



netidee

PROJEKTE

Safing

Endbericht | Call 15 | Projekt ID 5168

Lizenz CC-BY-SA

Inhalt

1	Einleitung.....	3
2	Projektbeschreibung.....	3
3	Verlauf der Arbeitspakete.....	5
3.1	Arbeitspaket 1 - Projektstart.....	5
3.2	Arbeitspaket 2 – Community Management	5
3.3	Arbeitspaket 3 – Portmaster Prüfung SSL/TLS Zertifikate	6
3.4	Arbeitspaket 4 – SPN Routenoptimierung.....	6
3.5	Arbeitspaket 5 – SPN Ausfallsicherheit	7
3.6	Arbeitspaket 6 – Projektende	7
4	Umsetzung Förderauflagen.....	7
5	Liste Projektergebnisse.....	7
6	Verwertung der Projektergebnisse in der Praxis.....	8
7	Öffentlichkeitsarbeit/ Vernetzung	9
8	Eigene Projektwebsite.....	9
9	Geplante Aktivitäten nach netidee-Projektende.....	9
10	Anregungen für Weiterentwicklungen durch Dritte	10

1 Einleitung

Durch die rasant fortschreitende Digitalisierung wird Privatsphäre ein immer wichtigeres Thema. Besonders durch die Pandemie wurden Personengruppen, die normalerweise nicht viel online surfen, gezwungen, neue Tools zu verwenden, die primär über das Internet funktionieren. Viele Unternehmen werden mit mehr Daten gefüttert als jemals zuvor.

Wir kämpfen daher umso härter für Privatsphäre im Netz. Der Portmaster und das SPN sollen helfen, dem/der NutzerIn wieder die Kontrolle über seine/ihre Daten zu haben.

2 Projektbeschreibung

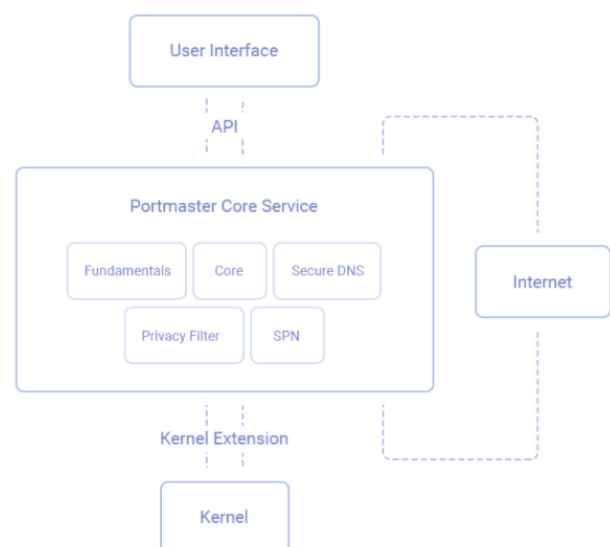
Ziele und Zielgruppe:

Unser Ziel ist es, eine bessere Zukunft mit echter online Privatsphäre für jeden zu ermöglichen. Anstatt Werkzeuge für Experten zu bauen, möchten wir allen Menschen ermöglichen, Freiheit in der heutigen Onlinewelt zu haben.

Safing zielt momentan noch auf technikaffine Personen, welchen wichtig ist, die volle Kontrolle über ihren Datenfluss zu haben. Ein/e typische/r NutzerIn verwendet höchstwahrscheinlich bereits eine Firewall oder ein VPN und ist entweder auf Windows oder Linux.

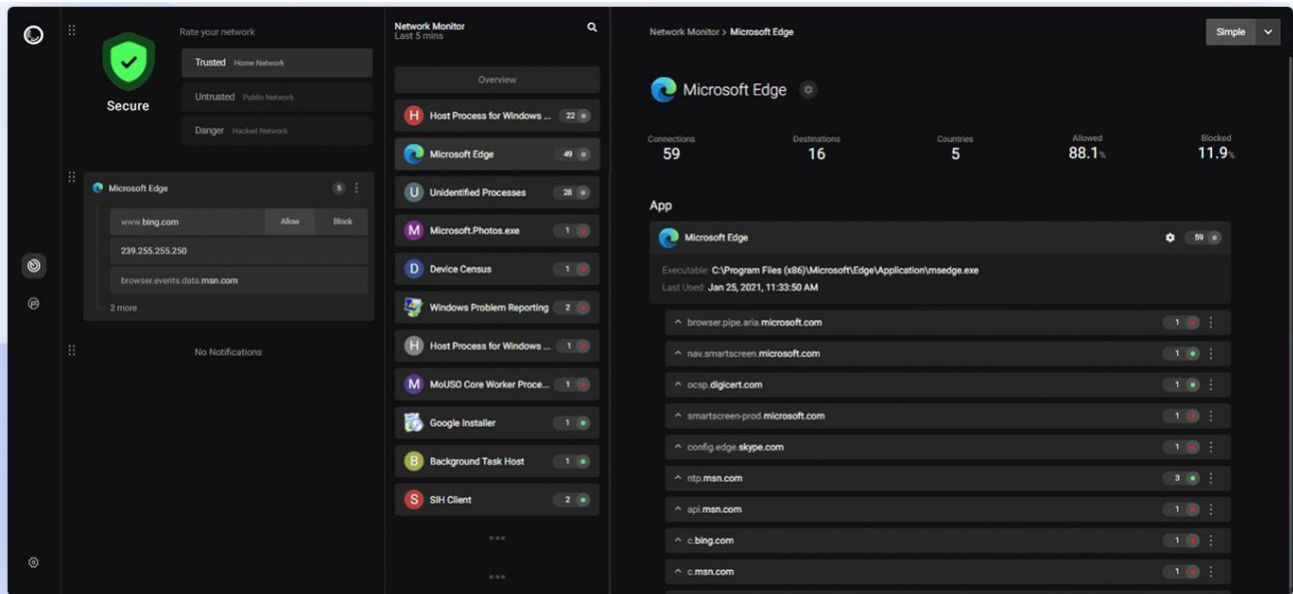
Portmaster – intelligente Application Firewall

Im Kern ist der Portmaster ähnlich zu einer Firewall, er regelt das Netzwerkverhalten des Rechners. Er kann aber um einiges mehr, weil er nicht nur das Netzwerk selbst, sondern tiefer in den Kernel und die auf dem Rechner laufenden Applikationen eintaucht. Es werden z.B. Applikationen und Zieldomain betrachtet und in Kombination verwendet. Auf diese Weise hat man eine viel feinere Kontrolle über die ein- und ausgehenden Verbindungen. Es ist möglich, facebook aus Spotify „heraus“ zu blockieren. Der Portmaster sitzt dank



der Kernel Extension so tief, dass er selbst das Betriebssystem betrachten und beeinflussen kann.

Der Portmaster verwendet Sicherheitslevel (trusted, untrusted & danger), um den NutzerInnen in einfachster Weise zu ermöglichen, die Software an aktuelle Bedürfnisse anzupassen. Man kann für die verschiedenen Sicherheitslevel unterschiedliche Einstellungen festlegen. Zum Beispiel kann einer Applikation der Internetzugriff verwehrt werden, sobald man sich in einem öffentlichen Netzwerk befindet. Diese bekommt aber wieder freien Internetzugang, wenn sich das Gerät mit dem Heimnetzwerk verbindet. Der Portmaster erstellt selbstständig Verhaltensprofile der verschiedenen Applikationen und passt den Sicherheitslevel dynamisch an.



Status

Der Portmaster befindet sich in der Alpha-Phase. Er läuft grundsätzlich schon stabil, aber er kommt noch nicht ganz an Beta-Software heran. In diesem Projekt lag der Fokus besonders auf der Prüfung der SSL/TLS Zertifikate.

Safing Privacy Network - SPN

Das SPN ist ein schnelles Privatsphärenetzwerk, das für jede Verbindung ins Internet einen eigenen Pfad baut. Es besteht aus Nodes, die netzartig miteinander verbunden sind. Anstatt direkt mit den Servern des Internets zu kommunizieren, können NutzerInnen sich durch das SPN mit dem Internet verbinden und so ihre Privatsphäre und Identität schützen. Innerhalb des Netzwerks werden die notwendigen Verbindungen zwischen einzelnen Nodes mit Hilfe des Algorithmus kalkuliert, um eine hohe Geschwindigkeit und Verfügbarkeit für alle NutzerInnen sichern zu können. Alle Nodes teilen dieselbe Grundinformation miteinander, damit jeder weiß, wie das Netzwerk aussieht und so die beste und effizienteste Route kalkuliert werden kann.

Aus der Sicht der/s NutzerIn fühlt sich das SPN ähnlich wie ein VPN-Service an. Der Unterschied ist aber beträchtlich: Bei einem VPN wird lediglich eine sichere Verbindung zu einem Server des

Anbieters aufgebaut. Von dort nehmen die Verbindungen ins Internet wieder lange Wege durch ungeschützte Netzwerke auf sich. Das SPN hingegen kombiniert den Zielort und den nächsten Server unseres Netzwerkes, um Verbindungen so kurz wie möglich dem ungeschützten Internet auszusetzen. Dadurch ist man aus Sicht des Internets an mehreren Orten gleichzeitig, der Zielservers weiß nicht, wo man ist, der Internetprovider (A1, Magenta, etc.) sieht nicht wohin man sich verbindet und sämtliche Daten sind geschützt. Man kann ohne Bedenken in öffentlichen Netzwerken surfen.

Status

Das SPN befindet sich noch in der Early-Alpha Phase, aber tendiert schon eher Richtung Alpha. Es wird bereits ausgiebig getestet und laufend stabilisiert. In diesem Projekt lag der Fokus besonders auf Ausfallsicherheit und Routenoptimierung.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 - Projektstart

Das Projekt ist ohne Probleme oder Komplikationen im Dezember 2020 gestartet. Die erste Förderrate wurde bereits im Dezember ausbezahlt und der erste Blogbeitrag wurde ebenfalls veröffentlicht. Es gab keinerlei Abweichungen, weder zeitlich noch inhaltlich. Die Erfahrung aus vorangegangenen Förderungen hat dazu beigetragen, dass der Projektstart schneller als üblich vonstatten ging.

3.2 Arbeitspaket 2 – Community Management

Wir haben im Laufe des Projektes einige Videos des Youtubers *TheLinuxExperiment* gesponsert und dadurch ein signifikantes Wachstum in unseren täglichen Nutzern beobachten können. Wir rechnen mit 5k Nutzern bis Ende des Jahres.

In unserem Podcast haben wir mit Ben Malisow, Autor des Buches *Exposed. How Revealing Your Data and Eliminating Privacy Increases Trust and Liberates Humanity*, eine spannende Diskussion über den Stellenwert von Privatsphäre geführt.

„*The Hated One*“, ein recht bekannter Youtuber in der Privacy Szene, war ebenfalls Gast bei unserem Podcast. Wir freuen uns über die wachsende Begeisterung unserer NutzerInnen. Diese Begeisterung spüren wir besonders, wenn wir die Supportanfragen lesen. Es kommen regelmäßig Nachrichten von Privatsphäre Enthusiasten, die anbieten, unsere Produkte und unsere Website auf eine andere Sprache zu übersetzen und uns somit zu unterstützen.

Wir haben beobachten können, dass Youtube-Sponsorings ein recht effektives Kommunikationsmittel sind und wir über diesen Kanal unsere Kernzielgruppe gut erreichen bzw. ansprechen können.

Die Mitgliederzahl von Safings Subreddit ist auf 520 angetiegen und auf Twitter sind es etwa 530. Seit dem Zwischenbericht hat sich die Anzahl der Sterne auf GitHub mehr als verdoppelt. Der Portmaster Channel hat nun über 1k Sterne.

3.3 Arbeitspaket 3 – Portmaster Prüfung SSL/TLS Zertifikate

Ist der größte Netzwerkstandard zur Verschlüsselung von Netzwerkverkehr. Der Portmaster soll die Fähigkeit erhalten, alle SSL/TLS Verbindungen genau zu überprüfen. Neben der korrekten Verwendung von Verschlüsselungen wird dabei die gesamte Zertifikatskette auf Gültigkeit geprüft. Diese Zertifikate werden auch mit einer Datenbank von gestohlenen und zurückgezogenen Zertifikaten abgeglichen.

Die Verschlüsselung und Vertrauenswürdigkeit konnten wir in einem Proof of Concept bereits testen. Mit der Fertigstellung kann die Software nun die SSL/TLS Verschlüsselung von Verbindungen erkennen und analysieren. Dabei werden die Verschlüsselungsparameter sowie die Zertifikate auf Richtigkeit geprüft. Es ist wichtig anzumerken, dass die Verschlüsselung selbst nicht „aufgebrochen“ oder ausgehebelt wird – viele andere Hersteller haben hierbei bereits großen Schaden angerichtet. Im Zuge der Implementierung hat sich auch eine wichtige Limitation gezeigt: Mit der Einführung von TLS 1.3 werden mehr Daten des Verbindungsaufbaus verschlüsselt. Dadurch können wir nicht mehr alle Daten über die Verbindung auslesen. Wie wir mit dieser Limitation umgehen, muss allerdings noch untersucht werden.

3.4 Arbeitspaket 4 – SPN Routenoptimierung

In diesem Arbeitspaket kam es zu einer Änderung. Wir haben ursprünglich geplant bis Mai damit fertig zu sein, jedoch war einer unserer Entwickler von November bis April in Karenz. Somit mussten alle Teammitglieder Aufgabenbereiche übernehmen, die zu einer neuen Evaluierung mancher Prioritäten führte. Daher haben wir die Routenoptimierung zeitlich verschoben.

In der zweiten Hälfte des Projektes wurden alle Aufgaben und Arbeiten wieder aufgenommen und fertiggestellt.

Letztes Jahr haben wir eine Karte des Internets erstellt und in diesem Projekt haben wir die softwareinterne Repräsentation dieser überholt und mit mehr Daten ausgestattet. Durch neue Schnittstellen ist eine tiefere Integration der Karte mit dem Routing-Algorithmus möglich. Dadurch können viel präziser und effizienter Routen berechnet werden. Mit den zusätzlichen Daten musste auch die Routenfindung überarbeitet werden, um die Geschwindigkeit und Zuverlässigkeit des Algorithmus zu gewährleisten.

Arbeitspaket 5 – SPN Ausfallsicherheit

In diesem Arbeitspaket lag der Fokus auf der Ausfallsicherheit des SPN. Es soll möglich sein, unterbrochene Verbindungen wieder aufzunehmen, indem man sich der mobilen Daten, der LAN-Verbindung oder eines WLANs bedient und diese Möglichkeiten der Verbindungen miteinander kombiniert.

Im Rahmen der notwendigen Überarbeitung des SPN Netzwerkstacks und der Stabilitätsenerweiterung wurde die essenzielle Flusskontrolle erweitert und verbessert. Die Flusskontrolle erfüllt nun alle Voraussetzungen, damit Verbindungen wieder aufgenommen werden können. Der letzte Schritt ist, dass der Zustand zwischengespeichert und auf eine neue Netzwerkverbindung übertragbar gemacht wird. Wenn das funktioniert, kann bei Verlust der Internetanbindung die Verbindung zum SPN inklusive der darüber gelegenen Datenströmen wieder hergestellt werden und damit eine unterbrechungsfreie Verbindung ins Internet ermöglicht werden.

3.5 Arbeitspaket 6 – Projektende

Dieses Arbeitspaket beschreibt den Abschluss der netidee Förderung. Wir sind mit allen Aufgaben und Zielen bis Ende des Projektzeitraums wie geplant fertig geworden. Es gab in der ersten Hälfte zeitliche Verzögerungen, die jedoch in der zweiten Hälfte des Projektes eingearbeitet wurden. Eine besondere Herausforderung waren die Änderungen im Personalbereich, die die Umverteilung der Arbeitszeiten und dadurch auch der Prioritäten und Aufgaben zur Folge hatten.

4 Umsetzung Förderauflagen

Es gibt keine vertraglich geregelten speziellen Förderauflagen.

5 Liste Projektergebnisse

1	Projektzwischenbericht	CC-BY-SA-4.0	https://www.netidee.at/safing-0
2	Projektendbericht	CC-BY-SA-4.0	https://www.netidee.at/safing-0
3	EntwicklerInnen-DOKUMENTATION	CC-BY-SA-4.0	https://www.netidee.at/safing-0

4	AnwenderInnen-DOKUMENTATION	CC-BY-SA-4.0	https://www.netidee.at/safing-0
5	Veröffentlichungsfähiger Einseiter	CC-BY-SA-4.0	https://www.netidee.at/safing-0
6	Dokumentation Externkommunikation	CC-BY-SA-4.0	https://www.netidee.at/safing-0
7	Portmaster – Prüfung SSL/TLS Zertifikate Der Portmaster soll die Fähigkeit erhalten, alle SSL/TLS Verbindungen genau zu überprüfen. Neben der korrekten Verwendung von Verschlüsselung wird dabei die gesamte Zertifikatskette auf Gültigkeit geprüft.	AGPL 3.0	https://github.com/safing/portmaster
8	SPN – Routenoptimierung Es ist möglich, dass Verbindungen trotz Ausfällen der Internetanbindung wieder aufgenommen werden können. Diese Technologie ermöglicht, dass eine Verbindung mehrere Pfade durch das Internet zugleich nimmt. Das erhöht die Geschwindigkeit und Stabilität. In dieser Form gibt es diese Möglichkeit nirgends sonst.	AGPL 3.0	https://github.com/safing/spn
9	Bericht: Validierung	CC-BY-SA-4.0	https://www.netidee.at/safing-0

6 Verwertung der Projektergebnisse in der Praxis

Der Portmaster ist bereits so weit entwickelt, dass er bald schon als Beta-Software eingestuft werden kann und die Alpha-Phase abschließt. Die stetig ansteigende Zahl an täglichen Nutzern ist ein gutes Indiz dafür, dass der Portmaster wirklich verwendet wird und den Erwartungen entspricht (und diese hoffentlich übertrifft). In Zukunft ist geplant, dass alle zwei Wochen neue Updates veröffentlicht werden.

Das SPN ist als Modul im Portmaster integriert, kann nun aktiviert und verwendet werden. Es wird momentan viel getestet und stabilisiert. Die ersten Kunden haben bereits Zugang zum Netzwerk und berichten ihre Erfahrungen und melden Probleme, die auftauchen. Wir verwenden das Feedback als Grundlage für Verbesserungsansätze.

7 Öffentlichkeitsarbeit/ Vernetzung

Im Frühjahr hatten wir eine virtuelle Firmenbesichtigung, bei welcher der Wirtschaftslandesrat Jochen Danninger zu Gast war. Es folgten Artikel in der NÖN und im Kurier über uns und unsere Projekte.

Wir haben immer öfter Gäste auf unserem Podcast und sponsern regelmäßig Videos auf YouTube. In der ersten Aprilwoche waren wir auf Puls 4 bei 2 Minuten 2Mio zu sehen. Nicht nur hat das unsere Nutzerzahl steigen lassen, sondern es wurden auch 2 Artikel veröffentlicht. Einer war vom Brutkasten, der andere von „Treding Topics“

Im Juli hatten wir ein weiteres Privatsphäre Start-Up namens Apocrat als Gast bei uns im Büro. Sie bieten eine AI-basierte Plug-and-Play-„Firewall“ für IoT-Geräte an. Bei diesem Treffen gab es bereits spannende Diskussionen und Gespräche, in denen wir über eine eventuelle Zusammenarbeit in der Zukunft Ideen sammeln konnten.

Das Team von *Techlore* ist in der Privacy-Szene auf YouTube bekannt dafür, dass sie ehrliche Reviews geben. Sie haben den Portmaster das SPN und Safing als Unternehmen unter die Lupe genommen. Von Anfang an wussten wir, dass wir keinen Einfluss auf das Ergebnis haben würden. Ihr Review ist jedoch sehr positiv ausgefallen und wir haben das Video auf unserer Homepage verlinkt.

Es sind weitere Vernetzungsarbeiten geplant. Wir haben viele Ideen, allerdings sind wir noch in der Konzeptionsphase und müssen im nächsten Schritt herausfinden, in welcher Reihenfolge wir diese Arbeiten umsetzen wollen.

8 Eigene Projektwebsite

Dies ist unsere Homepage: <https://safing.io/>

9 Geplante Aktivitäten nach netidee-Projektende

Unser Hauptfokus liegt auf dem Ausbau des SPNs, vor allem auf der Skalierung und der Stabilisierung. Wir möchten als Unternehmen weiterhin wachsen, hauptsächlich im Personalbereich, damit wir mehr Kapazitäten haben, um auch auf anderen Plattformen unser Produkt und unsere Dienstleistung anbieten zu können. Wir haben in erster Linie die Plattformen Mobile (Android) und MacOS im Visier.

Wie in Punkt 7 schon erwähnt, sind auch Zusammenarbeiten mit anderen Unternehmen in der Konzeptionsphase. In welcher zeitlichen Abfolge diese ablaufen werden, hängt stark davon ab wieviel zusätzliche Ressourcen wird zur Verfügung haben werden.

10 Anregungen für Weiterentwicklungen durch Dritte

Sobald das SPN eine bestimmte Stabilität erreicht, möchten wir uns den Community Nodes widmen. Diese waren von Anfang an Teil des Konzeptes des SPNs, um noch mehr Privatsphäre bieten zu können.

Wir sehen großes Potential in Kooperationen mit anderen Unternehmen, die Privatsphäre als Fokus haben, aber genauso in Projekten, die sich mit dem Bereich Smart City auseinandersetzen.

Als Weiterentwicklungsmöglichkeit für Dritte empfehlen wir im Bereich des Kinderschutzes zu entwickeln. Wir können uns zwar auch vorstellen, in diese Richtung Projekte anzufangen, jedoch liegen unsere Prioritäten momentan woanders.