Tor - The Onion Router

Ein Projekt in Network Security bei Dr Andreas Reinhardt

Christian, Rebischke

4. Juli 2015

Inhaltsverzeichnis

1 Einleitung

In den letzten Jahrzehnten ist die Menge der Daten die via das World Wide Web versendet werden rasant angestiegen. Ebenso angestiegen ist jedoch die Anzahl der Staaten die versuchen sich das World Wide Web als Machtinstrument zu sichern. Gerade die letzten Jahre im Zusammenhang mit der Snowden-Affäre haben uns gezeigt in welchem Umfang einige Staaten Überwachung und Spionage betreiben. Aber auch der Arabische Frühling hat uns klar gemacht, welche Macht das Volk haben kann wenn es Zugang zum Netz hat. Da ist es nicht verwunderlich, dass einige Staaten das Netz filtern oder zensieren wollen um ihren Status Quo zu stärken und beizubehalten. Genau an dieser Stelle kommt **Tor** ins Spiel. **Tor** ist das Akronym für **The Onion Router**. Mit der Hilfe von **Tor** ist es möglich der Zensur eines Staates oder der permanenten Überwachung des Netzes zu entgehen.

2 Modus Operandi der Netzüberwachung und Netzzensur

Bevor wir uns näher mit **Tor** befassen ist es sinnvoll sich erstmal vor Augen zuführen welche Arten der Netzüberwachung und Netzzensur existieren. Am verbreitesten ist eine Zensur auf Basis des Providers wie sie beispielsweise gerade in Österreich im Tatbestand der Urheberrechtsverletzung stattfindet. [3] Dort werden einfach via *DNS-Filter* die DNS-Anfragen für diverse Internetseiten umgeleitet. In anderen Gegenden der Welt kommen jedoch auch *Content-Filter* zum Einsatz. *Content-Filter* kann man noch unterteilen in diverse "Härtegrade". Gemeinsam haben aber alle, dass nach Content also nach Inhalt gefiltert wird. Dies kann man erreichen durch *Deep Packet Inspection*, einer Technik bei der beispielweise bei TCP-Paketen die Nuztlast überprüft wird und je nach Auffinden von bestimmten Begriffen dann das Paket nicht am Ziel ankommt. Ansonsten gibt es noch Software-seitige Content-Filter die besonders gerne in Internet Cafes eingesetzt werden (so passiert in Myanmar [4]). Ebenfalls denkbar ist aber auch das gezielte Sperren von IP-Adressen, Filterung anhand der URL und ein sogennanter *Connection Reset* der weitere Verbindungsversuche unter Verwendung des *TCP-RESET-Pakets* verhindert. Das wohl bekannteste Beispiel von Internetzensur ist China mit dem *Projekt Goldener Schild* hierzulande auch *Große Firewall von China* genannt. Das *Projekt Goldener Schild* verbindet viele der oben genannten Vorgehensweisen.

3 Wieso Tor?

Eine der Kernfragen die man sich über **Tor** stellt ist "Was macht **Tor** eigentlich besser als die Alternativen?". Schauen wir uns dazu mal einige dieser Alternativen an:

- Lokale Webhoster
  Lokale Anbieter von Internetseiten könnten die von der lokalen Regierung gesperrten Inhalte im Ausland lokal anbieten. So müsste zum Beispiel im Falle von China der Traffic nicht erst die Great Firewall of China passieren. Der Nachteil ist allerdings, dass der Webhoster eine Lizenz benötigt und vermutlich Rechtliche Schwierigkeiten bekommt wenn so ein *Spiegeln* der Internetseite publik wird.

- Socks- oder HTTP-Proxy
  Beim Socks- oder HTTP-Proxy wird einfach ein anderer Rechner zwischen die Verbindung geschaltet. Diese Art von Proxy wird meistens zum Anonymisieren einer Verbindung benutzt. Schwachpunkt an dem System ist, dass es nicht für jedes Protokoll und jede Anwendung Proxys gibt. Außerdem findet nicht bei jeder Verbindung eine Verschlüsselung statt, sondern nur wenn beispielsweise auch HTTPS verwendet wird. Dadurch das es sich meistens nur um ein System handelt ist es für den überwachenden Staat auch sehr einfach zurückzuverfolgen wer auf welchen Proxy zugegriffen hat. Liegt der Proxy im eigenen Land wäre es sogar denkbar über den fälschlicherweise als Proxy herausgegebenen Server den gesamten Internetverkehr zu sniffen der über diesen Proxy läuft. Der Proxy läuft also Anwendungsspezifisch auf *OSI-Layer 7*.

- VPN (Virtual Private Network)
  Der VPN ist vergleichbar mit einem Proxy. Ein VPN arbeitet jedoch auf *OSI-Layer 3* oder sogar *OSI-Layer 2*. Dies macht den VPN unabhängig von der Anwendung. Der gesamte Rechner hängt sozusagen in einem anderen Netz, der gesamte ausgehende Traffic vom Client geht nach Verbinden mit dem VPN-Server über diesen VPN-Server. Hizukommt, dass viele VPNs eine starke Verschlüsselung anbieten oder sogar das IPSec-Protokoll unterstützen wie beispielsweise *Strongswan*. Nachteile des VPNs sind ähnlich wie beim Proxy. Die jeweilige Regierung kann die IPs von dem VPN-Anbieter blacklisten, den VPN-Anbieter juristisch in die Mangel nehmen (falls er in juristischer Reichweite liegt) oder einfach ohne dem Wissen des VPN-Anbieters dessen Knoten überwachen und schauen was rein geht und was rauskommt.

Zusammengefasst kann man die Schwachpunkte der oben genannten Methoden als zu stark ausgeprägt betrachten als, dass sie wirklich eine sinnvolle Maßnahme gegen Netzzensur wie beispielsweise in China darstellen. Keine der oben genannten Methoden bietet eine Sicherheit auf Anonymität die Oppositionelle oder Whistleblower dringend nötig haben.
Dies ist der Grund für **Tor**.

4 Grundlegende Prinzipien von Tor

Die grundlegenden Prinzipien von **Tor** sind denkbar einfach. Wie man aus dem Namen bereits schließen kann ist **Tor** aufgebaut wie eine Zwiebel. Außerdem besitzt **Tor** das Prinzip des *Darknet*. Mehrere **Tor**-Knoten bilden also praktisch ein eigenes Intranet auf das wiederum nur **Tor**-Clients oder andere **Tor**-Knoten zugreifen können. Jeder **Tor**-Knoten kann eine einkommende Verbindung an einen weiteren **Tor**-Knoten weiterreichen. Sogenannte *Tor-Exit-Nodes* können dann eine Verbindung ins "echte Internet" herstellen. Es lassen sich beliebig viele dieser **Tor**-Knoten kaskadieren. Dadurch wird es äußerst schwierig für Überwachungsorgane festzustellen welche Verbindung zu welchem **Tor**-Nutzer gehört. Durch den Zwiebel-Artigen Aufbau ist die gesamte Verbindung verschlüsselt und jeder **Tor**-Knoten kennt nur seinen Nachfolger.

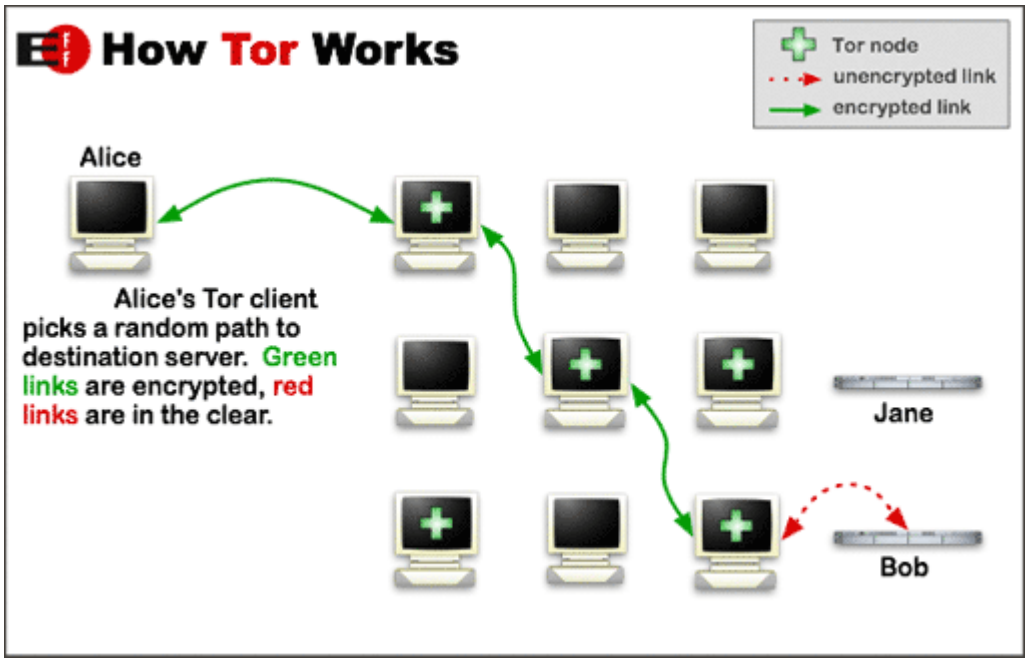

Abbildung 1: The Onion Router Netzwerk

5 Technische Details

5.1 Bestandteile des Tor-Netzwerks

Das **Tor**-Netzwerk hat folgende Bestandteile:

- Entry Guards
  Entry Guards sind sowas wie die Wächter des **Tor**-Netzwerks. Die Idee für Entry Guards kam auf als klar wurde, dass ein Angreifer einen oder mehrere **Tor**-Nutzer deanonymisieren kann wenn er Kontrolle über den Start und Endknoten hat. Alleine über die genaue Paketanzahl und zeitliche Abfolge könnte man einen Nutzer auf Dauer deanonymisieren. Um dies zu verhindern hat man feste Startknoten eingeführt. sogenannte Entry Guards. Somit sind die Startknoten statisch, nicht dynamisch wie man erst erwarten würde. Dadurch kann man die gesamte Anzahl der **Tor**-Nutzer auf einige Entry Guards verteilen. Dies hat zur Folge, dass der Angreifer (falls er einen Startknoten kontrolliert) immer nur die selbe Anzahl an Verbindungen bekommt. Somit lässt sich nicht mehr die aktuelle Zahl an **Tor**-Nutzern durch den Angreifer ermitteln. Außerdem verhindert dies eine Überwachung der Nutzer wenn beispielsweise eine Route gewählt wird mit Entry-Guards die nicht vom Angreifer kontrolliert werden. Wenn ein Nutzer jedoch einen komprommierten Entry-Guard erwischt erhöht dies die Chance auf Deanonymisierung wenn der Angreifer zufälligerweise noch beispielsweise den Exit-Node kompromittiert hat.

- Exitnodes
  Exitnodes sind sowas wie die Fenster vom Onion-Netz in das richtige Internet. Sie bilden einen Ausgang aus dem **Tor**-Netzwerk. Dadurch das der Exitnode nur den letzten Knoten in der Kaskade kennt ist es äußerst schwierig den genauen Urheber der Verbindung zu ermitteln.

- Hiddenserver
  Die sogenannten Hiddenserver sind Server im **Tor**-Netzwerk. Jeder **Tor**-Knoten kann auch zu gleich als Hiddenserver fungieren. Durch Hiddenserver ist es möglich nicht mehr das komplettverschlüsselte **Tor**-Netzwerk zu verlassen um auf Inhalte zuzugreifen. So lässt sich praktisch fast jeder Dienst als Hiddenserver betreiben. Angefangen bei einfachen Webservern bis hinzu SSH-Server. Beim Erstellen des Hiddenservers wird eine im **Tor**-Netzwerk eindeutige URL erstellt mit der Endung *.onion*. Anhand dieser URL kann man dann den Server ansprechen. Der Einsatz von Hiddenserver macht das Netzwerk um ein Vielfaches sicherer, da Traffic nun nicht mehr unbedingt über abhörbare Exitnodes laufen muss sondern im verschlüsselten **Tor**-Netzwerk bleibt. Desweiteren kann so ein Aufenthaltsort und Eigentümer des Hiddenservers komplett verschleiert werden. Client-Nutzer und Server-Inhaber bleiben so komplett anonym und können Inhalte tauschen. Diese Technik nennt man auch “ Rendezvous-Punkt”.

- Directoryserver
  Directoryserver bieten eine Art Inhaltsverzeichnis über die **Tor**-Knoten an. Bei jedem Verbindungsaufbau zum **Tor**-Netzwerk wird eine komplette Liste aller verfügbaren Knoten heruntergeladen.

- Bridges
  Die Bridges sind der maßgebende Ausschlagpunkt wieso **Tor** in so vielen Zensurbehafteten Staaten erfolgreich eingesetzt wird. Da alle Knoten durch die Directoryserver öffentlich bekannt sind ist es für Staaten besonders einfach diese komplette Liste zu sperren. Um den Bürgern trotzdem einen Zugriff auf das Netzwerk zu ermöglichen kann jeder Client auch als Bridge konfiguriert werden. Die genauen Kontaktdaten für diese Bridge können dann mündlich oder elektronisch weitergegeben werden oder bei einer *Bridge Authority* hinterlegt werden. [1]

- Bridge Authority
  Die Bridge Authority besteht aus 3 Pools. Pool 1 verteilt die Bridge-Adressen via Web. Pool 2 verteilt die Bridge-Adressen via Email und Pool 3 via Soziale Netzwerke. Dies macht es äußerst schwierig den Zugang zum **Tor**-Netzwerk zu unterbinden.

5.2 Verbindungsablauf

Abbildung 2 soll den Aufruf von http://www.google.de via **Tor** erläutern:

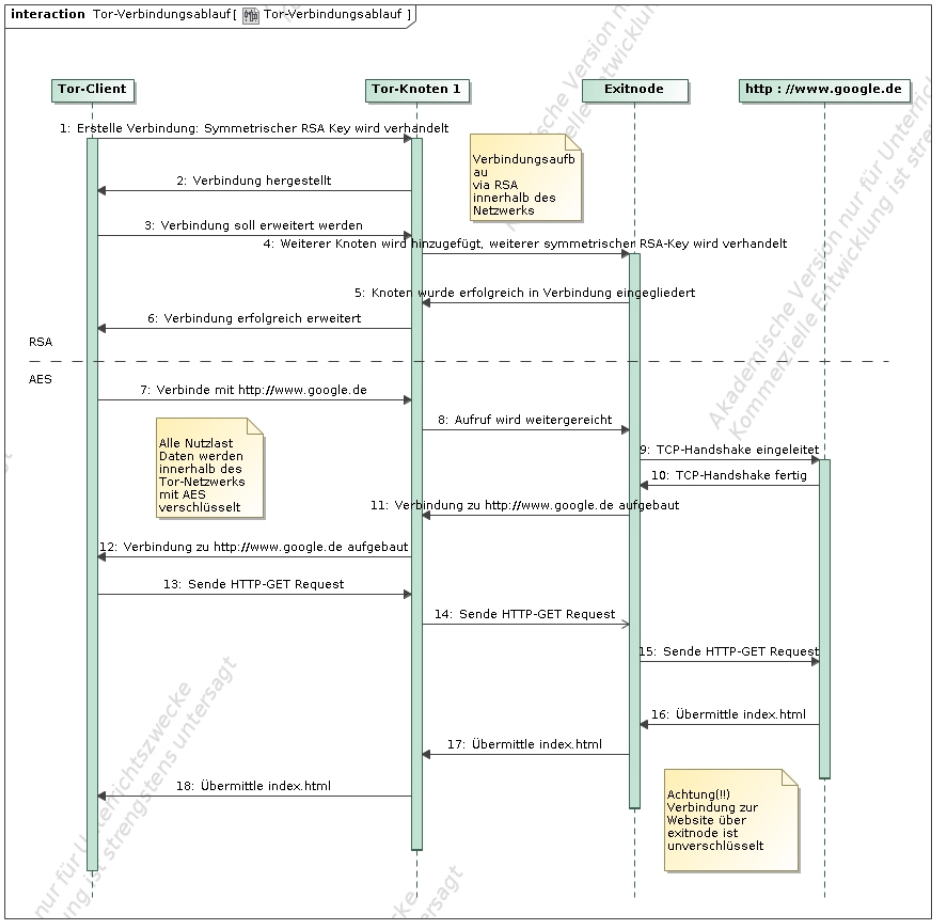

Abbildung 2: Tor-Verbindungsaufbau

Erläuterung: Beim Verbindungsaufbau vom Client zum ersten Knoten wird ein symmetrischer RSA Schlüssel benutzt. Dieser Schlüsselbund wird dann für jede weitere Erweiterung der Verbindung inkrementiert. Pro Knoten ein symmetrischer RSA-Schlüssel mehr. Der symmetrische RSA-Key ist dafür da um die Nutzlast zu verschlüsseln: Einen Diffi-Hellman-Handshake. Ist die Verbindung hergestellt werden alle Nutzerdaten innerhalb des **Tor**-Netzwerks mit AES verschlüsselt. [2] Das Obige Beispiel verdeutlicht gut wieso Hiddenserver so wichtig sind. Denn die Verbindung zwischen Exitnode und Website ist nicht mehr AES

verschlüsselt. In unserem Beispiel sogar nichtmal SSL verschlüsselt weil nicht die HTTPS-Instanz von Google aufgerufen wird.

6 Fazit

Es ist nun eindeutig klar, dass **Tor** eine sichere Alternative zu VPN und Proxies ist. Durch die Kaskadierung der einzelnen Tor-Knoten wird eine höhere Anonymität als bei VPN oder Proxy gewährleistet. Außerdem bietet **Tor** einen besseren Weg Zensurmaßnahmen wie die von China zu umgehen. Auch wenn es China immer wieder (unter Einsatz von Deep Packet Inspection) gelingt den Zugriff auf alle Bridges zu unterbrechen, in dem sie systematisch nach spezifischen **Tor**-Traffic suchen und die entsprechenden Verbindungen nullrouten.

7 Quellen

Literatur

[1] blocking. https://svn.torproject.org/svn/projects/design-paper/blocking.pdf. Aufgerufen: 2015-07-04.

[2] Design of Tor. https://svn.torproject.org/svn/projects/design-paper/tor-design.html. Aufgerufen: 2015-07-04.

[3] Netzsperren: ab heute in Österreich, bald in ganz Europa. https://netzpolitik.org/2014/eugh-legt-zensur-grundlagen-netzsperren-bei-urheberrechtsverstoessen-zulaessig/. Aufgerufen: 2015-07-04.

[4] Zensur im Internet. https://de.wikipedia.org/wiki/Zensur_im_Internet. Aufgerufen: 2015-07-04.

Abbildungsverzeichnis