifen, denn dadurch würde dieses Konto mit Ihrer Tor-Sitzung verknüpft. Claws eignet sich für den Zugriff auf ein anonym eingerichtetes E-Mail-Konto, das Sie nur über das Tor-Netzwerk aufsuchen.

Wenn Sie ein solches Konto haben, müssen Sie die E-Mail-Konfiguration einstellen (ein-/ausgehende Mailserver, Authentifizierung usw.). Wollen Sie das Konto regelmäßig verwenden, bietet es sich an, Ihre Claws-Profile und lokal gespeicherten E-Mails in einem persistenten Speicherbereich abzulegen (siehe Abschnitt 3.3.7).

Wenn es Ihnen zu unbequem ist, Ihren E-Mail-Zugang über mehrere Konfigurationskonsolen einzurichten, können Sie auch ein Konto auf einer Webmail-Site einrichten. Denken Sie jedoch daran, dass der Webmail-Dienst beim Zugriff über Tor möglicherweise feststellen kann, dass die Anmeldeinformationen für Ihr Konto von IP-Adressen stammen, die über die ganze Welt verstreut sind, was Folgen haben kann.

3.3.12 GNU Privacy Guard

GNU Privacy Guard (GnuPG, *https://www.gnupg.org*) ist der De-facto-Standard für Open-Source-Verschlüsselung. Mehr darüber erfahren Sie in meinem Buch »Simple Steps to Data Encryption«.

GnuPG ist in Tails installiert, allerdings gibt es im grafischen Desktop keine GnuPG-Anwendung.

Um eine Datei zu verschlüsseln oder zu signieren, eine signierte Datei zu validieren oder eine OpenPGP-Standarddatei zu entschlüsseln, rechtsklicken Sie im Dateibrowser darauf.

In der Textverarbeitung gedit (*Anwendungen* > *Zubehör*) können Sie auch Text verschlüsseln, entschlüsseln, signieren und verifizieren, indem Sie ihn markieren und die gewünschte Option auswählen.

Wenn Sie GnuPG in Tails regelmäßig nutzen, befinden sich Ihre eigenen Schlüssel (die keinerlei Rückschlüsse auf Ihre wahre Identität zulassen) sowie die Schlüssel der Personen, mit denen Sie korrespondieren, wahrscheinlich in einem GnuPG-Schlüsselbund. Es kann sehr bequem sein, diesen Schlüsselbund im persistenten Speicherbereich abzulegen.

Häufig ist es einfacher, GnuPG an der Kommandozeile auszuführen. Beispiele dafür, wie Sie mit GnuPG die Signaturen von Tails- und Tor-Downloads überprüfen, finden Sie in Anhang A.

4

Tor-Relays, Bridges und Obfsproxy

In diesem Kapitel geht es darum, wie Sie Tor erfolgreich einsetzen können, wenn ein mächtiger Gegner – etwa eine Regierung – den gesamten Netzwerkdatenverkehr von Tor filtert. Viele Benutzer können zwar schnell und einfach und ohne Probleme über Tor auf beliebige Internetdienste zugreifen, doch in manchen Ländern reicht das nicht aus.

Je nachdem, wie wichtig es Ihrem Gegner ist, unerwünschte Inhalte zu filtern, kann es sein, dass er jegliche Werkzeuge zur Umgehung von Zensurmaßnahmen verbietet. In manchen Fällen blockieren Firewalls eine Sitzung, wenn sie Tor-Netzwerkaktivitäten entdecken.

In diesem Kapitel erfahren Sie, wie eine solche landesweite Filterung abläuft.

Es gibt sehr viel akademische Forschung über Online-Anonymität und anonyme Netzwerkprotokolle. Das bedeutet, dass eine Menge sehr schlauer Leute daran arbeiten, Möglichkeiten zu finden, um Tor auszuhebeln – sowohl in der freien Welt als auch in abgeschotteten Gesellschaftsordnungen. Vor allem aber werden diese Forschungen veröffentlicht und stehen denjenigen zur Verfügung, die Online-Anonymität bekämpfen.

Wenn eine Lücke im Protokoll gestopft ist, versuchen die Gegner daher, andere Schwachstellen aufzuspüren, die es Ihnen erlauben, die Umgehung ihrer Zensurbestimmungen zu bekämpfen. Es herrscht also ein ständiges »Wettrüsten« zwischen dem Tor-Projekt und denjenigen, die Tor-Datenverkehr filtern wollen. Bei jedem Sieg einer Seite sieht sich die andere gezwungen, eine Lösung zu finden.

4.1 Wenn das normale Tor nicht ausreicht

Mit dem Begriff »Gegner« meine ich ganz allgemein eine wirtschaftliche oder politische Organisation, Gruppe oder Einzelperson, die über die erforderlichen Ressourcen verfügt, um Ihre gesamten Netzwerkaktivitäten zu überwachen und Sie dadurch daran zu hindern, frei zu kommunizieren, oder Sie für verbotene Aktivitäten zu bestrafen.

Wenn eine Regierung entscheidet, dass der gesamte Internetzugriff gefiltert werden muss, dann kann sie auch bestimmen, dass jegliche Werkzeuge, um die Zensur zu umgehen, blockiert werden, darunter auch Tor.

Ein gut dokumentierter Fall eines Landes, das Tor filtert, wird in dem Artikel »How China Is Blocking Tor« beschrieben (*http://arxiv.org/abs/1204.0447*). Er wurde 2012 geschrieben und beschreibt aufgrund von Forschungen vom Dezember 2012, wie die Große Chinesische Firewall (GFC) Tor-Datenverkehr aktiv blockiert (siehe auch den Artikel »How China Blocks the Tor Anonymity Network« in der MIT Technology Review auf *http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network*). Es geht hier darum, wie China im

Jahre 2011 den Tor-Datenverkehr sperren konnte, allerdings haben sich sowohl Tor als auch die Betreiber der GFC inzwischen immer wieder an die Maßnahmen der Gegenseite angepasst.

4.1.1 Wie China Tor blockiert hat

Die Abhandlung, verfasst von Philipp Winter und Stefan Lindskog von der Universität Karlstad, beschreibt, wie sie die Filterung des Tor-Datenverkehrs durch die GFC entdeckt haben. Tor-Verbindungen, die von China ausgingen, konnten innerhalb von 15 Minuten beendet werden. Außerdem wurden alle öffentlichen Tor-Relayknoten blockiert.

Die GFC hat den Zugriff auf drei verschiedene Weisen gesperrt, nämlich durch die Blockierung folgender Dinge:

- *Die Website des Tor-Projekts:* Versuche, eine Verbindung zur Website des Tor-Projekts auf *torproject.org* herzustellen, wurden gefiltert. Die Sperre dieser Website macht es für Benutzer in China schwierig, überhaupt erst an die erforderliche Tor-Software zu kommen, um anonyme Websitzungen zu starten.
- *Das öffentliche Tor-Netzwerk:* Es gibt neun Tor-Verzeichnisserver, die Informationen über die aktiven Tor-Relays verbreiten. Die Forscher stellten fest, dass die GFC in China den gesamten Zugriff zu diesen Servern blockierte. Die Firewall konnte auch fast alle Tor-Relays sperren, die im Tor-Konsensverzeichnis aufgeführt wurden.
- *Das Tor-Protokoll:* Um die Filterung der öffentlichen Tor-Relays zu umgehen, kamen Tor-Entwickler auf die Idee, »Bridge-Relays« zu verwenden. Dabei handelt es sich um Tor-Relays, die *nicht* öffentlich bekannt gegeben werden, sodass ein Gegner (z. B. China) sie nicht so leicht finden und filtern kann. Leider fanden die Chinesen eine Möglichkeit, Netzwerkverkehr zu erkennen, der das Tor-Protokoll verwendet. Das Ziel dieses Datenverkehrs wurde dann als Tor-Relay angesehen und seine IP-Adresse wurde den GFC-Filtern hinzugefügt.

Im weiteren Verlauf dieses Kapitels lernen Sie die Lösungen kennen, die zur Umgehung der GFC eingesetzt wurden, insbesondere Tor-*Bridges* (*https://www.torproject.org/docs/bridges.html.en*) und Obsfsproxy (*https://www.torproject.org/projects/obfsproxy.html.en*).

Ein Bridge-Relay funktioniert genauso wie jedes andere Tor-Transitrelay, allerdings wird es in keinen öffentlich zugänglichen Listen aufgeführt und wird im Allgemeinen nur dazu genutzt, an Orten, an denen öffentliche Tor-Relays blockiert werden, in das Tor-Netzwerk zu gelangen. Das Tor-Projekt experimentiert mit verschiedenen Mechanismen, um Tor-Benutzern Bridge-Relays auf eine Weise zur Verfügung zu stellen, die es staatlichen Gegnern schwer macht, sie zu erkennen.

Obfsproxy (»obfuscating proxy«, also »verschleiernder Proxy«) verschleiert die Header der Netzwerkpakete, sodass sie nicht wie Tor-Pakete, sondern wie regulärer Internetdatenverkehr aussehen. Dazu greift Obfsproxy auf zwei wichtige Prinzipien zurück:

- *Verschleierte Bridge:* Ein Zwischensystem, das verschleierten Tor-Datenverkehr annimmt und weiterleitet und dabei die Tor-Filterung aufgrund des Protokolls umgeht.
- *Plug-In-Transportproxy (Pluggable Transport):* Ein besonderes Plug-In-Programm, das rohen Tor-Netzwerkdatenverkehr annimmt und Netzwerkdatenverkehr ausgibt, der ein anderes Protokoll zu nutzen schient. Zurzeit sind bereits eine Reihe geplanter Transportproxys in Entwicklung (und eine kleine Anzahl ist bereits bereitgestellt). Mehr darüber erfahren Sie in »Tor: Pluggable Transports« auf *https://www.torproject.org/docs/pluggable-transports.html.en*).

4.1.2 Ist Tor ausgefallen oder brauchen Sie eine Bridge?

Wenn der Versuch, eine Verbindung mit Tor aufzunehmen, nicht klappt, kann das wie bei jeglicher Software drei Gründe haben:

- Sie machen etwas falsch.
- Etwas ist defekt.
- Jemand blockiert Tor.

Sie machen etwas falsch: Eines der Ziele bei der Gestaltung von Tor bestand darin, es für regelmäßige Anwender so benutzerfreundlich und leicht zugänglich zu machen wie möglich. Wenn Tor nicht korrekt funktioniert, sollten Sie das gleich bemerken, da der Tor-Browser beim Start die Prüfseite *https://check.torproject.org* aufruft. Liegt kein offensichtliches Problem vor (also etwa der Versuch, aus einer Region, in der Tor gesperrt wird, oder hinter einer Unternehmensfirewall auf Tor zuzugreifen), dann sollten Sie ein wenig Störungssuche betreiben. Als Erstes können Sie überprüfen, ob Sie auch eine validierte Version der Software installiert haben, und wenn das der Fall ist, das System neu starten. Einige Vorschläge zur Störungssuche erhalten Sie in »How to Troubleshoot Common Problems in Tor« (*https://securityinabox.org/en/tor_troubleshooting*).

Nehmen wir jedoch an, Sie haben alles genau überprüft, Sie haben Tor so eingerichtet, dass es die richtigen Ports und Proxyserver verwendet, und Sie haben keine andere Software, die Tor blockieren könnte (z. B. Antivirussoftware), dann besteht die nächste Möglichkeit darin, dass der zweite Punkt zutrifft.

Etwas ist defekt: Wie jede andere Software kann auch Tor Bugs aufweisen. Es werden relativ häufig Aktualisierungen des TBB veröffentlicht, sowohl um neue Funktionen einzuführen, als auch um Bugs zu korrigieren. Wenn Sie vermuten, dass ein Bug vorliegt, können Sie auf der Bug-Tracker- und Wiki-Seite des Tor-Projekts nachsehen, ob er bereits gemeldet wurde – oder ihn selbst melden (*https://trac.torproject.org/projects/tor*). Es ist auch möglich, in der Mailingliste des Tor-Projekts nachzusehen, ob es ein offenes Problem gibt und was Sie dagegen tun können. (Wo Sie dazu nachsehen müssen, erfahren Sie in Anhang C.)

Wenn es kein Bug ist und Sie alles richtig gemacht haben, dann kann es sein, dass Sie einer Filterung unterliegen, die den Zugang zu Tor verhindert. Mit anderen Worten ...

Sie werden blockiert: Jemand stört absichtlich Tor, um Verbindungen damit zu unterbinden. Beispielsweise wird in China und dem Iran aktiv nach Netzwerkdaten des Tor-Protokolls gesucht, um sie zu blockieren.

Manchmal ist es schwer, zwischen einem Defekt und einer Blockierung zu unterscheiden, da das Ergebnis – das Unvermögen, Verbindung mit Tor aufzunehmen – in beiden Fällen das gleiche ist. Das Gleiche gilt auch für den Unterschied zwischen Defekten aufgrund von versehentlichen Fehlern oder Bugs und solchen, die bewusst von Angreifern verursacht wurden.

Aus diesem Grund ist es eine gute Idee, Tor in einem relativ nachsichtigen oder offenen Netzwerk auszuprobieren, in dem keine Gegner aktiv sind, die gegen Sie arbeiten.

Weitere Informationen erhalten Sie unter den folgenden Adressen:

- Tor-Bugtracker (*https://trac.torproject.org/projects/tor/query*)
- Tor-Mailingliste (*https://lists.torproject.org/cgi-bin/mailman/listinfo*)

Wenn Sie sich in einem Netzwerk befinden, in dem Tor blockiert wird, brauchen Sie ein Bridge-Relay.

4.2 Bridge-Relays

Bridge-Relays (oder kurz Bridges) sind Tor-Relays, die nicht im Hauptverzeichnis aufgeführt sind. Da es keine vollständige öffentliche Liste gibt, kann ein Provider wahrscheinlich nicht alle Bridges blockieren, auch wenn er Verbindungen zu allen bekannten Tor-Relays filtert.

Listeneinträge für Tor-Bridges beginnen gewöhnlich mit dem Wort `bridge`, auf das die IP-Adresse und die Portnummer folgen:

```
bridge 172.16.27.48:443
```

Zwischen `bridge` und der IP-Adresse kann auch ein Modifizierer stehen:

```
bridge obfs3 172.16.27.48:420
```

Dieser Modifizierer gibt den Plug-In-Transportproxy (»Pluggable Transport«) an, der zusammen mit der Bridge verwendet werden soll. In diesem Beispiel steht `obfs3` für die Verschleierungsschicht des Tor-Protokolls, die dazu dient, Tor-Datenverkehr eben *nicht* wie Tor-Datenverkehr aussehen zu lassen. (Mehr darüber erfahren Sie weiter hinten.)

Einträge in Bridge-Listen enthalten manchmal ein zusätzliches kryptografisches Element, nämlich den *Fingerabdruck* des öffentlichen Schlüssels der Bridge. Das ermöglicht eine Authentifizierung, ist für die meisten Benutzer aber nicht notwendig, wenn sie Tor zur Verwendung einer Bridge einrichten, da das Tor-Netzwerkprotokoll sich für den Benutzer unsichtbar um die Authentifizierung kümmert. Ein Eintrag mit Fingerabdruck sieht wie folgt aus:

```
bridge obfs2 10.21.27.48:420
4352e58420e68f5e40bf7c74faddccd9d1349413
```

Da der Sinn einer Bridge darin besteht, einen Eintrittspunkt zum Tor-Netzwerk bereitzustellen, der sich vom Betreiber einer Firewall nicht leicht aufspüren lässt, lassen sich immer nur wenige Adressen von Bridges auf einmal per E-Mail oder im Web in Erfahrung bringen.

Alle Einzelheiten erfahren Sie im Dokument »Tor bridges specification« (*https://gitweb.torproject.org/torspec.git?a5blob_plain;hb5HEAD;f5attic/bridges-spec.txt*).

4.2.1 Bridge-Relays mithilfe der BridgeDB finden

Unter der folgenden Adresse unterhält das Tor-Projekt eine Webschnittstelle zu seiner Bridge-Datenbank (BridgeDB):

```
https://bridges.torproject.org/
```

Die Seite enthält eine kurze Erklärung von Tor-Bridges und ein Captcha, das Sie lösen müssen, um eine kurze Liste von Tor-Bridges in Empfang nehmen zu können.

Am unteren Rand der Seite wird außerdem ein Hinweis zur Verwendung von IPv6-Adressen gegeben. Diese Option ist nur sinnvoll, wenn Ihr System für IPv6 eingerichtet ist.

Außerdem gibt es die Möglichkeit, *Obfsproxy-Bridges* anzufordern, also solche, die den Tor-Datenverkehr mithilfe von Obfsproxy in ein Format umwandeln, das nach einem anderen Protokoll aussieht (um zu verhindern, dass er durch eine Firewall blockiert wird). Obfsproxy und Plug-In-Transportproxys (»pluggable transports«) werden weiter hinten in diesem Kapitel erklärt.

4.2.2 Bridge-Relays per E-Mail finden

Wenn Sie die Seite des Tor-Projekts nicht erreichen können, um dort die Adressen von Bridge-Relays anzufordern, haben Sie die Möglichkeit, eine E-Mail an den E-Mail-Roboter des Tor-Projekts zu senden, um solche Adressen zugeschickt zu bekommen. Dazu senden Sie eine Nachricht an folgende Adresse:

```
bridges@bridges.torproject.org
```

Der Text der Nachricht muss wie folgt lauten:

```
get bridges
```

Zurzeit erhalten Sie darauf nur dann eine Antwort, wenn Ihre E-Mail von einem Yahoo!- oder Gmail-Konto stammt. Das macht es für Gegner schwieriger, die Identität von mehr als einer Handvoll unveröffentlichter Bridge-Relays herauszufinden, da es bei Google und Yahoo! schwierig ist, Massen von gefälschten E-Mail-Adressen zu generieren. Die Verwendung von Gmail oder Yahoo ist außerdem erforderlich und empfehlenswert, da beide HTTPS verwenden, sodass die Nachricht verschlüsselt wird. Der Gegner kann daher nicht erkennen, dass Sie mit Tor kommunizieren und Bridge-Relays anfordern, und die Adressen in der Antwort nicht lesen.

Die Antwort vom Tor-Projekt sehen Sie in Abbildung 4.1.

```
[This is an automated message; please do not reply.]

Here are your bridge relays:

bridge 10.71.137.223:443
bridge 172.16.94.243:443
bridge 192.168.96.125:9001
```

Abbildung 4.1: Die Antwort des Tor-E-Mail-Robots unter `bridges@bridges.torproject.org` sieht wie in diesem Beispiel aus. Die hier gezeigten Adressen sind nur Beispiele und entsprechen nicht den Adressen tatsächlich vorhandener Bridges.

4.2.3 Andere Möglichkeiten Bridges zu finden

Wenn Sie weder per E-Mail noch über das Web an die Adresse eines Bridge-Relays gelangen können, haben Sie noch die Möglichkeit, auf persönliche Kommunikation zurückzugreifen. Falls Sie also mit jemandem Kontakt aufnehmen können, der Zugriff auf Tor hat, können Sie ihn bitten, sein Tor-System als Bridge einzurichten und Ihnen die IP-Adresse und den Port zu nennen. Alternativ können Sie (falls möglich) auch versuchen, sich auf irgendeine Weise an das Tor-Projekt zu wenden (per E-Mail, über die Website oder die Tor-Mailingliste), wo Ihnen wahrscheinlich irgendjemand weiterhelfen kann.

4.3 Tor zur Verwendung eines Bridge-Relays einrichten

Wenn Sie die Adresse einer Tor-Bridge haben, öffnen Sie in Vidalia *Einstellungen > Netzwerk* und klicken dann auf *Mein Provider blockiert Verbindungen zum Tor-Netzwerk*. Fügen Sie dann wie in Abbildung 4.2 gezeigt die einzelnen Bridge-Adressen hinzu. (Beachten Sie, dass die in dieser Abbildung gezeigten Adressen nicht echt sind.)

Die Angabe von mehr als einer Bridge-Adresse macht Ihre Tor-Verbindung stabiler, falls eine oder mehrere Bridges nicht mehr erreicht werden können.

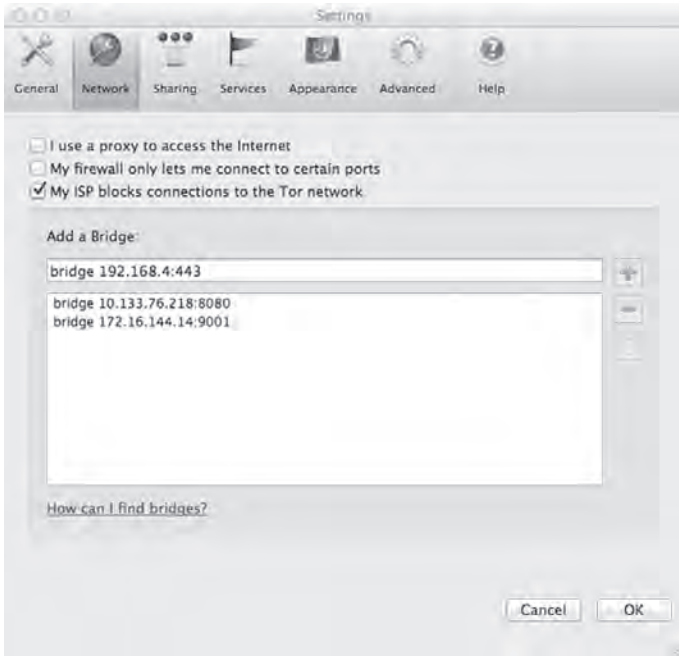

Abbildung 4.2: Hinzufügen von Bridge-Adressen in Vidalia. Die hier gezeigten Adressen sind nicht gültig, sondern stellen nur Beispiele dar.

Zurzeit können Sie auch IPv6-Bridges sowie Bridges anfordern, die bestimmte Plug-In-Transportproxys unterstützen. Geben Sie dazu anstelle von `bridges` folgende Schlüsselwörter im Text der E-Mail an:

- `ipv6`: Fordert IPv6-Bridges an.
- `transport` *NAME*: Fordert den Plug-In-Transportproxy mit dem angegebenen Namen an, z. B. `transport obfs2`.

Es werden noch weitere Plug-In-Transportproxys entwickelt. Die aktuellsten Informationen über die Verfügbarkeit erhalten Sie in »Tor: Pluggable Transports« auf *https://www.torproject.org/docs/pluggable-transports.html.en*).

4.4 Plug-In-Transportproxys und Obfsproxy

Die einfachsten Arten von Firewalls funktionieren ähnlich wie ein gewöhnlicher Nezwerkrouter: Sie nehmen Pakete von Hosts auf der einen Seite an und leiten sie auf der Grundlage der IP-Adressen von Sender und Empfänger weiter. Wenn ich versuche, eine Nachricht an einen Host zu schicken, den der Betreiber der Firewall als verboten einstuft, wird das Paket von der Firewall einfach verworfen, anstatt es ans Ziel zu leiten.

Gegner können ihre Firewalls so einrichten, dass Pakete von und zu Tor-Relays verworfen werden. Dazu müssen sie selbst Verbindung mit Tor aufnehmen und die öffentliche Liste der Tor-Relays herunterladen. Diese Sperrmaßnahme können Sie umgehen, indem Sie wie weiter vorn beschrieben Bridge-Relays verwenden. Es gibt jedoch noch ausgeklügeltere Vorgehensweisen, um Datenverkehr zu sperren.

Eine dieser Techniken ist die DPI (Deep Packet Inspection, »eingehende Paketuntersuchung«). Eine DPI-Firewall blockiert nicht nur den Datenverkehr von und zu Tor-Relays, sondern kann sich die Netzwerkpakete auch genauer ansehen. Sie beschränkt sich also nicht auf die Quell- und Zieladresse, sondern untersucht auch andere Teile des Paketheaders und die Art und Weise, wie das Paket aufgebaut und formatiert ist. Mit DPI können Gegner Tor-Daten erkennen und blockieren, auch wenn sie über ein Bridge-Relay gesendet werden.

Aber das ist noch nicht alles: Anschließend kann der Gegner auch den Zugriff zu allen Adressen sperren, die Tor-Datenverkehr senden oder empfangen, was die Nützlichkeit der Bridges herabsetzt oder gar völlig aufhebt.

Um DPI-Firewalls zu umgehen (zu denen auch die GFC gehört), hat das Tor-Projekt Plug-In-Transportproxys (»pluggable transports«) entwickelt. Auf der entsprechenden Website (*https://www.torproject.org/docs/pluggable-transports.html.en*) heißt es dazu:

> *Plug-In-Transportproxys wandeln den Tor-Datenverkehr zwischen Client und Bridge um. Dadurch sehen Zensoren, die den Datenverkehr zwischen*

Client und Bridge überwachen, unschuldig wirkenden Datenverkehr statt des tatsächlichen Tor-Datenverkehrs. Externe Programme können über die API für Plug-In-Transportproxys mit Tor-Clients und Tor-Bridges kommunizieren, was es einfacher macht, interoperable Programme zu erstellen.

Die Verwendung eines Plug-In-Transportproxys entspricht also dem alten Trick, Schmuggelware in harmlos aussehenden Objekten zu verstecken, also etwa Diamanten in Teddybären einzunähen. Über die Programmierschnittstelle für Plug-In-Transportproxys können Entwickler Werkzeuge herzustellen, die Tor-Pakete verschleiern und als harmlosen Webdatenverkehr erscheinen lassen.

4.4.1 Plug-In-Transportproxys

Das Schachtelwort Obfsproxy ist praktisch unaussprechlich und bedeutet eigentlich »obfuscating proxy«, also »verschleiernder Proxy«. Es handelt sich dabei um ein Werkzeug zum Umgehen von Zensurmaßnahmen, das den Tor-Datenverkehr zwischen Client und Bridge so verändert, dass er wie ganz normaler Internetdatenverkehr aussieht.

Zurzeit werden für Tor vier Transportproxys verwendet, nämlich Obfsproxy (*https://www.torproject.org/projects/obfsproxy.html.en*), Flash Proxy (*http://crpyto.stanford.edu/flashproxy/*), Fteproxy (wandelt Tor-Datenverkehr mithilfe von Format-Transforming Encryption in beliebige andere Formate um; *https://eprint.iacr.org/2012/494*) und Obfsclient (*https://github.com/Yawning/obsclient*).

Obfsproxy ist das Softwareframework, in dem die Plug-In-Transportproxys implementiert sind. Es ist in der normalen Version des TBB enthalten und unterstützt zurzeit zwei Arten von Plug-In-Transportproxys, nämlich obfs2 und obfs3.

Es sind weitere Transportproxys in Entwicklung, darunter die folgenden, die auch auf der entsprechenden Webseite des Tor-Projekts erklärt werden (*https://www.torproject.org/docs/pluggable-transports.html.en*):

- *StegoTorus:* Hierbei handelt es sich um eine Fork-Entwicklung von Obfsproxy, die das ursprüngliche Projekt erweitert, sodass es (1) Tor-Streams auf mehrere Verbindungen aufteilt, um einer Erkennung anhand typischer Paketgrößen zu entgehen und (b) den Datenverkehr in Spuren einbettet, die nach HTML, JavaScript oder PDF aussehen (*https://gitweb.torproject.org/stegotorus.git*).
- *SkypeMorph:* Transformiert Tor-Datenverkehr, sodass er wie Skype-Video-Datenverkehr aussieht (*http://cacr.uwaterloo.ca/techreports/2012/cacr2012-08.pdf*).
- *Dust:* Ziel dieses Projekts ist paketgestütztes (statt verbindungsgestütztes) Protokoll zum Schutz gegen DPI.

Wenn diese Projekte sich als nützlich erweisen und eine brauchbare Entwicklungsstufe erreichen, werden sie wahrscheinlich in irgendeiner Form in das TBB aufgenommen.

4.4.2 Flash Proxy

Mit Flash Proxy kann jeder seine Webbrowser zu einem Mini-Proxy machen, wenn er Zugriff auf Tor benötigt. Ursprünglich bezog sich die Bezeichnung »Flash« auf Adobe Flash, das mittlerweile aber nicht mehr Bestandteil von Flash Proxy ist. Denken Sie bei »Flash« lieber an »Blitz«, also an etwas, das kurz aufleuchtet und sofort wieder verschwindet.

Wenn Sie eine Webseite veröffentlichen, so können Sie ihr eine Flash-Proxy-Markierung (»Badge«) hinzufügen. Dieses Badge ist mit dem JavaScript-Code von Flash Proxy verlinkt, der aus Ihrem Computer vorüber-

gehend einen Proxyserver macht. Sie können Ihren Browser also als Proxy verwenden, aber nur so lange, wie die Seite mit dem Badge darin geöffnet ist.

Flash Proxy ist im normalen TBB enthalten, sodass Sie es zur Verbindungsaufnahme mit Tor nutzen können. Die Verwendung kann jedoch ein bisschen kompliziert sein, da Sie Ihr System möglicherweise zur Portweiterleitung einrichten müssen. Lesen Sie die aktuellen Anleitungen für die Verwendung von Flash Proxy (*https://trac.torproject.org/projects/tor/wiki/FlashProxyHowto*).

4.4.3 Plug-In-Transportproxys verwenden

Obfsproxy ist im TBB enthalten. Um dieses Framework zu installieren, folgen Sie den Anweisungen auf der Website des Tor-Projekts (*https://www.torproject.org/projects/obfsproxy-instructions.html.en*; für Benutzer von Debian- oder Ubuntu-Systemen siehe *https://www.torproject.org/projects/obfsproxy-debian-instructions.html.en*.)

Wenn Sie Tor mit installiertem Obfsproxy öffnen, werden wie üblich Vidalia und der Tor-Browser geöffnet, allerdings erfolgt der Zugriff jetzt über Obfsproxy-Bridges statt über normale Bridges oder das unverschleierte Internet. Ein Beispiel für die Anzeige von Obfsproxy-Bridges sehen Sie in Abbildung 4.3.

Um an die Adressen von Obfsproxy-Bridges zu gelangen, können Sie die Techniken verwenden, die schon weiter vorn zum Finden von Bridges beschrieben wurden (E-Mail und Web).

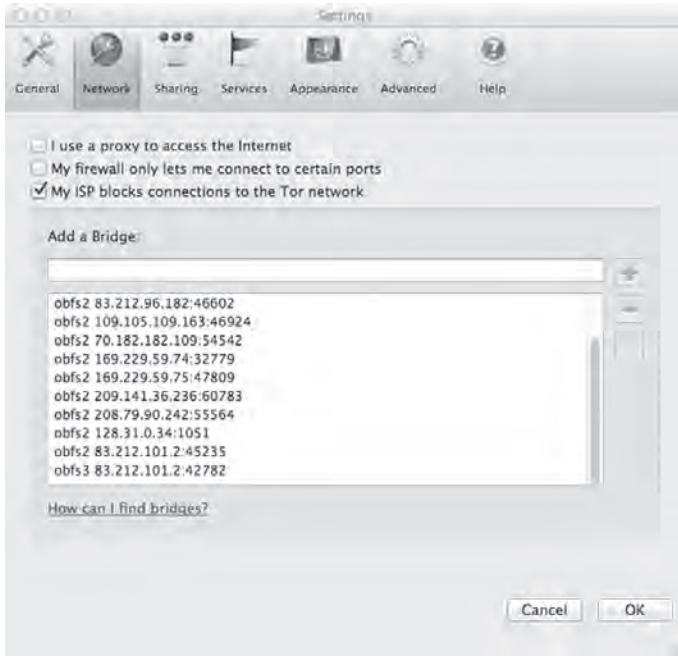

Abbildung 4.3: Bei der Verwendung von Obfsproxy zum Umgehen von DPI-Firewalls werden Obfsproxy-Bridges verwendet.

Tor-Ressourcen bereitstellen

Dieses Kapitel erklärt, wie Sie Ihre Ressourcen anderen für den Zugriff auf das Anonymisierungsnetzwerk von Tor zur Verfügung stellen können und welche Schwierigkeiten und Gefahren damit verbunden sind.

5.1 Einen Beitrag zum Tor-Netzwerk leisten – wie und warum?

Je mehr Computer über das Tor-Netzwerk miteinander verbunden sind, umso besser funktioniert es, denn je mehr Rechner Tor-Netzwerkdaten im Internet weiterleiten, umso unwahrscheinlicher ist es, dass ein Tor-Benutzer in dieser Masse auffällt.

Es ist eine gute Idee, sich mit Tor zu verbinden und Ihre Verbindung aus Austritts- oder Transitrelay oder Bridge zur Verfügung zu stellen, um Ihre überschüssige Netzwerkbandbreite mit anderen zu teilen – sofern dies nach

den Vertragsbedingungen Ihres Providers zulässig ist. Wenn ja, kann es für Sie ein befriedigender Gedanke sein, dass Sie politischen Aktivisten helfen, gefahrlos zu kommunizieren, oder dass über Ihre Bandbreite diplomatische Verlautbarungen aus aller Welt übertragen werden.

Die wirkungsvollste Möglichkeit, Bandbreite bereitzustellen, besteht jedoch darin, gemeinnützigen Vereinen, die Austrittsrelays betreiben, Geld zu spenden. Zurzeit gibt es zwei davon:

- *torservers.net (https://www.torservers.net):* Ein deutscher gemeinnütziger Verein, der eine breite Palette von Austrittsrelays unterhält.
- *Noisebridge (https://www.noisebridge.net/wiki/Noisebridge_Tor):* Eine gemeinnützige Organisation in den USA (nach § 501c3 des amerikanischen Rechts), die Spenden annimmt, um ihre bestehende Kapazität an Austrittsrelays auszubauen.

Wenn Sie über entsprechende Fähigkeiten in System- und Netzwerkverwaltung verfügen und die Vertragsbedingungen Ihres Providers es erlauben, können Sie auch Ihr eigenes System als Tor-Relay einrichten.

5.2 Welche Möglichkeiten haben Sie?

Bei der Konfiguration eines Relay müssen Sie sich die beiden folgenden wichtigen Fragen stellen:

- Soll an diesem Relay ein Austritt ins öffentliche Internet möglich sein?
- Wird das Relay als normales oder als Bridge-Relay geführt?

Beim zweiten Punkt ist zu beachten, dass für die Verbreitung der Relay-Adressen im Tor-Netzwerk zwei verschiedene Protokollstrukturen zuständig sind: Die *Bridge-Instanz* kümmert sich um alle Adressen für Tor-Bridges, die *Verzeichnisinstanz* dagegen um die Adressen aller regulären Tor-Relays (Transit- und Austrittsrelays).

Die verschiedenen Arten von Relays (Bridge, Austritts- oder Transitknoten) können also danach eingeteilt werden, was sie zulassen:

- *Austrittsrelay:* Ein Relay, das in den normalen Verzeichnisinstanzen veröffentlicht wird und einen Austritt ins öffentliche Internet erlaubt. Sie können an jeder Stelle in einer Tor-Verbindung eingesetzt werden (also auch im ersten und zweiten Hop), sind aber die einzigen, die auch im letzten Hop verwendet werden können.
- *Transitrelay:* Ein Relay, das in den normalen Verzeichnisinstanzen veröffentlicht wird, aber keinen Austritt ins öffentliche Internet erlaubt. Transitrelays können nur im ersten und zweiten Hop einer Tor-Verbindung eingesetzt werden. Sie werden auch *Mittelknoten* oder *Nicht-Austrittsknoten* genannt.
- *Bridge:* Ein Relay, das nur in der Brige-Instanz veröffentlicht wird. Es kann nur im ersten Hop einer Tor-Verbindung eingesetzt werden und das auch nur für Tor-Clients, die zur Verwendung dieser Bridge eingerichtet sind.

Um Ihre Verbindung zur Verfügung zu stellen, klicken Sie in Vidalia auf die Verknüpfung *Weiterleitung einrichten*. Dadurch gelangen Sie zur Registerkarte *Beteiligung* von Vidalia (siehe Abbildung 5.1).

Hier haben Sie die Auswahl, ein Nicht-Austrittsrelay (Transitrelay), ein Austrittsrelay oder eine Bridge zu betreiben:

- *Austrittsrelay:* Ein Tor-Knoten, der eine Weiterleitung vom Tor-Netzwerk ins öffentliche Internet zulässt. Austrittsrelays kennen die IP-Adressen der Dienste, die über Tor angesprochen werden, können daraus aber keine Rückschlüsse darauf ziehen, welche Tor-Clients diesen Zugriff wünschen. Jemand, der das Netzwerk überwacht, kann erkennen, dass Sie einen Tor-Austrittsknoten betreiben, und auch feststellen, welche Dienste darüber in Anspruch genommen werden, die Tor-Clients aber nicht ermitteln.

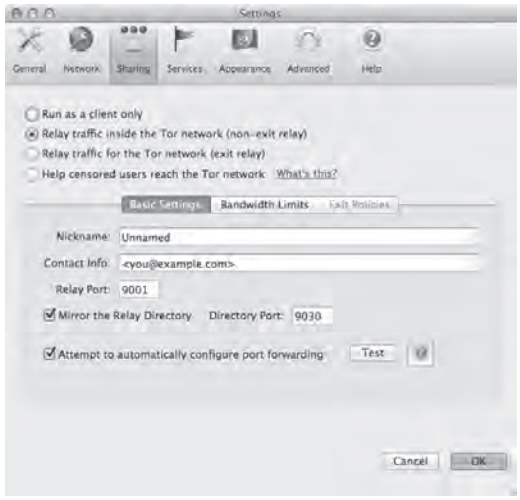

Abbildung 5.1: Einrichten eines Tor-Relays in Vidalia

- *Nicht-Austrittsrelays:* Ein Tor-Knoten, der Tor-Datenverkehr von anderen Tor-Knoten entgegennimmt. Dabei kann es sich sowohl um Tor-Clients als auch um andere Transitrelays handeln. Jemand, der das Netzwerk überwacht, kann erkennen, dass Sie einen Tor-Transitknoten betreiben, aber der gesamte Tor-Datenverkehr ist verschlüsselt, sodass Personen, die Zugriff auf Ihr System oder Ihr Netzwerk haben, nichts damit anfangen können.
- *Bridge:* Ein Tor-Knoten, der Tor-Datenverkehr von Tor-Clients annimmt, um den ersten Hop einer Tor-Verbindung aufzubauen. Die Adressen von Bridge-Relays können Tor-Benutzer im Web oder per E-Mail in Erfahrung bringen (siehe Kapitel 4). Da Ihre IP-Adresse nicht öffentlich aufgeführt oder verlinkt ist, sollte eine Firewall, die öffentliche Tor-Relays blockiert, nicht in der Lage sein, Ihre Bridge zu sperren. Führt die Firewall jedoch DPI (Deep Packet Inspection) durch, kann Ihr System als Tor-Relay erkannt werden. Jemand, der das Netzwerk überwacht, kann erkennen, dass Sie ein Tor-Relay betreiben, und auch die IP-Adressen der Tor-Clients herausfinden, die dieses Relay nutzen, aber nicht ermitteln, zu welchen Zielen im öffentlichen Internet die Verbindungen dieser Clients führen.

Welche Option sollten Sie wählen? Auf der Website des Tor-Projekts heißt es (auf *https://www.torproject.org/docs/fq.html.en#RelayOrBridge*):

> *Sollten Sie nun also ein normales Relay oder ein Bridge-Relay betreiben? Wenn Sie Mengen an Bandbreite zur Verfügung haben, sollten Sie auf jeden Fall ein normales Relay ausführen. Wenn Sie bereit sind, als Austritt zu fungieren, sollten Sie auf jeden Fall ein normales Relay ausführen, da wir mehr Austrittsknoten benötigen. Wenn Sie nicht als Austritt fungieren können und nur wenig Bandbreite zur Verfügung haben, stellen Sie eine Bridge bereit. Vielen Dank für Ihren Beitrag!*

5.3 Welche Risiken gehen Sie ein?

Ihre Netzwerkressourcen zu Tor beizutragen hat auch einen Nachteil. Der Vorteil besteht in dem befriedigenden Gefühl, eine gute Tat zu tun, doch Sie wissen ja: Jede gute Tat findet ihre Strafe. Aber im Ernst, die möglichen Risiken fallen in die folgenden drei Kategorien:

- Beschwerden über Missbrauch
- Kosten für Bandbreite
- Ihr Provider findet es nicht gut

Wenn Sie Ressourcen auf diese Weise für Tor zur Verfügung stellen, werden natürlich ein Teil Ihrer Bandbreite und Ihrer Systemkapazität für Tor-Verbindungen genutzt. Das kann für Sie Kosten verursachen (wenn Sie keinen Pauschaltarif für »unbegrenzte« Dienste haben, sondern Ihren Provider nach genutzter Bandbreite bezahlen). Wie bereits erwähnt, bevorzugen es manche Provider, wenn ihre Kunden ihre Bandbreite nicht zur Unterstützung von Tor bereitstellen. Um Probleme zu vermeiden, sollten Sie mit Ihrem Provider sprechen, bevor Sie Ihr System als Relay irgendeiner Art einrichten.

Das lässt noch den Punkt der Missbrauchsbeschwerden offen. Einzelheiten finden Sie unter »So what should I expect if I run an exit relay?« (*https://www.torproject.org/docs/faq-abuse.html.en#TypicalAbuses*). Es handelt sich dabei meistens um Fälle der Art, dass ein anonymer Benutzer über Ihr Austrittsrelay eine Verbindung zu einem Gmail-Konto aufnimmt, das aus irgendeinem Grund von den Strafverfolgungsbehörden überwacht wird. Da Ihr System im Namen des anderen Systems arbeitet, wird Ihre IP-Adresse mit diesem Konto verknüpft. Dann müssen Sie den Strafverfolgungsbehörden erklären, dass Sie nur einen Tor-Austrittsknoten betreiben.

Wenn Sie Systemadministrator sind, können Sie die Antwort auf solche Beschwerden ziemlich einfach automatisieren, aber normale Benutzer tun besser daran, solche Probleme ganz zu vermeiden.

Alternativ können Sie ein Austrittsrelay auch so einrichten, dass es Datenverkehr abweist, der für Sie Schwierigkeiten bedeuten kann.

5.4 Einrichtung eines Tor-Relays

Der erste Schritt, um Ihr System als Tor-Relay einzurichten, besteht darin, Tor auszuführen. Dabei spielt es keine Rolle, ob Sie reguläres Tor oder Obfsproxy verwenden (siehe Kapitel 4).

Die Einrichtung eines Tor-Relays erfordert umfassendere technische Kenntnisse als die reine Nutzung von Tor, und es lohnt sich nicht, wenn Sie immer nur kurze Tor-Sitzungen auf Ihrem Computer durchführen. Ein Relay zu betreiben bedeutet gewöhnlich, dass Sie sich dazu verpflichten, Tor für längere Zeit laufen zu lassen, etwa für Tage, Wochen oder sogar Monate, und nicht nur für wenige Stunden.

Unter gewissen Umständen kann es jedoch auch nützlich und hilfreich sein, ein kurzlebigeres Relay auszuführen, insbesondere wenn Sie jemanden kennen, der ein ansonsten unbekanntes Bridge-Relay benötigt (mehr dazu weiter hinten). Als Erstes müssen Sie sich die Systemvoraussetzungen

ansehen und die Folgen bedenken, die der Betrieb eines Tor-Relays nach sich ziehen kann. Nachdem Sie sich entschieden haben, welche Art von Relay Sie unterhalten möchten, führen Sie die weiter hinten beschriebenen Einrichtungsverfahren durch.

5.5 Anforderungen und Konsequenzen

Grundvoraussetzung für den Betrieb eines Tor-Relays ist zurzeit eine zuverlässige Netzwerkverbindung mit einer verfügbaren Bandbreite von mindestens 20 Mbit/s für Tor-Datenverkehr. Nachdem das Relay ganz in die Tor-Infrastruktur eingefügt ist, werden Sie wahrscheinlich feststellen, dass es eine Menge an Bandbreite verschlingt. Das sollten Sie auch berücksichtigen.

Bevor Sie das Relay einrichten, sollten Sie nachlesen, wie Sie das auf sichere Weise tun und wie Sie mit Problemen umgehen, die beim Betrieb eines Tor-Relays auftreten können.

Es ist nur selten eine gute Idee, ein Relay in Ihrem Heimnetzwerk zu betreiben. Das kann die Vertragsbedingungen Ihres Providers verletzen und erhebliche Spitzen in der Netzwerknutzung hervorrufen (was Ihre Gebühren in die Höhe treiben oder für eine Beendigung des Dienstes sorgen kann). Außerdem kann die Sache sehr kompliziert werden, wenn sich der Datenverkehr des Tor-Relays und Ihrer eigenen Netzwerknutzung vermischen. Lesen Sie zur Vorbereitung den Artikel »Tips for Running an Exit Node with Minimal Harassment« (*https://blog.torproject.org/blog/tips-runningexit-node-minimal-harassment*).

Im Idealfall befindet sich Ihr Tor-Relay also in einem eigenen Netzwerk und auf einem anderen System als dem, das Sie normalerweise nutzen. Angeschlossen werden sollte es über einen Provider, der eine solche Verwendung zulässt, und die Netzwerkverbindung sollte zuverlässig sein und ausreichend Bandbreite bieten. Das absolute Minimum beträgt zurzeit 2 Mbit/s. Beachten Sie, dass der auf der Tor-Website angegebene offizielle Mindestwert in Zukunft steigen kann.

Bevor Sie ein Transit- oder Austrittsrelay einrichten, sollten Sie sich zunächst an einem Bridge-Relay versuchen, da dazu nicht ganz so viel Bandbreite erforderlich ist und die Auswirkungen auf den Betreiber geringer sind.

5.6 Nicht-Austrittsrelay

Um ein System als Nicht-Austrittsrelay einzurichten, wählen Sie in Vidalia die Option *Relais-Verkehr im Tor-Netzwerk (kein ausgangs Relais)* [sic!]. Daraufhin können Sie folgende Grundeinstellungen vornehmen:

- *Spitzname:* Der Name, durch den Relay im Netzwerk bezeichnet wird. Ein solcher Spitzname ist zwar optional, aber sehr nützlich, vor allem, wenn Sie mehr als ein Relay betreiben.
- *Kontaktinformation:* Eine E-Mail-Adresse (plus OpenPGP-Schlüssel-ID oder Fingerabdruck, falls gewünscht und verfügbar). Auch diese Angabe ist optional. Sie werden über die hinterlegte Adresse nur angesprochen, wenn es ein wichtiges Sicherheitsupdate für Tor gibt oder wenn ein Problem mit Ihrem Relay vorliegt.
- *Verteiler-Port:* Die Portnummer, auf der Ihr System auf Tor-Netzwerkanfragen lauscht. Der Standardport ist 9001, aber wenn er blockiert wird, kann ein anderer Port verwendet werden (meistens 443).
- *Das Tor-Verteiler-Verzeichnis spiegeln:* Dies bedeutet, dass Ihr Relay als Informationsquelle für Tor-Clients dient, die nach Informationen über andere Tor-Relais suchen, um ihre Verbindungen einzurichten. Diese Einstellung ist für Transit- und Austrittsrelays optional, für Bridges aber obligatorisch. Die hier angegebene Portnummer muss eine andere sein als der zuvor angegebene Relayport (»Verteiler-Port«). Der Standardwert lautet 9030.
- *Versuche automatisch, die Port-Weiterleitung zu konfigurieren:* Die Schaltfläche *Test* gehört zu dieser Option und prüft, ob eine automatische Einrichtung der Portweiterleitung möglich ist. Eine Portwei-

terleitung ist für Relays hinter Routern oder Firewalls erforderlich, die den eingehenden Netzwerkzugriff auf Ihr System normalerweise verstecken oder unterbinden würden.

Auf einer zweiten Registerkarte können Sie Bandbreiteneinschränkungen angeben. Es stehen verschiedene Werte für den Anteil Ihres Hochgeschwindigkeits-Internetzugangs zur Auswahl, den Sie für Tor-Datenverkehr zur Verfügung stellen möchten. Der Mindestwert beträgt 256 Kbit/s, der Höchstwert 1,5 Mbit/s. Sollte das für Sie immer noch zu hoch bzw. zu niedrig sein, können Sie auch eine eigene durchschnittliche oder maximale Bandbreite angeben, die Sie für Tor bereitstellen möchten.

5.7 Austrittsknoten

Die Einrichtung eines Austrittsknotens ruft mehr Schwierigkeiten hervor, da Ihr System dann in direktem Kontakt mit den Servern steht, die der Tor-Client zu erreichen versucht. Das kann ein Problem darstellen, wenn diese Server für anstößige Zwecke verwendet werden und Ihre IP-Adresse mit Aktivitäten in diesem Zusammenhang in Verbindungg gebracht wird.

Ein Austrittsrelay richten Sie auf die gleiche Weise ein wie ein Nicht-Austrittsrelay, wobei Sie jedoch zusätzlich die Möglichkeit haben, Austrittsrichtlinien (»Exit-Regeln«) festzulegen. Damit können Sie einschränken, zu welchen Arten von Servern Tor-Clients über Ihr Relay zugreifen können. Wenn Sie den Zugang beispielsweise auf *Sichere Websites (SSL)* beschränken, leitet Ihr Relay nur Datenverkehr an Websites weiter, die HTTPS unterstützen. Anderer Datenverkehr wird nicht akzeptiert.

Die Austrittsrichtlinien gehören zu den Angaben über Ihr Relay, die im Tor-Netzwerk bekannt gemacht werden. Wenn ein Benutzer also einen E-Mail-Server erreichen möchte, die entsprechenden Protokolle aber in Ihren Austrittsrichtlinien blockiert sind, muss er sich für die Verbindung ein anderes Austrittsrelay suchen.

Durch die Deaktivierung *aller* Protokolle machen Sie aus Ihrem Austrittsein Nicht-Austrittsrelay. Das ist einfacher, als gleich bei der Einrichtung anzugeben, dass Sie eine solche Art von Relay betrieben möchten. Es ist zwar wünschenswert (und für die Zwecke des Tor-Netzwerks am praktischsten), wenn Ihr Austrittsrelay so viele Protokolle wie möglich unterstützt, allerdings kann man das nicht von jedem verlangen, der bereit ist, seine Systemressourcen zur Verfügung zu stellen. Auch ein reiner Eintrittsknoten ist für das Tor-Netzwerk nützlich und wertvoll, und das Gleiche gilt auch für einen reinen HTTPS-Austrittsknoten. Damit können Sie auch Ihre Gefährdung verringern, da der gesamte ans öffentliche Internet weitergeleitete Datenverkehr dann (mit HTTPS) verschlüsselt wird.

5.8 Bridge-Relay

Die Einrichtung eines Bridge-Relays ähnelt der eines Austritts- oder Transitrelays, allerdings können Sie noch festlegen, wie die Adresse Ihrer Bridge verbreitet wird. Sie können die allgemeinen Einstellungen und die Bandbreiteneinschränkung vornehmen, müssen sich aber nicht um Austrittsrichtlinien kümmern.

Der große Unterschied besteht darin, dass Sie die Möglichkeit haben, die Adresse Ihres Bridge-Relays automatisch verbreiten zu lassen, indem Sie das entsprechende Kontrollkästchen am unteren Rand der Registerkarte *Beteiligung* aktivieren. Nachdem Ihre Bridge initialisiert ist (nachdem Sie sie also eingerichtet und dann auf *OK* geklickt haben), generiert das System eine Textzeile, die zur Identifizierung der Bridge dient. Sie sieht wie folgt aus:

```
10.110.171.18:9001 F5C81437057BCD0C58AE50079DD788045B3A9AFE
^              ^    ^
IP-Adresse     Port Fingerabrdruck
```

Die oberste Zeile ist ein Beispiel für eine Bridge-Adresse. (Es handelt sich hierbei jedoch nicht um eine echte Bridge-Adresse!)

Der erste Teil ist die IP-Adresse einschließlich Portnummer (9001). Darauf folgt ein 40-Byte-Fingerabdruck, der zur Authentifizierung der Bridge dient.

Wenn Sie eine Bridge für eine bestimmte Person einrichten, die einen solchen Zugang benötigt, dann können Sie dieser Person den Datenstring zukommen lassen, sodass sie ihren Tor-Client zur Verwendung der Bridge einrichten kann. Dadurch können Sie jemandem helfen, ohne die Adresse Ihrer Bridge an irgendjemand anderen als an diese Person weiterzugeben (wobei Sie jedoch einen sicheren Kanal benötigen, um mit dieser Person kommunizieren zu können).

Das ist eine Möglichkeit, über die Personen mit gutem Zugang zum Tor-Netzwerk einzelnen Personen helfen können, die hinter staatlichen DPI-Firewalls sitzen.

Verborgene Tor-Dienste

Bei einem Anonymisierungsprotokoll wie Tor ist es naturgemäß möglich, dass ein Knoten in dem Anonymisierungsnetzwerk nicht nur als Client fungiert (um etwa anonym Websites im öffentlichen Internet aufzusuchen), sondern auch als Server, der von anderen Clients innerhalb dieses Netzwerks erreicht werden kann, während sein tatsächlicher Standort (seine IP-Adresse) unbekannt bleibt.

Bei der Verwendung von Tor, um die Anonymität eines Clients zu gewährleisten, der auf das weltweite Internet zugreift, fungiert das Tor-Netzwerk selbst (die Menge aller Systeme, die als Tor-Relays eingerichtet sind) als einzelner Netzwerkproxy.

In diesem Fall muss der Benutzer innerhalb des Tor-Netzwerks nur auf die Tor-Relays zugreifen und auf nichts sonst. Das bedeutet aber, dass es ein Tor-Netzwerkprotokoll geben muss (und auch tatsächlich gibt!), das die grundlegenden Netzwerkfunktionen (wie Verzeichnisdienste und Routingprotokolle) und Datenformate unterstützt, sodass der Rest der Infra-

struktur den Systemen die anonyme Kommunikation erlaubt, ob sie nun als Clients oder Server fungieren. Auf diese Weise bietet das Anonymisierungsnetzwerk als Nebenprodukt die Möglichkeit, einen Server anonym auszuführen.

6.1 Gründe für die Verwendung verborgener Dienste

Die erste Frage, die bei verborgenen Tor-Diensten gestellt wird, ist die nach »guten« Verwendungszwecken dafür. Das liegt wahrscheinlich an der großen Aufmerksamkeit, die diesen Diensten in den Medien geschenkt werden, wenn sie für ungesetzliche Zwecke verwendet werden, und den Ruf nach einer Reglementierung von Tor, den frustrierte Politiker und Strafverfolgungsbeamte erklingen lassen.

Warum sprechen wir hier von »gut« (und »böse«)? Wie jedes andere Werkzeug sind auch verborgene Tor-Dienste nicht an sich gut oder schlecht, sondern können für gute oder schlechte Zwecke verwendet werden. Solche Dienste können zwar in der Tat von Kriminellen genutzt werden (und werden es auch!), aber auch von Personen, die sich für Menschenrechte, persönliche Freiheit und Opferschutz einsetzen.

Der Unterschied besteht darin, dass Kriminelle ihre Aktivitäten auch ohne das Tor-Netzwerk durchführen würden, indem sie noch andere Verbrechen begehen und etwa Mobiltelefone stehlen, E-Mail-Konten hacken, sich die Identitäten anderer Personen aneignen usw. Gesetzestreue Bürger würden dagegen nicht auf solche Maßnahmen verfallen, um ihre Privatsphäre zu schützen.

Jeder Dienst, der im Internet veröffentlicht werden kann, lässt sich als verborgener Tor-Dienst bereitstellen. Am häufigsten ist jedoch die Einrichtung verborgener Webserver. Sie können aber auch E-Mail-, Dateiübertragungs- und Chatserver als verborgene Dienste einrichten.

Die Seite »Using Tor hidden services for good« des Tor-Projekts (*https://blog.torproject.org/blog/using-tor-good*) ist ein guter Ausgangspunkt, um sich einige Beispiele für verborgene Dienste anzusehen und sich über die Vorteile ihrer Nutzung klar zu werden. Der folgende kurze Überblick zeigt einige wenige dieser »guten« Verwendungszwecke:

- In einigen Ländern werden Menschen durch staatlich geförderte Angriffe daran gehindert, ein Blog zu führen. Eine Lösung besteht darin, von jemandem in einem anderen Land einen verborgenen Server einrichten zu lassen, über den dem Blog neue Inhalte hinzugefügt werden, und die Inhalte dann als statisches HTML im öffentlichen Internet bereitzustellen.
- Wenn jemand einen Spiegel einer Nachrichten- oder Aktivisten-Website unterhält, ist dieser Spiegel (zumindest für Tor-Benutzer) auch dann noch verfügbar, wenn eine Regierung die Original-Website schließt.
- Verborgene Dienste sind für diejenigen nützlich, die Mitteilungen von Informanten veröffentlichen oder einsehen wollen, ohne sich den Einschränkungen oder der vollständigen Zensur durch Organisationen oder Regierungen zu unterwerfen, die mit der Veröffentlichung dieser Informationen nicht einverstanden sind. Beispiele finden Sie auf *http://globaleaks.org/* und *https://wikileaks.org/*.

Andere mögliche »gute« Verwendungszwecke für verborgene Tor-Dienste sind beispielsweise Chat- oder andere Social-Media-Dienste, bei denen die einzelnen Benutzer nicht identifiziert werden können. Dadurch kann ein Forum für die uneingeschränkte freie Rede in solchen Teilen der Welt eingerichtet werden, in denen Regierungen oder Unternehmen öffentliche Äußerungen lieber überwachen und zensieren.

6.2 Funktionsweise von verborgenen Tor-Diensten

Um einen verborgenen Tor-Server zu betreiben, brauchen Sie als Erstes ein System, das mit dem Tor-Netzwerk verbunden ist. Es gibt zwar auch

Möglichkeiten, ohne Tor auf solche Dienste zuzugreifen, allerdings bieten sie keine Anonymität und Sicherheit für die Benutzer (siehe Abschnitt 6.2.3).

Um die Anonymität des Herausgebers zu wahren, muss der Server zunächst einmal ein Tor-Netzwerkknoten sein (der anonym mit dem Tor-Netzwerk verbunden ist). Allerdings ist mit dem (anonym) angeschlossenen Computer dann immer noch eine Netzwerkadresse (eine anonyme Adresse) verbunden: Wenn ich *diese* Adresse kenne, kann ich mit dem Web- oder E-Mail-Server Verbindung aufnehmen, der auf diesem Computer läuft, wo auch immer er steht und wer auch immer ihn unterhält.

Es ist hier sinnvoll, sich das Tor-Netzwerk einfach nur als ein Medium vorzustellen, durch das die Knoten anonym miteinander kommunizieren. Dadurch können Sie die Einzelheiten der Tor-Verbindungen außer Acht lassen und sich besser auf die Interaktionen zwischen den anonymen Knoten konzentrieren.

6.2.1 Das Tor-Protokoll für verborgene Dienste

Das Tor Hidden Service Protocol (siehe *https://www.torproject.org/docs/hidden-services.html*) beschreibt, wie die verborgenen Tor-Dienste funktionieren. Bei der Einrichtung eines solchen Dienstes wählt der Server zufällig drei Tor-Relays als *Eintrittspunkte* aus. Anschließend richtet er zu jedem dieser Relays eine eigene, vollständige Tor-Verbindung ein, sodass alle Eintrittspunkte mit unterschiedlichen IP-Adressen verbunden sind. Der verborgene Server ist durch kryptografische Maßnahmen immer noch eindeutig identifizierbar. Es spielt keine Rolle, hinter welcher IP-Adresse er sich verbirgt, da er seine Identität durch seinen eigenen geheimen Schlüssel beweisen und damit zeigen kann, dass er zu dem *Pseudo-URL* (der sogenannten *Onion-Adresse*) gehört, die von seinem öffentlichen Schlüssel abgeleitet werden kann.

Wenn diese drei Tor-Verbindungen eingerichtet sind, kann der verborgene Server die Daten veröffentlichen, die erforderlich sind, um ihn zu erreichen – nämlich die Eintrittspunkte und die Identifizierungsdaten, die auf kryptografische Weise bestätigen, dass die für den verborgenen Dienst bestimmte Kommunikation auch tatsächlich dort ankommt.

Diese Daten registriert der verborgene Server auf den Systemen, die die *Verzeichnisdatenbank für verborgene Dienste* vorhalten. Wenn jemand Kontakt mit dem verborgenen Dienst aufnehmen möchte, sendet er eine Anfrage an diese Datenbank, die ihn dann zu einem der Eintrittspunkte leitet. Von dort aus handeln der Tor-Client und der verborgene Server eine Verbindung über einen *Rendezvouspunkt* aus. Zu diesem Zeitpunkt liegen drei Tor-Relays zwischen dem Client und dem Rendezvouspunkt, und auch der Server ist durch drei Tor-Relays vom Rendezvouspunkt abgeschirmt.

Anders ausgedrückt, sieht die ganze Sache wie folgt aus:

```
Tor-Client <==>
   Tor-Eintrittsrelay <==>
      Tor-Transitrelay <==>
         Tor-Transitrelay <==>
            <==> RENDEZVOUSPUNKT <==>
         Tor-Transitrelay <==>
      Tor-Transitrelay <==>
   Tor-Eintrittsrelay <==>
Verborgener Server
```

Die Einführungspunkte kennen den Client und den Server nur über die Tor-Anonymisierungsverbindungen. Die Anonymität wird noch dadurch verstärkt, dass Client und Server den Eintrittspunkt nur so lange nutzen, bis sie den Rendezvouspunkt ausgehandelt werden. Bei jeder Verbindungsaufnahme zwischen Client und Server wird ein anderer Rendezvouspunkt verwendet, sodass es schwierig bis unmöglich wird, den Standort eines verborgenen Dienstes durch Überwachung und Vergleich des Netzwerk-

datenverkehrs herauszufinden. Nicht einmal die Eintrittspunkte haben die Möglichkeit, Rückschlüsse auf die IP-Adresse des verborgenen Servers zu ziehen, da sie nur mit den Tor-Transitknoten verbunden sind, durch die der Server an das Netzwerk angeschlossen ist, und nicht mit dem Server selbst.

6.2.2 Pseudo-URLs

Verborgene Tor-Dienste können vom öffentlichen Internet aus nicht direkt angesprochen werden, denn statt eines regulären Internet-Domänennamens (wie *example.com* oder *example.org*) haben sie einen Pseudo-URL. Die Namen dieser Dienste sehen zwar ähnlich aus wie normale Domänennamen, verwenden aber statt einer der üblichen Top-Level-Domänen (wie *.com*, *.edu*, *.de* oder *.info*) die Endung *.onion* (was eine Anspielung auf das sogenannte Onion-Routing ist, auf dem das Tor-Projekt beruht).

Der erste Teil des Domänennamens ist ein 16-stelliger String (ausschließlich aus Zahlen und Buchstaben), der aus dem öffentlichen Schlüssel des verborgenen Dienstes abgeleitet ist (siehe Abschnitt 6.3, »Verborgene Tor-Dienste einrichten«). Diese Namen wirken wir zufällige Zeichenketten, erlauben dem Server aber, auf Anfragen zu antworten, indem er sich anhand seines geheimen Schlüssels authentifiziert und dadurch als der Inhaber des öffentlichen Schlüssels zu erkennen gibt, der hinter dem 16-Byte-Dienstnamen steht.

Tabelle 6.1 zeigt einige Beispiele für verborgene Tor-Dienste und deren Tor-Adressen.

Die Onion-Domänennamen bilden Pseudo-URLs, so wie anhand der Domänennamen im öffentlichen Internet URLs aufgebaut werden. Um beispielsweise einen Dienst wie FTP (File Transfer Protocol) zu erreichen, erstellen Sie einen Pseudo-URL wie den folgenden:

```
ftp://kj22ic3odyoqeac7.onion
```

Um eine Seite auf einer *.onion*-Website anzusprechen, können Sie den Verzeichnis- oder Dateinamen ebenso hinzufügen wie bei einem regulären URL:

```
http://kj22ic3odyoqeac7.onion/blog/this-is-a-blog-entry-title
```

Beachten Sie, dass verborgene Dienste gewöhnlich nicht als HTTPS-Websites veröffentlicht werden, denn dann müsste der Herausgeber ein kryptografisches Zertifikat beziehen, was seine Anonymität unterlaufen würde. Außerdem sind die Inhalte, die von und zu einem verborgenen Dienst gesendet werden, naturgemäß ausreichend verschlüsselt, um gegen eine Netzwerküberwachung geschützt zu sein – was genau das ist, was durch HTTPS erreicht werden soll. (Siehe auch den Kasten »HTTPS und HTTPS Everywhere« in Kapitel 1.)

Tabelle 6.1: Beispiele für verborgene Tor-Dienste und ihre Adressen

Beschreibung	Adresse
Die Website des Tor-Projekts als verborgener Dienst	*http://idnxcnkne4qt76tg.onion/*
Das Tor-Paketarchiv mit der gesamten veröffentlichten Software des Projekts	*http://j6im4v42ur6dpic3.onion/*
Die offizielle Bug-Tracker- und Wiki-Seite des Tor-Projekts	*http://vwp5zrdfwmw4avcq.onion/*
Das offizielle Medienarchiv des Tor-Projekts mit allen Tor-Bildern, -Videos und ähnlichen Dateien	*http://p3igkncehackjtib.onion/*
Duck Duck Go (anonyme Websuche)	*http://3g2upl4pq6kufc4m.onion/*
New Yorker Strongbox, zur anonymen Übermittlung von Dateien oder Mitteilungen an die Redaktion der Zeitschrift New Yorker	*http://tnysbtbxsf356hiy.onion*

Achtung: Der verborgene Dienst des Tor-Projekts stellt exakt dieselbe Website zur Verfügung, wie sie auch auf *torproject.org* zu finden ist. Alle Links zu anderen Websites des Projekts (z. B. zum Bug-Tracker, zur Wiki-Seite oder zum Projektblog) führen daher ins öffentliche Internet und nicht zu den *.onion*-Versionen dieser Websites. Die Onion-Adressen finden Sie auf der folgenden Seite.

6.2.3 Web-Onion-Proxys

Tor ist Netzwerk, ebenso wie das öffentliche Internet. Wenn jemand von dem einen Netzwerk Verbindung aufnehmen möchte, braucht er zunächst einmal eine physische Netzwerkverbindung – drahtlos, über Kabel oder über ein besonderes System, das physisch mit beiden Netzwerken verbunden ist.

Wenn die Systeme in den beiden Netzwerken dieselben Protokolle für den Datenaustausch verwenden, z. B. TCP/IP in Netzwerken wie dem Internet, dann sind für das Zusammenspiel neben der Netzwerkverbindung nur die gemeinsamen Protokolle erforderlich.

Das Tor-Netzwerk nutzt jedoch einen eigenen Satz von Protokollen (die Tor-Protokolle), die oberhalb von TCP/IP ausgeführt werden, wohingegen das Internet nur TCP/IP einsetzt. Zur Verbindung mit einem verborgenen Tor-Dienst müssen Sie also Tor ausführen. Es gibt jedoch noch eine andere Möglichkeit, nämlich über das Internet Verbindung mit einem System aufzunehmen, das sowohl an das Tor-Netzwerk als auch an das Internet angeschlossen ist.

Es gibt eine Reihe von Websites zu diesem Zweck: Sie nehmen die Onion-Adresse eines verborgenen Tor-Dienstes entgegen und fungieren als Proxy, um diesen Dienst zu erreichen.

Zu diesen Onion-Proxydiensten gehören unter anderem die folgenden:

- tor2web (*http://tor2web.org/*)
- Onion.to (*http://onion.to/*)
- Onion.sh (*http://onion.sh/*)

Solche Proxys können zwar recht komfortabel ein, um einen kurzen Blick auf die verborgenen Dienste zu werfen, allerdings bieten sie für die Benutzer keinen echten Schutz, ja, sie können sogar ein zusätzliches Risiko darstellen, da die Betreiber dieser Proxywebsites Informationen aus den Sitzungen mit

den verborgenen Servern aufzeichnen können. Die Herausgeber der verborgenen Dienste sind nach wie vor abgeschirmt, aber Ihre Aktivitäten auf deren Websites lassen sich von einem Gegner relativ leicht überwachen und auf Sie zurückführen.

6.2.4 Was in den Schatten lauert

Es gibt eine ganze Reihe verborgener Dienste im Tor-Netzwerk. Einige davon sind »geöffnet« und suchen nach neuen Benutzern, andere bieten eine Dienstleitung für eine bestimmte Zielgruppe – und wieder andere werden veröffentlicht, weil ihre Herausgeber einen Eindruck hinterlassen, schockieren, verstören oder beleidigen wollen.

Wenn Sie nach verborgenen Diensten Ausschau halten, nur um ein bisschen herumzusurfen, werden Sie auf viel mehr scheußliche Dinge stoßen, als Sie es aus dem öffentlichen Internet gewohnt sind – abstoßende Bilder, widerwärtige Ansichten und Websites, die kriminelle Produkte und Dienstleitungen anpreisen und anbieten. Auch Urheberrechtsverletzungen und Betrügereien sind gang und gäbe.

Nehmen wir nur einen der berüchtigtsten verborgenen Dienste: Silk Road, eine Website für den Drogenhandel. Die korrekte Onion-Adresse dafür können Sie problemlos im Internet in Erfahrung bringen (*silkroadvb5piz3r.onion*), allerdings werden Sie dort auch auf die Adressen betrügerischer Websites stoßen, deren Pseudo-Onions ähnlich aussehen wie die echte, aber zu Anmeldeseiten führen, auf denen die Anmeldeinformationen von Silk-Road-Benutzern abgeschöpft werden.

Da es für verborgene Tor-Dienste keine zentrale Instanz, keine Regeln und keine Möglichkeit gibt, solche Regeln durchzusetzen, müssen Sie beim Zugreifen auf einen verborgenen Dienst äußerst vorsichtig sein. Die Personen, die hinter solchen Diensten stehen, können sich straflos alles erlauben.

6.3 Verborgene Tor-Dienste einrichten

Um einen verborgenen Tor-Dienst zu betreiben, ist im Prinzip nicht mehr nötig, als einen Netzwerkdienst auf einem Tor-Client einzurichten und die Konfiguration dann so zu ändern, dass der gesamte Zugriff auf diesen Dienst über das Tor-Netzwerk erfolgt. Technisch ist das mit dem Aufbau eines proprietären Netzwerkspeichersystems (wie Novell NetWare) vergleichbar, das über TCP/IP im weltweiten Internet zugänglich ist.

Für verborgene Dienste muss die Tor-Netzwerksoftware so eingerichtet werden, dass sie Anforderungen aus dem Tor-Netzwerk entgegennimmt und zu der Software (auf dem System mit dem verborgenen Server) weiterleitet, die den Netzwerkdienst ausführt (z. B. ein reguläres TCP/IP-Serverprogramm wie ein Web- oder Mailserver).

Wenn Sie also einen verborgenen Tor-Server betreiben möchten, dann müssen Sie über alle Fähigkeiten verfügen, um einen regulären, nicht verborgenen Dienst auf einem mit dem Internet verbundenen Server einzurichten – und darüber hinaus wissen, wie Sie einen Tor-Client ausführen.

Die Einrichtung eines Tor-Clients zur Ausführung eines verborgenen Dienstes kann in vier Schritte eingeteilt werden (laut »Configuring Hidden Services for Tor«, *https://www.torproject.org/docs/tor-hidden-service.html.en*):

- Tor ans Laufen bekommen.
- Einen Server lokal auf einem System installieren, auf dem Tor läuft.
- Den verborgenen Dienst einrichten. Dazu müssen lediglich zwei Zeilen zur Tor-Konfigurationsdatei *torrc* hinzugefügt werden.
- Tipps, Hinweise und Anregungen beachten. Mit anderen Worten: Es nicht so einfach!

Wenn Tor läuft und Sie auf Ihrem Tor-System einen Server haben, können Sie den verborgenen Dienst über Vidalia einrichten (siehe Abbildung 6.1). Das sollten Sie jedoch nur als ersten Schritt betrachten. Es sind noch weitere Änderungen am System erforderlich, um sicherzustellen, dass der Dienst auch wirklich ganz verborgen ist.

Die Einrichtung eines verborgenen Dienstes ist ziemlich einfach, wenn Sie auf Ihrem System einen Webserver eingerichtet haben und die Tor-Clientsoftware dort installieren und ausführen können. Allerdings ist es weniger einfach, dafür zu sorgen, dass dies auch auf sichere Weise, mit einem Maximum an Anonymität und einem Minimum an Risiko geschieht, erkannt zu weden.

6.3.1 Tor zum Laufen bekommen

Wie Sie nach der Verwendung des TBB oder von Tails bereits wissen, ist es ziemlich einfach, Tor auf Ihrem System ans Laufen zu bekommen. In den bisherigen Anleitungen fehlt allerdings eine Frage: »Wo führe ich meinen verborgenen Tor-Dienst aus?«

Zur Sicherheit wird empfohlen, dies nicht auf Ihrem privaten Computer zu tun, denn das würde Aufmerksamkeit erregen, insbesondere, wenn der verborgene Dienst viel Datenverkehr hervorruft. Ein Gegner kann außerdem die Bereitschaftszeiten des verborgenen Dienstes mit den Zeiten vergleichen, an denen Ihr Computer ein- oder ausgeschaltet ist. Wenn der Dienst immer dann nicht mehr zur Verfügung steht, wenn Sie Ihren Computer ausschalten, lässt sich daraus schließen, dass Sie diesen Dienst ausführen.

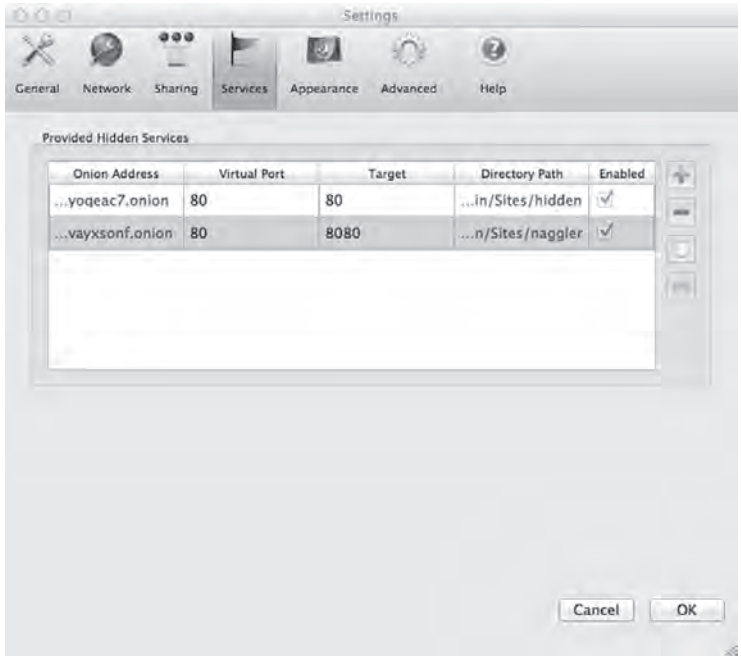

Abbildung 6.1: Einrichten von verborgenen Tor-Diensten in Vidalia

Wenn Sie vorhaben, einen anonymen Dienst zu betreiben, müssen Sie vorsichtig vorgehen, um Ihre Anonymität gegenüber den Gegnern zu wahren, mit denen Sie es zu tun haben. Berücksichtigen Sie dazu die folgenden Möglichkeiten (nach Hinweisen von Roger Dingledine, Tor-Projektleiter und einer der ursprünglichen Entwickler von Tor):

- Führen Sie Tor auf einer *virtuellen Maschine (VM)* aus und sorgen Sie dafür, dass sie die IP-Adresse und den Domänennamen des Systems, auf dem sie läuft, nicht herausfinden kann. Durch die Nutzung einer VM haben Sie als Systemadministrator mehr Einfluss darauf, was der Tor-Client tun kann und was nicht.
- Führen Sie Tor auf einem *virtuellen privaten Server (VPS)* aus und »stellen Sie die VM auf einen VPS in einem Land, das Ihren Gegner hasst. Wenn irgendjemand in den Webserver und die VM eindringt, hat er dann immer noch ein frustrierend langwieriges bürokratisches Verfahren vor sich«, wie Dingledine schrieb. Das funktioniert am bes-

ten, wenn das Land, in dem sich der VPS befindet, auch eine datenschutzfreundliche Gesetzgebung hat (und in dem sich Beamte und Angestellte von Serverhostingunternehmen nicht so leicht bestechen lassen).

Diese Vorgehensweise (eine VM auf einem VPS in einem feindlichen Land) sorgt für mehrere Schutzschichten rund um den verborgenen Server:

- Die VM kann verschlüsselt und aus der Ferne neu gestartet und sogar komplett gelöscht werden, sodass niemand die IP-Adresse oder den Domänennamen des Computers herausfinden kann, auf dem sie läuft.
- Die VM befindet sich auf einem VPS und ist daher nur eine von vielen, die auf derselben physischen Hardware läuft. Das macht es für einen Gegner zusätzlich schwierig, den Datenverkehr zu entwirren und zu analysieren.
- Der VPS befindet sich in einem Land, das Ihrem Gegner gegenüber nicht freundlich gesonnen (und wahrscheinlich dem Datenschutz gegenüber aufgeschlossen) ist. Das stellt Ihrem Gegner zusätzliche bürokratische Hindernisse in den Weg.

Nachdem Sie nun also Tor auf sichere Weise installiert haben, besteht der nächste Schritt darin, die Serversoftware zu installieren.

6.3.2 Den Server installieren

Der am häufigsten verwendete (und dadurch anhand der vielen Tutorials und Installationsskripte auch am einfachsten zu installierende) Webserver ist zwar Apache (*http://httpd.apache.org/*), doch ist er für die Bereitstellung anonymer Dienste nicht zu empfehlen. Apache mag zwar ein kugelsicherer und unter gewöhnlichen Umständen ziemlich sicherer Webserver sein, doch sind im Laufe der Zeit viele an sich großartige Funktionen hinzugekommen, von denen einige von Gegnern missbraucht werden können.

In dem bereits weiter vorn zitierten Artikel schlägt Dingledine vor, »einen guten, soliden Webserver wie nginx auszuführen«. (nginx – sprich: *engine x* – ist ein Open-Source-Webserver, der häufig für verborgene Dienste herangezogen wird; siehe *http://nginx.org/*). Dingledine hat nicht etwa gesagt: »Verwenden Sie nginx!«, sondern hat nur etwas »wie nginx« empfohlen: quelloffen, reif, häufig genutzt und ohne zu viele Kinkerlitzchen, die Schwachstellen für die Anonymität darstellen können, aber für die große Mehrheit der Benutzer (ohne Tor) nicht als »Sicherheitsproblem« eingestuft werden.

Die Verwendung eines guten, sicheren Webservers – von dem Sie wissen, dass er sicher läuft – fügt den oben genannten noch eine weitere Schutzschicht hinzu. Den ersten Schutz für einen verborgenen Dienst bildet der Server.

6.3.3 Den verborgenen Dienst einrichten

Wenn Sie Vidalia zum Einrichten des verborgenen Dienstes einrichten, gibt es zwei Zeilen aus, die Sie der Tor-Konfigurationsdatei *torrc* hinzufügen müssen, und startet den Dienst automatisch. Diese beiden Zeilen sehen ähnlich wie die folgenden aus:

```
HiddenServiceDir /Library/Tor/var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:8080
```

Unter Windows ergibt sich:

```
HiddenServiceDir C:\Users\username\Documents\tor\hidden_service
HiddenServicePort 80 127.0.0.1:8080
```

Die erste Zeile nutzt die Direktive `HiddenServiceDir`, um das vollständig qualifizierte Verzeichnis für den verborgenen Dienst anzugeben. In dieses Verzeichnis stellen Sie die Inhalte für den Dienst.

Die zweite Zeile gibt mithilfe der Direktive `HiddenServicePort` den *virtuellen* Port an (denjenigen, den der Benutzer zu verwenden scheint, um Verbindung mit Ihrem Dienst aufzunehmen), gefolgt von der IP-Adresse und dem Port, den Verbindungen zu dem verborgenen Dienst *tatsächlich* nutzen. In diesen Beispielen ist der virtuelle Port 80, also der Standardport für ungesichertes HTTP. Bei der tatsächlichen Adressangabe 127.0.0.1 handelt es sich um die *Loopback*-Adresse (die der Computer als »dieser Computer« interpretiert) mit dem Port 8080, einem alternativen Port für Webverbindungen.

Im Allgemeinen sollten Sie die Loopback-Adresse als Adresse des verborgenen Dienstes beibehalten, denn sie bietet keinerlei Informationen für eine mögliche Deanonymisierung (da sie definitionsgemäß auf das System verweist, auf dem Tor ausgeführt wird). Die Portadresse jedoch muss möglicherweise in Abhängigkeit von der Art des verborgenen Dienstes geändert werden (80, 443 und 8080 werden gewöhnlich für Webserver verwendet, wohingegen andere Server andere Ports nutzen, z. B. 25 für E-Mail-Dienste und 20 für Dateiübertragung).

Sobald die neue Konfiguration aktiviert ist (durch einen Neustart oder die Erstkonfiguration in Vidalia), führt Tor automatisch einige Verwaltungsarbeiten durch:

- Tor erstellt ein Paar aus privatem und öffentlichem Schlüssel und schreibt die Datei *private_key* in das Verzeichnis des verborgenen Dienstes (siehe Abbildung 6.2).
- Tor generiert auf der Grundlage des öffentlichen Schlüssels einen Pseudo-URL (die *.onion*-Adresse) für den verborgenen Dienst.
- Tor schreibt die Datei *hostname*, die in einer einzigen Zeile den Pseudo-URL enthält.

Auf der Registerkarte *Dienste* von Vidalia können Sie an der rechten Seite auf die dritte Schaltfläche von oben klicken, um die *.onion*-Adresse des Dienstes in die Zwischenablage Ihres Systems zu kopieren. Das macht es einfacher, sie korrekt zu verwenden und weiterzugeben.

6.3.4 Tipps, Tricks und Fallgruben

Unabhängig davon, wie Sie Ihren verborgenen Dienst eingerichtet haben, ist es immer sinnvoll, zusätzliche Maßnahmen zu ergreifen, um seine Kontinuität und Anonymität sicherzustellen.

Wenn der verborgene Dienst längere Zeit über eine einzige *.onion*-Adresse zugänglich sein soll – oder wenn Sie ihn von einer VM ausführen (was sehr empfohlen wird) –, sollten Sie eine Sicherheitskopie der Datei *private_key* (siehe Abbildung 6.2) anlegen und schützen. Diese Datei enthält die Textversion des geheimen Schlüssels für den verborgenen Dienst. Wenn sie einem Gegner in die Hand fällt, kann er damit eine gefälschte Version Ihres Dienstes anbieten, wobei die Benutzer keine Möglichkeit haben, zu erkennen, ob Sie sich auf Ihrem Server befinden oder auf dem des Gegners.

Wenn Sie daher eine Sicherheitskopie dieser Datei anlegen, müssen Sie das auf eine Weise tun, die es dem Gegner unmöglich macht, an den Schlüssel zu gelangen. Sie können sie verschlüsselt auf einer CD oder einem USB-Stick ablegen und dieses Medium dann in einen Safe legen. Es ist auch möglich, den Dateiinhalt auszudrucken und in einem Safe unterzubringen. Auf keinen Fall aber sollten Sie einen Ausdruck an die Pinnwand in Ihrem Büro heften oder eine unverschlüsselte Kopie der Datei auf Ihrem Computer speichern.

```
-----BEGIN RSA PRIVATE KEY-----
+cmMqNyiCMz4StSaiNRIXOgJm+a+4AHPJgFViaosg+ks/yvAqzU0h8HsTyTtNQKB
MIICXgIBAAKBgQDMopDdM2NXZl+snvFM3nSjaVFhx62yL0iZlf43eKMo+lC3NZvj
AoGBAJHpULYJEEqfmpSxeIlBDZX/YKICCR5GjNPGmc/f2yc65RbdyNxTnZ0IQtne
q0a/ewWqHKSm8Us0IbFzOS+djBVAbpwmmxJNAXkZrVk7AYwIDAQABY6v7uu5ATNe
8HfSisEr/2zwJhCczoFWqiGZoWDfpKXk3KrPMMDPVEIpTeM0BQpf2J5CihXPBn8B
KDQOt/XSwwJBAM94JOR9AJe0dcEtKB/06NX5v4C9fNiF07mg7uVaCjQxiDec/gnz
Pl30vO3pkR6j41iIR6YG5+TdnyvXh1qhivhA69dCqDgsRRo1zqxtx/O4WPrHAkBj
fCRyPxixah9hNMhvMxo4Pk5m855Ne7p/QeECQQCHYm2zZ5KqeGJJymNwLCT6gQqx
Ko/NaUOGIcamPlWCtTC34yUWWZ3lLlaAhUd98BWBAkEA/ICyRXfDsTHYOSa3TbW2
XUgkGDfFAB3u3VOUPg54xhrIfzdcFzJjjVoR6fdX8NFpV7CjsNx5C6QiXX2oIWSI
eo1IrdQkqq1llwiGhjzhAkEA0BsD5OYdsU87LPw7CaV0ehJloU1lgrat/XE0jM4z
Z9R9aetjxMJ7CZDlJup8w8pe++uarxyQH6z3VVn4QhdbVixeRjygFeFninInkOLC
2tjuw5ggZRhIMZn7GfHM3pNhzVgerPx3yRi1cCS0ez9wYA==
-----END RSA PRIVATE KEY-----
```

Abbildung 6.2: Der Inhalt der Datei *private_key*

Auf einem einzigen Tor-Client können Sie auch mehr als einen verborgenen Dienst ausführen, indem Sie einfach weitere `HiddenServiceDir`/`HiddenServicePort`-Konfigurationsdateien hinzufügen. (In Abbildung 6.1 können Sie erkennen, dass zwei verborgene Dienste eingerichtet sind.) Dabei müssen Sie jedoch zwei verschiedene Ports angeben, damit Ihr Server erkennen kann, welcher Dienst auf dem lokalen Host jeweils angesprochen wird.

Wenn Sie auf einem Tor-Client einen verborgenen Dienst ausführen, sollten Sie Tor nur als Client betreiben und nicht als Relay, denn das würde die Leistung Ihres Dienstes beeinträchtigen. Vor allem aber ruft die Ausführung eines Relays auf einem System, das einen verborgenen Dienst unterhält, eine Schwachstelle hervor, die von Gegnern ausgenutzt werden kann. Es gibt Angriffsmöglichkeiten, bei denen es leichter ist, einen verborgenen Server aufzuspüren, wenn er auf einem Tor-Relay läuft. (Dies ist jedoch eine komplizierte Vorgehensweise, und es ist noch nicht bewiesen, dass sie bei verborgenen Diensten in der Praxis funktioniert.)

Mehr über die Dinge, die Sie beim Betrieb eines verborgenen Dienstes beachten müssen, finden Sie in dem Artikel »Hidden services need some love« (*https://blog.torproject.org/blog/hidden-services-need-some-love*) im

Blog zum Tor-Projekt. Wenn Sie vorhaben, einen solchen Dienst einzurichten, ist dieser Artikel Pflichtlektüre, um mehr über die damit verbundenen Gefahren und Probleme zu erfahren. Zu den hier angesprochenen Aspekten gehören Dinge wie die Skalierung von verborgenen Diensten, um eine große Anzahl von Benutzern zu unterstützen, Probleme mit Protokollen, die bestimmte Arten von DoS-Angriffen ermöglichen (Denial of Service), Schwachstellen im Protokoll, die bestimmte Arten von Angriffen zulassen, und Vorgehensweisen zur Verbesserung von Anonymität und Leistung.

7

E-Mail-Sicherheit und Vorgehensweisen zur Förderung der Anonymität

Wie bereits in Kapitel 1 erwähnt, konnte David Petraeus seine eigene E-Mail-Kommunikation nicht geheim halten. Wenn schon der ehemalige Direktor der CIA nicht in der Lage ist, seine Anonymität zu wahren, können Sie erkennen, dass der Schutz Ihrer E-Mails schwieriger ist, als es auf den ersten Blick zu sein scheint.

Sicherer und anonymer E-Mail-Verkehr werden durch verschiedene Einflüsse erschwert:

- E-Mail-Provider – ob nun Ihr Internetprovider oder ein Webmaildienst wie Google Mail oder Yahoo! Mail – wissen bereits, wer Sie sind und wo Sie zu finden sind (z. B. über Ihre IP-Adresse), oder wollen es

von Ihnen wissen. Webmail-Anbieter verlangen oft die Angabe einer E-Mail-Reserveadresse oder einer Telefonnummer.

- E-Mail-Provider können die IP-Adressen protokollieren, von denen aus auf Ihr E-Mail-Konto zugegriffen wird. Wenn Sie also ein anonymes E-Mail-Konto einrichten können, dann dürfen Sie nur anonym mithilfe von Tor darauf zugreifen. Schon ein Zugriff über das öffentliche Internet kann Ihrem Gegner genügend Informationen geben, um Ihre echte Identität mit dem anonymen E-Mail-Konto in Verbindung zu setzen.
- Nicht alle Webmail-Anbieter erlauben einen HTTPS-Zugriff auf ihre E-Mail-Konten, sodass die Nachrichten zwischen dem Tor-Austrittsknoten und dem Webmailserver ausspioniert werden können. Ein HTTPS-Zugriff wird immer häufiger angeboten, allerdings müssen Sie unbedingt darauf achten, dass die Nachrichten vom Server zum Client durchgängig verschlüsselt werden.
- Manche Webmail-Provider blockieren den Kontozugriff oder die Kontoerstellung von Tor-Austrittsknoten. Wenn Sie nicht in der Lage sind, Tor zu nutzen, kann Ihr Provider (oder jemand anderes durch die Dienste des Providers) Ihre Webmail-Aktivitäten teilweise oder ganz überwachen.
- Sofern Sie nicht alle Nachrichten verschlüsseln – und nur verschlüsselte Nachrichten annehmen –, können Ihre gesendeten und empfangenen Mails für jeden zugänglich sein, der Zugriff auf die Systeme Ihres E-Mail-Providers hat. Manche Provider verschlüsseln Ihre Daten, behalten aber die Kontrolle über die Schlüssel, sodass ein Gegner mit genügend Einfluss (oder Rechtsmitteln) den Klartext Ihrer Mitteilungen einsehen kann.

Dieses Kapitel beschreibt, warum und wie Sie E-Mail anonym über Tor verwenden sollten und wie Sie zumindest einige der genannten Probleme umgehen können.

Es gibt verschiedene Möglichkeiten zur Nutzung von E-Mail und damit auch, je nachdem, aus welchen Gründen Sie anonym bleiben wollen, verschiedene Möglichkeiten, um Ihre Spuren zu verwischen.

Eine Sache, die Sie immer im Hinterkopf behalten müssen, ist der Unterschied zwischen E-Mail-Anonymität und E-Mail-Pseudonymität. In manchen Fällen möchte jemand eine E-Mail-Adresse nur ein einziges Mal verwenden, etwa um eine Nachricht an einen Empfänger zu senden, ohne eine Antwort erhalten zu können, oder um eine Nachricht zu senden und eine einzige Antwort zu erhalten.

In diesem Kapitel sehen wir uns vier verschiedene Vorgehensweisen an, um E-Mail-Anonymität bzw. -Pseudonymität zu wahren. Dabei werden auch jeweils die Gründe für die Wahl der jeweiligen Methoden angegeben.

7.1 Einweg-Konten

Um auf einer Website oder bei einem Dienst Beiträge einstellen, Kommentare abgeben oder auf irgendeine Weise mit anderen Benutzern online in Verbindung treten zu können, müssen Sie sich oft registrieren. Die meisten Websites verlangen dazu die Angabe einer E-Mail-Adresse. Das geschieht teilweise zum Selbstschutz (um zu verhindern, dass Betrüger automatisiert neue Konten für bösartige Zwecke anlegen), aber auch, um die Mitglieder zu identifizieren. Das kann dazu dienen, mit den Mitgliedern zu kommunizieren, aber auch dazu, ihre E-Mail-Adressen oder sonstigen Benutzerdaten an Dritte zu verkaufen.

Die Angabe Ihrer echten E-Mail-Adressse (die Rückschlüsse auf Ihre wahre Identität zulässt) können Sie oft vermeiden, indem Sie eine Einweg-Adresse verwenden. Solche temporären oder Wegwerf-Adressen können in unterschiedlicher Form von verschiedenen Websites bezogen werden. Betrachten Sie beispielsweise die Dienste, die in den folgenden Abschnitten vorgestellt werden.

7.1.1 10minutemail.com

Diese Website stellt Ihnen auf ihrer Startseite eine E-Mail-Adresse bereit, die Sie beispielsweise angeben können, wenn eine neugierige Website eine gültige E-Mail-Adresse zur Registrierung verlangt. Die Seite wird regelmäßig aktualisiert, um etwaige Nachrichten anzuzeigen, die an dieses Konto gesendet wurden. Wie der Name schon deutlich macht, ist diese E-Mail-Adresse nur zehn Minuten lang gültig, sofern Sie keine Verlängerung beantragen. Nachdem die Zeit abgelaufen ist, verschwinden (augenscheinlich) Ihre E-Mail-Adresse und die Nachrichten.

Mit diesem und ähnlichen Diensten sind jedoch einige Probleme verbunden:

- Sie müssen den Betreibern der Website vertrauen, dass sie weder Ihre IP-Adresse noch irgendwelche Nachrichten protokollieren, die über ihren Dienst laufen.
- Diese Website bietet keine HTTPS-Unterstützung, weshalb Ihre temporäre E-Mail-Adresse sowie alle Nachrichten, die Sie darüber empfangen, von jedem, der sich in Ihrem lokalen Netzwerk befindet, auf einfache Weise überwacht werden können.
- Wenn Ihr Provider Ihren Datenverkehr protokolliert, ist es offenkundig, dass Sie diesen Dienst nutzen (sofern Sie nicht über Tor darauf zugreifen).
- Manche Websites halten sich über die Domänen von Anbietern für temporäre E-Mail-Adressen auf dem Laufenden, und lassen eine Registrierung mithilfe eines solchen Kontos nicht zu.

7.1.2 Anonymous Email (http://www.5ymail.com/)

Diese Website ermöglicht es Ihnen, eine Nachricht einschließlich Dateianhängen »anonym« zu verschicken. Eines der besonderen Merkmale dieses Dienstes besteht darin, dass Sie darüber benachrichtigt werden

können, wenn Ihre Nachricht gelesen wird. Dazu müssen Sie aber eine gültige E-Mail-Adresse angeben, was jegliche Form von Anonymität zunichte macht.

Neben diesen Nachteilen weist 10minutemail.com ein weiteres Problem auf. Sie haben nämlich die Wahl, ob Sie Ihre Nachrichten kostenlos oder gegen eine Gebühr senden lassen wollen. Wenn Sie sich für die kostenlose Nutzung entscheiden, wird Ihrer Nachricht Werbung angehängt. Dadurch erfährt der Empfänger (und jeder, der *dessen* E-Mail-Verkehr überwacht), dass Sie diesen Dienst nutzen, was einem Gegner einen Ausgangspunkt gibt, um Sie zu identifizieren. Wenn Sie für die Nachrichtenübermittlung bezahlen, bleiben Sie auch nicht anonym, da Sie eine Kreditkartennummer oder ein PayPal-Konto angeben müssen.

7.1.3 Vermeiden Sie diese Dienste

Alles, was Sie über diese Art von »anonymen« E-Mail-Diensten senden oder empfangen, kann vom Anbieter eingesehen werden, selbst wenn Sie den Kontakt zu diesem Anbieter über Tor herstellen. Dieser Anbieter ist im Allgemeinen nicht verpflichtet, Ihre persönlichen Daten zu schützen. Daher sollten Sie sehr sorgfältig die Geschäftsbedingungen prüfen, unter denen der Dienst angeboten wird.

Wenn Sie einem Webmail-Provider (wie Gmail) eine solche E-Mail-Adresse als »Reserve« für den Notfall angeben, müssen Sie sich darüber im Klaren sein, dass die Bestätigungsmail, die der Provider sendet, in seinem Netzwerk ausspioniert werden kann (sofern der Anbieter der Wegwerf-Adresse nicht HTTPS einsetzt). Außerdem kann jeder, der Zugriff auf die Server des Anbieters Ihrer Einweg-Adresse hat, die Nachricht einsehen, selbst dann, wenn Sie mit Tor auf dieses Konto zugreifen.

Dienste dieser Art können Ihre Identität nicht vor entschlossenen Gegnern schützen. Vermeiden Sie sie, sofern es nicht absolut notwendig ist, sie zu nutzen. Es gibt bessere Möglichkeiten.

7.2 Anonyme Remailer-Dienste

Der bekannteste Remailer-Dienst ist Hushmail (*https://www.hushmail.com/*). Er umgeht mehrere der Probleme, die mit temporären E-Mail-Adressen verbunden sind, indem er HTTPS verwendet und Ihre Nachrichten verschlüsselt, während sie gespeichert werden. Wenn Sie eine E-Mail an einen anderen Hushmail-Benutzer senden, bleibt Ihre Nachricht auch verschlüsselt. Sie können sie auch selbst nach den OpenPGP-Standards verschlüsseln. (Anderenfalls würde die Nachricht als Klartext übertragen, sodass sie ausspioniert werden kann.)

Allerdings behält sich Hushmail die Möglichkeit vor, die in Ihrem Konto verschlüsselten Daten zu entschlüsseln. Wenn die Betreiber »eine rechtswirksame Aufforderung nach der Gesetzgebung von British Columbia (Kanada) erhalten, also der Gerichtsbarkeit, in der sich unsere Server befinden« (so die Website von Hushmail), werden sie dieser Aufforderung nachkommen.

Hushmail stellt gegenüber den meisten Anbietern von temporären oder Wegwerf-Adressen einen großen Schritt nach vorn dar, kann Ihre Privatsphäre aber nicht vor gerichtlichen Beschlüssen oder vor Gegnern schützen, die über einen Gerichtsbeschluss oder andere Mittel Zugriff auf die Server von Hushmail bekommen.

Hushmail ist gut etabliert, wird von Unternehmen genutzt und entspricht sogar den Vorgaben der US-amerikanischen Gesetzgebung zum Schutz von Patientendaten. Wenn Sie ausschließlich über Tor auf Hushmail zugreifen und alle Ihre Nachrichten mit einem starken Verschlüsselungsprogramm wie GnuPG verschlüsseln, sollte Hushmail für die meisten Zwecke ausreichen. Denken Sie aber immer daran, dass jegliche unverschlüsselte, also im Klartext übertragene Nachrichten an Ihr Hushmail-Konto von einem Gegner mit Zugriff auf die Hushmail-Server eingesehen werden können.

7.3 Anonyme E-Mail-Kommunikation über Tor

Hierzu richten Sie über Tor ein Konto bei einem normalen Webmaildienst (wie Gmail oder Yahoo! Mail) ein. Der wichtige Punkt bei dieser Vorgehensweise besteht darin, dass der gesamte Zugriff auf das E-Mail-Konto über Tor ablaufen muss. Dadurch stellen Sie sicher, dass Ihr Standort (der sich über die IP-Adresse ermitteln lässt, von der aus Sie ins öffentliche Internet gehen) niemals preisgegeben oder mit dem E-Mail-Konto in Verbindung gebracht wird.

Bei der Auswahl eines E-Mail-Dienstes müssen Sie nach den folgenden Punkten Ausschau halten:

- Erstens muss der Dienst HTTPS unterstützen, damit ein Gegner, der das lokale Netzwerk überwacht, keinen Zugriff auf den Klartext Ihrer Passwörter oder E-Mails bekommt. Zurzeit unterstützen nur Gmail und Yahoo! HTTPS.
- Bei der Verbindungsaufnahme mit dem Dienst und der Registrierung eines Kontos müssen Sie über Tor vorgehen. Aufgrund der Funktionsweise von Tor deuten manche Websites die Verbindung als einen versuchten Angriff, wenn Sie von derselben IP-Ursprungsadresse (einem Tor-Austrittsrelay) mehrere Anforderungen erhalten. In einem solchen Fall können Sie versuchen, die Identität in Vidalia zu wechseln, oder ein wenig warten, bevor Sie es erneut versuchen.
- Entscheiden Sie sich für einen E-Mail-Dienst, der weder die Angabe einer vorhandenen E-Mail-Adresse noch eine Mobiltelefonnummer (an die SMS zu Ihrer Authentifizierung gesendet werden) verlangt. Wenn Sie Ihre persönliche E-Mail-Adresse oder Ihre Telefonnummer angeben, sind Sie nicht mehr anonym.

Yahoo! verlangt manchmal, aber nicht immer die Angabe einer E-Mail-Adresse. Das hängt davon ab, wo sich der Tor-Austrittsknoten befindet, den Sie verwenden.

Webmail-Provider ändern Ihre Richtlinien von Zeit zu Zeit. Beispielsweise hat Yahoo! Mail bis vor kurzem kein HTTPS unterstützt. Für Gmail müssen Sie entweder eine E-Mail-Adresse und eine Mobiltelefonnummer angeben.

Welche Informationen Sie bereitstellen müssen, kann davon abhängen, was der Dienst für Ihren Standort hält. Beispielsweise müssen Sie bei Yahoo! manchmal eine Mobiltelefonnummer angeben und manchmal nicht. Das richtet sich danach, von wo aus Sie scheinbar Verbindung aufnehmen, was Yahoo! anhand der IP-Adresse des von Ihnen benutzten Austrittsrelays bestimmt. Werden Sie nach einer solchen Nummer gefragt, fordern Sie in Vidalia eine andere Identität an und versuchen es noch einmal.

Nach der jetzigen Lage der Dinge ist Yahoo! Mail wahrscheinlich die beste Möglichkeit, denn bei diesem Dienst können Sie sich ohne Angabe einer vorhandenen E-Mail-Adresse registrieren, er unterstützt HTTPS und erlaubt es Ihnen, über Tor ein Konto zu eröffnen und darauf zuzugreifen.

Wenn Sie in Yahoo! oder Gmail eine anonyme E-Mail-Adresse erstellen können, dürfen Sie auf dieses Konto niemals außerhalb von Tor zugreifen (vor allem dann, wenn Sie es über Tor eingerichtet haben).

Es mag verlockend erscheinen, zur Registrierung bei Gmail ein Wegwerf-Konto zu verwenden. Denken Sie aber daran, dass ein Gegner, der Ihre Netzwerkverbindung überwacht, wahrscheinlich den Klartext aller Nachrichten sehen kann, die über dieses Konto übertragen werden. Damit kann er aber auch Ihr Gmail- (oder sonstiges) Konto bequem entanonymisieren.

Denken Sie auch daran, dass die Inhalte und die Empfänger Ihrer E-Mails mehr als alles andere zu Ihrer Entanonymisierung beitragen können. Auch wenn Ihre Nachrichten und Adressen auf dem Weg vom und zum Server durch HTTPS geschützt sind, sollten Sie vorsichtig sein, wenn Sie glauben, dass Ihr E-Mail-Provider die Inhalte Ihres Kontos überwacht.

7.4 Anonyme E-Mail-Kommunikation als verborgener Tor-Dienst

Am besten ist es, wenn Sie jemanden kennen (und ihm vertrauen!), der einen E-Mail-Server als verborgenen Tor-Dienst betreibt. Bei einem Konto auf einem solchen Server können Sie ziemlich sicher sein, dass die einzigen Schwachstellen auf die Sicherheitskenntnisse des Serveradministrators und seine Fähigkeit zurückzuführen sind, den Server und seine Inhalte vor entschlossenen Gegnern zu schützen.

Durch die Abwicklung der E-Mail-Kommunikation über einen verborgenen Tor-Dienst können Sie Ihre Informationen und Ihre Identität schützen – aber nur so weit, wie Sie den Personen, die den Dienst betreiben, vertrauen. Ein Gegner, der Zugriff auf den Mailserver hat, kann alle von Ihnen gesendeten und empfangenen Nachrichten im Klartext sehen und erkennen, mit wem Sie korrespondieren.

Wenn Sie einen öffentlichen Internet-Maildienst (wie Yahoo! oder Gmail) verwenden, können Sie zumindest sicher sein, dass Sie es mit einem renommierten Unternehmen zu tun haben, das Richtlinien und Vorschriften zum Datenschutz erfüllt (wobei jedoch immer die Möglichkeit besteht, dass Angestellte von einem Gegner gezwungen oder bestochen werden, private Informationen preiszugeben).

Es gab einen Webmaildienst namens Tor Mail, der auch als verborgener Dienst ausgeführt wurde, aber nichts mit dem Tor-Projekt zu tun hatte. Die Personen, die diesen Dienst betreiben, haben ihre Identität nicht offengelegt. Mittlerweile ist Tor Mail abgeschaltet.

7.5 Anonymität und Pseudonymität

Eine anonyme E-Mail-Adresse wird pseudonym, sobald sie erneut verwendet wird. Ein anonymer Informant, der eine einzige anonyme E-Mail

gesendet hat, wird durch die zweite Mail als ein ganz bestimmter anonymer Informant erkennbar, nämlich als der Urheber der ersten Nachricht. Wenn dieselbe Quell-E-Mail-Adresse verwendet wird *und* diese E-Mail-Adresse auch für eine Antwort genutzt werden kann, dann muss der Informant außerordentlich vorsichtig sein, um seine Identität zu schützen.

Pseudonymität kann ausreichend und in einigen Fällen sogar zu bevorzugen sein, insbesondere dann, wenn ein Informant Informationen in beiden Richtungen austauschen muss, also z. B. um auf Fragen von Journalisten oder von Strafverfolgungsbehörden einzugehen.

7.6 Tipps für die anonyme E-Mail-Kommunikation

Wie bereits erwähnt, können Ihre E-Mail-Aktivitäten Ihre Anonymität gefährden. Wie bei allen anderen Internetdiensten, die Sie über Tor nutzen, müssen Sie auch bei E-Mails immer daran denken, welche Daten Sie bei den verschiedenen Tätigkeiten preisgeben.

Beispielsweise sollten Sie von einem anonymen E-Mail-Konto aus niemals Nachrichten an Ihr persönliches E-Mail-Konto senden – und auch nicht an Freunde, Verwandte, Kollegen oder andere Personen, die nicht anonyme Verbindungen zu Ihnen haben.

Die Lektüre dieses Buches ist ein guter Ausgangspunkt, aber darüber hinausgehende Recherche ist eine gute Sache. Die EFF bietet mit dem Artikel »A Tutorial on Anonymous Email Accounts« (*https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts*) einen guten Überblick darüber, wie Sie die E-Mail-Kommunikation anonym einrichten und nutzen. Auch in den folgenden Abschnitten erhalten Sie einige Tipps und Anregungen.

7.6.1 Die Anonymität bei der E-Mail-Kommunikation wahren

Die technischen Maßnahmen, um Ihre Anonymität im E-Mail-Verkehr zu wahren, sind ganz einfach: Nehmen Sie ausschließlich über Tor Verbindung mit Ihrem E-Mail-Konto auf und verwenden Sie nur einen Webmaildienst, der HTTPS unterstützt. Denken Sie aber auch daran, dass jeder, der Zugang zu dem E-Mail-Server hat, auf den Klartext Ihrer Nachrichten zugreifen kann. Daher ist es sinnvoll, Ihre Nachrichten zu verschlüsseln. Doch selbst dann kann ein Gegner herausfinden, mit wem Sie korrespondieren (da sich die E-Mail-Adressen im Gegensatz zu den Inhalten nicht verschlüsseln lassen). Daher müssen Sie Vorsicht walten lassen.

Neben der Verwendung von Tor und HTTPS sollten Sie zur Wahrung Ihrer Anonymität Folgendes beachten:

- Schlagen Sie Ihren Korrespondenzpartnern vor, ebenfalls anonyme E-Mail-Konten zu verwenden. Ihre Identität kann dadurch erkannt werden, mit wem Sie kommunizieren. Das kann durch die Befragung dieser Personen geschehen, aber auch schon durch Analyse (wenn jemand mit drei von vier Partnern kommuniziert, die zusammen ein Geschäft betreiben, dann kann ein Gegner daraus schließen, dass dieser jemand der vierte Partner ist).
- Geben Sie in Ihren Nachrichten keinerlei Informationen an, über die Sie identifiziert werden können, also beispielsweise wer Sie sind, wo Sie sich zu einem bestimmten Zeitpunkt befinden, in welcher Organisation Sie tätig sind, wo Sie wohnen, oder irgendwelche anderen Dinge, die Rückschlüsse auf Ihre Identität zulassen.
- Verschlüsseln Sie alle Nachrichten. Dadurch kann Ihr E-Mail-Provider Ihre Nachrichten nicht untersuchen oder ohne Ihre Kenntnis und Ihre Zustimmung entschlüsseln. Wenn Sie Ihre Nachrichten vom Provider verschlüsseln lassen, kann er sie dagegen auch ohne Ihr Wissen und Ihre Zustimmung entschlüsseln.

7.6.2 Verwenden Sie immer Tor

Durch die Verwendung von Tor wird Ihre IP-Adresse wirkungsvoll vor dem Server verborgen, auf den Sie zum Abrufen und Senden von E-Mails zurückgreifen. Daher gilt: Regel Nr. 1: Verwenden Sie immer Tor; Regel Nr. 2: Siehe Regel Nr. 1.

Greifen Sie niemals ohne Tor auf Ihr anonymes E-Mail-Konto zu. Sie können davon ausgehen, dass Ihr E-Mail-Provider Protokolle des gesamten Clientzugriffs einschließlich der IP-Adressen führt, von denen aus Sie Verbindung aufgenommen haben. Wenn diese IP-Adressen zu Tor-Austrittsknoten gehören, bleibt Ihre Anonymität sehr wahrscheinlich gewahrt. Greifen Sie dagegen von einem Nicht-Tor-Knoten auf Ihr Konto zu, kann es mit diesem Knoten in Verbindung gebracht werden.

Es gibt viele Möglichkeiten, durch die Sie beim Zugriff Ihre Identität verraten können:

- Wenn der Zugriff von Ihrem privaten Computer zu Hause über Ihren Internetprovider erfolgt, kann das anonyme E-Mail-Konto zu Ihnen zurückverfolgt werden, da der E-Mail-Dienst Ihre IP-Adresse protokolliert, die über Ihren Internetprovider wiederum mit Ihnen in Verbindung gebracht werden kann.
- Wenn der Zugriff von einem Internetcafé aus erfolgt, in dem Sie sich ausweisen müssen (beispielsweise verlangen viele öffentliche Bibliotheken einen Identitätsnachweis, um einen ihrer PCs nutzen zu können), kann ein Ermittler die IP-Adresse vom E-Mail-Provider in Erfahrung bringen und dann in der Bibliothek oder dem Café Einsichtnahme in die Aufzeichnungen verlangen, die angeben, wer zu welchem Zeitpunkt welchen Rechner genutzt hat.
- Auch Zugriffsmuster können zur Aufdeckung der Identität herangezogen werden. Ein gutes Beispiel dafür ist die Petraeus-Affäre, bei denen der Zugriff auf das »anonyme« Gmail-Konto von verschiedenen Standorten mit dem Reiseverlauf einer Person abgeglichen wurde.

7.6.3 Verwenden Sie stets HTTPS

Die Verwendung von Tor ist zur Wahrung der Anonymität notwendig, aber nicht hinreichend. Beim Durchlaufen des Tor-Netzwerks sind alle Daten verschlüsselt, aber sofern nicht HTTPS eingesetzt wird, erfolgt die Übertragung der Daten vom Tor-Austrittsrelay zum Server (und zurück) in Klartext.

Die Verwendung HTTPS Everywhere (*https://www.eff.org/https-everywhere*) ist für die Nutzung des Internets ganz allgemein empfehlenswert, ob Sie nun anonym bleiben wollen oder nicht. Diese Vorkehrung ist im TBB enthalten. Entscheidend ist also, dass Sie einen E-Mail-Provider auswählen, der einen HTTPS-Zugriff auf Ihr Konto ermöglicht.

7.7 Schritt für Schritt: Ein anonymes E-Mail-Konto einrichten

Eine gute Wahl zur Einrichtung eines anonymen E-Mail-Kontos bietet Yahoo!, da dieser Dienst zurzeit einen HTTPS-Zugriff auf E-Mails ermöglicht, die Kontoeinrichtung und den Mailzugriff über das Tor-Netzwerk erlaubt und nicht (immer) die Angabe einer alternativen E-Mail-Adresse oder einer Telefonnummer verlangt.

Die Einrichtung eines E-Mail-Kontos bei Yahoo!, über das sich Ihre Identität nicht so leicht herausfinden lässt, ist ganz einfach:

- Starten Sie das TBB, vergewissern Sie sich, dass alles richtig eingerichtet ist und Sie Tor verwenden, und suchen Sie Yahoo! auf (*http://de.yahoo.com*).
- Sie müssen zunächst eine neue Yahoo!-ID erstellen. Öffnen Sie daher über die Schaltfläche *Anmelden* oder *Mail* die Anmeldeseite und klicken Sie auf *Account erstellen*.

- Füllen Sie das Registrierungsformular aus. Geben Sie dabei weder eine alternative E-Mail-Adresse noch eine Telefonnummer an.

Geben Sie beim Ausfüllen des Registrierungsformulars nicht Ihren echten Namen an, und achten Sie darauf, dass alle erfundenen Informationen, die Sie bereitstellen, plausibel klingen, aber nicht mit Ihnen in Verbindung gebracht werden können. Denken Sie auch daran, dass Anonymität in großer Gesellschaft besser funktioniert. Wenn Sie als Ihr Heimatland die Neutrale Zone zwischen Saudi-Arabien und dem Irak oder Wallis und Futuna angeben, machen Sie Ihr Konto dadurch äußerst auffällig. Wählen Sie lieber ein bevölkerungsreicheres Land mit starker Internetanbindung.

Validierung der Tor-Software

A.1 Tor-Software mit GNU Privacy Guard validieren

GNU Privacy Guard (GnuPG) ist die führende OpenPGP-kompatible Software für die Verschlüsselung mit öffentlichen Schlüsseln und damit auch für die Validierung von digitalen Signaturen. Sie ist in den meisten Linux-Distributionen im Lieferumfang enthalten. Die einfachste und sicherste Möglichkeit, sich die nötige Software zur Validierung signierter Downloads zu beschaffen, besteht also darin, eine vertrauenswürdige Linux-Version zu erwerben.

Um einen Tor-Download zu validieren, gehen Sie wie folgt vor:

- Laden Sie das gewünschte Paket herunter (die TBB-Version für Ihr System). Diese Datei trägt einen Namen wie *TorBrowser-2.3.25-6-osx-i386-de.zip*.
- Laden Sie die Signaturdatei herunter, die einen Namen wie *TorBrowser-2.3.25-6-osx-i386-de.zip.asc* trägt. (Mit anderen Worten, Sie hat den gleichen Namen wie die heruntergeladene Datei, aber mit dem zusätzlichen Suffix *.asc*.) Wenn Sie auf der Tor-Projektwebsite auf den Link *sig* klicken, wird die Signatur auf einer neuen Seite angezeigt (siehe nachfolgende Abbildung). Speichern Sie diese Seite (oder laden Sie sie herunter, indem Sie bei gedrückter Alt-Taste darauf klicken).
- Öffnen Sie die Kommandozeile (Eingabeaufforderung) Ihres Systems, wechseln Sie in das Downloadverzeichnis und geben Sie folgenden Befehl ein:

```
gpg --keyserver hkp://pool.sks-keyservers.net --recv-keys
  0x63FEE659
```

  Mit diesem Befehl laden Sie den Signierschlüssel vom Erinn Clark herunter, dem Mitglied des Tor-Projekts, das für das Signieren von TBB-Downloads zuständig ist. (Vergewissern Sie sich aber auf der Website des Tor-Projekets, dass das immer noch der Fall ist!) Dadurch wird Clarks öffentlicher Schlüssel Ihrem GnuPG-Schlüsselbund hinzugefügt.

- Der nächste Schritt besteht darin, den OpenPGP-Fingerabdruck für diesen Schlüssel mit folgendem Befehl zu überprüfen:

```
gpg --fingerprint 0x63FEE659
```

Das System gibt nun Folgendes aus:

```
pub   2048R/63FEE659 2003-10-16
Key fingerprint = 8738 A680 B84B 3031 A630 F2DB 416F 0610
  63FE E659
uid                  Erinn Clark <erinn@torproject.org>
uid                  Erinn Clark <erinn@debian.org>
uid                  Erinn Clark <erinn@double-helix.org>
sub   2048R/EB399FD7 2003-10-16
```

Wenn die zweite Zeile (die mit `Key fingerprint` beginnt) nicht mit dem übereinstimmt, was Sie hier (und auf der Tor-Website) sehen, dann liegt ein Problem vor.

- Ist alles in Ordnung, geben Sie den folgenden Befehl ein, um den Download zu überprüfen:

```
gpg --verify *download-file*.zip.asc *download-file*.zip
```

Das Ergebnis (wenn die Signatur als gültig erkannt wird) sieht ähnlich aus wie die Ausgabe in Abbildung A.1. Die Zeile `WARNING` besagt, dass Sie auf den Schritt verzichtet haben, Clarks Schlüssel ausdrücklich zu verifizieren. Das ändert jedoch nichts an der Tatsache, dass die digitale Signatur verifiziert wurde und die heruntergeladenen Dateien gefahrlos verwendet werden können.

Ein Beispiel dafür, wie eine digitale TBB-Signatur aussieht, finden Sie in Abbildung A.2.

Weitere Einzelheiten über die Verwendung von GnuPG erfahren Sie in »Simple Steps to Data Encryption« (Peter Loshin, Syngress 2013).

```
$ gpg --verify TorBrowser-2.3.25-6-osx-i386-en-US.zip.asc
TorBrowser-2.3.25-6-osx-i386-en-US.zip
gpg: Signature made Thu Apr 4 23:21:29 2013 EDT using RSA key
  ID 63FEE659
gpg: requesting key 63FEE659 from hkp server keys.gnupg.net
gpg: key 63FEE659: public key „Erinn Clark <erinn@torproject
  .org>“ imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust
  model
gpg: depth: 0 valid: 10 signed: 0 trust: 0-, 0q, 0n, 0m,0f, 10u
gpg: next trustdb check due at 2014-11-12
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
gpg: Good signature from „Erinn Clark <erinn@torproject.org>“
gpg: aka „Erinn Clark <erinn@debian.org>“
gpg: aka „Erinn Clark <erinn@double-helix.org>“
gpg: WARNING: This key is not certified with a trusted
  signature!
gpg: There is no indication that the signature belongs to the
  owner.
Primary key fingerprint: 8738 A680 B84B 3031 A630 F2DB 416F
  0610 63FE E659
```

Abbildung A.1: Diese Ausgabe zeigt, dass die digitale Signatur für einen TBB-Download verifiziert werden konnte.

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (Darwin)
iQEcBAABAgAGBQJRXkM5AAoJEEFvBhBj/uZZQ5kIAOCPXWHC/Q5OsP79SnY5
CEOkqBub5XUgl0DdIZal27qNf3lAlbbC0S9PdcLZPrm1HJyrT+Wyxc3QGS/
oJgqKCx9/WM7DCg+jsg4z4NU8Yk6U9oGpJaTw7/CkUptdlqvY/tNMGLs0er-
MyOyVwg/Kd01vk3GCe8oeyNtUmq0K7D99ZrPjOjqUN7ShBo1+WyLWkKwJMvFop
swnfJqDcPwUHqD/26JfFSGbJjT+jUU+lCwuFCuSIuCYSUckoEtVN0IfoDVs8M
UuM38zJieJ8hl7SPeo1SOI66bWHK3/AwQ9no7bFGonf0TdY4Bt+CdZEjvoyp/
DyzTh53J/24iYXrU7Pn+M==R5XS
-----END PGP SIGNATURE-----
```

Abbildung A.2: Der Inhalt der Datei mit der digitalen Signatur für einen TBB-Download

A.2 Tails-Distributionen mit GnuPG validieren

Um einen Tails-Download zu validieren, gehen Sie folgendermaßen vor:

- Laden Sie die neueste Tails-Version herunter. Die Datei trägt einen Namen wie *tails-i386-0.17.2.iso*.
- Laden Sie die Signaturdatei herunter, deren Name *tails-i386-0.17.2.iso.pgp* oder ähnlich lautet. Dazu klicken Sie auf der Tails-Website auf den Link *Cryptographic Signature*.
- Öffnen Sie die Kommandozeile (Eingabeaufforderung) des Systems, wechseln Sie zum Downloadverzeichnis und geben Sie folgenden Befehl ein:

  ```
  gpg --keyserver hkp://pool.sks-keyservers.net --recv-keys
  0xBE2CD9C1
  ```

  Mit diesem Befehl laden Sie den Signierschlüssel des Tails-Entwicklerteams herunter, das dafür zuständig ist, Tails-Downloads zu sig-

nieren. Allerdings sollten Sie auf der Tails-Website nachsehen, ob das immer noch der Fall ist. Der öffentliche Schlüssel der Tails-Entwickler wird durch diesen Befehl Ihrem GnuPG-Schlüsselbund hinzugefügt. Die Ausgabe sehen Sie in Abbildung A.3.

```
$ gpg --keyserver hkp://pool.sks-keyservers.net --recv-keys
  0xBE2CD9C1
gpg: requesting key BE2CD9C1 from hkp server pool.sks-
  keyservers.net
gpg: key BE2CD9C1: public key „Tails developers (signing key)
  <tails@boum.org>“ imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust
  model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

Abbildung A.3: Den Signierschlüssel des Tails-Entwicklerteams herunterladen

```
$ gpg --verify ~/Downloads/tails-i386-0.17.2.iso.pgp
~/Downloads/tails-i386-0.17.2.iso
gpg: Signature made Sun 07 Apr 2013 08:57:06 AM EDT using RSA
  key ID BE2CD9C1
gpg: Good signature from „Tails developers (signing key)
  <tails@boum.org>“
gpg: aka „T(A)ILS developers (signing key) <amnesia@boum.org>“
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the
  owner.
Primary key fingerprint: 0D24 B36A A9A2 A651 7878 7645 1202
  821C BE2C D9C1
```

Abbildung A.4: Die heruntergeladene ISO-Datei für Tails anhand ihrer digitalen Signatur überprüfen

- Der nächste Schritt besteht darin, den OpenPGP-Fingerabdruck dieses Schlüssels mit dem folgenden Befehl zu überprüfen:

```
gpg --fingerprint 0xBE2CD9C1
```

  Das System gibt daraufhin Folgendes zurück:

```
pub   4096R/BE2CD9C1 2010-10-07 [expires: 2015-02-05]
Key fingerprint = 0D24 B36A A9A2 A651 7878 7645 1202 821C
  BE2C D9C1
uid     Tails developers (signing key) <tails@boum.org>
uid     T(A)ILS developers (signing key) <amnesia@boum.org>
```

  Wenn die zweite Zeile (die mit `Key fingerprint` beginnt) nicht mit dem übereinstimmt, was Sie hier (und auf der Tails-Website) sehen, dann liegt ein Problem vor.

- Ist alles in Ordnung, geben Sie den folgenden Befehl ein, um den Download zu überprüfen:

```
gpg --verify *download-file*.pgp *download-file*
```

  Das Ergebnis (wenn die Signatur als gültig erkannt wird) sieht ähnlich aus wie die Ausgabe in Abbildung A.4. Die Zeile `WARNING` besagt, dass Sie auf den Schritt verzichtet haben, den Schlüssel der Tails-Entwickler ausdrücklich zu verifizieren. Das ändert jedoch nichts an der Tatsache, dass die digitale Signatur verifiziert wurde und die heruntergeladenen Dateien gefahrlos verwendet werden können.

Weitere Einzelheiten über die Verwendung von GnuPG erfahren Sie in »Simple Steps to Data Encryption« (Peter Loshin, Syngress 2013).

A.3 Mit welchen PGP-Schlüsseln sind welche Pakete signiert?

Zum Signieren von Tor und zugehörigen Paketen werden die folgenden Schlüssel verwendet (laut Tor-Projektwebsite, *https://www.torproject.org/docs/signing-keys.html.en*, Stand April 2015):

- Das Entwicklerteam für den Tor-Browser (0x93298290), Mike Perry (0x0E3A92E4), Georg Koppen (0x4B7C3223), Nicolas Vigier (0xD0220E4B) und Linus Nordberg (0x23291265) signieren die Ausgaben des Tor-Browsers.
- Roger Dingledine (0x28988BF5 und 0x19F78451) oder Nick Mathewson (0x165733EA oder der Unterschlüssel 0x8D29319A) signieren die Tarballs mit dem Tor-Quellcode.
- Erinn Clark (0x63FEE659) hat ältere TBBs und viele andere Pakete signiert und mit ihrem anderen Schlüssel (0xF1F5C9B5) auch RPMs. Andrew Lewman (0x31B0974B, 0x6B4D6475) hat Pakete für RPMs, Windows und OS X signiert.
- Das Tor-Projektarchiv (0x886DDD89) signiert die Repositorys und Archive auf *deb.torproject.org*.
- Damian Johnson (0x9ABBEEC6) signiert Arm-Releases.
- Sebastian Hahn (0xC5AA446D) und David Fifield (0xC11F6276) signieren Plug-In-Transportproxys. Manchmal signiert Sebastian auch TBBs.
- Das Tails-Team (0xBE2CD9C1) signiert die Tails-Versionen.
- Weitere Entwickler sind Peter Palfrader (0xC82E0039 oder der Unterschlüssel 0xE1DEC577) und Jacob Appelbaum (0xD255D3F5C868227F).

Die Fingerabdrücke der Schlüssel sehen wie folgt aus:

```
pub   1024D/28988BF5 2000-02-27
Key fingerprint = B117 2656 DFF9 83C3 042B  C699 EB5A 896A
  2898 8BF5
    uid                  Roger Dingledine <arma@mit.edu>

pub   4096R/19F78451 2010-05-07
Key fingerprint = F65C E37F 04BA 5B36 0AE6  EE17 C218 5258
  19F7 8451
    uid                  Roger Dingledine <arma@mit.edu>
    uid                  Roger Dingledine <arma@freehaven.net>
    uid                  Roger Dingledine <arma@torproject.org>
    sub   4096R/0DCC0FE1 2013-05-09 [expires: 2014-05-09]

pub   3072R/165733EA 2004-07-03
Key fingerprint = B35B F85B F194 89D0 4E28  C33C 2119 4EBB
  1657 33EA
    uid                  Nick Mathewson <nickm@alum.mit.edu>
    uid                  Nick Mathewson <nickm@wangafu.net>
    uid                  Nick Mathewson <nickm@freehaven.net>
    uid                  [jpeg image of size 3369]
    sub   3072R/8D29319A 2004-07-03
    sub   3072R/F25B8E5E 2004-07-03

pub   2048R/63FEE659 2003-10-16
Key fingerprint = 8738 A680 B84B 3031 A630  F2DB 416F 0610
  63FE E659
    uid                  Erinn Clark <erinn@torproject.org>
    uid                  Erinn Clark <erinn@debian.org>
    uid                  Erinn Clark <erinn@double-helix.org>
    sub   2048R/EB399FD7 2003-10-16
```

```
pub   1024D/F1F5C9B5 2010-02-03
Key fingerprint = C2E3 4CFC 13C6 2BD9 2C75  79B5 6B8A AEB1
  F1F5 C9B5
    uid                  Erinn Clark <erinn@torproject.org>
    sub   1024g/7828F26A 2010-02-03

pub  1024D/31B0974B 2003-07-17
Key fingerprint = 0295 9AA7 190A B9E9 027E  0736 3B9D 093F
  31B0 974B
    uid                  Andrew Lewman <andrew@lewman.com>
    uid                  Andrew Lewman <andrew@torproject.org>
    sub   4096g/B77F95F7 2003-07-17

pub   4096R/6B4D6475 2012-02-29
Key fingerprint = 0291 ECCB E42B 2206 8E68  5545 627D EE28
  6B4D 6475
    uid                  Andrew Lewman <andrew@torproject.org>
    uid                  Andrew Lewman <andrew@torproject.is>
    sub   4096R/BE713AC6 2012-02-29

pub   2048R/886DDD89 2009-09-04 [expires: 2014-09-03]
Key fingerprint = A3C4 F0F9 79CA A22C DBA8  F512 EE8C BC9E
  886D DD89
    uid                  deb.torproject.org archive signing key
    sub   2048R/219EC810 2009-09-04 [expires: 2014-08-29]

pub   1024D/9A753A6B 2009-09-11
Key fingerprint = 553D 7C2C 626E F16F 27F3  30BC 95E3 881D
 9A75 3A6B
    uid                  Tomás Touceda <chiiph@gmail.com>
    sub   1024g/33BE0E5B 2009-09-11
```

```
pub   1024D/5FA14861 2005-08-17
Key fingerprint = 9467 294A 9985 3C9C 65CB  141D AF7E 0E43
  5FA1 4861
    uid                  Matt Edman <edmanm@rpi.edu>
    uid                  Matt Edman <Matt_Edman@baylor.edu>
    uid                  Matt Edman <edmanm2@cs.rpi.edu>
    sub   4096g/EA654E59 2005-08-17

pub   1024D/9ABBEEC6 2009-06-17
Key fingerprint = 6827 8CC5 DD2D 1E85 C4E4  5AD9 0445 B7AB
  9ABB EEC6
    uid                  Damian Johnson (www.atagar.com)
  <atagar1@gmail.com>
    uid                  Damian Johnson <atagar@torproject.org>
    sub   2048g/146276B2 2009-06-17
    sub   2048R/87F30690 2010-08-07

pub   8192R/683686CC 2013-09-11
Key fingerprint = C963 C21D 6356 4E2B 10BB  335B 2984 6B3C
  6836 86CC
    uid              Mike Perry (Regular use key) <mikeperry@
  torproject.org>
    sub   4096R/0E3A92E4 2013-09-11 [expires: 2014-09-11]
    sub   4096R/BC40FFA0 2013-09-11 [expires: 2014-09-11]

pub   1024D/22F6856F 2006-08-19
Key fingerprint = DDB4 6B5B 7950 CD47 E59B  5189 4C09 25CF
  22F6 856F
    uid                  Robert Hogan <robert@roberthogan.net>
    sub   1024g/FC4A9460 2006-08-19

pub   2048R/4279F297 2013-01-02
Key fingerprint = 97BB 9413 1873 FFD3 1331  64CC 7EB4 5C0A
  4279 F297
    uid                  Alexandre Allaire <alexandre.allaire@
  mail.mcgill.ca>
    sub   2048R/76D943F1 2013-01-02
```

```
pub   4096R/C5AA446D 2010-07-14
Key fingerprint = 261C 5FBE 7728 5F88 FB0C  3432 66C8 C2D7
  C5AA 446D
    uid                  Sebastian Hahn <mail@sebastianhahn.net>
    sub   2048R/A2499719 2010-07-14
    sub   2048R/140C961B 2010-07-14

pub   4096R/C82E0039 2003-03-24
Key fingerprint = 25FC 1614 B8F8 7B52 FF2F  99B9 62AF 4031
  C82E 0039
    uid                  Peter Palfrader
    uid                  Peter Palfrader <peter@palfrader.org>
    uid                  Peter Palfrader <weasel@debian.org>

pub   4096R/BE2CD9C1 2010-10-07 [expires: 2015-02-05]
Key fingerprint = 0D24 B36A A9A2 A651 7878  7645 1202 821C
  BE2C D9C1
    uid                  Tails developers (signing key)
  <tails@boum.org>
    uid                  T(A)ILS developers (signing key)
  <amnesia@boum.org>

pub   8192R/C11F6276 2012-07-21
Key fingerprint = AD1A B35C 674D F572 FBCE  8B0A 6BC7 58CB
  C11F 6276
    uid                  David Fifield <david@bamsoftware.com>
    sub   4096R/D90A8E40 2012-07-21
    sub   4096R/5CD388E5 2012-07-21

pub   4096R/23291265 2010-05-07
Key fingerprint = 8C4C D511 095E 982E B0EF  BFA2 1E8B F349
  2329 1265
    uid                  Linus Nordberg <linus@nordberg.se>
    uid                  Linus Nordberg <linus@nordu.net>
    uid                  Linus Nordberg <linus@torproject.org>
    uid                  [jpeg image of size 2906]
    sub   4096R/153E576C 2013-04-23 [expires: 2014-04-23]
```

```
pub   4096R/4B7C3223 2013-07-30
Key fingerprint = 35CD 74C2 4A9B 15A1 9E1A  81A1 9437 3AA9
  4B7C 3223
    uid               Georg Koppen <gk@torproject.org>
    uid               Georg Koppen <groeg@vfemail.net>
    uid               Georg Koppen <georg@getfoxyproxy.org>
    sub   4096R/97955E07 2013-07-30 [expires: 2014-07-30]
    sub   4096R/AC3A821D 2013-07-30 [expires: 2014-07-30]
    sub   4096R/A97A53DC 2014-07-08 [expires: 2015-07-08]
    sub   4096R/E5AE3C98 2014-07-08 [expires: 2015-07-08]

pub   4096R/D0220E4B 2014-03-19
Key fingerprint = 4A90 646C 0BAE D9D4 56AB  3111 E5B8 1856
  D022 0E4B
uid                 Nicolas Vigier (TBB Builds Signing Key)
  <boklm@torproject.org>

pub   4096R/D255D3F5C868227F 2014-06-27 [expires: 2024-06-24]
Key fingerprint = D2C6 7D20 E9C3 6C2A C5FE  74A2 D255 D3F5
  C868 227F
    uid                 Jacob Appelbaum <jacob@appelbaum.net>
    sub   3072R/02636620744301A2 2014-06-27 [expires: 2015-06-27]
    sub   3072R/1A055A481801A819 2014-06-27 [expires: 2015-06-27]

pub   4096R/90BC9192B06291B2 2014-06-27 [expires: 2024-06-24]
Key fingerprint = 043E 0E69 DD56 BA59 5905  8756 90BC 9192
  B062 91B2
    uid                 Jacob Appelbaum <error@debian.org>
    sub   3072R/F78ED60FFE4F141F 2014-06-27 [expires: 2015-06-27]
    sub   3072R/986D6BCEF02A9C9C 2014-06-27 [expires: 2015-06-27]
    sub   2048R/89AA6E5D2C6A7F40 2014-10-22 [expires: 2016-10-21]
```

```
pub   4096R/FA7F0E44D487F03F 2014-06-27 [expires: 2024-06-24]
Key fingerprint = D6A9 48CF 297F 7539 30B4  756A FA7F 0E44
  D487 F03F
    uid                  Jacob Appelbaum <jacob@torproject.org>
    sub   3072R/611B45DE2517F1BA 2014-06-27 [expires: 2015-06-27]
    sub   3072R/035D7A9A67D22BC0 2014-06-27 [expires: 2015-06-27]

pub   4096R/0x4E2C6E8793298290 2014-12-15
Key fingerprint = EF6E 286D DA85 EA2A 4BA7  DE68 4E2C 6E87
  9329 8290
    uid   Tor Browser Developers (signing key) <torbrowser@
  torproject.org>
    sub   4096R/0x2E1AC68ED40814E0 2014-12-15
    sub   4096R/0x7017ADCEF65C2036 2014-12-15
    sub   4096R/0x2D000988589839A3 2014-12-15
```

B

Wenn Tor-Downloads gesperrt werden

In diesem Anhang erfahren Sie, wie Sie an die Tor-Software gelangen können, wenn Sie der Blockade oder Filterung durch einen Gegner unterliegen. Schauen Sie aber auf jeden Fall auf der Website des Tor-Projekts nach. Dort finden Sie ausführlichere Informationen, weitere Möglichkeiten und die aktuellsten Notlösungen für den Zugriff auf das Tor-Netzwerk.

Staatliche Firewalls können den Zugriff auf die Tor-Projektwebsite (*https://www.torproject.org*) ziemlich einfach sperren. Wie bereits in Kapitel 4 erwähnt, blockiert die Große Chinesische Firewall (GFC) den Zugriff auf URLs, die den String *torproject.org* enthalten. Sogenannte »Spiegel« oder »Mirror« (Server, die die offiziellen Server des Tor-Projekts »widerspiegeln« oder identisch mit ihnen sind) bleiben jedoch zugänglich.

Wenn eine Firewall oder ein Filter den Zugang zum Server des Tor-Projekts blockiert, können Sie die Tor-Software trotzdem beziehen, indem Sie sich an einen der Spiegel wenden. Die Schwierigkeit besteht darin, die URLs dieser Spiegel herauszufinden, ohne blockiert oder gefiltert zu werden.

Außerdem ist es Gegnern möglich, den Zugang zu den Tor-Spiegeln zu sperren. Für diesen Fall gibt es einen Mechanismus, durch den Sie eine Kopie von Tor per E-Mail anfordern können.

Wenn alle Stricke reißen, können Sie Tor auch von einem anderen Tor-Benutzer beziehen, wobei Sie jedoch sehr vorsichtig sein müssen.

Denken Sie immer daran – und ganz besonders, wenn Sie Schwierigkeiten haben, die Tor- oder Tails-Software zu beziehen –, die digitalen Signaturen der Downloads zu überprüfen.

B.1 Tor-Spiegel

Um eine Liste der Tor-Spiegel zu beziehen, wird empfohlen, in Google nach »tor mirrors« zu suchen (*https://encrypted.google.com/search?q5tor1mirrors*) und dann im Google-Ergebniscache nachzusehen. (Das oberste Ergebnis ist meistens die Seite »Tor Mirrors« auf der Website des Tor-Projekts auf *https://www.torproject.org/getinvolved/mirrors.html.en*, die von der staatlichen Firewall höchstwahrscheinlich gesperrt wird.)

Um den Google-Cache einzusehen, klicken Sie auf das kleine, grüne, auf dem Kopf stehende Dreieck neben dem (ebenfalls grün dargestellten) URL für die Spiegelseite des Tor Projekts und wählen *Im Cache*. Daraufhin wird eine von Google zwischengespeicherte Kopie der Liste angezeigt, auf der Sie auch die URLs finden, mit denen Sie direkt Verbindung zu den Spiegelsites erhalten.

B.2 Tor per E-Mail

Der Download des TBB ist zurzeit (April 2015) etwa 35 MB groß. Eine Datei dieser Größe an eine E-Mail anzuhängen, kann schwierig sein. Es ist aber möglich, und wenn Sie nicht in der Lage sind, die Website des Tor-Projekts oder irgendwelche Spiegel zu erreichen, können Sie Tor per E-Mail erhalten, indem Sie eine Nachricht an die Adresse *gettor@torproject.org* senden und als Text Ihr Betriebssystem angeben, also *windows*, *linux* oder *osx*. Es gibt noch weitere E-Mail-Adressen (Aliase), von denen Sie die gleiche Antwort halten. Aktuelle Informationen erhalten Sie in dem Artikel »GetTor Robot« auf *https://www.torproject.org/projects/gettor.html*.

Diese E-Mail-Adresse ist ein Alias für einen E-Mail-*Roboter*, der Ihnen eine Liste von Links zusendet, über die Sie Tor von weit verbreiteten Clouddiensten herunterladen können.

Beachten Sie dabei die folgenden Tipps:

- *Verwenden Sie zur Anforderung von Tor per E-Mail ein Gmail- oder Yahoo!-Konto.* Da diese Anbieter es erschweren, Massen von E-Mail-Konten zu generieren, besteht bei der Nutzung ihrer Dienste ein geringeres Risiko für das Tor-Projekt, auf eine E-Mail-Anforderung zu antworten. Gegner, die die Aktivitäten des Tor-Projekts stören wollen, können große Mengen von gültigen E-Mail-Adressen erzeugen und einen Denial-of-Service-Angriff (DoS) durchführen, indem sie die Tor-E-Mail-Server mit zahllosen Anforderungen überschwemmen.
- *Wenn Sie keine Antwort bekommen, schauen Sie im Bug-Tracker des Tor-Projekts nach.* Manchmal geht etwas schief, ohne dass die Mitarbeiter des Tor-Projekts es merken. Beispielsweise funktionierte der GetTor-E-Mail-Roboter im Frühjahr 2013 eine Zeit lang nicht korrekt. Ein Benutzer hat das Problem auf der Bug-Tracking-Website (*https://trac.torproject.org/projects/tor*) gemeldet, sodass es kurz darauf korrigiert werden konnte.

B.3 Weitere Möglichkeiten

Wenn Sie jemanden kennen, der Tor verwendet, können Sie ihn bitten, Ihnen eine Kopie der Software zu überlassen. Das setzt aber voraus, dass Sie dieser Person wirklich sehr stark vertrauen.

Sollten Sie sich für diese Vorgehensweise entscheiden, darf es für Sie kein Problem darstellen, dass diese Person über Ihre Nutzung von Tor im Bilde ist. Sie müssen auch darauf vertrauen, dass sie nicht gegen Ihre Interessen arbeitet, entweder wissentlich (weil sie auf irgendeine Weise dazu gezwungen wird) oder unwissentlich (weil ihr Computer gehackt wurde, um ihre Kommunikation zu überwachen oder ihre Tor-Software mit einem Keylogger zu infizieren).

Wenn alle Versuche, Tor über das Internet zu erhalten (über die Website, per E-Mail, über den Google-Cache und Spiegelwebsites) fehlschlagen, können Sie sich postalisch oder telefonisch an das Tor-Projekt wenden. Vollständige Kontaktinformationen einschließlich E-Mail-Adressen für den Support, Postanschrift, Telefonnummer, SMS- und IRC-Adressen finden Sie in Anhang C.

Hilfe suchen und Antworten erhalten

Das Tor-Projekt und Tails sind freie Software, die unter der 3-Klausel-Version der BSD-Lizenz veröffentlicht wird (»BSD 3-Clause« oder auch »neue« oder »revidierte« BSD-Lizenz genannt). Dies ist eine sehr freizügige Open-Source-Lizenz, die die Weiterverbreitung als Quellcode oder Binärsoftware erlaubt, sofern bei der weiterverbreiteten Software die gleichen Rechte eingeräumt werden.

Das bedeutet, dass jeder die Software und ihren Quellcode auf jede beliebige Art und Weise nutzen kann.

Wenn Sie bei der Verwendung der Software also auf irgendwelche Probleme stoßen, haben Sie die Möglichkeit, sich den Quellcode anzusehen, Bugs zu entfernen oder zusätzliche Funktionen hinzufügen und die Software weiterhin zu benutzen.

Die meisten Benutzer sind sicherlich nicht gewillt, solche Veränderungen selbst vorzunehmen, und haben auch weder die Fähigkeiten noch die Zeit dazu. Da die Projekte aber möglichst offen durchgeführt werden, haben Sie Zugriff auf die Bug-Berichte zu Tor und Tails mit Hinweisen zu ausstehenden Fehlerkorrekturen, und auf Mailinglisten und IRC-Kanäle, um über Tor und Tails zu diskutieren. Sie können auch Bugs melden, und wenn Sie Tails verwenden, geht das über die Anwendung Whisperback sogar anonym (siehe Kapitel 3).

Auf den Websites zu Tor und Tails werden große Mengen von Informationen veröffentlicht. In diesem Anhang finden Sie einige der wichtigsten Informationsquellen für die Störungssuche bei Problemen mit einer Tor- oder Tails-Sitzung.

C.1 Tor

Praktisch alles, was im Rahmen des Tor-Projekts geschieht, wird dokumentiert und veröffentlicht, und zwar gewöhnlich auf der Bug-Tracker- und Wiki-Seite.

C.1.1 Bug-Tracker/Wiki

Das Tor-Projekt unterhält eine kombinierte Bug-Tracker- und Wiki-Seite. Es lohnt sich, diese Seite mit einem Lesezeichen zu versehen, da sie eine zentrale Informationsquelle darstellt, über die Sie bei Problemen mit Tor Hilfe erhalten:

```
https://trac.torproject.org/projects/tor
```

Die Seite ist auch als verborgener Dienst zu erreichen:

```
http://vwp5zrdfwmw4avcq.onion/
```

C.1.2 Tor-FAQ

Die offizielle Haupt-FAQ-Liste zu Tor finden Sie unter folgenden Adressen:

```
https://www.torproject.org/docs/faq
http://idnxcnkne4qt76tg.onion/docs/faq.html.en
```

Auf der Bug-Tracker- und Wiki-Seite wird eine weitere FAQ-Liste veröffentlicht:

```
https://trac.torproject.org/projects/tor/wiki/doc/TorFAQ
```

Beachten Sie den Hinweis ganz oben auf der Seite: »Diese FAQ-Liste wird in die allgemeine FAQ-Liste übernommen. Die Antworten in dieser Liste können veraltet, falsch oder überholt sein.«

Beachten Sie, dass es »können ... sein« heißt. Viele dieser Fragen wurden vor Jahren beantwortet, und viele der Antworten sind nun nur noch in der »offziellen« FAQ-Liste zu finden. Allerdings können manche der Fragen und Antworten immer noch nützlich und von Belang sein. Wenn die offizielle FAQ-Liste Ihre Frage also nicht beantwortet, kann es sich lohnen, einen Blick in diesen Fragenkatalog zu werfen.

C.1.3 Tor-Dokumentation

Die Tor-Dokumentation steht hier zur Verfügung:

```
https://www.torproject.org/docs/documentation
http://idnxcnkne4qt76tg.onion/docs/documentation.html.en
```

»Kurzanleitungen« in verschiedenen Sprachen finden Sie unter folgender Adresse:

```
https://www.torproject.org/docs/short-user-manual.html.en
```

C.1.4 Verborgene Tor-Server

Um anonym auf die Website zuzugreifen, verwenden Sie den folgenden Pseudo-URL:

```
http://idnxcnkne4qt76tg.onion/
```

Beachten Sie, dass fast alle Links auf dieser Seite zu Seiten des verborgenen Tor-Dienstes führen. Der Link zur Bug-Tracker/Wiki-Seite gehört jedoch nicht dazu, sondern verweist auf die öffentliche Seite.

Die Downloadlinks verweisen auf die Seiten auf dem verborgenen Tor-Server, sodass es möglich ist, das TBB von dem verborgenen Server herunterzuladen. (Allerdings erfolgt der Downloadvorgang dabei erheblich langsamer als von der öffentlichen Website.)

C.2 Das Tor-Projekt

Das Tor-Projekt ist eine gemeinnützige Organisation nach § 501(c)(3) der US-amerikanischen Gesetzgebung mit Sitz in den USA.

C.2.1 Kontaktinformationen

Die offizielle Anschrift der Organisation lautet:

The Tor Project

969 Main Street, Suite 206

Walpole, MA 02081-2972, USA

Weitere Möglichkeiten zur Kontaktaufnahme mit dem Tor-Projekt erhalten Sie auf folgender Seite:

```
https://www.torproject.org/about/contact.html
```

Dort finden Sie Adressen, um über folgende Medien in Verbindung mit dem Tor-Projekt zu treten:

- E-Mail (Support und Mailinglisten)
- Das Microblogging-Konto von Tor (*https://identi.ca/torproject*)
- IRC-Kanäle
- SMS (experimentell und weder sicher noch anonym)
- Telefon (weder sicher noch anonym)

C.2.2 Menschen und Organisationen hinter dem Tor-Projekt

Um mehr über die Menschen und Organisationen herauszufinden, die hinter dem Tor-Projekt stehen – sei es als Mitarbeiter oder als Sponsoren –, sehen Sie sich unter den folgenden Links um:

- Der Jahresbericht des Tor-Projekts von 2012 (*https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf*) gibt einen Überblick über das Tor-Projekt, seine Finanzen und seine Aktivitäten im Jahr 2012.
- »Core Tor People« (*https://www.torproject.org/about/corepeople.html*) ist eine alphabetische Liste mit kurzen Beschreibungen der Menschen, die offiziell am Tor-Projekt mitarbeiten.
- »Tor: Sponsors« (*https://www.torproject.org/about/sponsors.html*) führt die Sponsoren des Projekts auf, getrennt nach zurzeit aktiven und ehemaligen Sponsoren. Zu den Spendern gehören unter anderem die Human Rights Watch, das Naval Research Laboratory, die National Science Foundation und Google.
- »Tor: Financial Reports« (*https://www.torproject.org/about/financials.html*) ist eine Liste von Links zu allen verfügbaren Finanzberichten des Projekts.

Stichwortverzeichnis

Symbole

A

B

C

D

E

F

G

H

I

R

S

T

U

V

W

Y

Z

Peter
Loshin

Ohne Vorkenntnisse

Schritt für Schritt zum sicheren Linux auf dem USB-Stick

Anonym im Internet mit Tor und Tails

Möchten Sie, dass jeder Ihre E-Mails mitliest, und haben Sie ein gutes Gefühl, wenn Ihnen am Bildschirm ständig jemand über die Schulter blickt – haben Sie nichts zu verbergen? Dann können Sie doch auch direkt Ihre Passwörter für E-Mail und Bankkonto veröffentlichen. Ach, soweit wollen Sie dann doch nicht gehen? Nach den ganzen Enthüllungen durch Edward Snowden sollten wir uns alle der steten Überwachung im Internet bewusst sein. Man kann sich anonym im Netz bewegen, zwar mit Aufwand, aber es geht. Wie, das zeigt Ihnen dieses Buch.

Funktionsweise von Tor mit Grafiken erklärt

Nutzen Sie Tor und machen Sie Ihre Tür zu

Über die IP-Adresse kann Ihr aktueller Standort ermittelt werden. Browsercookies speichern häufig Informationen, um den Benutzer eindeutig zu identifizieren. Grundsätzlich ist also bekannt, was Sie zuletzt in der Suchmaschine gesucht haben und welche Webseiten Sie angesteuert haben. Wenn Sie das nicht möchten, dann beschäftigen Sie sich mit Tor. Tor ist ein Werkzeug zur Wahrung der Anonymität, das Anonymisierungsprotokolle für gewöhnliche IP-Adressen nutzt. Mit dem Tor-Browser-Bundle (TBB) steht alles zur Verfügung, um ohne Vorkenntnisse das Tor-Netzwerk zu nutzen.

Aus dem Inhalt:

Noch mehr Anonymität ist möglich

Der Tor-Browser ist schnell installiert, nur hat man immer noch das teilweise unsichere Betriebssystem. Weitere Schutzmechanismen bietet die Linux-Distribution Tails aus dem Tor-Projekt. Tails ist nicht auf das reine Surfen im Internet beschränkt, sondern beinhaltet einige Softwarepakete für die täglich anfallenden Aufgaben. Damit sollten Sie gewappnet sein, um sich im Internet zu bewegen, ohne Spuren zu hinterlassen. So können Sie wieder selbst entscheiden, welche Ihrer Informationen öffentlich zugänglich sein sollen.

9 783645 604161