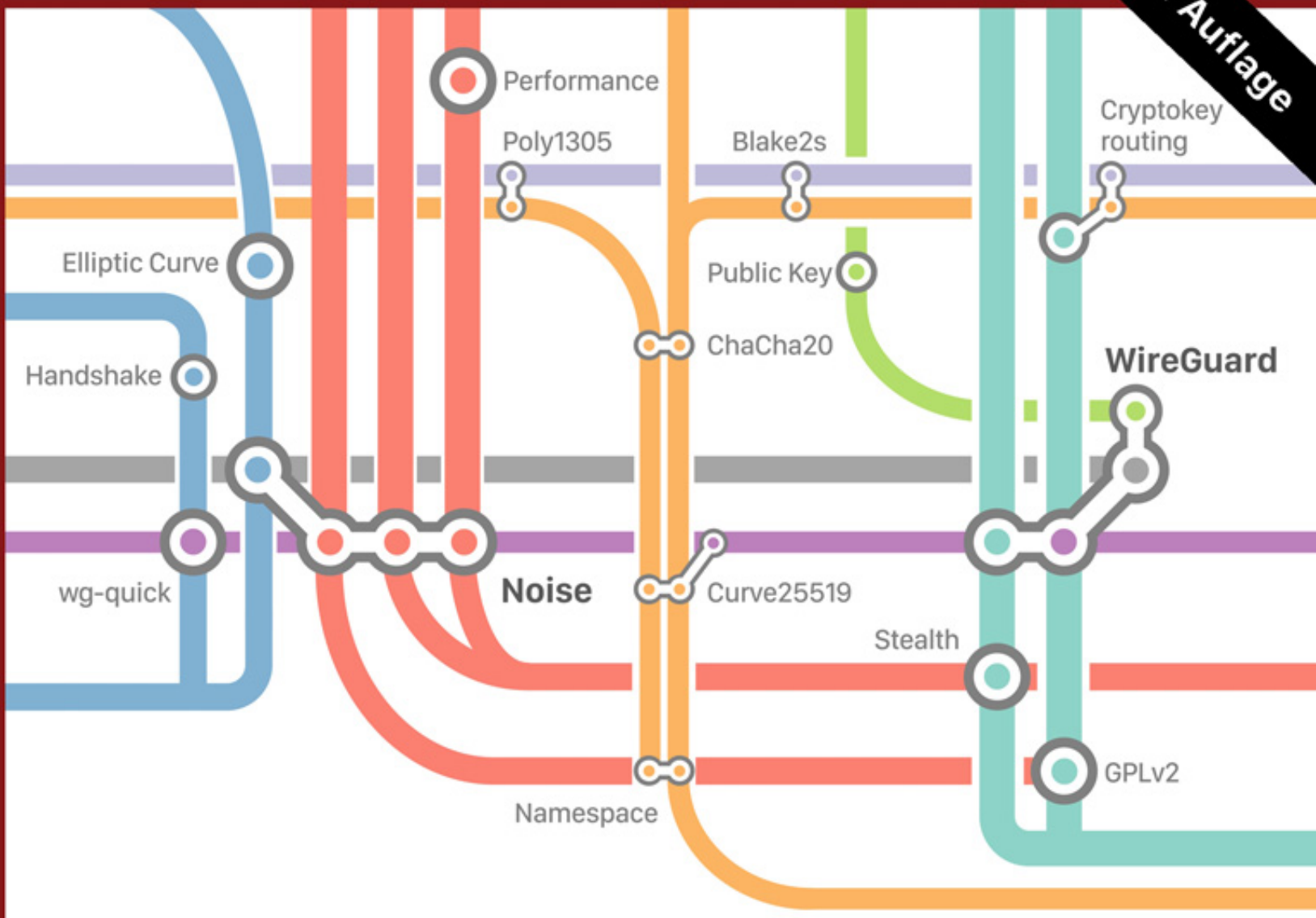
2. Auflage



WireGuard im Einsatz

Markus Stubbig

Aktualisierte Auflage

Inhaltsverzeichnis

Vorwort

Es ist so weit: WireGuard zieht in den Linux-Kernel ein! Damit ist WireGuard kein exotisches Modul mehr, was der Paketmanager einer Distribution nachinstallieren muss. Allerdings hat es bis Kernelversion 5.6 gedauert, die im März 2020 erschien. Damit hat WireGuard eine ungewöhnlich lange Entwicklungszeit und eine noch längere Testphase hinter sich. Für eine Security-Software ist das positiv, denn so bleibt genug Zeit, um peinliche Bugs und kritische Löcher zu stopfen.

Der Sprung in den Linux-Kernel dürfte die Popularität von WireGuard weiter stärken. Damit ist nicht nur die Fangemeinde gemeint, sondern auch kommerzielle Anbieter von Firewalls und VPN-Diensten. Diese haben jetzt eine Entscheidungsgrundlage und können darauf vertrauen, dass WireGuard nicht morgen von der Bildfläche verschwindet.

WireGuard ist leichter einzurichten als IPsec oder OpenVPN. Daher geht es in diesem Buch nicht ausschließlich um die Einrichtung, sondern auch um den Einsatz von WireGuard auf anderen Betriebssystemen, das Zusammenspiel mit weiteren Netzwerkfeatures, Tipps und einen kleinen Exkurs in die Kryptografie.

Viel Spaß beim Ausprobieren, Staunen und Fluchen.

Vorwort der ersten Auflage

VPN-Tunnel sind überall. Sie verlaufen zwischen Firmenstandorten, ermöglichen Fernzugriff auf den heimischen DSL-Router und die meisten Laptops haben einen VPN-Client vorinstalliert.

Die Grundlagen von VPN sind nicht neu: Der Klassiker IPsec entstand vor mehr als zwei Jahrzehnten und beschützt seitdem die Kommunikation seiner Teilnehmer.

Andere kluge Köpfe und Hersteller haben es sich nicht nehmen lassen und ihre eigene VPN-Technik erschaffen: Die Palette reicht von PPTP, L2TP, GRE, OpenVPN bis zu vielen proprietären VPN-Anwendungen, die sich in TLS hüllen. Im weiteren Sinne lässt sich auch SSH, VXLAN und sogar DNS als Tunnel betreiben. Die Liste der Implementierungen ist lang.

Warum gibt es zusätzlich WireGuard und auch noch ein Buch darüber?

WireGuard hat eigentlich dieselben Ziele wie OpenVPN: Einfach und offen, wobei OpenVPN diese Ziele im Laufe der Jahre und Releases scheinbar aus den Augen verloren hat.

WireGuard deckt die meisten VPN-Szenarien ab und ist erstaunlich schnell bei der Einwahl. Dagegen gibt es Einsatzbereiche, die WireGuard schlecht oder gar nicht beherrscht.

Das Buch über WireGuard möchte dem Leser den Einstieg erleichtern, die Unterschiede zu anderen VPN-Techniken verdeutlichen und praktisches Wissen vermitteln. Die Kapitel fokussieren auf den täglichen Einsatz und erklären nur oberflächlich die verwendete Kryptografie. Denn

WireGuard ist ein zuverlässiger Begleiter, auch wenn elliptische Kurven und ChaCha20 Fremdwörter sind.

Zuletzt möchte das Buch ein vollständiges Bild liefern, was WireGuard kann und in welchen Szenarien es die ideale Software ist, um ein Netz bestmöglich zu sichern.

Ressourcen

https://www.wireguard.com
Die Homepage von WireGuard liefert einen guten Einstieg ins Thema und verlinkt zur Dokumentation, zum Download-Bereich und informiert über den Entwicklungsstatus.

https://git.zx2c4.com/WireGuard
Die Entwickler hosten den Programmcode als öffentliches Git-Repository, wo jeder Einblick in den Fortschritt hat und sich an den Quellen bedienen kann. Daneben gibt es viele Implementierungen und Erweiterungen.

http://www.noiseprotocol.org
Das *Noise Protocol Framework* liefert den Programmcode für die Kryptofunktionen und eine hervorragende Dokumentation zu den elliptischen Kurven.

https://github.com/wireguard-im-einsatz
Auf GibtHub befindet sich zusätzliches Material zum Buch und das aktuelle Korrekturverzeichnis.

Schriftkonventionen

`Nichtproportionalschrift` zeigt die erzeugte Ausgabe eines Kommandos.

`Schreibmaschinenschrift` wird für Konfigurationen und Schlüsselwörter benutzt, die buchstabengetreu eingetippt werden müssen.

`Nichtproportionalschrift Fett` zeigt Befehle, die eine Ausgabe erwarten.

`Hervorhebungen` weisen auf besondere Wörter oder Zeilen innerhalb von Kommandos oder Bildschirmausgaben hin.

```
ein-sehr-langer-kommando-aufruf --mit --sehr \ --vielen
"Optionen"
```

Kommandos mit vielen Argumenten können länger als eine Zeile sein. Für die bessere Übersicht werden diese Kommandos mehrzeilig abgedruckt und um zwei Zeichen eingerückt. Am Ende jeder Zeile steht der Backslash als Hinweis darauf, dass es in der nächsten Zeile weitergeht.

Rechtliches

Warennamen und Bezeichnungen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Es ist davon auszugehen, dass viele der Warennamen gleichzeitig eingetragene Warenzeichen sind oder als solche zu betrachten sind.

Bei der Zusammenstellung von Texten, Bildern und Daten wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Der Autor lehnt daher jede juristische Verantwortung oder Haftung ab. Für Verbesserungsvorschläge und Hinweise auf Fehler ist der Verfasser (E-Mail: wireguard.buch@gmail.com) dankbar.

Kapitel 1

Einleitung

WireGuard bezeichnet sich selber als eine schnelle, moderne und sichere VPN-Software. Im Grundprinzip ermöglicht WireGuard die verschlüsselte Kommunikation zwischen zwei Endgeräten. Damit erreicht WireGuard – genau wie jede andere VPN-Software – den gesicherten Datenaustausch über unsichere Transportnetze.

WireGuard möchte vielseitig und einfach sein. Der Hersteller bietet seine Software vorkompiliert für eine Reihe von Betriebssystemen an. Die Einrichtung verläuft unkompliziert, sodass ein VPN-Tunnel bereits nach wenigen Minuten einsatzbereit ist.

WireGuard setzt auf moderne Kryptoalgorithmen. Die Algorithmen wurden so gewählt, dass sie eine exzellente Mischung aus Sicherheit und Leistung ergeben, die selbst ohne Hardwarebeschleunigung fantastische Durchsatzraten beschert.

Und das Beste ist: WireGuard ist kostenlos nutzbar, quelloffen und wird unter der freien Lizenz GPL veröffentlicht. Damit steht der Verbreitung von WireGuard nichts mehr im Weg.

Was ist VPN?

Wenn zwei entfernte Netze miteinander kommunizieren wollen, dann läuft das klassischerweise über eine eigene Leitung bzw. über ein privates Netzwerk. Ob Standleitung