Richtlinie zum „Software-Sprint“

OONI_RiseupVPN
Mit IPv6 und OONI RiseupVPN's Konnektivität steigern

Schlussbericht

Zuwendungsempfänger:

Johannes & Nuyts Gbr, Ebereschenweg 18, 91058 Erlangen

§ Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS20S47 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

· Kurze Darstellung der Aufgabenstellung und Motivation

§ Was war Deine Motivation? Welches Problem wolltest Du mit Deinem Projekt lösen? Wie war die geplante Vorgehensweise zur Problemlösung (auch Angabe der wichtigsten Meilensteine)?

Der nicht-kommerzielle Dienst RiseupVPN startete Anfang 2019, um Nutzer:inneneine freie, sichere und unzensierte Online-Kommunikation zu ermöglichen. Zielsetzung des geförderten Projektes war es, die Konnektivität des VPN-Dienstes zu verbessern.
Zum einen wird der VPN-Dienst - wie auch kommerzielle Dienste anderer VPN-Anbieter - in manchen Fällen von staatlichen oder privatwirtschaftlichen Institutionen blockiert. Die Meldungen solcher Blockaden fand bisher unsystematisch und unvollständig durch einzelne Nutzer:innen statt, die sich persönlich auf den Hilfeseiten von Riseup meldeten. Mithilfe der Förderung trugen wir dazu bei, dass Zensurversuche im Internet durch das Projekt OONI (Open Observatory of Network Interference) umfangreicher dokumentiert wird und versetzten Riseup in die Lage, einen detaillierten Einblick über Blockadeversuche ihrer Infrastruktur zu erhalten.
Zum anderen arbeiteten wir an RiseupVPN's Unterstützung des Internetprotokolls IPv6, um Anwender:innen Zugriff auf Webinhalte über das VPN ermöglichen, die nur über IPv6 erreichbar sind.

Wir hatten uns für den Förderzeitraum sechs Meilensteine gesetzt. Wir mussten aus organisatorischen und technischen Gründen die Meilensteine anpassen. Die Meilensteine, die sich auf OONI bezogen, zogen wir dabei nach vorne.

1. Recherche und Dokumentation IPv6 bezogener Netzwerktechniken und ihren Einfluss auf Metadatenverlust

2. Entwicklung einer Testumgebung zur Erkennung von Metadatenverlusten

3. Serverseitige Integration von IPv6 und Aktualisierung der ProviderAPI

4. Clientseitige Auswertung der ProviderAPI und Implementierung einer adaptivenFirewall

5. Entwicklung von OONI Tests für den OONI-Probe Client (Android)

6. Implementierung eines Provider-Dienstes zum Abfragen und Auswerten der OONI-Datenbank

· Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Welche Bezüge gibt es zu den Themenfeldern „Civic Tech“ und „Data Literacy“ des Software Sprints oder zu weiteren gesellschaftlich relevanten Zielen bzw. Lösungsansätzen?

Freier Zugang zu Informationen ist ein wichtiger Baustein für die demokratische Meinungs- und Willensbildung. Ein uneingeschränkter Zugang zu sozialen Plattformen ermöglicht es Menschen, sich zu vernetzen und Gehör zu verschaffen, soziale Missstände zu kritisieren und gesellschaftlichen Wandel von der Basis aus zu organisieren. Davon lebt eine Demokratie des 21. Jahrhunderts.
Mit dem geförderten Projekt verbesserten wir ein konkretes Werkzeug, RiseupVPN, das genutzt werden kann, um sich einen freien Zugang zu Informationen zu verschaffen und sich privatwirtschaftlicher Überwachung ein Stück weit zu entziehen.

Der OONI-Teil unseres Projektes ermöglicht es dem VPN-Betreiber Riseup frühzeitig und systematisch zu erkennen, wo Nutzer:innen keinen oder eingeschränkten Zugang zu ihrer Infrastruktur erhalten. Darüber hinaus ist die erweitere Datenbasis zur Nutzbarkeit des VPNs öffentlich verfügbar und steht beispielsweise Wissenschaftler:innen zur Verfügung, die zum Thema Internetzensur forschen und publizieren.

· Ausführliche Darstellung der Ergebnisse

§ Welche konkreten Ergebnisse hast Du erzielt? Konnten alle Meilensteine erreicht werden? Welche zusätzlichen Erkenntnisse hast Du aus der Projektarbeit gewonnen, auch im Hinblick auf die Begleitung durch die Open Knowledge Foundation?

IPv6

Im Rahmen der Förderung wurden IPv6-basierte Technologien und ihre Einflüsse auf eine sichere VPN-Architektur recherchiert, u.a. zu Technologien der Netzwerkaddressübersetzung (NAT64), P2P-Verkehr (NPTv6), IPv6 Multicast und WebRTC. Die Ergebnisse wurden in einem Blogpost auf https://leap.se veröffentlicht und die daraus gewonnen Erkenntnisse flossen in die weitere Entwicklungsarbeit ein.

Der auf Ansible basierende serverseitige Installationsprozess der genutzten VPN-Software wurde bearbeitet , um IPv6 zu unterstützen. Es wurde die serverseitige Firewall geändert,

um die korrekte Weiterleitung des IPv6-Datenverkehrs sicherzustellen. Die Konfigurationsschnittstelle (API) des Backends wurde angepasst, um die IPv6-Adresse eines jeden VPN-Gateways an Clients zu kommunizieren.

Es wurde ein Mechanismus entwickelt, um clientseitig (RiseupVPN Android) die IPv4/IPv6 Unterstützung eines Gateways abzurufen und auszuwerten.

OONI

Wir haben im Rahmen des Arbeitspaketes "OONI" der OONI-Test-Sammlung eine technische Spezifikation für RiseupVPN hinzugefügt sowie eine leicht verständliche Beschreibung der Netzwerktests auf ooni.org veröffentlicht.

Auf Basis der Spezifikation entwickelten wir OONI-Netzwerktests zur Überprüfung der Erreichbarkeit RiseupVPN's Konfigurationsschnittstelle sowie aller im Betrieb befindlichen VPN-Gateways. Die Tests validieren dabei die Erreichbarkeit von IPs, die korrekte Auflösung von DNS sowie das Aufbauen einer TCP-Verbindung auf allen angebotenen Ports eines VPN-Gateways.

Die Netzwerktests wurden in die Software-Bibliothek OONI-Probe Engine integriert.

Es wurden die OONI-Probe Clients für Android, iOS, Desktop und das Command-Line-Interface (CLI) angepasst, um die Netzwerktests der aktualisierten Software-Bibliothek OONI-Probe Engine aufzurufen und die Testergebnisse darstellen zu können.

Es wurde eine Software namens OONI-Exporter entwickelt, die als Rückkoppelungsmechanismus fungiert, über welchen die gesammelten Testergebnisse in regelmäßigen Abständen abgefragt und in das Server-Monitoring-System Prometheus eingespeist werden. Die Testergebnisse lassen sich nach Netzwerken, Regionen, einzelnen Gateways und anderen Kategorien filtern sowie grafisch darstellen.

· Zielgruppe, Nutzen und mögliche Weiterentwicklungen

§ Welcher Nutzen ergibt sich für die Zielgruppe aus den Ergebnissen Deines Projekts? Welche weiter-gehenden Effekte ergeben sich aus der Open-Source-Stellung der Ergebnisse? Gibt es Ideen für die Weiterentwicklung Deiner Lösung und Pläne zu deren Umsetzung?

Riseup hat nun die Möglicheit besser auf Blockadeversuche zu reagieren, etwa durch das Ändern einzelner Gateway-IPs, das Aufsetzen weiterer Server, die bestehende Obfuskierungsprotokolle wie obfs4 unterstützen oder durch das Einsetzen neuer Umgehungstechnologien. Die Effektivität dieser Umgehungstechnologien lässt sich dabei durch das entwickelte System bemessen.

Durch die Open-Source-Stellung der Ergebnisse können die entwickelten Tests als Blaupause für Organisationen dienen, die die VPN-Software von LEAP nutzen, um eigene Netzwerktests in OONI zu integrieren. Die von uns im Förderzeitraum entwickelte Software "OONI-Exporter" zur Abfrage der Testergebnisse vom OONI-Backend und zur Integration in Prometheus ist sofort für andere LEAP-basierte Provider nutzbar.

Als weiteren Entwicklungsschritt planen wir die Generalisierung der OONI-Netzwerktests, sodass ganz ohne programmatischen Aufwand andere LEAP-basierte Provider ihre Netzwerktests in die OONI-Clients integrieren können, die dann von Freiwilligen weltweit ausgeführt werden.

Auch von den IPv6-bezogenen Verbesserungen werden alle Provider, die die VPN-Backend- und Clientsoftware nutzen, profitieren, da sie in den kommenden Releases über ein Update zur Verfügung stehen werden.

Im Rahmen der Förderung konnten wir IPv6 Unterstützung prototypisch umsetzen. In weiteren Entwicklungszyklen werden wir die entwickelte backendseitige Lösung auf parallel zum Förderprojekt stattgefundene architektonische Änderungen des Backends anpassen. Die nötigen Anpassungen auf Seiten des Clients wurden exemplarisch für RiseupVPN Android implementiert. Die Desktop-Clients müssen diesbezüglich nachgezogen werden.

Endanwender:innen werden nach der produktiven Einfühung der IPv6-Unterstützung von kürzeren Ladezeiten profitieren, da das für Nutzer:innen transparent stattfindende Aushandeln der unterstützten Internet-Protokoll-Version ohne Timeouts vonstatten gehen wird. Andere Inhalte werden erst durch die Innovation über das VPN verfügbar. Damit kann zukünftig der Nutzungsfall ausgeschlossen werden, dass das VPN selektiv ausgeschaltet und damit der eigene Schutz im Internet herabsetzen wird, um einzelne Webinhalte konsumieren zu können. Mit den Arbeiten im Rahmen der Förderung haben wir dafür wegweisende Schitte vorgenommen.

Hat die Arbeit in dem Projekt Dich in Deiner persönlichen, fachlichen Weiterentwicklung unterstützt?

Insbesondere die Arbeit an der Unterstützung von IPv6 hat uns vor technische und fachliche Herausforderungen gestellt. Im Netzwerkbereich haben wir viel geübt und dazugelernt.

Durch das Förderprojekt konnten wir die Arbeitsorganisation des OONI-Softwareentwicklungsteams kennen lernen, was uns neue Implulse für unsere weitere Zusammenarbeit im Rahmen der VPN-Software brachte.

· Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

§ Gab es Arbeiten bzw. Lösungsansätze, die nicht weiter verfolgt wurden? Was waren die Hinter-gründe, und wie bist Du alternativ vorgegangen?

Um unsere Entwicklung bezüglich der IPv6-Unterstützung zu validieren, planten wir ein Web-Tool zur Analyse möglicher IP-Leaks aufzusetzen. Dafür hatten wir bereits in der Vorbereitungsphase des Förderprojektes mögliche geeignete Open-Source-Werkzeuge identifiziert. Wir mussten später feststellen, dass die einzig geeignete Testsoftware von ExpressVPN jedoch ausschließlich lokal auf den Entwicklungsrechnern läuft. Wir nutzten es während der Arbeit, verzichteten jedoch darauf, einen Online-Dienst selber zu entwickeln und aufzusetzen, da dies den verfügbaren zeitlichen Rahmen überschritten hätte.

· Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

§ Wo können sich Interessenten detailliert über Deine Projektergebnisse informieren (z.B. Webseite, GHitHub, Veröffentlichungen)?

Über die Projektergebnisse berichteten wir in Form eines Blogposts unter:
https://demoweek.prototypefund.de/projects/14-riseupvpn-ooni-ipv6.html
Der Quellcode der im Rahmen des Förderprojektes angepasst wurde findet sich unter folgenden Adressen:

OONI Spezifikationen https://github.com/ooni/spec 3-clause BSD license (BSD-3-Clause)
OONI Probe CLI und miniooni CLI: https://github.com/ooni/probe-cli 3-clause BSD license (BSD-3-Clause)
OONI probe-engine, Netzwerktest-Bibliothek: https://github.com/ooni/probe-engine 3-clause BSD license (BSD-3-Clause) (inzwischen zusammengeführt mit OONI Probe CLI)
OONI probe iOS Client: https://github.com/ooni/probe-ios BSD 2-clause license
OONI probe Android Client: https://github.com/ooni/probe-android BSD 2-clause license
OONI probe Desktop Client: https://github.com/ooni/probe-desktop BSD 3-Clause

OONI Exporter https://0xacab.org/leap/ooni-exporter GPLv3
Prometheus Pushgateway Docker Container: https://0xacab.org/leap/container-platform/prometheus-pushgateway GPLv3

RiseupVPN Android: https://0xacab.org/leap/bitmask_android GPL-3.0
RiseupVPN Server / LEAP Server platform: "lilypad" https://0xacab.org/leap/container-platform/lilypad GPL-3.0
Menshen, Geolocation und Gatewaystatus-Service https://0xacab.org/leap/menshen GPL-3.0
Bitmask Hilfeseiten https://0xacab.org/leap/bitmask_help

· Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Gab es im Projektverlauf Ereignisse, die eine Anpassung der Planung erforderlich machten – z.B. Mehr- oder Minderaufwand bei der Bearbeitung von Teilaufgaben?

Die von uns weiterentwickelte VPN Backendsofware befand sich während des Projektbeginns noch in einer Alpha-Phase. Sie wird momentan noch nicht produktiv eingesetzt, aber die existierende Backendsoftware des Providers Riseup zukünftig ersetzen. Wir hatten aufgrund unzureichender Dokumentation und einiger Softwarefehler deutlich mehr Zeit benötigt, Entwicklungsserver aufzusetzen. Wir nutzen die Erkenntnisse, die wir dabei gewannen, um Fehler zu melden, zu beheben und die Dokumentation zu verbessern. Dies war nicht Teil der ursprünglichen Planung, erwies sich aber als nötig, um bei den IPv6-bezogenen Arbeitspaketen Fortschritte erzielen zu können.

· Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

§ Gab es Entwicklungen anderer Personen oder Institutionen, die Einfluss auf Deine Arbeiten und die Zielsetzung hatten? Wenn ja, worin bestand dieser und wie bist Du damit umgegangen?

Während des Förderprojektes fanden einige grundsätzliche Änderungen am Backend durch andere am Softwareprojekt Beitragende statt, mit dem Ziel den Deploymentprozess neuer Server zu vereinfachen. Uns stellten diese Entwicklungen vor die Herausforderung, die IPv6-bezogenen Arbeiten an die architekonischen Änderungen anzupassen und die parallel stattfindenden Arbeiten zu synchronisieren.

Wir möchten uns an der Stelle beim Softwareentwicklungsteam von OONI als externe Institution bedanken, das durch seine unterstützende und beratende Tätigkeit bei der Evaluation unserer Pull Requests und durch eigene Initiativen entscheidend zum Erfolg des Projektes beigetragen hat.

Das OONI Projekt verfügt über ein quelloffenes Verzeichnis an Spezifikationen wie unterschiedliche Protokolle, Anwendungen und Webseiten (DNS, Netzkonnektivität, Tor...) auf ihre Erreichbarkeit getestet werden. Diese Tests werden von Mitgliedern der OONI Community auf ihren mobilen Endgeräten mithilfe der OONI Probe App ausgeführt. Die Ergebnisse werden in einer zentralen Datenbank gespeichert und sind über eine Schnittstelle abrufbar. Wir werden der OONI Testsuite Spezifikationen für RiseupVPN hinzufügen. Einerseits werden bereits existierende OONI Tests weiterentwickelt, u.a. für OpenVPN, DNS, OBFS4, welche von RiseupVPN genutzte Komponenten und Protokolle sind. Anderseits werden neue Tests zur Erreichbarkeit der Provider API, d.h. der serverseitigen Schnittstelle, die RiseupVPN Clients zur Selbstkonfiguration nutzen, sowie zur Leistung und Konnektivität der Gateways, mit denen die Clientseine VPN Verbindung aufbauen, entwickelt. Serverseitig wird unter Zuhilfenahme der OONI-API eine automatisierte Abfrage der Testergebnisse implementiert. Die Ergebnisse werden dabei zum Monitoringsystem von RiseupVPN weitergeleitet und dort für die Administrator:innen visualisiert.