F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung
Informatik
Wintersemester 2015

Seminar: IT-Sicherheit

Thema:

The Invisible Internet Project – I2P

Eingereicht von:	Jonas Thomsen (Matrikelnr.100051)
Erarbeitet im:	7. Semester
Abgegeben am:	03.01.2016
Betreuerin:	Prof. Dr. Gerd Beuster Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. (0 41 03) 80 48 - 38

Inhaltsverzeichnis

1. Einleitung

1.1 Was ist I2P

Durch zum Beispiel Verbindungs- und Vorratsdatenspeicherung, werden die Bewegungen und die Kommunikation im Internet zunehmend mehr protokolliert. In Ländern wie z.B. Frankreich, hat der jeweilige Internetserviceprovider das Recht die Verbindungsdaten zu speichern.[1] Zudem gibt es seit Anbeginn des Internet den Wunsch nach Anonymität. Gründe dafür können verschiedener Natur sein, jedoch ist es auch im Telemediengesetz festgehalten, dass die Nutzer des Internets ein Recht auf Anonymität und die Verwendung von Pseudonymen haben.[2] Probleme sind jedoch, dass die Nutzer weltweit agieren und so die Gesetze gelten, wo z.B. die Seiten gehostet werden. Zudem gibt es seit den Enthüllungen von Edward Snowden weitere Erkenntnisse, dass die Anonymität auch durch Verschlüsselungstechniken, wie z.B. SSL/TSL nicht immer gegeben ist.[3] Um dieser Probleme entgegen zu wirken, wurde schon 2003 ein Projekt ins Leben gerufen, welches eine anonyme Kommunikation ermöglichen soll.[4]

Der Name des Projektes ist „I2P“ und steht für das „Invisible Internet Project“. Entwickelt wurde und wird es noch von anonymen Entwicklern, die nur durch Pseudonyme bekannt sind. Teilweise haben diese in Vollzeit an diesem Projekt gearbeitet. Die Geldgeber des Projektes sind weitestgehend unbekannt. Die beiden Hauptentwickler nennen sich „eche|on“ und „zzz“.[4]

Das Projekt hat das Ziel, ein anonymes Netzwerk zu bilden, indem es für Anwendungen einen Kommunikationslayer bereitstellt, der es den Anwendern ermöglicht, sicher und anonym Nachrichten austauschen zu können. Es soll die Auslesung, das Abhören und Beobachten von Kommunikation durch 3. Parteien z.B. der NSA erschweren.[3] Anwender des Netzwerkes könnten Aktivisten, Journalisten, sogenannte „Whistleblower“, aber auch gewöhnliche User sein.

---

[1] Vgl. Spiegel Online - Was über sie gesammelt werden soll

[2] Vgl. § 13 Abs. 6 des Deutschen Telemediengesetzes

[3] Vgl. Heise - Die Angriffe auf Verschlüsselung durch NSA und GCHQ

[4] Vgl. The Invisible Project - Einführung

I2P ist wie die bekannteren Netzwerke TOR oder Freenet ein Overlay-Netzwerk, welches parallel zum normalen Internet existiert, oftmals werden diese auch „Darknet“ bezeichnet.[5]

Das Invisible Internet Projekt stellt eine Netzwerk-Software auf Java Basis bereit, welches dem Anwender einen speziellen Router und Netzwerkprotokolle zur Verfügung stellt. Zudem liefert das Software-Bundle weitere Anwendungen die auf die Architektur des Netzwerkes aufsetzen, wie z.B. den E-Mail-Client „I2P-Bote“, der ein dezentrales und Ende-zu-Ende verschlüsseltes E-Mail-System ermöglicht. [5] [6]

Das Netzwerk wird weltweit benutzt, wobei die meisten User aus Europa, Nordamerika und Russland kommen. In Asien, Australien, Afrika und Südamerika wird es hingegen kaum benutzt (siehe Abb.1).

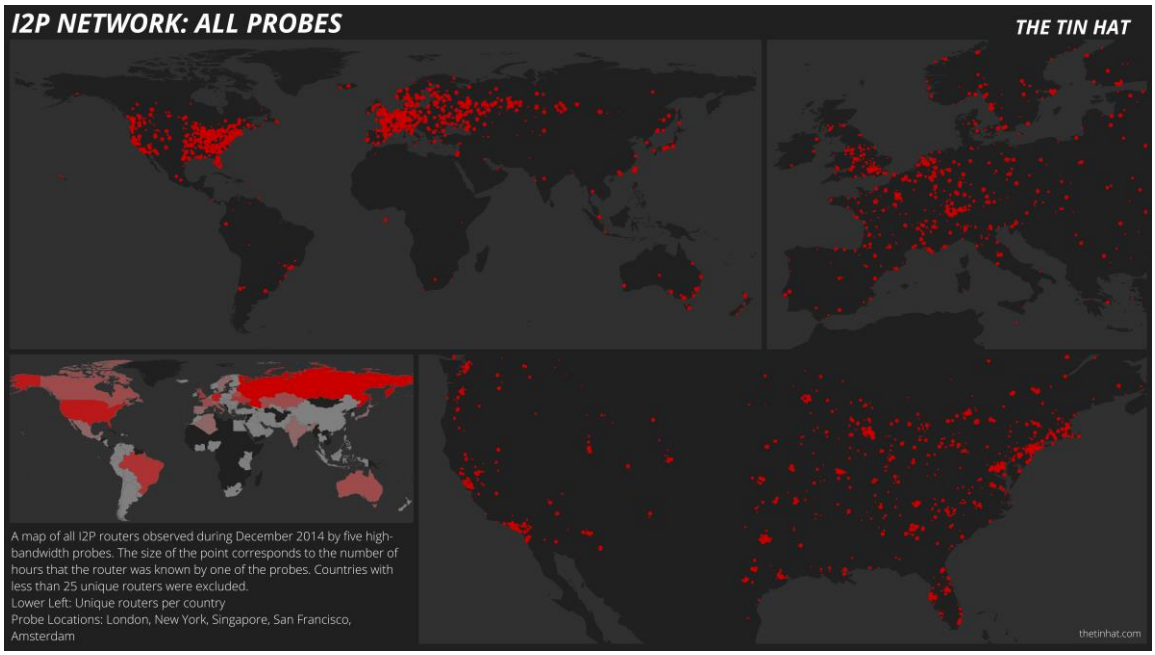

Abb. 1 Netzwerk-Übersicht vom Dezember 2014

[5] Vgl. Golem - Das alternative Tor ins Darknet

[6] Vgl. The Invisible Project - Einführung

Den Hauptteil des Netzwerkes bilden IP-Adressen aus Russland. Auch in den USA sowie in Deutschland gibt es prozentual zur Gesamtheit einen großen Anteil an Teilnehmern(siehe Abb.2).

Hieran wird auch deutlich, dass die I2P-Router nicht anonym sind. Es ist also möglich zu einer IP-Adresse, das Vorhandensein eines I2P-Routers zu ermitteln. Sinn des Netzwerkes ist jedoch nicht die Verschleierung der einzelnen Router, sondern die Verschleierungen der einzelnen Kommunikationen, zwischen den einzelnen Routern.

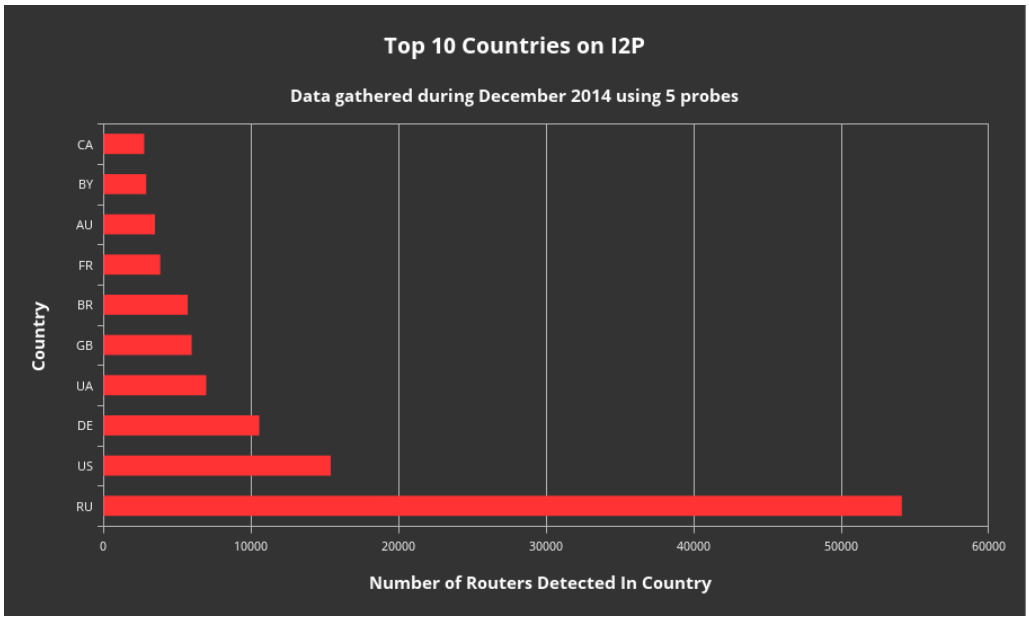

Abb. 2 Top 10 der Teilnehmer nach Ländern

1.2 Wie funktioniert I2P

Der Nutzer kann sich den I2P-Router als Software runterladen und diesen bei sich im System einrichten. Nun übernimmt der I2P-Router die Kommunikation ins Netz. Verfügbar sind alle gängigen Internet-Protokolle wie z.B. HTTP, SMTP, IRC oder POP3. Die Verschlüsselung zwischen zwei Routern ist Ende-zu-Ende verschlüsselt. Dies wird durch einer Reihe an kryptographischen Verfahren erreicht (siehe 2.5 Kryptographie). Daten zwischen den Routern werden größtenteils per UDP versendet, jedoch ist auch TCP möglich. Diese werden

jedoch anonym verwendet, um so keinen Rückschluss auf die IP-Adressen der Absender zu geben.

Der Router baut zunächst sogenannte Erkundungstunnel auf, mit denen er das Netz durchsucht. Diese Erkundungstunnel werden ebenfalls benutzt um Clienttunnel aufzubauen. Dies wird im I2P als sog. „Bootstrapping“ bezeichnet. Er kennt standardmäßig nur ein paar mitgelieferte Router, sog. „Seednodes“. Diese verweisen auf die aktuellen sog. FloodFill-Router, die dazu da sind, das Wissen der Router im I2P über das Netz zu verteilen. Die FloodFill-Router synchronisieren sich dabei selbstständig, damit sie immer die aktuellen Datensätze halten. Jeder Teilnehmer im I2P-Netz kann ein FloodFill-Router werden. Ausgewählt werden diese z.B. aufgrund hoher Bandbreite und guter Erreichbarkeit. Über die zentralen FloodFill-Router erhält der Client nun Informationen über weitere Router im Netzwerk. Hier publiziert der Client ebenfalls seine Kontaktinformationen, damit er gefunden werden kann.[7] (Siehe 2.1 Aufbau des Netzwerkes)

Diese bestehen unter anderem aus einem öffentlichen Schlüssel, der mittels einer Hashfunktion eine Position im Netzwerk angibt. Mit Hilfe des Algorithmus namens „Kademlia“, wird zwischen den einzelnen Routern der Abstand durch eine XOR-Verknüpfung berechnet. Hierbei spielt der geografische Abstand keine Rolle, sondern nur die mathematische Entfernung der Zahlen. Dieser Algorithmus dient ebenfalls zur gleichmäßigen Verteilung des Wissens über die Netzknoten, sodass jeder nur die in der „Nähe“ gelegen Router kennt. Jeder teilnehmender Router pflegt bei sich eine lokale Tabelle mit den anderen partizipierenden Routern. Diese werden im I2P-Umfeld auch Ziele oder „Destinations“ genannt. Diese Tabelle kann der Router bei Anfragen von anderen Routern weitergeben kann. So entsteht ein verteiltes Wissen über die Teilnehmer des Netzwerkes (siehe 2.4 Netzwerkdatenbank). Nach der ersten Konfiguration des Routers kann es bis zu einer Stunde dauern, bis das Netzwerk nutzbar ist, da der Vorgang der Informationsgewinnung solange dauert.[7]

---

[7] Vgl. The Invisible Project - Technische Einführung

1.3 Wie ist der momentane Entwicklungsstand

Die momentane Version von I2P ist die Version 0.9.23 (Stand 22.11.2015). Hieran erkennt man, dass es noch keine 1.0 Version gibt, also ein Major Release. Es gibt eine Roadmap, die von der Version 0.9 bis hin zur 3.0 einige Meilensteine festlegt. Zum 1.0 Release fehlen noch umfangreiche Codereviews mit Bewertungen von Schwachstellen, sowie der generellen Sicherheit bzw. Anonymität. Diese soll von externen Experten durchgeführt werden. Zudem sollen noch weitere Funktionen implementierten werden, wie z.B. die Benutzerdefinierte Nachrichtenverzögerung (ab Version 3.0). Auch Dokumentationen der einzelnen Funktionen und weitere Übersetzungen fehlen noch.[8]

Auch die Website des Projektes ist teilweise veraltet, so ist z.B. die letzte Änderung der Gefahrenanalyse im November 2010 passiert und lt. Webseite korrekt für die Version 0.8.1. [9]

[8] Vgl. The Invisible Project - Entwicklungsplan

[9] Vgl. The Invisible Project - Gefahrenanalyse

2. Technische Realisierung

2.1 Aufbau des Netzwerkes

2.1.1 Konzept der Tunnel

Das I2P-Netzwerk besteht aus einer Menge an I2P-Routern. Innerhalb des Netzwerkes, fungieren alle Router als Hop, also als Stellvertreter, die Datenpakete annehmen und weiterleiten. Die Pakete werden im I2P-Netz durch Tunnel übermittelt. Ein Tunnel beschreibt immer einen verschlüsselten gerichteten Weg von Routern.[10] [12]

Jeder dieser Router hat eingehende und ausgehende Tunnel, dies variiert je nach Rechenleistung und Bandbreite. Die eingehenden Tunnel des Routers, dienen zum Empfangen von Nachrichten, die ausgehenden Tunnel zum Versenden von Nachrichten (siehe Abb. 3).[11]

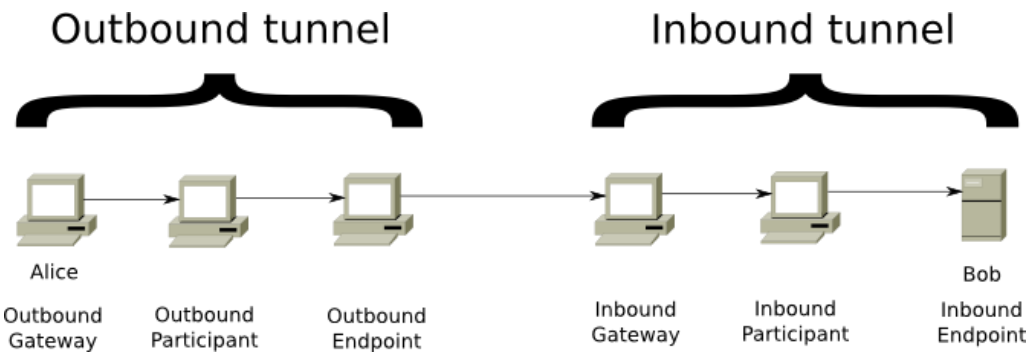

Abb.3 Ausgehender und eingehender Tunnel

2.1.2 Erkundungstunnel

Im I2P-Netzwerk unterscheidet man zwischen Erkundungstunnel und Clienttunnel. Die Erkundungstunnel haben eine geringere Bandbreite und dienen zum Testen anderer Tunnel, zum Senden von Anfragen, sog. „Lookups“ an die Netzwerkdatenbank und zum Aufbau von Clienttunneln. [12]

---

[10] Vgl. The Invisible Project - Tunnels

[11] Vgl. Kai Raven - Das I2P-Netzwerk

[12] Vgl. The Invisible Project - Technische Einführung

2.1.3 Clienttunnel

Clienttunnel dienen zum Übermitteln von Datenpaketen für Protokolle wie z.B. HTTP. Sie haben eine höhere Bandbreite gegenüber den Erkundungstunneln. Jeder Service im I2P-Netzwerk hat eine Adresse, eine sog. „Destination“ unter der er erreichbar ist. Diese Destination ist der öffentliche Schlüssel, bzw. der Hashwert davon. Hier wird unterschieden zwischen festen Adressen für Server und wechselnden Adressen für Clients. Ein Betreiber einer Webseite, einer sog. „Eepsite“, die nur innerhalb des I2P-Netzes erreichbar ist, benötigt beispielsweise eine feste Adresse, ein Client hingegen nicht. Dieser würde bei einer Anfrage an den Server, einfach seine Antwortadresse mitsenden. Die Adressen der Clients ändern sich mit jedem Neustart des Routers.[13] [14]

Am Ende eines jeden Tunnels befindet sich das Ausgangsgateway. Möchte der Router nun also eine Nachricht versenden, so muss er diese über einen seiner Ausgangstunnel die Nachricht versenden lassen. Der Router der das Ausgangsgateway darstellt, erhält nun die Nachricht mit der Information, an welches Eingangsgateway er die Nachricht weiterleiten soll. Der Router, der das Eingangsgateway darstellt, wird vom Empfänger der Nachricht ausgewählt. Ein ausgehender Tunnel führt also immer wieder zu einem eingehenden Tunnel. Die Nachricht wird anschließend in dem Eingangstunnels des Empfängers weiter geroutet, bis die Nachricht das Ziel erreicht hat. Jeder Router im I2P-Netz kann ein Teil eines Tunnels für andere Anwender sein.[13]

Die Anzahl der Router, die man für seinen Tunnel haben möchte, konfiguriert man mittels des Hop-Counters. Dieser gibt an, wie viele I2P-Router die Nachricht weiterleiten. Sinnvoll ist hier einen Wert von 2-3 Routern zu verwenden. [15]

---

[13] Vgl. The Invisible Project - Technische Einführung

[14] Vgl. Kai Raven - Das I2P-Netzwerk

[15] Vgl. The Invisible Project - Tunnels

2.1.4 Auswahl der Router

Ein Tunnel wird aufgebaut, in dem er zunächst seine teilnehmenden Router anhand von Profilen aussucht. Dies wird im I2P als „Peer Selection“ bezeichnet. Diese Profile beinhalten z.B. Angaben über die vermutete Bandbreite, wie oft der Router an anderen Tunnel teilgenommen hat, wann der Router zuletzt im I2P-Netz verfügbar war oder wie schnell die Antwort aus einer Netzwerkabfrage kam. Jeder einzelne Router führt diese Statistiken und macht sie den anderen Routern verfügbar. Diese sind jedoch relativ klein, sodass ein Router die Möglichkeit hat tausende Profile zu vergleichen. Zudem werden inaktive oder schlechte hier herausgeworfen um die Datenmenge zu verringern.[16] [17]

2.2 Adressen im I2P-Netzwerk

Ein I2P-Router der einen Dienst anbieten möchte, wie z.B. das Hosten einer „Eepsite“ benötigt einen Domainnamen. Diese haben immer die Top-Level-Domain „i2p“, also beispielsweise *www.i2p2.i2p*. Durch ein internes Lookup-Verfahren, ähnlich wie beim Domain Name System, werden diese URL-Strings einem Hashwert zugewiesen unter dem die Seite erreichbar ist. Jeder Teilnehmer kann publizierte Adressen, z.B. in Foren, in sein lokales Adressbuch einfügen und auch über die Anwendung „SusiDNS“ andere Adressbücher importieren. Zunächst wird versucht in der lokalen Hashtabelle nach zu sehen, ob ein Eintrag vorhanden ist. Danach erst wird die Netzwerkdatenbank befragt. Sofern kein Eintrag vorhanden ist, wird eine Fehlermeldung ausgegeben.[18]

---

[16] Vgl. The Invisible Project - Technische Einführung

[17] Vgl. The Invisible Project – Tunnels

[18] Vgl. Kai Raven - Das I2P-Netzwerk

2.3 Anonymität

Die Anonymität und das Verschleiern der IP-Adressen, ist eines der wichtigsten Kriterien für ein Overlay-Netzwerk. Dies wird durch das Garlic Routing erreicht. Wenn ein Router eine Nachricht weiterleitet, weiß er nur, wer der letzte Sender und wer der nächste Empfänger der Nachricht ist. Im I2P-Netz sind besten Falls 4-6 Router zwischen den eigentlichem Ersteller und dem Ziel der Nachricht, was eine gute Sicherheit bietet.[19] [20]

Dadurch, dass der Router eigene aber auch fremde Datenpakete empfängt, wird eine gewisse Anonymität erzeugt, da man von außen betrachtet nicht zuordnen kann, ob das Datenpaket für den Router bestimmt war, oder ob er nur ein Hop in dem Tunnel war. Das Weiterleiten fremder Datenpakete ist keine Pflicht im I2P-Netzwerk. Der Anwender kann hier selber den Grad der Anonymität und Performance im Netz wählen, wobei es nicht empfehlenswert ist, die Weiterleitung zu deaktivieren, da sonst dritte alle Datenpakete einer Person zuordnen können und dadurch kann auch die Anonymität anderer Teilnehmer gesenkt werden. [19]

Je größer das Netzwerk wird, desto höher ist die Anonymität. Aufgrund der Vielzahl der Datenpakete die ein einzelner Router empfängt, kann eine dritte Person schwieriger die Datenpakete ausfindig machen, die für den jeweiligen Router bestimmt sind. [19]

Es wird ein dynamisches Netz gebildet, indem der Router ständig neue Tunnel aufbaut und schließt, je nach Anfragen von ihm selbst oder von anderen Routern. Dies ist ein weiterer Grund für die nötige Komplexität von möglichen Angriffen.[21]

---

[19] Vgl. Kai Raven - Das I2P-Netzwerk

[20] Vgl. Kademlia: A Peer-to-peer Information

[21] Vgl. The Invisible Project - Einführung in die Arbeitsweise von I2P

2.4 Mögliche Einordnung in der OSI-Modell

Durch Bibliotheken ermöglicht I2P auch Funktionen, wie z.B. eine sichere Streaming-Kommunikation wie TCP. I2P setzt gemäß des OSI-Modells über der Transportschicht auf, wobei die Vermittlungsschicht durch eine anonyme Vermittlungsschicht überdeckt wird, I2P überdeckt dabei die Schicht über Ipv4(IPv6). Die Überdeckung von TCP wird durch eine anonyme Transportschicht realisiert, der sogenannten „Streaming Lib“. Ähnlich wie auch im OSI/ISO 7 - Referenzmodell findet sich auch hier die Anwendungsschicht wieder. Jedoch wird diese durch anonyme I2P spezifisch Anwendungen überlagert. (Siehe Abb3.) Mit diesem Konzept ist es möglich, I2P im Internet zu betreiben.[22]

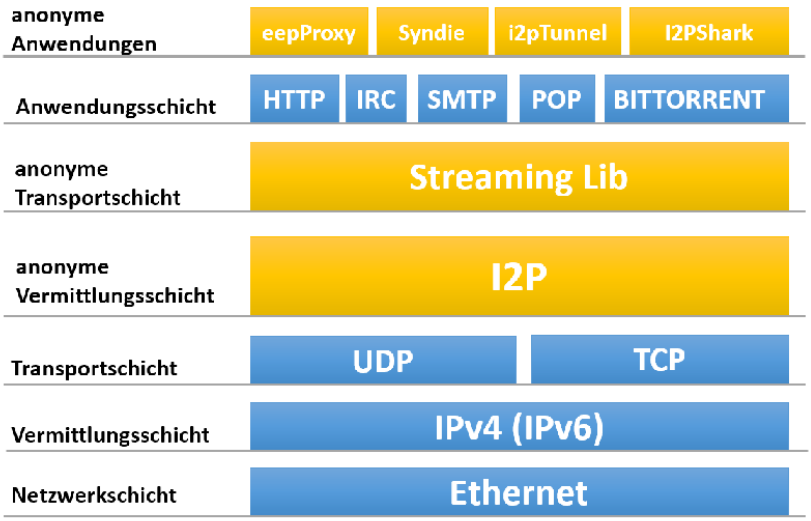

Abb. 3 Mögliche Einordnung von I2P in der OSI-Referenzmodell

[22] Vgl. PlanetPeer - Das deutsche I2P-Handbuch

2.5 Garlic Routing

Für das Weiterleiten der Datenpakete wird ein sogenanntes „Garlic Routing“ (Knoblauch) benutzt. Dieses wurde von Michael J. Freedman erstmals dokumentiert und ist eine Art Erweiterung des „Onion Routings“ (Zwiebel).[23]

Beim Onion Routing, wird eine Nachricht bzw. ein Datenpaket mehrfach verschlüsselt. Die Anzahl der Verschlüsselungsebenen bestimmt der Hop-Counter, der angibt, wie viele Zwischenstationen ein Datenpaket zwischen Anfangs- und Endpunkt eines Tunnels benutzt. Je nach Anzahl wird dieses in verschiedenen Schichten verschlüsselt. Bei jedem Hop wird eine Schicht des Datenpaketes mit dem jeweiligen privaten Schlüssel des Hops entschlüsselt, wobei der Hop nur die Informationen des nächsten Hops erhält, also die IP-Adresse des nächsten. Der Rest der Nachricht bleibt weiterhin verschlüsselt. Dies führt dazu, dass nur der für den das Datenpaket bestimmt war, die Nachricht auch wirklich lesen kann.

Beim Garlic Routing werden nun mehrere Nachrichten in ein Datenpaket gekapselt. Diese Nachrichten werden darauf hin nochmals verschlüsselt und anschließend zusammen in einer größeren Nachricht versendet.[23] [24]

---

[23] Vgl. The Invisible Project – Galic Routing

[24] Vgl. Infosec - Einführung in Anonyme Netzwerke

2.6 Netzwerkdatenbank

Die I2P Netzwerkdatenbank ist eine verteilte Datenbank (Distributed Hash Table), die mittels „Kademlia“ realisiert wird. Kademlia ist ein Algorithmus entwickelt von Petar Maymounkov und David Mazieres. Durch ihn kann ein selbstorganisiertes Netzwerk aufgebaut werden, in dem es möglich ist mit jedem Teilnehmer zu kommunizieren.

Jeder Knoten in dem Netzwerk bekommt eine Node-ID. Im Falle des I2P-Netzwerkes ist es ein 256-SHA Hashwert des öffentlichen Schlüssels. Jeder I2P-Router benutzt dieselbe Hashfunktion, damit sichergestellt ist, dass ein Knoten eindeutig ist. Durch eine Anfrage an die FloodFill-Router erhält der Knoten Informationen über das Netzwerk, im Gegenzug muss der neue Knoten seine ID ebenfalls hier angeben. Geroutet wird über die Nähe der ID’s mittels einer XOR –Verknüpfung der Hashwerte. Möchte Alice nun Bob eine Nachricht schicken, so würde der Algorithmus die Nachricht an denjenigen schicken, der in Alice Adressbuch am nächsten ist. Dieser würde wieder suchen welche ID am nächsten an Bob ist. Somit wird sich durch das Netz bewegt, bis letztendlich die Nachricht bei der IP-Adresse von Bob angelangt ist.[25] [26] [27]

Abfragen an die Netzwerkdatenbank oder das direkte Wegsuchen kommen nie vom Ziel, bzw. dem I2P-Router selbst. Dieser benutzt stets seinen aktuellen Gateway-Router, um diese Abfragen zu tätigen. Aufgrund des Garlic-Routing weiß dieser nur wer vor ihm die Nachricht geroutet hat und wen er diese senden soll, somit wird hier eine Anonymität erzeugt.[28]

---

[25] Vgl. Kai Raven - Das I2P-Netzwerk

[26] Vgl. PlanetPeer - Das deutsche I2P-Handbuch

[27] Vgl. The Invisible Project – Die Netzwerkdatenbank

[28] Vgl. The Invisible Project – Galic Routing

Es gibt zwei Arten von Einträgen in der Datenbank. Zum einen enthält es die Kontaktdaten des Routers und zum anderen die Ziel-Kontaktinformationen, sog. „LeaseSets“. [29]

Zur Sicherstellung der Integrität, wird jeder Eintrag in die Datenbank von dem Ersteller des Eintrages unterzeichnet und von jedem, der sie bei sich speichert oder weitergibt, nochmals verifiziert. Zudem haben die Daten einen Stempel wie lange diese verwendet werden sollen. So kann man ältere und irrelevante Einträge aus der Datenbank einfach löschen und diese durch neue Einträge ersetzen. [29]

Routerinformationen

Der Router speichert seine Identität ab. Diese enthält einen 2048 Bit ElGamal-Schlüssel, eine Signatur und ein Zertifikat. Hinzu kommen noch Adressdaten unter denen er erreicht werden kann, den öffentlichen Schlüssel. Zudem speichert er einen Zeitstempelt ab, an dem er die Daten angelegt hat. Optional folgt eine Reihe an Textoptionen, die z.B. Bandbreiten Angaben haben können. Hinzu kommen noch weitere Informationen, wie die Version der genutzten Bibliothek (coreVersion) oder die Version des Routers (router.version) um die Kompatibilität zu Features zu bestimmen. Zum Schluss signiert er die Daten um die Datenintegrität zu gewährleisten. [29]

LeaseSets

Die LeaseSets bilden eine Gruppe von Tunneleinstiegspunkte für einen bestimmten Client. Diese enthalten die Identität des Tunnel-Gateway-Routers, identifiziert durch den Hashwert seine öffentliche Schlüssels, eine 4 Byte Nummer als Tunnel ID und eine Angabe, wann der Tunnel schließen wird. Das LeaseSet selbst, ist in der Netzwerkdatenbank unter dem Hashwertes des Ziels gespeichert. [29]

[29] Vgl. The Invisible Project – Die Netzwerkdatenbank

2.7 Kryptographie

Die Kommunikation von Client zu Client wird Ende-zu-Ende verschlüsselt. Die Verschlüsselung geschieht durch einen öffentlichen und einen privaten Schlüssel. Der private Schlüssel wird in das Arbeitsverzeichnis abgelegt, der öffentliche Schlüssel, im I2P-Netzwerk „Destination Key“ oder auch nur „Destination“ genannt, wird veröffentlicht und dient zur Identifikation des Endpunktes.[30]

Der Schlüsselaustausch wird mittels der Erweiterung (ElGamal / AES+Session-Tag-Verschlüsselungsverfahren) des Diffie-Hellman-Algorithmus realisiert (2048 Bit).Dies geschieht zwischen jedem einzelnen Router. Für die Verschlüsselung zwischen den Routern wird AES-256 eingesetzt, also eine sehr starke Verschlüsselung. Diese wird z.B. in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe verwendet.[30] [31]

Um die Datenintegrität zu gewährleisten, wird eine Nachricht mittels eines 1024 Bit DSA-Schlüssels signiert. [30]

2.8 Unterstützte Dienste

I2P unterstützt gängige Dienste der Kommunikation. Es ermöglicht den Nutzern das anonyme Hosten von Webseiten sogenannter „Eepsites“. Diese sollen ebenfalls keine Rückschlüsse auf den Ersteller bzw. Betreiber des Webservers geben. Es gibt zudem Übergänge in das öffentliche Internet um auch ein anonymes Browsen zu ermöglichen.[32]

Hinzu kommt ein integriertes Webmail-Interface, sowie Plugins für Emails ohne die Nutzung zentraler Server. Zudem unterstützt I2P Blogging und Foren, Echtzeit-Chats, File-Sharing und einen Dezentralen Datenspeicher.[32]

---

[30] Vgl. The Invisible Project – Low-Level Cryptography Details

[31] Vgl. Committee on National Security Systems: CNSS Policy No. 15

[32] Vgl. Golem - Das alternative Tor ins Darknet

3. Gefahrenanalyse

3.1 Wo sind mögliche Schwachstellen

Die Entwickler des I2P-Netzwerkes sind sich bewusst, dass es keine absolute Sicherheit gibt. Sie haben das Ziel, dass sie mögliche Angriffe schwerer und komplexer machen. Zudem wollen sie weitere wissenschaftliche Untersuchungen forcieren. Das I2P-Team hat ein umfassendes Gefahrenmodell entwickelt, worauf ich im Folgenden teilweise eingehen werde. [33]

3.2 Brute-Force-Angriff

Ein Brute-Force-Angriff wird von einem globalen passiven oder aktiven Gegner durchgeführt. Dieser versucht alle Nachrichten zu beobachten, die sich zwischen den Knoten bewegen und Rückschlüsse auf Pfade zu geben. Dieser Angriff ist gegen ein I2P-Netzwerk nicht einfach, da alle Router ständig senden und dabei ihre Pfade, sowie die Nachrichten Größe ändern. Hinzu kommt, dass die Nachrichten verschlüsselt sind, diese also nicht direkt ausgelesen werden können. Jedoch kann ein sehr leistungsfähiger Angreifer Brute-Force verwenden, um bestimmte Trends zu erkennen.[33]

Wenn ein Angreifer z.B. 5 GB zu einem I2P-Ziel sendet, so kann er alle Router ausschließen, die keine 5 GB bekommen haben. Hier wird jedoch noch an Verzögerungen des Netzes gearbeitet, die dem entgegenwirken sollen.[33]

[33] Vgl. The Invisible Project – Gefahrenanalyse

3.3 Timing-Attacken

Die I2P-Nachrichten werden unidirektional ausgetauscht, zudem kommt, dass nicht zwangsläufig eine Antwort gesendet werden muss. Jedoch könnte man bei bestimmten Protokollen, wie z.B. dem HTTP-Protokoll, bestimmte Muster erkennen. Die Anwendbarkeit ist nicht ganz klar, wie das Netzwerk sich bei den Variationen von Nachrichten und den Warteschlangen verhält. Auch die zwischenzeitliche Drosselung des Datenverkehrs und die Zeiten der Nachrichtenübergabe, können hier einen Angriff erschweren. Bei Protokollen auf denen eine direkte Antwort notwendig ist, kann es jedoch durchaus möglich sein, Rückschlüsse auf den I2P Router zu ziehen. Hierbei spielt die Größe des Netzwerkes eine Rolle, je kleiner das Netzwerk, desto größer die Wahrscheinlichkeit Gesetzmäßigkeiten heraus zubekommen.[34]

3.4 Denial of Service Attacken

Es gibt eine Vielzahl von Denial of Service Attacken. Einer kann der Flooding-Angriff sein. Hierbei könnte versucht werden, das Netzwerk, ein Peer, ein Ziel oder einen Tunnel mit Daten so zu überfluten, dass diese zusammenbrechen. Dies ist bei I2P durchaus möglich und es wird nichts gegen das Standard IP-Layer-Flooding unternommen. Eine Attacke indem eine Vielzahl von Nachrichten übermittelt wird, ist ebenfalls mögliche, jedoch kennt der Angegriffene, den Angreifer aufgrund der vorhandenen Absenderadresse und könnte so andere Teilnehmer warnen. Es ist möglich hier eine neue Implementation hinzuzufügen, die es einem erlaubt, mehr Tunnel zum empfangen von Nachrichten zu erstellen, umso kleineren Attacken standhalten zu können.[34]

---

[34] Vgl. The Invisible Project – Gefahrenanalyse

4. Vergleiche mit anderen Netzwerken

4.1 TOR

Der wesentliche Unterschied neben dem Onion-Routing beim TOR-Netzwerk und dem Garlic-Routing beim I2P-Netzwerk ist das Design-Ziel. Beim I2P-Netzwerk ist das Ziel, anonym Nachrichten innerhalb des Netzwerkes zu versenden. TOR zielt mehr auf das anonyme Surfen außerhalb des Netzwerkes ab. Hier sind die Vorteile der geringere Overhead und ein schnellerer Datendurchsatz. Zudem wurden bereits wissenschaftliche Forschungen über die Architektur durchgeführt, hinzu kommt, dass TOR um ein wesentliches Größer als I2P.[35]

I2P ist insgesamt langsamer als das TOR Netzwerk. Hier kann jedoch auch der Anwender selbst einen Kompromiss zwischen Sicherheit und Bandbreite eingehen, dies kann er bei TOR in dieser Form nicht. Obwohl es auch bei I2P einige wenige Outproxies gibt, ist das Netz ursprünglich so konzipiert worden, dass die Kommunikation innerhalb des Netzwerkes sicher ist und keine oder nur wenig Kommunikation ins normale Netz erfolgt. Hier hat I2P durchaus einen Vorteil, da hier jeder Teilnehmer Daten weiterleitet, anders als bei TOR, wo es feste „Relays“ gibt. Dies erlaubt einem Anwender eine Verneinung, dass die gerouteten Datenpakete ihm gehörten.[36]

Ein weiterer Unterschied zum TOR – Netzwerk ist die Netzwerkdatenbank. Diese befindet sich bei TOR auf einem zentralen Verzeichnisserver. Im Unterschied dagegen, sind sämtliche Netzwerkinformationen im Netz verteilt.[36]

---

[35] Vgl. Golem - Das alternative Tor ins Darknet

[36] Vgl. The Invisible Project – Comparison: Tor

5. Abschlussbetrachtung

5.1 Ergebnisse und praktischer Nutzen

I2P steht klar im Schatten vom Tor-Netzwerk. Beide haben ihre Vorteile und gerade beim I2P-Netzwerk gibt es genügend Potential, etwas sicherer zu sein als TOR, da man ein geschlossenes Netzwerk bilden kann. Jedoch ist das Netzwerk sehr benutzerunfreundlich was die „Usability“ angeht. Der Anwender hat beim erstmaligen Starten des Clients sehr viele Einstellungen zu tätigen, dies könnte viele Anwender überfordern oder auch abschrecken. Dies möchte I2P jedoch nachbessern und legt darauf einen Fokus. Die Einfachheit wie beim TOR-Netzwerk ist nicht gegeben. Hinzu kommt, dass es bei weitem nicht so große Aufmerksamkeit bei Universitäten oder Geheimdiensten hat. Dies ist ein weiterer Grund, weshalb es noch nicht gut erforscht ist.

5.2 Ausblicke und Anregungen

Das Konzept von I2P ist nicht trivial und wird auch nicht immer richtig wiedergegeben. Dies haben die Recherchen ergeben, in denen die Nutzung von I2P etwas falsch dargestellt wurde.[37]

Zudem gibt es auch widersprüchliche Darstellungen bestimmter Eigenschaften des Netzwerkes, speziell was die Outproxies angeht.[38]

Die vorliegende Arbeit bezieht sich hauptsächlich auf die Informationen aus der offiziellen Webseite des Projektes.

Diese war leider nur wenig lokalisiert. Eine gute Übersetzung könnte eine größere Masse an Usern ansprechen und so dem Bekanntheitsgrad des Netzwerkes steigern. Ebenfalls ist der Inhalt der Seite pflegebedürftig. Man findet hier kaputte links, hinzukommt, dass manche Teile der Seite seit über einem Jahr nicht mehr aktualisiert oder gepflegt wurden.

---

[37] Vgl. Ubuntuusers - I2P

[38] Vgl.Thomas Mayer- Anonyme Internetnutzung mit dem Invisible Internet Project(I2P)

Um eine gute Anonymisierung zu gewährleisten, muss I2P zwangsläufig bekannter werden. Jedoch müssten dafür auch einfache und klarere Dokumentationen vorliegen, damit der Anwender sich überhaupt damit beschäftigen kann. Dies geschieht jedoch lt. Roadmap noch, es bleibt also abzuwarten, wie sich das Invisible Internet Project in den kommenden Jahren weiterentwickelt.

Abbildungsverzeichnis

Literaturverzeichnis

AAsche (2015) I2P: https://wiki.ubuntuusers.de/Baustelle/I2P (Abruf: 22.11.2015)

Committee on National Security Systems(2003) CNSS Policy No. 15, Fact Sheet No. 1. 2003, S. 2 *http://csrc.nist.gov/groups/ST/tool-kit/documents/aes/CNSS15FS.pdf* (Abruf: 03.01.2016)

Golem (2015) Invisible Internet Project | Das alternative Tor ins Darknet: *http://www.golem.de/news/invisible-internet-project-das-alternative-tor-ins-darknet-1502-112316.html* (Abruf: 03.01.2016)

Heise (2014) 31C3: Die Angriffe auf Verschlüsselung durch NSA und GCHQ: *http://www.heise.de/newsticker/meldung/31C3-Die-Angriffe-auf-Verschluesse-lung-durch-NSA-und-GCHQ-2507004.html* (Abruf: 03.01.2016)

Kai Raven (2014) Das I2P-Netzwerk: *http://wiki.kairaven.de/open/anon/netz-werk/p/anet08* (Abruf: 03.01.2016)

Infosec Institute (2012) Einführung in die Anonymisierungsnetzwerke - Tor vs I2P: *http://resources.infosecinstitute.com/anonymizing-networks-tor-vs-i2p/* Abruf (22.11.2015)

Maymounkov, Peter/ Mazières, David – Kademlia: A Peer-to-peer Information System Based on the XOR-Metric: *https://pdos.csail.mit.edu/~petar/pa-pers/maymounkov-kademlia-lncs.pdf* (Abruf: 03.01.2016)

PlanetPeer (2011) Das deutsche I2P-Handbuch: *http://www.planetpeer.de/wiki/index.php/Das_deutsche_I2P-Handbuch* (Abruf: 22.11.2015)

Spiegel Online (2015) Vorratsdatenspeicherung: Was künftig über Sie gesammelt werden soll: *http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-was-ueber-sie-gesammelt-werden-soll-a-1028910.html* (Abruf: 15.02.2016)

The Invisible Internet Project (2015) I2P: *https://geti2p.net* (Abruf: 22.11.2015).

Thomas Mayer (2007) Anonyme Internetnutzung mit dem Invisible Internet Project(I2P): *http://www.heise.de/tp/artikel/25/25273/1.html* (Abruf: 22.11.2015)

The Tin Hat (2015) Through A Network, Darkly | A Geographic Look At I2P: *https://thetinhat.com/blog/2015/01/05/i2p-survey.html* (Abruf:22.11.2015)