Richtlinie zum „Software-Sprint“

OpenVPN-Client – Robuster OpenVPN-Client mit geringem Ressourcenverbrauch

DLR PT-SW Berlin
Eing.am:
16. Sep. 2019
Eingangsnr.: 5216

Schlussbericht

Zuwendungsempfänger:

Hannes Mehnert

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S44 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

OpenVPN-Client ist eine auf dem Unikernel MirageOS aufsetzende, zuverlässige und einfach zu bedienende OpenVPN-Implementierung, die z.B. Zusammenarbeit von unterschiedlichen Standorten aus mit Hilfe einer kryptographisch sicheren Verbindung.

Die Motivation war eine Alternative zu den existierenden OpenVPN-Implementierungen, die in der fehlerträchtigen Programmiersprache C geschrieben sind, zu entwickeln. Auch das Schreiben einer Spezifikation des OpenVPN-Protokolls war Motivation.

Die Meilensteine waren wie folgt:

- Nach 1,5 Monaten: eine Spezifikation des OpenVPN Protokolls, die wir während der Projektlaufzeit noch detaillierter ausführen werden.

- Nach 3 Monaten ist die Unterstützung von „tun“ Interfaces in MirageOS

- Nach 4 Monaten eine erste OpenVPN Bibliothek inklusive Tests und einen Konfigurations-Dateiformat Parser

- Nach 5 Monaten ist ein OpenVPN Unikernel fertiggestellt

- In dem verbleibenden Monat: Interoperabilitäts-Tests und weitere Dokumentation

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

Die Zielgruppe sind Aktivisten, Journalisten, und Open Source Nutzer. Wir wollen ein Drop-in replacement für OpenVPN-Client entwickeln - und das Konfigurationsformat übernehmen - um einen leichten Umstieg zu ermöglichen. Im Rahmen der Förderung wurde auch ein OpenVPN-Server entwickelt.

Der OpenVPN-Client bietet einen wichtigen Beitrag zu dem Themenfeld Sicherheit. Der Server ist zusätzlich ein wichtiger Beitrag in den Themenfeldern Sicherheit und Infrastruktur, da er unabhängige und robuste Infrastruktur für alle zum selbst Betreiben verfügbar macht

Ausführliche Darstellung der Ergebnisse

Im Projektverlauf wurden die Programmier-meilensteine größtenteils erreicht, mit einiger Verzögerung, die Dokumentation und Spezifikation ist leider nicht in gewünschtem Ausmaß fertig geworden.

- Nach 3,5 Monaten war ein erster OpenVPN-Client, der mit einem bestehenden OpenVPN-Server eine Verbindung aufbauen konnte, entwickelt worden. Dieses beinhaltet den Meilenstein „OpenVPN Bibliothek und Konfigurations-Dateiformat Parser“

- Ein OpenVPN-Client, der ein „tun“ Interface verwendet, war nach 4 Monaten fertiggestellt. Dies ist keine direkte Integration in MirageOS, hat aber für das OpenVPN-Client Projekt den gleichen Effekt.

- Nach 4,5 Monaten war ein OpenVPN Unikernel, der den Tunnel an andere virtuelle Maschinen zur Verfügung stellt, entwickelt

Ohne die Förderung hätten wir das Projekt nicht finanziert bekommen. Die wöchentlichen Standup-Meetings im Chat waren eine gute Möglichkeit, um mit den anderen Gruppen in Kontakt zu bleiben.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Der Nutzen der Zielgruppe ist ein OpenVPN-Client mit geringem Speicherverbrauch. Dies ist zB für Benutzer von QubesOS sehr interessant, wo bereits an einer Integration gearbeitet wird. Die Entwicklung der OpenVPN-Bibliothek (statt nur einer Applikation) führte schon zu der Wiederverwendung der Bausteine als Server-Applikation! Nur durch die Offenlegung des Source codes können andere unabhängig der Software vertrauen, dass sie genau das tut, was sie soll, und nichts anderes. Durch die Entwicklung habe ich mehr über das OpenVPN-Protokoll gelernt, ein weit verbreitetes VPN Protokoll, und wie sowas implementiert wird.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Das Hinzufügen von Timeouts zum initialen Prototypen, um Protokollkonform zu sein, führte zu der Erkenntniss, dass viel Code nochmals umgeschrieben werden musste. Bei der Entwicklung der Auswahl des Server-Endpunktes führte wieder zu der Erkenntniss, dass hier viel Code umgeschrieben werden musste, und die Interaktion zwischen Unikernel und Bibliothek nochmals überdacht werden musste.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Eine Projektwebseite befindet sich noch im Aufbau. Die OpenVPN-Bibliothek wird in das OCaml package Archiv released werden, sobald sie in einem guten Zustand ist.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Das Analysieren (Reverse-Engineering) des Protokolls war aufwendiger als erwartet. Das Formulieren der Spezifikation hat den Zeitrahmen gesprengt, und ist somit nicht fertig geworden – aber in der Freizeit nach der Förderung wird daran weiter gearbeitet.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Der OpenVPN-Client Unikernel verwendet zwei virtuelle Netzwerkkarten, die eine ist mit dem Internet verbunden, wo der Tunnel zum OpenVPN-Server aufgebaut wird. Die andere ist mit den virtuellen Maschinen verbunden, deren Datenverbindungen über den Tunnel rausgeschickt werden. Die Möglichkeit, mehrere Netzwerkkarten mit MirageOS (und moderne Hypervisor wie KVM. BHyve oder seccomp) zu verwenden, wurde erst während des OpenVPN-Projektes von einem externen Entwickler in der Slowakei fertiggestellt. Diese Projekte ergänzen sich, und wir haben uns viel über die Anforderung, das Design, und der konkreten Implementierung von mehreren Netzwerkkarten ausgetauscht. Diese Erweiterung von MirageOS wird in den nächsten Wochen released, sowie das OpenVPN-Projekt als ersten Nutzer.