Tor-Nodes einfach betreiben, jetzt

Chemnitzer Linux-Tage 2025
Senf (https://senf.space/)
Sonntag (2025-03-23), 12-13 Uhr, Raum V6
ID: 135

Tor bietet als Overlay-Netzwerk Möglichkeiten, einen anonymisierten und zensurresistenten Internetzugang zu ermöglichen [hist]. Die Motivationen, Tor zu nutzen, sind vielfältig. Ich bin der Auffassung, dass weder Staat, Provider, Admins, Mitbewohner, Eltern, Gastgeber, etc. entscheiden oder Kenntnis darüber haben sollen, welche Inhalte von Nutzenden konsumiert werden. Denn nur ein unüberwachter und unzensierter Internetzugang bietet auch einen uneingeschränkten Zugang zu Wissen und Kultur, und zur Teilhabe in unserer digitalen Gesellschaft [ds23]. Der Vortrag "Tor-Nodes einfach betreiben, jetzt" soll ermutigen, einen kleinen Beitrag hierfür zu leisten, in der Hoffnung, damit für eine bessere Welt zu sorgen.

Die Ziele Anonymisierung und Zensurresistenz werden gleichermaßen erreicht, indem der Verkehr durch mehrere (bei Tor drei) regelmäßig wechselnder Netzknoten geleitet wird; wobei die Pakete "zwiebelschalenartig" vom Client mehrfach verschlüsselt werden, von denen jeder Node je eine entschlüsselt. Dieses Konzept ist eine Abwandlung des Konzeptes der Mixkaskaden, welches bereits in den 1980er Jahren von Andreas Pfitzmann erforscht und später ein Schwerpunkt seiner Forschungsarbeit an der TU Dresden wurde [sire].
Der Zugriff auf Dienste im Clearnet (die Meisten verstehen hierunter das "Internet", ist aber nur eine echte Teilmenge dessen) erfolgt über Exit-Nodes. Sie bedürfen besonderer Pflege und werden im Vortrag nicht betrachtet, da auch mir hier die Erfahrung fehlt.
Hidden services (erkennbar an der TLD .onion) weden durch rendezvous points ausschließlich innerhalb des Tor geleitet und benötigen somit keinen Exit.

Allgemein schätze ich persönlich die Anzahl uns zur Verfügung stehender Nodes im Tor als zu gering ein. Weltweit hatten 2024 rund 5,5 Milliarden Wesen einen Internetzugang [itu]. Angesichts mannigfaltiger staatlicher Repressionen kann davon ausgegangen werden, dass einem Großteil jener ein freier Zugang zu Wissen und Kultur somit verwehrt wird [fon]. Tor genießt eine hohe Verbreitung unter den Anonymisierungsdiensten, ist aber mit ca. 8000 Nodes [mtr-ns] im Verhältnis zur möglichen Nutzerzahl sehr klein. Zudem ist davon auszugehen, dass eine Teilmenge bad nodes sind, also von Aktueren (z.B. Geheimdienste) mit dem Ziel betrieben, Nutzer zu deanonymisieren [phbn].

Mir ist es außerdem wichtig, im Tor eine höhere Heterogenität zu erreichen. Ich verspreche mir hierdurch eine höhere Ausfallsicherheit, insbesondere bei gezielten Angriffen auf unsere Infrastruktur, sowie eine Verbesserung der Anonymisierung, da eventuell vorhandene Schwachstellen sich weniger stark auf das Gesamtnetz auswirken.

Im Tor befanden sich in den letzten 3 Monaten etwa 550 Nodes, welche eine *BSD als Plattform nutzen; Bridges eingeschlossen. In Relation hierzu stehen ca. 7300 Linux-basierte Nodes; also grob 93% machen dessen Netz aus [mtr-os]. Auf Linux-Webservern dominieren Debian und dessen Derivate [w3t]. Ein Angriff auf das Tor über den Umweg der Distribution würde somit einen enormen Schaden auch auf das Tor verursachen.
Hier möchte ich motivieren, Nodes mit *BSD zu betreiben und zeige, dass dies auch nicht schwierig ist.

Betrachten wir die Nutzung der Hoster [mtr-as], erkennen wir schnell, dass von den 968 genutzten autonomous systems sich grob 10 "Blasen" gebildet haben, die einen Großteil des Netzes ausmachen. Die Diversität ist hier größer, aber dennoch besteht Verbesserungsbedarf.

Ich werde zeigen, wie ich durch Zufall ein neues AS in das Netz bringen konnte und ermutige auch anhand von Erfahrungsberichten, dass sich auch Nodes an heimischen Internetzugängen mit dynamischen Adressen (IPv4, ohne DSLite ist Voraussetzung) betreiben lassen.

Seit 2019 betreibe ich einige Bridges, seit 2023 auch zunehmend Relays, aber keine Exits. In dieser Zeit hatte ich keinerlei rechtlichen Probleme; und alle Freunde, mit denen ich sprach, die non-exit relays pflegen, schlossen sich dieser Erfahrung an.
Solange in unserem Rechtsraum der Betrieb und die Nutzung von Anonymisierungsdiensten nicht verboten ist, sollten wir diese Freiheit nutzen und somit auch Wesen helfen, welche keinen freien Internetzugang haben.

Der "Mischbetrieb" von Nodes mit weiteren Diensten auf einem Server ist problemlos möglich, selbst mit einem Mailserver. Bereits vorhandene Infrastruktur lässt sich somit nutzen, ohne dass weitere Kosten anfallen. Außerdem lassen sich (sofern keine Bridge konfiguriert wurde) auch gleich vorhandene Dienste als hidden service bereitstellen, um eine Nutzung dieser innerhalb des Tor zu ermöglichen.

Ich muss zugeben, dass ich meine Nodes auch mit händischer Konfiguration ohne nennenswerten Wartungsaufwand betreibe. Vielleicht begehe ich Fehler; dies lässt sich in der anschließenden Diskussion klären; ich bin gespannt.

Desweiteren gehe ich nicht davon aus, dass aus vielfältigen Gründen [phvp] diese Möglichkeiten von monolithischen VPN-Diensten erbracht werden können. Von deren Nutzung rate ich strikt ab.

[mtr-os] https://metrics.torproject.org/platforms.csv?start=2024-11-07&end=2025-02-05
[mtr-as] https://metrics.torproject.org/bubbles.html#as
[mtr-ns] https://metrics.torproject.org/networksize.html
[w3t] https://w3techs.com/technologies/details/os-linux
[itu] https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
[fon] https://freedomhouse.org/countries/freedom-world/scores?sort=asc&order=Total%20Score%20and%20Status
[phbn] https://www.privacy-handbuch.de/handbuch_24j.htm
[ds23] https://senf.space/1984.pdf; ab Frame 22
[hist] https://www.torproject.org/about/history/
[sire] https://dud.inf.tu-dresden.de/sireneLit.shtml
[phvp] https://www.privacy-handbuch.de/handbuch_97e.htm