Contribution ID: **74** Type: **not specified**

WireGuard: Next-Generation Secure Kernel Network Tunnel

Thursday, 15 November 2018 09:45 (45 minutes)

WireGuard [1] [2] is a new network tunneling mechanism written for Linux, which, after three years of development, is nearly ready for upstream. It uses a formally proven cryptographic protocol, custom tailored for the Linux kernel, and has already seen very widespread deployment, in everything from smart phones to massive data center clusters. WireGuard uses a novel timer mechanism to hide state from userspace, and in general presents userspace with a “stateless” and “declarative” system of establishing secure tunnels. The codebase is also remarkably small and has been written with a number of defense in depth techniques. Integration into the larger Linux ecosystem is advancing at a health rate, with recent patches for systemd and NetworkManager merged. There is also ongoing work into combining WireGuard with automatic configuration and mesh routing daemons on Linux. This talk will focus on a wide variety of WireGuard’s innards and tentacles onto other projects. The presentation will walk through WireGuard’s integration into the netdev subsystem, its unique use of network namespaces, why kernel space is necessary is necessary, the various hurdles that have gone into designing a cryptographic protocol specifically with kernel constraints in mind. It will also examine a practical approach to formal verification, suitable for kernel engineers and not just academics, and connect the ideas of that with our extensive continuous integration testing framework across multiple kernel architectures and versions. As if that was not already enough, we will also take a close look at the interesting performance aspects of doing high throughput CPU-bound computations in kernel space while still keeping latency to a minimum. On the topic of smartphones, the talk will examine power efficiency techniques of both the implementation and of the protocol design, our experience in integrating this into Android kernels, and the relationship between cryptographic secrets and smartphones suspend cycles. Finally we will look carefully at the WireGuard userspace API and its usage in various daemons and managers. In short, this presentation will examine the networking and cryptography design, the kernel engineering, and the userspace integration considerations of WireGuard.

[1] https://www.wireguard.com
[2] https://www.wireguard.com/papers/wireguard.pdf

I agree to abide by the anti-harassment policy

Yes

Primary author: DONENFELD, Jason

Presenter: DONENFELD, Jason

Session Classification: LPC Main Track

Track Classification: Refereed talk