Schutz der Privatsphäre: DNS-Daemon Stubby macht Fortschritte

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“> <figcaption class=„akwa-caption“><p class=„caption akwa-captiontext“>Stubby in Action: Ist die Software installiert und aktiviert, ändert sie die DNS-Konfiguration so, dass sie die DNS-Anfragen des Betriebssystems selbst erhält (sie gehen an die lokale IP-Adressen 127.0.0.1 oder, bei IPv6 an ::1). Diese gibt sie dann selbst TLS-verschlüsselt weiter. </figcaption></figure> Die Entwicklung steckt zwar noch in den Kinderschuhen, aber inzwischen gibt es immerhin zwei Tools für macOS und Android, mit denen man ein Datenschutz-freundlicheres DNS einfach per Mausklick nutzen kann. Der quelloffene DNS-Privacy-Daemon namens Stubby ist erstmals mit einer graphischen Oberfläche für macOS erschienen[1]. Stubby wird parallel auch für andere Betriebssysteme entwickelt und verschickt TLS-verschlüsselte DNS-Anfragen an geeignete Resolver. So trägt die Software zu mehr Privatheit bei der Internet-Kommunikation bei. Denn übliche, im Betriebssystem eingebaute Stub-Resolver verschicken DNS-Anfragen unverschlüsselt, sodass man leicht auslesen kann, welche Web-Seiten der Absender der DNS-Anfrage besucht. Stubby verwendet die Spezifikation „DNS over TLS“ der Internet Engineering Task Force (RFC 7858[2]). Die Technik setzt Resolver voraus, die TLS-verschlüsselte Anfragen annehmen. Und natürlich sind solche Resolver nur dann hilfreich, wenn die Betreiber die DNS-Anfragen der Nutzer nicht protokollieren. Eine Liste haben die Betreiber des Projekts „DNS-Privacy“ auf ihrer Web-Seite[3] veröffentlicht. <h5 id=„nav_vorerst_nur_für1“>Vorerst nur für Testzwecke</h5> Am sicheren Stub-Resolver für PCs arbeiteten bislang vor allem Sara Dickinson und die Partner des DNS-Privacy-Projekts. Es handele sich um eine Vorschauversion, ein „Alpha-Release der Version 0.1.0“, unterstrich Dickinson in einer Mail an heise online. Bislang wurde die Software auf macOS Sierra und High Sierra getestet. An mehreren Punkten gilt es noch zu feilen, sodass sich die Software keinesfalls für den Produktivbetrieb eignet: Der Sleep-Modus kann Stubby aus der Bahn werfen und manchmal ist er ohne Einfluss von Außen verwirrt. Was man dann tun kann, beschreibt die Entwicklerin im Bereich Known Issues[4] auf der Download-Seite der Software. Weitere wichtige Schritte bei der Entwicklung sind die klare Unterscheidung des strikten Datenschutzmodus (nur verschlüsselt) vom opportunistischen (wenn vorhanden). Auch soll die Transparenz bei Veränderungen der Netzwerkkonfiguration verbessert werden. Später soll es für Stubby auch auf Windows und Linux ein GUI geben. <h5 id=„nav_dns_privacy_für2“>DNS-Privacy für Android</h5> Auch Android-Nutzer können seit ein paar Wochen DNS über TLS

testen. Die Software entstammt den Tastaturen von Erik Kline und Ben Schwarz (beide sind Google-Mitarbeiter) und ist auf der zugehörigen Website erhältlich[5]. Nach dem Herunterladen können Nutzer zwischen drei Optionen wählen: privacy mode, opportunistic mode oder privacy-off mode – also durchgängiger Standardbetrieb ohne Verschlüsselung. Beim jüngsten Treffen der Internet Engineering Task Force konnten die Autoren für eine Demonstration auf den TLS-fähigen Server ihres Kollegen Warren Kumari zugreifen. Wer die Software in freier Wildbahn testen will, kann einen der Resolver von der Liste des DNS-Privacy-Projekts im Android-Gerät einstellen. <h5 id=„nav_dns_privacy_für3“>DNS-Privacy für das Heimnetz</h5> Die DNS-Resolver Unbound, Knot und BIND setzen das RFC 7858 schon länger um und laufen stabil. Alle drei sind aber nur für die Steuerung per Kommandozeile ausgelegt. Wie man Unbound mit DNS-Privacy zum Beispiel auf einem Raspi für ein ganzes Netz einrichtet, erklärt der c't-Artikel „Privatsphäre per Tunnel[6]“ Schritt für Schritt. (Monika Ermert) / (dz[7])<br class=„clear“/> <hr/> URL dieses Artikels:
<small>

```
http://www.heise.de/-3918634
```

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

```
<strong>[1]</strong> https://dnsprivacy.org/wiki/display/DP/Stubby+GUI+for+macOS
```

</small>
<small>

```
<strong>[2]</strong> https://www.heise.de/netze/rfc/rfcs/rfc7858.shtml
```

</small>
<small>

```
<strong>[3]</strong> https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers
```

</small>
<small>

```
<strong>[4]</strong> https://dnsprivacy.org/wiki/display/DP/Stubby+GUI+for+macOS
```

</small>
<small>

```
<strong>[5]</strong> https://android-review.googlesource.com/q/topic:dns-dev-opt+(status:open+OR+status:merged
```

</small>
<small>

```
<strong>[6]</strong> https://www.heise.de/ct/ausgabe/2017-20-Domain-Name-Service-Datenschutz-selbstgebaut-3825108.html
```

</small>
<small>

```
<strong>[7]</strong> mailto:dz@ct.de
```

</small>
 Copyright © 2017 Heise Medien </html>