Missing Link: Wie sicher ist der Anonymisierungsdienst Tor?

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>Missing Link: Wie sicher ist der Anonymisierungsdienst Tor?</h1> Stefan Mey </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: Shutterstock/Irina Anosova)</figcaption></figure> Tor gilt als Wunderwaffe gegen den Überwachungswahn von Geheimdiensten. Wie gut lässt sich die Technologie knacken? Ist Tor tatsächlich NSA- und BND-proof? Der Tor-Browser wird für den Kauf und Verkauf von Drogen im Darknet genutzt, aber auch von Menschen, deren Freiheit oder gar Leben vom Funktionieren der Software abhängt. Deswegen ist ein besonders kritischer Blick auf die versprochene Anonymität nötig. <header class=„a-boxheader“ data-collapse-trigger=„“>„Missing Link“</header><div class=„a-boxtarget a-boxcontent a-inline-textboxcontent a-inline-textboxcontent–horizontal-layout“ data-collapse-target=„“><figure class=„a-inline-textboximage-container“></figure> Was fehlt: In der rapiden Technikwelt häufig die Zeit, die vielen News und Hintergründe neu zu sortieren. Am Wochenende wollen wir sie uns nehmen, die Seitenwege abseits des Aktuellen verfolgen, andere Blickwinkel probieren und Zwischentöne hörbar machen. <ul class=„a-inline-textboxlist“><li class=„a-inline-textboxitem“>Mehr zum Feuilleton „Missing Link“ [1] Die Arbeit an dieser Technologie voller Widersprüche [2] begann Mitte der 90er-Jahre an einem Forschungslabor des US-Militärs. Heute ist Tor ein ungewöhnliches Gemeinschaftsprojekt der globalen digitalen Zivilgesellschaft und der US-Regierung. Die Zivilgesellschaft, vor allem die deutsche Community, stellt die Infrastruktur: die Tor-Verschleierungsknoten. Für sie ist Tor der wichtigste Gegenspieler autoritärer Eingriffe ins Internet. Mit dem Tor-Browser kann man anonym im World Wide Web surfen und Zensur aushebeln, im Tor-Darknet lassen sich Adressen weder löschen noch verorten. Entwickelt wird die Technologie von der Organisation The Tor Project, die sich traditionell über

Fördertöpfe der US-Regierung finanziert. Die Technologie ist prinzipiell anfällig für Angreifer mit großen Ressourcen. Wie solide schützt der Tor-Browser tatsächlich und wie gut lässt sich die Anonymisierungstechnologie knacken? Ein Überblick über die Schwächen von Tor, über mögliche Attacken und Gegenmaßnahmen. <h3 class=„subheading“ id=„nav_schwachstelle0“>Schwachstelle Mensch</h3> Leichtsinniges Verhalten kann für Probleme sorgen: Man verwendet den Tor-Browser, loggt sich aber bei einem sozialen Netzwerk oder einem E-Mail-Dienst mit einem Profil ein, das man auch in anderen Kontexten verwendet. Oder man installiert wild Browser-Erweiterungen. Tor basiert auf Firefox, und für den Firefox-Browser sind Hunderte praktischer Erweiterungen verfügbar, mit denen man beispielsweise bequem Screenshots machen oder Werbung blockieren kann. Einige dieser Plugins werden von Firefox geprüft und für sicher befunden. Es kann aber sein, dass man sich mit kommerziellen Erweiterungen quasi Schadware in den Tor-Browser holt, Plugins die Browser-Nutzung mitschneiden und die gesammelten Informationen verkaufen. Dafür gibt es Beispiele in der Vergangenheit. <h3 class=„subheading“ id=„nav_sicherheitslücke1“>Sicherheitslücken und Hintertüren</h3> Außerdem kann die Tor-Software Sicherheitslücken enthalten. Da der Tor-Browser ein modifizierter Firefox-Browser ist, wirken sich auch Lücken in Firefox [3] auf die Tor-Sicherheit aus. In regelmäßigen Abständen fordert der Tor-Browser auf, ein Update zu installieren. Meist geht es bei den Updates darum, gefundene Sicherheitslücken zu beheben. Solche Lücken können gezielt platziert werden oder auch unbeabsichtigt in die Software gelangen. Eine gängige Erwiderung ist, dass so etwas bei Tor nicht passieren könne, da die Software Open Source ist: Der Code ist öffentlich einsehbar und kann auf Mängel oder gar Hintertüren hin untersucht werden. In der Praxis bietet das dennoch keinen absoluten Schutz. Nur ein Bruchteil der Bevölkerung kann programmieren oder komplexe Programmcodes bewerten. Moritz Bartl vom deutschen Tor-Verein Zwiebelfreunde e. V. [4] hält aufgrund des besonderen Charakters der Tor-Community den Programmcode dennoch für sehr sicher: „Bei Tor schauen tatsächlich viele Leute regelmäßig auf den Code und überprüfen ihn unabhängig vom Tor Project. Tor war und ist immer noch stark universitär geprägt. Deswegen unterscheidet sich Tor von vielen anderen Freie-Software-Projekten, bei denen nicht klar ist, ob es tatsächlich unabhängige Reviews der Code-Basis gibt.“ Tatsächlich ist Tor ein Liebling der Wissenschaft. In wissenschaftlichen Studien wird jede denkbare Angriffsmöglichkeit auf Tor durchgespielt und öffentlich diskutiert. <h3 class=„subheading“ id=„nav_tor_als2“>Tor als „Honigtopf“</h3> Bei allen Technologien der „digitalen Selbstverteidigung“, neben Tor zählt dazu beispielsweise auch E-Mail-Verschlüsselung, gibt es die Debatte, ob diese nicht unfreiwillig als „Honey Pot“ fungieren: als eine Art soziale Filter, mit denen Personen unbeabsichtigt auf sich aufmerksam machen. Indem sie den Tor-Browser nutzen, zeigen Menschen, dass ihnen der Schutz der eigenen Kommunikation wichtiger als anderen ist – und dass sie für eine Überwachung womöglich besonders interessant sind. Das Dilemma besteht, und es lässt sich nicht auflösen. Es besteht, solange nur eine kleine Minderheit der Bevölkerung Verschlüsselungs- und Anonymisierungstechnologien verwendet. <h3 class=„subheading“ id=„nav_der_browser_und3“>Der Browser und sein „Fingerabdruck“</h3><figure class=„a-inline-image a-u-inline“> <figcaption class=„a-caption“>Torflow visualisiert die Datenströme im Tor-Netzwerk. Die meisten Knoten befinden sich in Europa und den USA. (Screenshot)</figcaption> (Bild: <a href=„https://torflow.uncharted.software“ rel=„external noopener“

target=„_blank“>Torflow [5]) </figure> Der Tor-Browser schützt sehr gut vor Überwachung mittels IP-Adressen. Er schützt auch vor einer anderen Browser-typischen Datenquelle: Cookies. Die meisten Webseiten hinterlassen beim Besuch kleine Datenschnipsel im Browser, die Informationen über den jeweiligen Webseitenbesuch enthalten. Beim nächsten Besuch der Webseite kann diese Information wieder ausgelesen und verwendet werden, um beispielsweise Protokolle über das Surfverhalten von Usern zu erstellen. Webseiten können in Tor zwar Cookies ablegen, doch deren Wirkung verpufft. Wird der Tor-Browser geschlossen, löscht er alle Cookies. Wovor der Tor-Browser allerdings nur wenig schützt, ist eine komplizierte und besonders perfide Technologie: das Browser-Fingerprinting. Bei dieser Methode berechnet die aufgerufene Webseite einen technischen Fingerabdruck aus den verschiedenen Software- und Hardware-Eigenschaften des PCs oder Smartphones. Über die Kombination dieser Merkmale können Geräte unter Umständen wiedererkannt und durchs Netz verfolgt werden, je nach Ausmaß des Fingerprintings unterschiedlich genau. Beim Surfen im Internet schickt jeder Browser standardmäßig einige Basis-Informationen an die Webseite, beispielsweise die Spracheinstellung des Browsers. Zusätzlich können Webseiten weitere Eigenschaften auslesen, etwa, welche Schriften im Browser installiert sind oder wie hoch und breit der verwendete Bildschirm ist. Bei einem besonders dreisten Browser-Fingerprinting werden außerdem gezielt Bauteile des Geräts getestet. Ohne, dass man es merkt, wird dabei im Browser eine unsichtbare Grafik oder ein unhörbarer Ton erzeugt. Da die Grafik- und Audio-Karten jedes Geräts minimale Abweichungen aufweisen, weist auch jede Grafik und jeder Ton Geräte-typische Abweichungen auf – so, wie das Schriftbild jeder Schreibmaschine einzigartig ist. Mit dieser Methode ist es möglich, Geräte und damit Nutzer:innen punktgenau wiederzuerkennen – auch dann, wenn der Browser IP-Adressen verschleiert und Cookies standardmäßig löscht. Browser-Fingerprinting ist noch wenig erforscht. Eingesetzt wird die Methode oft nicht von den eigentlichen Webseiten, sondern von eingebauten Drittparteien, etwa von Werbenetzwerken oder Analysediensten. Der Tor-Browser versucht, sich dagegen zu wehren [6], etwa, indem er die tatsächliche Bildschirmgröße verschleiert [7]. Den meisten Fingerprinting-Elementen kann er im Standardmodus aber nichts entgegensetzen. Das gezielte Auslesen von Geräteeigenschaften, etwa das Testen von Bauteilen, läuft über JavaScript – das sorgt aber auch für ein Einfallstor zur Überwachung. Der einzig funktionierende Schutz vor aggressivem Fingerprinting ist, diese Technologie zu deaktivieren. Manche Webseiten funktionieren dann problemlos weiter, andere hingegen nicht. Der Tor-Browser sieht drei Sicherheitsstufen [8] vor. Im „Standard“-Modus funktioniert JavaScript überall. Im „Sicherer“-Modus wird man vom Browser gefragt, wenn Webseiten Bilder oder Töne erzeugen wollen. Im „Am sichersten“-Modus ist JavaScript komplett deaktiviert. Tipp Eins: Wenn Sie das testen wollen, rufen Sie mit dem Tor-Browser die Webseite AmIUnique.org [9] auf und klicken auf „View my browser fingerprint“. Wenn Sie Tor in seinen Standardeinstellungen verwenden, lautet die Diagnose meist: „Yes! You are unique among the … fingerprints in our entire dataset.“ Klicken Sie nun auf das kleine Schild rechts oben in der Adresszeile, verändern Sie die Sicherheitsstufe von „Standard“ auf „Am sichersten“ und wiederholen Sie den Schritt. Sie sehen: Von den 65 berücksichtigten Attributen basieren 59 auf JavaScript und lassen sich in dem Modus nicht auslesen. Tipp Zwei: FPMON [10], eine

Browsererweiterung für Chrome, entwickelt vom Wissenschaftler Julian Fietkau an der TU Berlin, zeigt an, inwiefern Webseiten Fingerprinting betreiben. Es gibt einen Workaround für Firefox [11], allerdings nur als temporäres Add-on, das nach Schließen des Browsers wieder verschwunden ist. <h3 class=„subheading“ id=„nav_die_kunst_der4“>Die Kunst der Korrelation</h3> Schließlich gibt es noch die „Holzhammer-Methode“, und die ist die gefährlichste: Ein Angreifer versucht, Tor zu knacken, indem er großflächig Daten sammelt, quasi von außen auf das Tor-Netzwerk schaut und die technischen Muster der Datenströme vergleicht. Tor leitet Datenverkehr um, verändert ihn aber nicht. Die Datenströme jeder Tor-Verschleierungsroute sehen deshalb auf allen Teilstrecken gleich aus – auf der Strecke vom Tor-Browser zum ersten Knoten, von Knoten zu Knoten und vom letzten Knoten zur Webseite oder Darknet-Seite. Das ermöglichst eine Angriffsform namens „End-to-End Confirmation“ („Ende-zu-Ende-Abgleich“). Eine De-Anonymisierung von Tor ist möglich, wenn ein Angreifer die erste Teilstrecke (zwischen User und Einstiegsknoten) und die letzte Teilstrecke (zwischen letztem Knoten und Webseite bzw. Darknet-Seite) beobachtet und herausfinden kann, dass beide Elemente zur gleichen Verschleierungsroute gehören. Dafür braucht es zwei Schritte: Zuerst schaut der Angreifer auf alle Datenströme, die innerhalb eines Zeitfensters von wenigen Millisekunden ins Tor-Netzwerk hineingehen und das Netzwerk wieder verlassen. Diese Datenströme versucht er einander zuzuordnen. Wie beim Kartenspiel Memory sucht man als Angreifer Paare, die zusammengehören. Um die zu finden, vergleicht man technische Muster. Beim Besuch einer Webseite werden die benötigen Informationen in einer Abfolge kleiner Datenpakete verschickt. Webseiten und ihre Unterseiten sind unterschiedlich groß und enthalten unterschiedliche Elemente. Deshalb erzeugen sie bei der Übertragung unterschiedliche Muster. Erkennt man zwei gleiche Muster, ist klar: Datenstrom Eins und Datenstrom Zwei sind Teil der gleichen Tor-Verschleierungsroute. Die De-Anonymisierung ist geglückt. Gegen einen solchen Angriff kann Tor prinzipiell nicht schützen. In einer Auflistung häufig gestellter Fragen auf Torproject.org heißt es, es sei „für einen Beobachter, der sowohl dich als auch die Zielwebseite oder deinen Tor-Exit-Knoten sehen kann, möglich, die Zeitpunkte deines Datenverkehrs zu korrelieren, wenn er in das Tor-Netzwerk eintritt und auch wenn er es verlässt. Tor bietet keinen Schutz gegen ein solches Bedrohungsmodell.“ <h3 class=„subheading“ id=„nav_webseiten_finger5“>Webseiten-Fingerprinting</h3> Beim End-to-End-Confirmation-Angriff matcht man ein- und austretende Tor-Datenströme. Für diese Korrelation braucht es einen Geheimdienst mit sehr großen Ressourcen. Für einen anderen Angriff namens „Website Fingerprinting“ reicht ein lokaler Angreifer, der nur die Verbindung zwischen User und erstem Tor-Knoten sieht. Das kann beispielsweise der Internetanbieter sein oder eine Sicherheitsbehörde, die auf dessen Daten Zugriff hat. Beim Webseiten-Fingerprinting matcht man einen eintretenden Datenstrom mit einem Eintrag in einer Datenbank. Der Angreifer ruft im Vorfeld auf Vorrat mit dem Tor-Browser Tausende Webseiten, die er gern beobachten würde, auf. Er berechnet deren technische Fingerabdrücke bei der Übertragung der Daten und speichert sie in einer Datenbank. Sollen dann Datenströme „echter“ Nutzer:innen interpretiert werden, genügt ein Vergleich mit der Datenbank. Ist das Muster des Datenstroms in der Datenbank enthalten, ist klar: Diese Webseite wird gerade mit dem Tor-Browser aufgerufen. Studien zur Effektivität von Webseiten-Fingerprinting kommen zum Schluss, dass bis zu 90 Prozent der Webseiten und deren einzelne Unterseiten eindeutig erkannt werden können. Allerdings betrachten die stets nur eine „kleine Welt“ aus wenigen untersuchten Webseiten. Im tatsächlichen Internet hingegen greifen Milliarden an Usern auf Millionen von Webseiten mit Milliarden von Unterseiten zu. Ein Luftschloss ist Webseiten-Fingerprinting dennoch nicht. Ein Großteil der Internetnutzung konzentriert sich auf eine kleine Zahl sehr populärer Webseiten. Angreifer können schon zu guten Ergebnissen kommen,

wenn sie einige Hunderte besonders populäre Webseiten und deren Unterseiten analysieren. Beim Darknet funktioniert Webseiten-Fingerprinting sogar noch besser als im „großen“ World Wide Web. Das Darknet ist tatsächlich eine kleine Welt, und das politisch interessante Darknet ist noch viel kleiner. Geschmälert werden kann der Erfolg von Website Finterprinting außerdem dadurch, dass Webseiten oft dynamisch sind. Die Inhalte unterscheiden sich leicht, je nachdem, von wo man aus darauf zugreift. Außerdem werden unterschiedliche Werbeanzeigen eingeblendet. Umso dynamischer eine Webseite ist, umso schwieriger lässt sie sich einem zuvor erstellten Fingerabdruck zuordnen. Auch an dem Punkt ist das Darknet anfälliger. Darknet-Webseiten sind oft technisch anspruchslos. Man versucht, möglichst wenig überflüssige Software einzubauen, um die Angriffsflächen für Überwachung oder polizeiliche Ermittlungen zu reduzieren. Da sie öfter als Webseiten im Clearnet statisch sind, lassen sie sich besser durch Webseiten-Fingerprinting erkennen. <h3 class=„subheading“ id=„nav_mögliche6“>Mögliche Angriffspunkte für Tor-Attacken</h3> Egal, ob globaler Angriff mittels End-to-End-Confirmation oder lokaler Angriff über Website-Fingerprinting: In jedem Fall braucht es Daten von den Rändern oder aus dem Inneren des Tor-Netzwerks, damit eine De-Anonymisierung oder ein Erkennen von Webseiten gelingen kann. An verschiedenen Stellen können interessante Daten abgegriffen werden: <ul class=„ztitel“>
Tor-Knoten Es gibt etwa 6.200 [12] Tor-Knoten (und neben diesen normalen Tor-Knoten noch etwa 1.300 versteckte Bridge-Knoten zur Aushebelung von Tor-Blockaden), die sehr ungleich verteilt sind. Zwei Drittel des Tor-Datenverkehrs laufen über vier Länder, allen voran Deutschland mit einem Anteil von 31 Prozent, dann folgen die USA (15 Prozent), die Niederlande (11 Prozent) und Frankreich mit 9 Prozent (siehe „Consensus Weight“ unter metrics.torproject.org [13], Stand 19.11.2021). Als offenes Netzwerk ist Tor anfällig für Unterwanderung. Wer hinter den großen Knoten-Familien steht, ist oft bekannt. Vor allem gilt das für Exit-Knoten, die letzte Stufe in der Verschleierungsroute, die die Verbindung zwischen Tor-Netzwerk und „normalen“ Internet herstellt. Die werden oft von Organisation aus dem deutschsprachigen Raum betrieben: allgemeine Digitalorganisationen wie Digitalcourage oder spezialisierte Tor-Vereine wie F3Netze, Artikel10, Zwiebelfreunde oder die Wiener Foundation for Applied Privacy. Hinter einigen großen Knoten stehen auch Einzelpersonen, etwa ein aus dem Umfeld von Berlin stammender IT-Aktivist, der in der Tor-Community unter seinem Pseudonym niftybunny bekannt ist. Stand 19.11.2021 stammen die drei größten Exit-Knotenbetreiber aus Deutschland. Auf Platz Eins steht der Verein F3Netze, mit Sitz im unterfränkischen Haßfurt. Über dessen Knoten laufen 8,1 Prozent des Exit-Datenverkehrs. Auf Platz Zwei stehen die Verschleierungsstationen des Hamburger Vereins Artikel10 (7 Prozent) und auf Platz Drei die Knotenfamilie For-Privacy.net von niftybunny (6,1 Prozent). (OrNetStats [14]) Knoten können allerdings auch anonym betrieben werden, auch von Geheimdiensten und Polizeibehörden. Bösartige Knoten könne es geben, meint Moritz Bartl vom Verein Zwiebelfreunde. Es gebe bei Tor allerdings eine Art soziale Kontrolle, zumindest die großen Betreiber:innen kennen sich: „Es gibt keine Anzeichen dafür, dass Geheimdienste und Staaten massenhaft Tor-Knoten betreiben. Ich kenne die meisten Leute, die hinter den leistungsstarken und schnelleren Tor-Servern stehen, und das sind die wirklich relevanten Knoten.“ Im Jahr 2020 hat sich allerdings gezeigt, wie leicht das Netzwerk dann doch unterwandert werden kann. Eine Hackergruppe hatte im großen Maßstab Exit-Knoten betrieben, die die Verbindung zwischen letzten Tor-Knoten und einer Webseite herstellen. In Spitzenzeiten lag die Wahrscheinlichkeit bei bis zu 24 Prozent, beim Tor-Browsen an einen solchen Knoten zu geraten. Als die Unterwanderung auffiel, wurden die

betrügerischen Knoten aus dem Tor-Netzwerk geworfen, die Cyberkriminellen fügten aber immer wieder neue hinzu. Das Tor-Community-Mitglied nusenu, das die Attacke öffentlich gemacht hatte [15], hält es für wahrscheinlich, dass solche Angriffe weitergehen. Hinter dem Angriff steckten klassische Cyberkriminelle: Sie versuchten mithilfe der Knoten, Bitcoin-Überweisungen via Tor auf eigene Konten umzuleiten. Die Knoten flogen auf, weil sie für einen ungewöhnlich hohen Zuwachs an Bandbreite sorgten und Datenverkehr manipulierten. Schwieriger wird die Enttarnung, wenn Knoten auf den ersten Blick verlässlich ihren Job machen, unbemerkt aber spionieren und Datenverkehr mitschneiden. Nusenu schätzt, dass hinter 60 Prozent der Exit-Knoten bekannte Gruppen oder Persönlichkeiten der Tor-Community stehen. Das bedeutet: Bei 40 Prozent weiß man nicht, wer sie mit welchen Motiven betreibt. Knoten und Knotenfamilien sehen stets nur einen Bruchteil des Tor-Netzwerks. Für Sicherheitsbehörden können sie dennoch von Nutzen sein: Sie können blinde Flecken im sonstigen Tor-Überwachungsprogramm einer Sicherheitsbehörde ergänzen und sie können bei zielgerichteten Angriffen helfen. Mithilfe spezieller Attacken auf Tor-Einstiegsknoten ist es möglich, die Auswahl eines gänzlich neuen Tor-Pfads bei Usern zu erzwingen – in der Hoffnung, dass die nächste Verschleierungsroute einen Knoten beinhaltet, der von der Sicherheitsbehörde kontrolliert wird. Bild 1 von 4<h2>Tor Knoten (4 Bilder) [16]</h2> <figure></figure> [17]<h3>Zahl der Tor-Knoten</h3><figcaption>Zahl der Tor-Knoten: Zahl der „normalen“ Knoten und der versteckten „Bridge“-Knoten, die zum Einsatz kommen, wenn Internetprovider Tor-Knoten blockieren. (Screenshot Metrics.torproject.org, 19.11.2020)
(Bild: Tor Metrics [18])</figcaption><ul class=„ztitel“>
Internetanbieter Stets Einblick in die erste Tor-Strecke haben Internetanbieter. In Deutschland sind es vor allem die Deutsche Telekom, die britische Vodafone und die spanische Telefónica, die Internet in die Wohnungen und auf die Handys der Menschen bringen. Da diese Unternehmen die Interverbindung herstellen, kennen sie bei einer Nutzung von Tor den ersten Tor-Knoten, der angesteuert wird, sowie den Datenstrom zwischen User und erstem Tor-Knoten. <ul class=„ztitel“>
Aufgerufene Webseiten Die aufgerufenen Webseiten hingegen kennen die letzte Tor-Strecke. Mehr als 100 Millionen Webadressen sind weltweit registriert. Die Nutzung konzentriert sich aber überproportional auf wenige große Webseiten. Zum einen sind das die länderspezifischen großen kommerziellen Nachrichtenseiten, zum anderen die großen US-Anbieter. Auch in Deutschland gehören viele der meistgenutzten Seiten zu US-Firmen, etwa die Suchmaschine Google [19], das Videoportal Youtube [20], der Onlineshop Amazon [21], das Streamingportal Netflix [22], der Dateispeicher Dropbox

[23] und die sozialen Netzwerke [24] Facebook und Instagram. <ul class=„ztitel“>
Autonome Systeme Das Internet setzt sich aus etwa 100.000 miteinander kommunizierenden Einzelnetzen zusammen, den sogenannten Autonomen Systemen. Während die großen Exit-Knoten oft eigene Einzelnetze nutzen, laufen viele Einstiegsknoten über die Autonomen Systeme kommerzieller IT-Provider – besonders oft über die Systeme von drei Anbietern. Etwa 18 Prozent des Einstiegs-Datenverkehrs laufen auf den deutschen IT-Provider Hetzner (bei dem sich 363 Tor-Knoten eingemietet haben), 13 Prozent entfallen auf das französische Unternehmen OVH sowie 7 Prozent auf die französische Online SAS/Scaleway (siehe „Guard“-Wahrscheinlichkeit auf OrNetStats, Stand, 19.11.2021 [25]). Die Autonomen Systeme sehen die gleichen Verbindungsdaten wie die Tor-Knoten, die sich bei ihnen eingemietet haben: die vorhergehende und die nächste Verschleierungsstation sowie das Muster des jeweiligen Datenstroms. <ul class=„ztitel“>
Internet-Austauschknoten Im Internet gibt es außerdem so etwas wie Datenkreuzungen. An diesen Internet-Austauschknoten treffen sich Internetanbieter wie die Telekom und Inhalteanbieter wie heise online und übergeben sich ihre Daten. Auch der Datenverkehr zwischen Tor-Usern, Tor-Knoten und Webseiten oder Darknet-Seiten nimmt oft den Weg über solche Austauschknoten. Von diesen Datenkreuzungen gibt es weltweit nur etwa 500. Der Frankfurter DE-CIX betreibt den größten Einzel-Austauschknoten weltweit und ist der zweitgrößte Betreiber von Internet-Austauschknoten. Da die Knoten viele Daten sehen, sind sie eine beliebte Datenquelle für Geheimdienste. Der deutsche Bundesnachrichtendienst etwa greift Daten vom DE-CIX [26] ab. <h3 class=„subheading“ id=„nav_wer_könnte_tor7“>Wer könnte Tor knacken?</h3> Es gibt also viele digitale Punkte, an denen Daten für die De-Anonymisierung von Tor abgegriffen werden können. Gibt es einen quasi allwissenden, globalen Angreifer, der Zugriff auf so viele Daten hat, dass er stets beobachten kann, welche Datenströme ins Tor-Netzwerk hineingehen und das Netzwerk wieder verlassen? Die Enthüllungen des ehemaligen Geheimdienstmitarbeiters Edward Snowden legen nahe, dass zumindest die US-Regierung mit ihrem technischen Geheimdienst NSA in einer solchen Position sein könnte. Die US-Digitalwirtschaft dominiert das weltweite Internet und US-Gesetze verpflichten heimische Unternehmen, ihre Daten Geheimdiensten zur Verfügung zu stellen. Bekannt ist außerdem, dass Geheimdienste ihre Datenschätze teilen. Die Staaten des „Five Eyes“-Abkommens (USA, Großbritannien, Kanada, Australien und Neuseeland) tauschen sehr eng Daten miteinander aus. Deutschland gehört, zusammen mit Frankreich, den Niederlanden, Italien und anderen europäischen Ländern, zur Gruppe der „14 Eyes“, die ausgewählte Daten miteinander tauschen. Einen perfekten globalen Angreifer bräuchte man eigentlich nicht, meint die Sicherheitsforscherin Katharina Kohls, die zurzeit an der Radboud University Nijmegen in den Niederlanden arbeitet und verschiedene Studien zur Tor-Sicherheit [27] durchgeführt hat. Sie verweist auf die zentralisierten Punkte der allgemeinen Internet-Infrastruktur und auf die Daten-Ballungen im Tor-Netzwerk. Es könnte sein, dass allein, wenn die Geheimdienste der wichtigsten Tor-Länder Deutschland, Frankreich, USA und Holland Daten tauschen, die Dienste schon große Teile des Tor-Netzwerks beobachten können. Die Korrelation von Datenströmen klappe in wissenschaftlichen Untersuchungen mit begrenzten Testgruppen sehr gut, so Kohls. Es sei allerdings unklar, wie gut die De-Anonymisierung auch im riesigen weltweiten Internet funktioniere. In der Wissenschaft halte man diese Angriffsmöglichkeit aber trotz aller Unsicherheit für ein ernstzunehmendes

Problem. Tor funktioniere gut für die Abwehr von Massenüberwachung bei Alltagskommunikation. Eine massenhafte De-Anonymisierung aller Tor-User sei sehr aufwändig, auch Geheimdienste hätten nicht unbegrenzte Ressourcen. Wenn es um gezielte Attacken gegen einzelne User gehe, sähe die Rechnung hingegen anders aus, wobei auch da niemand etwas Genaues sagen könne. <h3 class=„subheading“ id=„navquot_tor8“>„Tor funktioniert sehr gut für den Alltagsgebrauch“</h3><figure class=„a-u-inline-right a-inline-image a-u-inline“> <figcaption class=„a-caption“>Katharina Kohls</figcaption> </figure> Die IT-Sicherheitsforscherin Katharina Kohls (im Interview unten) hat verschiedenen Studien zur Tor-Sicherheit [28] durchgeführt und dabei mögliche Angriffsszenarien durchgespielt. Die Informatikerin ist zurzeit Assistant Professor in der Digital Security Group der Radboud University in Nijmegen, Niederlande. <p class=„frage rteabs–frage“>Einer der gefährlichsten Angriffe auf Tor ist ein Vergleich ein und austretender Datenströme. Wie kann man sich das vorstellen? <p class=„antwort rteabs–antwort“>Eine solche Attacke nutzt die Metadaten von Datenströmen. Erstens schaut ein Angreifer auf den zeitlichen Zusammenhang. Das heißt auf die Datenströme, die innerhalb weniger Millisekunden ins Tor-Netzwerk reingehen und das Netzwerk verlassen. Für diese Gruppe vergleicht er zweitens die technischen Muster. Datenströme bestehen aus einzelnen Paketen, die in unterschiedlichem Abstand aufeinanderfolgen. Sind die Paketmuster identisch, ist klar: Ein ein- und ein austretender Datenstrom gehören zum gleichen Tor-Pfad. So lässt sich herausfinden, welche IP-Adresse auf User-Seite auf welche Ziel-IP-Adresse zugreift, die zu einer Webseite, einer Darknet-Seite oder einem sonstigen Internetdienst gehört. Das ist De-Anonymisierung. <p class=„frage rteabs–frage“>Lässt sich Datenverkehr immer durch solche Musteranalysen zuordnen? <p class=„antwort rteabs–antwort“>In Untersuchungen mit einer begrenzten Zahl an simulierten Nutzer:innen und Webseiten klappt das. Wie es im großen weltweiten Internet aussieht, lässt sich schwer sagen. Die Wissenschaft hält solche Angriffe prinzipiell für ein ernstzunehmendes Problem. Allerdings steht die Untersuchung der Wirksamkeit solcher Angriffe im wissenschaftlichen Kontext nicht an erster Stelle. <p class=„frage rteabs–frage“>Gibt es überhaupt einen quasi allwissenden Angreifer, der sämtlichen Tor-Datenverkehr beobachten kann? Die NSA beispielsweise? <p class=„antwort rteabs–antwort“>Auch das kann niemand mit Sicherheit sagen. Allerdings braucht es für Tor nicht unbedingt einen globalen Angreifer. Die Tor-Knoten konzentrieren sich auf wenige Länder. Hinzu kommen die zentralisierten Strukturen des allgemeinen Internets. Schneidet ein Geheimdienst beispielsweise Daten am Frankfurter Internet-Austauschknoten DE-CIX mit, sieht er extrem viel Traffic aus Deutschland. Wenn allein die Sicherheitsbehörden der vier wichtigsten Tor-Länder Deutschland, Frankreich, USA und Niederlande zusammenarbeiten, könnte das schon große Teile von Tor abdecken. <p class=„frage rteabs–frage“>Inwiefern ließen sich Angriffe auf Tor verhindern? <p class=„antwort rteabs–antwort“>Indem man die Muster der Datenströme verschleiert. Eine Möglichkeit wäre, dass Tor-Knoten unterschiedliche lange Verzögerungen einfügen oder dass sie mehrere Datenströme sammeln und im Schwall weiterleiten. Das würde das zeitliche Muster verfälschen, damit würde Tor allerdings langsamer werden, was nicht praktikabel ist. Außerdem könnten Tor-Knoten Dummy Traffic einfügen – künstlich erzeugte Datenpakete, die alle Tor-Datenströme gleich aussehen lassen.
Diese Methode kann funktionieren. Sie würde jedoch die Menge der übertragenen Daten erhöhen, und es ist unklar, ob das das Tor-Netzwerk nicht ans Limit bringen würde. <p class=„frage rteabs–frage“>Wie anonym ist Tor Ihrer Meinung nach unterm Strich tatsächlich? <p class=„antwort rteabs–antwort“>Tor funktioniert sehr gut für den Alltagsgebrauch, um sich datensparsam im Internet zu bewegen. Durchgehende Attacken auf die Anonymität aller Tor-User sind unwahrscheinlich, da auch die

Überwachungsressourcen von Geheimdiensten nicht unbegrenzt sind. Anders ist es, wenn ein Angreifer gezielt eine Person finden oder beobachten will. Wobei auch hier nicht klar ist, wie zielsicher die De-Anonymisierung in der Praxis funktioniert.
Interessant ist: Wenn Leute mit Tor etwas Illegales gemacht haben und die Polizei sie gefunden hat, geschah das nicht wegen Tor, sondern weil die Polizei sie über Fehler oder Sicherheitslücken an anderen Stellen überführen konnte. <h3 class=„subheading“ id=„nav_schützt_tor_vor9“>Schützt Tor vor der NSA?</h3> Ist es also schlicht eine Legende, dass auch der mächtigste Angreifertypus – die NSA oder ein Zusammenschluss großer Geheimdienste – vor Tor kapituliert? Laut internen Dokumenten des BND [29], die das Blog Netzpolitik.org im Jahr 2017 veröffentlicht hat, erstellte der deutsche Auslandsgeheimdienst bereits 2009 ein Konzept „für die Rückverfolgung von Internetverkehren, die mit dem Tor-System anonymisiert wurden“. Der BND ging insgesamt „von einer hohen Überwachungsdichte“ aus und hielt Tor deshalb für nicht sicher genug, um Geheimdienstaktivitäten zu verschleiern. Im Jahr 2014 hatte sich das Bundesamt für Sicherheit in der Informationstechnik knapp zum Thema Tor-Sicherheit geäußert. Der Linken-Politiker Andrej Hunko hatte sich bei der Bundesregierung in einer Kleinen Anfrage erkundigt, inwiefern sie „Tor für ein brauchbares Werkzeug zur Aufrechterhaltung der digitalen Privatsphäre“ hält. Die Antwort [30] fiel überraschend zurückhaltend aus: „Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist Tor für niedrigen bis mittleren Schutzbedarf ein brauchbares Werkzeug zur Aufrechterhaltung der digitalen Privatsphäre.“ Mit hoher Wahrscheinlichkeit kannte das BSI eine NSA-interne Präsentation zu Tor [31], die im Dokumentenschatz von Edward Snowden enthalten war. „Tor stinkt“ – so beginnt die Präsentation von 2012. Darin beklagt sich der technische Geheimdienst der USA: „Wir werden niemals in der Lage sein, alle Tor-User zu allen Zeiten zu de-anonymisieren.“ Mit manueller Analyse sei es möglich, einen sehr kleinen Teil der Tor-User zu enttarnen. Es sei aber nicht möglich, eine bestimmte Person auf Anforderung zu de-anonymisieren. Andere Folien lassen erkennen, dass die NSA aktiv daran arbeitet, Tor besser zu verstehen und knacken zu lernen. Unter anderem ist von einem gemeinsamen Anti-Tor-Workshop mit dem britischen Geheimdienst GCHQ die Rede. Auf einer Folie heißt es, dass man Zugriff auf Tor-Knoten habe, aber nur auf sehr wenige. Nun gehe es darum, die Zahl zu erhöhen und herauszufinden, inwiefern auch Partner-Geheimdienste Knoten betreiben. Es werden Ideen für mögliche Angriffe auf Tor zusammengetragen, zum Beispiel, Datenverkehr so umzuleiten, dass er über „befreundete“ Knoten läuft. Diese interne Analyse wirkt, als ob Tor im Jahr 2012 für die NSA ein Rätsel und ein großes Ärgernis war. Die Präsentation endet allerdings erstaunlich versöhnlich. Die Abschlussfolie greift das „Tor stinkt“ vom Anfang auf und fährt fort: „Aber es könnte schlimmer sein.“ Man werde die Erfolgsrate beim De-Anonymisieren von Tor sicherlich erhöhen können. Es werde wohl niemals möglich sein, auf eine Erkennungsrate von 100 Prozent zu kommen, aber das sei auch nicht unbedingt nötig. Seit 2012 ist viel Zeit vergangen. Die NSA und andere Geheimdienste dürften sehr viel mehr über Tor gelernt haben. Wie gut oder schlecht die NSA mittlerweile Tor knacken kann, kann niemand sagen. Es bräuchte einen neuen Edward Snowden mit neuen Enthüllungen. <h3 class=„subheading“ id=„nav_was_könnte_tor10“>Was könnte Tor tun?</h3> Zumindest in der Theorie gibt es eine simpel klingende Lösung für das Problem der Musteranalysen: Man macht die technischen Muster der Datenströme kaputt. Eine Option wäre, das zeitliche Muster

zu stören. Tor-Knoten würden Datenströme nicht sofort weitergeben, sondern mit unterschiedlich großen Verzögerungen. Alternativ könnten sie Datenströme verschiedener User sammeln und zeitgleich im Schwall weiterschicken. Das würde eine zeitliche Zuordnung von ein- und austretendem Datenverkehr erschweren, Tor aber langsamer und für Anwendungen wie Videochats oder das Streamen von Videos unattraktiv machen. Deshalb schließt Tor diese Option für sich aus. Eine andere Möglichkeit ist künstlich erzeugter „Dummy-Traffic“: Tor-Knoten verändern das Muster der Datenpakete so, dass der ein- und der ausströmende Datenverkehr der gleichen Tor-Route nicht mehr gleich aussieht. Eine gemeinsame Studie [32] von Wissenschaftler:innen und einem Entwickler des Tor Projects hatte 2015 verschiedene Lösungsmöglichkeiten für Webseiten-Fingerprinting durchgespielt und eine Methode namens „Adaptive Padding“ [33] entwickelt. Dabei werden nicht alle Datenströme auf die gleiche Art verändert. Das würde Tor nach Meinung der Forscher:innen zu sehr verlangsamen und das Tor-Netzwerk mit zu viel zusätzlichem Datenverkehr überlasten. Stattdessen werden nur ungewöhnlich aussehende, leicht wiederzuerkennende Datenströme verändert: Wenn Tor-Datenströme auffällig lange Pausen zwischen Paketen enthalten, werden künstliche Dummy-Pakete eingefügt. Wenn hingegen ungewöhnlich viele Pakete aufeinanderfolgen, werden einzelne Pakete kurzzeitig angehalten. Mit dem Ergebnis waren die Forscher:innen zufrieden: Während ohne Fingerprinting-Schutz 91 Prozent der Webseiten erkannt werden konnten, gelang das bei Adaptive Padding nur bei 20 Prozent der Webseiten. Die Methode ist darauf angelegt, vor Webseiten-Fingerprinting durch einen lokalen Angreifer zu schützen. Schützt die Methode auch vor End-to-End-Confirmation durch einen globalen Angreifer wie die NSA? Das könne er nicht sagen, meint Marc Juarez von der Katholieke Universiteit Leuven in Belgien, der an der Studie mitgearbeitet hat. Und er kenne auch niemanden, der das erforscht hat. Moritz Bartl vom Zwiebelfreunde-Verein meint aber, dass die Methode auch großflächige End-zu-Ende-Angriffe zumindest etwas erschweren müsste. 2015 wurde die Adaptive-Padding-Technik vorgestellt und seitdem weiterentwickelt. Umgesetzt wurde sie allerdings noch nicht. Im Mai 2019 [34] veröffentlichte das Tor Project eine Testversion, mit der Forscher:innen die Adaptive-Padding-Methode in eigenen experimentellen Umgebungen ausprobieren und untersuchen können. Wann die Methode tatsächlich ins Live-Tornetzwerk integriert wird, ist noch nicht bekannt. <h3 class=„subheading“ id=„nav_was_kann_man11“>Was kann man selbst tun?</h3> Fassen wir zusammen: Tor kann viel, ist aber auch empfindlich für verschiedene Arten von Angriffen. Je größer die Ressourcen des Angreifers sind, desto eher kann dieser Tor knacken. Das ist allerdings aufwändig, so dass eine permanente De-Anonymisierung aller User unwahrscheinlich ist. Zielgerichtete Angriffe auf einzelne Personen hingegen sind denkbar. Ein im Darknet kursierender Tipp, um sich gegen die Schwächen von Tor zu schützen, lautet, Tor mit einem Virtual-Private-Network-Dienstleister (VPN) zu kombinieren, einem privatwirtschaftlichen Anonymisierungsdienst. Es gibt die Möglichkeit, Tor an erste Stelle und VPN an zweite Stelle zu schalten oder andersherum, so dass jeweils nur die IP-Adresse des VPN-Anbieters sichtbar ist. Neben Tor, so die Theorie, kommt damit noch eine zweite Ebene hinzu, die Geheimdienste zu knacken haben. Das klingt logisch, Moritz Bartl hält von der Methode allerdings wenig: Zum einen würde man neben dem dezentralen Tor-Netzwerk einen zentralisierten, kommerziellen Anbieter mit ins Spiel bringen, bei dem massenhaft Daten über die eigene Browsernutzung anfallen. Zum anderen müsse gefragt werden, ob sich nicht auch

Geheimdienste für den VPN interessieren: „Wenn man davon ausgeht, dass Leute über so viele Ressourcen verfügen, dass sie Tor de-anonymisieren können, lachen die über VPN-Dienste, die sie viel leichter abhorchen können. Wenn Tor unsicher ist, sind VPN noch viel unsicherer.“ Eine andere Möglichkeit, ist, selbst einen Puffer einzubauen: Man nutzt den Tor-Browser in bestimmten sensiblen Situationen nicht von zu Hause aus, sondern verbindet sich „draußen“ mit einem offenen WLAN, zum Beispiel dem Hotspot eines Cafés oder einer Bibliothek. Dabei gibt es allerdings eine Tücke: Wenn PCs sich mit WLANs verbinden, sehen die jeweiligen Netzwerke die MAC-Adresse des Geräts. Darüber kann ein Computer identifiziert werden. Die Mac-Adresse müsste vor und nach der sensiblen Tor-Browser-Sitzung verändert werden, was die Zuordnung verhindert. Das Tor-basierte Betriebssystem Tails [35] verändert die MAC-Adresse standardmäßig. Dem Fingerprinting-Problem kann man mithilfe der „Schutzschild“-Funktion des Tor-Browsers begegnen. Der „Sicherer“-Modus schützt teilweise, im „Am sichersten“-Modus ist JavaScript komplett deaktiviert, so dass keinerlei detailliertes Auslesen von Geräteeigenschaften mehr möglich ist. Die Einstellmöglichkeiten öffnen sich mit einem Klick auf einen kleinen grauen Schild rechts oben im Tor-Browser. Im sichersten Modus funktionieren manche Webseiten allerdings nicht, beispielsweise Youtube.com. Und eine Nebenerkenntnis der 2015er-Studie zum „Adaptive Padding“ war eine schlichte Schutzmöglichkeit gegen Webseiten-Fingerprinting, die sich selbst umsetzen lässt: in Tor mehrere Sachen gleichzeitig machen. Das „Multitab“-Prinzip funktioniert folgendermaßen: Man öffnet in einem Tab die „eigentliche“ Webseite, die man geheim halten will. In einem engen Zeitfenster davor oder danach öffnet man parallel ein weiteres Tab oder mehrere Tabs und ruft dort andere Webseiten auf. Zwar erzeugt der Browser für jeden Tab einen seperaten Tor-Pfad, der erste Knoten ist aber stets der gleiche, erläutert Marc Juarez, einer der Autoren der Studie: „Wenn jemand die Tor-Strecke zwischen dem Browser und dem Einstiegsknoten belauscht, kann er deshalb nicht zwischen den verschiedenen Tor-Pfaden unterscheiden.“ Zwar haben neue Studien mittlerweile gezeigt, dass ausgefeiltere Webseiten-Fingerprinting-Attacken auch den Schutz durch Multitab-Browsing reduzieren können. Es scheint dennoch so zu sein, dass Webseiten-Fingerprinting durch das Öffnen von „Dummy-Tabs“ zumindest deutlich erschwert wird. <header class=„a-boxheader“ data-collapse-trigger=„“>Über den Autor</header><div class=„a-boxtarget a-boxcontent a-inline-textboxcontent“ data-collapse-target=„“><figure class=„a-inline-textboximage-container“><figcaption class=„a-caption a-caption–textbox“>Darknet – Waffen, Drogen, Whistleblower. Wie die digitale Unterwelt funktioniert(Bild: Stefan Mey)</figcaption></figure> Der Text ist ein Auszug aus dem Buch „Darknet – Waffen, Drogen, Whistleblower. Wie die digitale Unterwelt funktioniert“ C.H.Beck 2021 [36] von Stefan Mey (3. vollständig überarbeitete Ausgabe, 240 Seiten 16,95 Euro). Der Autor hat minimale Ergänzungen vorgenommen, Zahlen aktualisiert und Bilder sowie Links hinzugefügt. () <hr /> URL dieses Artikels:
<small>

```
https://www.heise.de/-6272025
```

</small> Links in diesem Artikel:
<small>

[1] https://www.heise.de/thema/Missing-Link

</small>
<small>

[2] https://www.heise.de/meldung/Missing-Link-Von-Zwiebeln-Knoten-und-Moneten-Tor-in-Zahlen-4287404.html

</small>
<small>

[3] https://www.heise.de/news/Angreifer-koennten-Firefox-und-Tor-Browser-Schadcode-Add-ons-unterschieben-4879895.html

</small>
<small>

[4] https://www.zwiebelfreunde.de/

</small>
<small>

[5] https://torflow.uncharted.software

</small>
<small>

[6] https://blog.torproject.org/browser-fingerprinting-introduction-and-challenges-ahead

</small>
<small>

[7] https://support.torproject.org/tbb/maximized-torbrowser-window/

</small>
<small>

[8] https://tb-manual.torproject.org/de/security-settings/

</small>
<small>

[9] https://amiunique.org/

</small>
<small>

[10] https://github.com/fpmon/fingerprinting-monitor

</small>
<small>

[11] https://github.com/fpmon/fingerprinting-monitor/i

```
ssues/6
```

</small>
<small>

```
<strong>[12]</strong> https://metrics.torproject.org/networksize.html
```

</small>
<small>

```
<strong>[13]</strong> https://metrics.torproject.org/rs.html#aggregate/cc
```

</small>
<small>

```
<strong>[14]</strong> https://nusenu.github.io/OrNetStats/#exit-families
```

</small>
<small>

```
<strong>[15]</strong> https://nusenu.medium.com/how-malicious-tor-relays-are-exploiting-users-in-2020-part-i-1097575c0cac
```

</small>
<small>

```
<strong>[16]</strong> https://www.heise.de/bilderstrecke/bilderstrecke_6272516.html?back=6272025
```

</small>
<small>

```
<strong>[17]</strong> https://www.heise.de/bilderstrecke/bilderstrecke_6272516.html?back=6272025
```

</small>
<small>

```
<strong>[18]</strong> https://metrics.torproject.org/networksize.html
```

</small>
<small>

```
<strong>[19]</strong> https://www.heise.de/thema/Google
```

</small>
<small>

```
<strong>[20]</strong> https://www.heise.de/thema/YouTube
```

</small>
<small>

```
<strong>[21]</strong> https://www.heise.de/thema/Amazon
```

</small>
<small>

[22] https://www.heise.de/thema/Netflix

</small>
<small>

[23] https://www.heise.de/thema/Dropbox

</small>
<small>

[24] https://www.heise.de/thema/Social-Media

</small>
<small>

[25] https://nusenu.github.io/OrNetStats/#autonomous-systems-by-cw-fraction

</small>
<small>

[26] https://www.heise.de/meldung/De-CIX-Anhoerungsruege-im-Fall-der-BND-Spionage-abgewiesen-4259736.html

</small>
<small>

[27] https://kkohls.org/publications.html

</small>
<small>

[28] https://kkohls.org/publications.html

</small>
<small>

[29] https://www.heise.de/meldung/Leaks-BND-bruestet-sich-mit-Angriffskonzept-fuer-Anonymisierungsnetzwerk-Tor-3832156.html

</small>
<small>

[30] https://dserver.bundestag.de/btd/18/026/1802674.pdf#page=4

</small>
<small>

[31] https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf

</small>
<small>

[32] https://arxiv.org/pdf/1512.00524.pdf

</small>
<small>

[33] https://www.heise.de/meldung/Leicht-gepolstert-Massnahmen-gegen-Website-Fingerprinting-Angriffe-auf-Tor-3043435.html

</small>
<small>

[34] https://blog.torproject.org/new-release-tor-0405

</small>
<small>

[35] https://tails.boum.org/

</small>
<small>

[36] https://www.chbeck.de/mey-darknet/product/32823389

</small>
<small>

[37] mailto:bme@heise.de

</small>
 Copyright © 2021 Heise Medien </html>