

Tor – Licht und Schatten

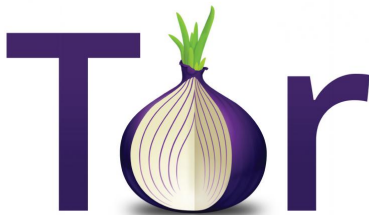
Linux-Infotag Augsburg 2017

22. April 2017



Andreas Steil
Linux Consultant & Trainer
B1 Systems GmbH
steil@b1-systems.de

Das Tor-Netzwerk: Licht und Schatten



Agenda: Das Tor-Netzwerk

- Allgemeines und Entstehungsgeschichte
- Funktionsweise
- Licht- & Schatten-Seiten
- Schwachstellen & Gefahren
- Tor in der Praxis
- kurze Demo von Tails

Allgemeines und Entstehungsgeschichte

Warum Tor?

... aus der UN-Menschenrechtscharta:

„Jeder Mensch hat das Recht auf freie Meinungsäußerung; dieses Recht umfasst die Freiheit, Meinungen unangefochten anzuhängen und Informationen und Ideen mit allen Verständigungsmitteln ohne Rücksicht auf Grenzen zu suchen, zu empfangen und zu verbreiten.“

(Artikel 19 - Meinungs- und Informationsfreiheit)

Allgemeines zu Tor

- Tor = Netzwerk zur Anonymisierung (Sicherheitssoftware); Echtzeitanonymisierungsdienst
- ursprünglich ein Akronym für *The Onion Routing* / *The Onion Router*
- auch „Dark Web“, „Deep Web“
- Entwickler: Roger Dingledine und Nick Mathewson
- in C programmiert
- unter der BSD-Lizenz veröffentlicht
- für mehrere Betriebssysteme (Linux, Windows, Android, iOS, ...)

Geschichte von Tor

- 1995: erste Ideen, erstes Design (ursprünglich Anonymitätssystem für US-Navy)
- 2001: Design nicht mehr nur rein militärisch (aus Eigennutz) Roger Dingledine und Nick Mathewson (MIT-Absolventen) wurden als Entwickler engagiert
- 2002: Gründung des Tor-Projekts (Beginn der Arbeit durch Matej Pfajfar an der Universität Cambridge)
- 2011: Auszeichnung mit dem Preis für gesellschaftlichen Nutzen der *Free Software Foundation*

Wer steckt hinter dem Tor-Projekt?

- ursprünglich *Office of Naval Research* (ONR) und *Defense Advanced Research Projects Agency* (DARPA) (2001-2006)
- heute amerikanisches Non-Profit-Unternehmen (US 501(c)(3))
- mehrere Festangestellte, ca. 70 Mitarbeiter der Kern-Community, mehrere Tausend ehrenamtliche Helfer
- Finanzierung: 60 % Zuwendungen der US-Regierung / 40 % private Spenden (auch NRO) (Stand 2011)
- Weitere Unterstützer (Beispiele):
 - Electronic Frontier Foundation (EFF) (2004-2005)
 - Voice of America
 - Google
 - Human Rights Watch
 - Auswärtiges Amt (2015)

Wer nutzt Tor?

- ? (Unbekannte)
- Aufklärer
- Whistleblower
- Oppositionsbewegungen
- Aktivisten
- Anarchisten
- Journalisten
- ...
- aber auch:
 - Kriminelle
 - Kranke
 - Betrüger
 - ...

Inhalte des Tor-Netzwerkes

- Wikileaks (z. B.
`https://zqctlwi4fecvo6ri.onion.cab/wiki/WikiLeaks`)
- Facebook (`https://facebookcorewwi.onion`)
- Veröffentlichungen
- (illegale) Angebote
- „Hidden Services“
- Veröffentlichungen
- ...
- aber auch:
 - geheime Firmendokumente
 - Krankenakten
 - nicht-öffentliche Regierungspläne
 - ... und Schlimmeres!

Größe des Tor-Netzwerkes

- Anzahl der Tor-Knoten: 7384 (Stand: April 2017)
- Anzahl der Exit Nodes: 800 (Stand: April 2017)
- Anzahl der Tor-Bridges: 650
- Datenübertragungsrate: 72 Gbit/s (Stand: Februar 2016)
- weltweit ca. 36 Millionen Nutzer (Stand: Februar 2016)

Wer nutzt Tor?

The anonymous Internet

Daily Tor users
per 100,000
Internet users



Average number of
Tor users per day
calculated between
August 2012 and
July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham
(@geoplace)
and Stefano De Sabbata
(@maps4thought)
Internet Geographies at
the Oxford Internet Institute
2014 - geography.ox.ac.uk

 Oxford Internet Institute
University of Oxford

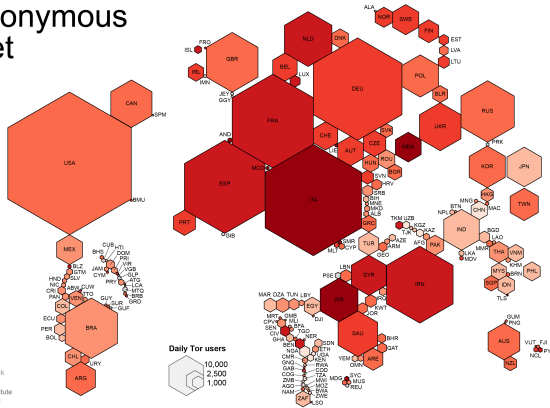


Abbildung: Quelle: Information Geographies Website at the Oxford Internet Institute

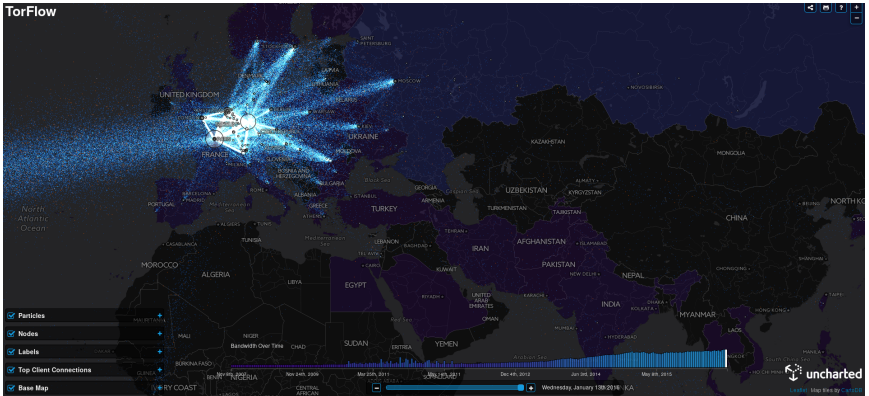


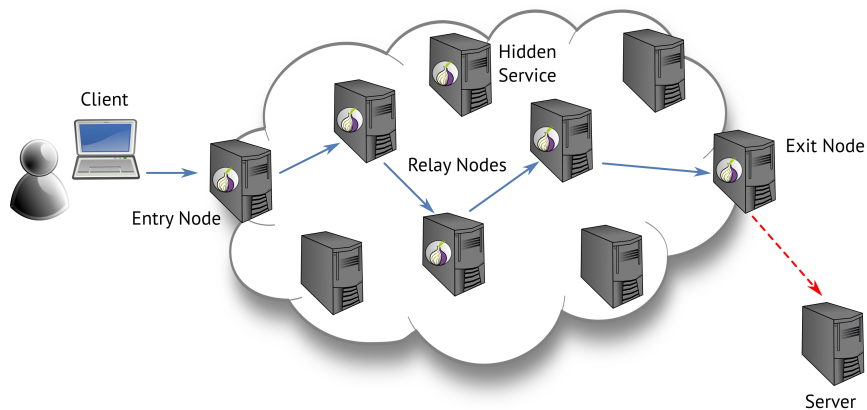
Abbildung: Quelle: <https://torflow.uncharted.software>

Funktionsweise

Funktionsweise: Prinzipien

- Routing-Netzwerk, bei dem jedes Paket (mindestens) 3 Hops (= Relay Nodes) durchläuft
($\Rightarrow$ Echtzeitanonymisierungsdienst)
- eigener Routing-Mechanismus ($\neq$ klassisches IP-Routing)
- Je mehr Nutzer, desto größer die Anonymität des Einzelnen.
- Je mehr Nutzer, desto geringer die Gefahr der Korrumpierung.
- Jeder Knoten kennt bei der Paketvermittlung nur seinen Vorgänger und Nachfolger.
- Nach außen ist nur die IP-Adresse des Exit Nodes sichtbar.
- ursprüngliche Grundidee:
Jeder Nutzer ist immer auch gleichzeitig Relay Node.
aber: nicht praktikabel (Bandbreite, Verwaltungsinformationen)

Der Weg durchs Tor-Netz



Der Weg durchs Tor-Netz

Onion Circuits	
Circuit	Status
radio0, Iridium33, shinefinknothing	Built
radio0, netfreedom2, PrivacyRepublic0002	Built
radio0, Cyberpunknet, OzDqSJWwi2NFpDubvxp	Built
radio0, losttrail, apx1	Built
radio0, nij02, pablobm002, PiratPartiet	Built
radio0, saisamon, LOLHillary	Built
radio0, quadhead, LetoAms	Built
radio0, sevenofnine, redteam01	Built
radio0, Torstein, Selene	Built
radio0, Whoopz, Karadoc	Built
radio0, frand, boyd	Built
radio0, Unnamed, AccessNow003	Built
radio0, Unnamed, PhantomTrain5	Built
radio0, BISMARCK, calliprhukenasty10	Built
radio0, Clover1, koto	Built
radio0, Cornitor, apx3	Built
radio0, nikittorrelay, IPredator	Built

radio0
Fingerprint: 068308AD070849A71B8C1DB06C2509E82C40B908
Published: 2017-03-18 20:21:12
IP: 91.121.230.208 (France)
Bandwidth: 64.75 Mb/s
nikittorrelay
Fingerprint: C994C4603FA7B83B8AB31A9B3F5E9C1DBBE243B
Published: 2017-03-18 14:51:46
IP: 77.95.10.242 (Russian Federation)
Bandwidth: 1.89 Mb/s
IPredator
Fingerprint: BC630CBBB518BE7E9F4E09712AB0269E9DC7D626
Published: 2017-03-18 15:08:02
IP: 197.231.221.211 (Liberia)
Bandwidth: 166.02 Mb/s

Der Weg durchs Tor-Netz

- 1 Der Nutzer installiert auf seinem Computer den Tor-Client.
- 2 Programm lädt beim Start eine Liste aller vorhandenen und verwendbaren Relay Nodes (Tor-Server) herunter.
- 3 Nach Empfang der Liste wählt der Client eine zufällige Route über die Tor Relays.
- 4 Web-Anfrage wird an einen Entry Node geschickt und beginnt dort seinen Weg durch das Tor-Netzwerk.
- 5 Die Kommunikation innerhalb des Tor-Netzes wird zwischen den Relay Nodes jedesmal verschlüsselt übertragen.
- 6 Am Exit Node verlässt die Web-Anfrage das Tor-Netzwerk und wird an den Ziel-Server weitergeleitet.
(Obacht: Tor-Verschlüsselung beendet!).
- 7 Die Verbindungsstrecke wird ungefähr alle 10 Minuten geändert.

Funktionsweise: Komponenten

- Tor-Clients (Onion Proxy)
- Eintrittsknoten (Entry Nodes, Entry Guards)
- Tor-Knoten (Tor-Server, Relay Nodes, Middle Relays)
- Austrittsknoten (Exit Nodes, Exit Relays)
- Verzeichnis / Directory Server (Directory Authorities)
- Bridges (Bridge Relays)

Tor Client

- Client als anfragender Endpunkt des Nutzers
- Software Bundle aus Tor Client und Tor Browser
(gleiche Software auch für Relay Nodes, Entry Nodes, ...)

Entry Nodes

- Client wählt aus einer Liste mit Entry Nodes (auch: Entry Guards) zufällig eine kleine Menge aus (standardmäßig drei).
- Entry Guards können dabei nur Knoten werden, die längere Zeit laufen, über diese Zeit eine hohe Verfügbarkeit aufwiesen und eine überdurchschnittliche Übertragungskapazität haben.
- Entry Guards werden nicht dynamisch gewählt, sondern als erste Knoten auf allen aufgebauten Routen wieder verwendet (oft über mehrere Wochen).
- Betrieb eines eigenen Entry Nodes erhöht die Anonymität, da ein außenstehender Beobachter nicht erkennen kann, ob die Anfragen des Servers aus dem Netzwerk oder von einem selbst kommen.

Relay Nodes

- Vermittlungsknoten
- kennt von Datenpaketen nur vorherige und nachfolgende Knotenadresse
- langsame Relay Nodes können Flaschenhals einer Verbindung bilden
- prinzipiell kann jeder Rechner mit Tor-Software ein Relay Node werden
(durch explizite Konfiguration)

Exit Nodes

- auch Exit- oder Austritts-Server oder -Knoten
- letzter Tor-Knoten vor dem Zugriff ins „normale“ Netz
- Nicht jeder Exit Node leitet beliebige Daten weiter!
- IP-Adresse des Exit-Node = sichtbare Adresse des Absenders
- vorher unverschlüsselte Daten sind ab hier wieder unverschlüsselt!
- unverschlüsselte Daten können vom Exit Node gelesen werden
- Gefahr: Tor-Verschlüsselung wird beendet!
⇒ Verbindung absichern ! (Ende-zu-Ende-Verschlüsselung, z. B. HTTPS)
- Betrieb gefährlich; in Deutschland: Störerhaftung!!!

Das Verzeichnis

- einfaches, zentralisiertes Verzeichnisprotokoll
- Directory Authorities / Directory Server (Verzeichnisserver)
⇒ „Trusted Directory“
- Zertifikate / öffentliche Schlüssel der Verzeichnisserver im Tor-Quellcode
⇒ gewährleistet authentische Verzeichnisdaten
- Beim Starten lädt Tor mit Hilfe der Verzeichnisserver eine Liste aller vorhandenen und verwendbaren Tor-Server.
(Liste mit digitalen Signaturen auf Verzeichnissen)
- Relays cachen das Verzeichnis.

... aber:

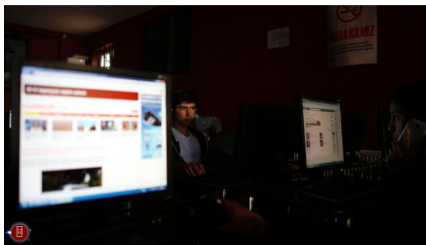
SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Q Mein SPIEGEL

≡ NETZWELT Schlagzeilen | Wetter | DAX 12.048,57 | TV-Programme | Abo

Nachrichten > Netzwelt > Netzpolitik > Tor-Netzwerk > Tor und VPN: Türkei will anonymes Surfen unmöglich machen

Internet-Zensur
Türkei will anonymes Surfen unmöglich machen

Viele Türken nutzen VPN-Verbindungen und Anonymisierungsdienste wie Tor, um sich im Internet Informationen zu beschaffen. Die Regierung geht nun offenbar hart gegen solche Dienste vor.



Internetcafé in Ankara

REUTERS

Abbildung: Quelle: www.spiegel.de/netzwelt/netzpolitik/tor-und-vpn-tuerkei-will-anonymes-surfen-unmoeglich-machen-a-1126540.html

Lösung: Tor-Bridges (Bridge Relays)

- Liste aller Tor-Nodes ist öffentlich $\Rightarrow$ leicht zu sperren
- Bridge Relays = alternative Entry Nodes zum Tor Netzwerk
- keine Listen, sondern dynamische Adressen $\Rightarrow$ schwer zu sperren
- Bridges können Nutzung von Tor vor ISP verstecken
- Zweck: Zensur und Zugriffssperren umgehen
- Jeder Nutzer kann Tor-Client als Bridge konfigurieren und Internetadresse dann anderen mitteilen oder bei einer vertrauenswürdigen Zentralinstanz (Bridge Authority) hinterlegen.
- Adressen unter <https://bridges.torproject.org/bridges> oder per Mail
- Beispiel: China, Iran, Türkei, ...

Versteckte Dienste

- auch: *Hidden Services* bzw. *Tor Onion Services*
- Dienste, die nur im Tor-Netz angeboten werden (Deep Web)
- Tor bietet dem Empfänger von Informationen Anonymität; *Hidden Services* bieten dem Sender von Informationen Anonymität:
Versteckte Dienste sind nur über das Tor-Netzwerk – nicht aus dem „normalen“ Internet – erreichbar.
- durchgehende Verschlüsselung, von einem Ende zum nächsten (keine Gefahr durch Exit Node)
- z. B. für Websites mit sensiblen Informationen (WikiLeaks, ...; aber auch Facebook & Co.)

Onion Services

- haben .onion-Adressen
- Onion-Name dient gleichzeitig der Überprüfung der Verschlüsselung
- verhindern ein Abhören der Verbindung
- Beispiele:
 - Facebook: <https://facebookcorewwi.onion/>
 - Metager: <http://b7cxf4dkdsko6ah2.onion/>
 - Duck Duck Go: <http://3g2upl4pq6kufc4m.onion/>
 - The Hidden Wiki: <http://zqktlwi4fecvo6ri.onion/wiki/>

A Hidden Service: Mafialeaks

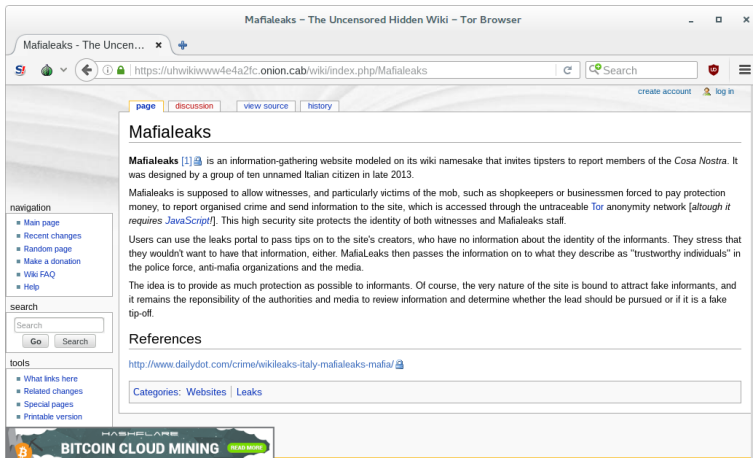


Abbildung: Beispiel für einen „Hidden Service“

Tor: Licht und Schatten

Schatten (alphabetisch)

Anonymität kann missbraucht werden ...
(... und wird missbraucht !)

- Auftragskriminalität
- Drogen
- Fälschungen (Ausweispapiere, Geld, Zertifikate, ...)
- Kinderpornos
- Terrorismus
- Waffen
- Wirtschafts- und Wissenschaftsspionage
- Quelle für Tatort-Bösewichte
- ...

Licht

- gewährt Menschen unzensierten Zugang zum Internet mit der Kontrolle über Privatsphäre und Anonymität
- hilft gegen Unterdrückung, Zensur, Informationsmangel, Überwachung, ...
- ermöglicht Veröffentlichung geheimgehaltener Daten (z. B. Wikileaks)
- Ägypten, China, Iran, ...

Edward Snowden verwendete *Tails* um im Juni 2013 Informationen über *PRISM* an die *Washington Post* und den *Guardian* zu übermitteln.

Tor: Schwachstellen und Gefahren

Schwachstellen und Gefahren

- Tor bietet keine Anonymität gegen jeden Angreifer!
- eigenes Verhalten entscheidend!
- Am Exit Node wird Tor-Verschlüsselung aufgehoben!
⇒ Böse Exit Nodes können Verkehr überwachen und unverschlüsselten Verkehr ausspionieren.
- Angreifer, die den ersten Knoten (Exit Node) und den letzten Knoten (Exit Node) einer Verbindung kontrollieren
- Angreifer, die viele Relays kontrollieren
- Software selbst
- Browser
- SSL
- DNS-Leaking
- vorheriges Abgreifen von Daten
- ?

Erkennbarkeit

- Ports (konfigurationsabhängig)
- Zertifikate (z. B. `www.abc35...42xy.com`)
⇒ ISP weiß um die Benutzung von Tor! (Abhilfe: VPN)
- unverschlüsselte Verbindungen durch Exit Node! (z. B. Klartextübertragung von Anmeldedaten)
- Zusammenhang von Paketanzahl und zeitlicher Abfolge der Paketen
- Fingerprinting (z. B. Hardware-Komponenten, Größe des Browser-Fensters, Mausbewegungen, ...)

0-Day

- Schwachstelle: Browser
- Exploit einer „Use-After-Free-Lücke“ (Fehler im Speichermanagement) zur Enttarnung von Tor-Nutzern
Code auf dem Rechner der Tor-Nutzer kann ausgeführt werden
- betroffen: Firefox-Browser Versionen 41 bis 50 (Windows)
- setzt aktiviertes Javascript voraus
- sendet eindeutigen Identifier (Unique Identifier) an einen Server

XKeyscore

- Ausspäh-Programm, das Nutzer des Tor-Netzwerkes und der Linux-Distribution Tails automatisch in eine Datenbank der NSA einträgt
- veröffentlicht durch Norddeutsche Rundfunk und der Westdeutsche Rundfunk im Sommer 2014 nach Prüfung des Quellcodes von XKeyscore

Schutzmaßnahmen

- aktuelle Version nutzen!
- Linux von CD/DVD booten (USB-Stick anfälliger wegen Beschreibbarkeit)
- Verbindung von Tor und VPN
- eigenes Verhalten!
⇒ z. B. nur gesicherte Verbindungen nutzen
(HTTPS, POPS, IMAPS, SFTP, ...)

Tor und VPN

- Tor über VPN
 - erst Verbindung zum VPN-Server, dann über Tor-Netzwerk ins Internet (Computer → VPN → Tor → Internet)
 - sichtbare IP-Adresse: Exit Node
- VPN über Tor
 - erst Verbindung zum Tor-Netzwerk, dann über VPN-Server ins Internet (Computer → Tor → VPN → Internet)
 - VPN-Client muss für Zusammenarbeit mit Tor konfiguriert werden; aber: nur wenige VPN-Provider unterstützen das
 - sichtbare IP-Adresse: VPN-Server

Tor über VPN

- Vorteile:
 - ISP weiß nicht, dass Nutzer Tor verwendet (sieht aber VPN-Nutzung)
 - Entry Node sieht nicht echte IP-Adresse, sondern IP-Adresse des VPN-Servers
- Nachteile:
 - VPN-Provider kennt echte IP-Adresse
 - kein Schutz vor „schlechten“ Exit Nodes (Nicht-SSL-Verkehr könnte mangels Verschlüsselung überwacht werden)
 - Exit Nodes werden oft blockiert (Liste frei verfügbar)
- Hinweis:

Tor Bridges können die Nutzung von Tor vor einem ISP verstecken. (ISP könnte Tor-Verkehr dann nur durch „Deep Packet Inspection“ entdecken.)

VPN über Tor

- Vorteile:
 - wegen Verbindung zu VPN-Server über Tor kann VPN-Provider echte IP-Adresse nicht sehen (nur die des Exit Node)
 - in Verbindung mit anonymer Bezahlung via Tor kann VPN-Provider trotz möglicher Logs Nutzer nicht identifizieren
 - schützt vor „schlechten“ Exit Nodes, da Daten vom VPN-Client vor dem Betreten (und Verlassen) des Tor-Netzwerks verschlüsselt werden
 - übergeht alle möglichen Blockierungen von Exit Nodes
 - ermöglicht Wahl der Server Location
 - gesamter Internet-Verkehr wird über Tor geroutet
- Nachteile:
 - VPN-Provider kann Internet-Verkehr sehen (aber nicht einem Nutzer zuordnen)
 - nur wenige VPN-Provider unterstützen Tor

Tor in der Praxis

Programme

Tor Browser vorkonfigurierte Kombination aus Tor (Client) und einer modifizierten Version des Browsers Mozilla Firefox ESR (mit NoScript, HTTPS Everywhere, Tor Button und Tor Launcher)

Tor Messenger Instant Messenger, basiert auf Instantbird mit OTR zur Verschlüsselung und Tor zur Anonymisierung

Polipo und Privoxy Proxy zwischen Tor-Client und Browser

Orbot Tor-Proxy für Google Android

Orweb speziell für das Tor-Netzwerk optimierter, quelloffener Browser für Android

Onion Browser Browser für Apple iOS , der Seitenaufrufe über das Tor-Netzwerk durchführt

Sicherheitsstufen bei der Nutzung von Tor

- niedrigste Sicherheit:
Tor-Browser im normalen Betriebssystem
- mehr Sicherheit:
Tor-Browser in einer virtuellen Maschine
- noch mehr Sicherheit:
Betriebssystem und Tor-Software von USB-Stick / SD-Card
(noch sicherer von CD/DVD)
- ganz viel Sicherheit:
zusätzlich: Kombination Tor und VPN
- eigener Entry Node bzw. Tor-Bridge

Tor konfigurieren

- in /etc/tor/torrc oder bei Bundle Data/Tor/torrc
- DataDirectory
- Group und User
- PidFile
- ClientOnly
- SocksPort und SocksListenAddress (Standard: 9050)
- ...

Tor konfigurieren in torrc (Beispiel):

```
DataDirectory /var/lib/tor
Group tor
User tor
PidFile /var/run/tor.pid
ClientOnly 1
SocksPort 4444
```

Tor Relay konfigurieren

Tor Relay konfigurieren (in torrc):

```
ORPort 443  
Exitpolicy reject *:.*  
Nickname irgendwer  
ContactInfo irgendwer@...
```

(ab 2 Mbit/s Up-/Download)

Tor BridgeDB

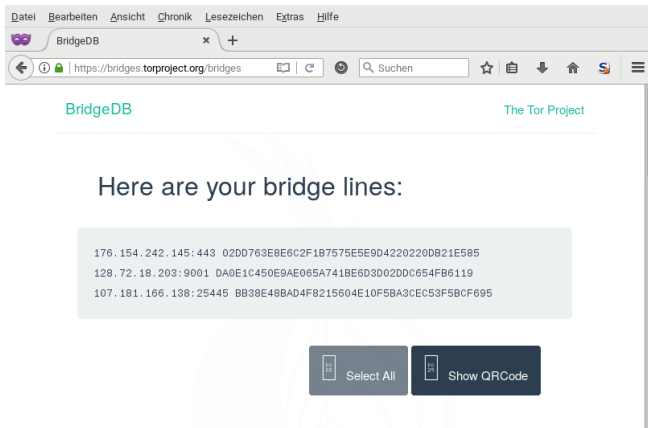


Abbildung: Bridge-Adressen unter
<https://bridges.torproject.org/bridges>

Bridge konfigurieren

- Bridge-Adressen unter <https://bridges.torproject.org/>
- oder: Mail mit Text `get bridges` (oder protokollbezogen z. B.: `get transport obfs3`) an `bridges@bridges.torproject.org` (nur Gmail, Riseup! oder Yahoo!)

Mail-Antwort von `bridges@bridges.torproject.org` (Beispiel):

```
obfs3 60.16.182.53:9001 cc8...123
obfs3 87.237.118.139:444 abc...b56
obfs3 60.63.97.221:443 dada...89c
```


Bridge bereit stellen

Tor Bridge konfigurieren (in torrc):

```
SocksPort 0  
ORPort auto  
BridgeRelay 1  
Exitpolicy reject *:*
```

The Amnesic Incognito Live System (Tails)

- fertiges Bundle als gehärtetes Live-System mit dem Ziel der Internet-Anonymität
- Debian-basierte Leit-Distribution für Tor
- beinhaltet Tor-Client, Tor-Browser, IRC-Client, Mail-Client, Instant Messenger und einigen Sicherheits-Tools
- hardwareunabhängiger Start von DVD, USB-Stick, SD-Karte
- oder in virtueller Maschine (nicht ganz so sicher)
- wurde von Snowden für Veröffentlichungen benutzt
- Homepage: <https://tails.boum.org/>

Ein paar Links zum Tor-Projekt:

- Das Tor-Projekt:
<https://www.torproject.org/>
- Tor-Dokumentation:
<https://www.torproject.org/docs/documentation.html.en>
- Aktuelle Daten wie Bandbreite, Benutzer, Server, Traffic:
<https://metrics.torproject.org/>
- Tails-Homepage:
<https://tails.boum.org/>
- Aktuelle Nachrichten zu Tor auf netzpolitik.org:
<https://netzpolitik.org/tag/Tor/feed/>

Ein paar Links zum Tor-Projekt:

- „Security and anonymity vulnerabilities in Tor“, Vortrag von Roger Dingledine, Leiter des Torprojekts, 25th Chaos Communication Congress, 2008:
<https://events.ccc.de/congress/2008/Fahrplan/track/Hacking/2977.en.html/>
- Liste der Tor-Exit-Nodes:
<https://check.torproject.org/exit-addresses>
- Eine Tor-Node-Liste:
<https://www.dan.me.uk/tornodes>
- Animation des Tor-Datenverkehrs:
<https://torflow.uncharted.software/>
- ...

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de
oder +49 (0)8457 - 931096