Wireguard

For Fun and Networking

Andrew Denner
Saint Louis Linux Users Group

October 22, 2020

About our Presenter

Andrew Denner

- http://denner.co
- twitter: @adenner
- Senior Software Developer
- Linux Tinkerer


Slides at http://denner.co

Hardware is hard...


It fails at the worst time...

It’s replacement also failed. (High quality woot)


Rasbery Pi 4 to the rescue...


The show must go on


Networking is
important

Especially in 2020

What are my options?

PPTP

OpenVPN

IPSec


Wireguard

PPTP

- Stands for ”Point-to-Point Tunneling Protocol”
- Introduced in 1995 and was improvement on PPP
- Initially Windows implementation
- Basic TCP based tunnel on port 1723
- Most compatible and simple but not very secure
  - NSA likely cracked PPTP traffic
  - MS-CHAP V1 & 2 are cracked (authentication)
  - MPPE uses RC4 Stream Cipher

IPSec IKEv2

- Part of IPSec Protocol RFC7296
- Uses fixed ports so easier to block
- Can use large Suite of crypto algorithms (3DES, AES, Blowfish, Camellia et.al.)
- No known major vulnerabilities but rumors of NSA exploit
- in theory faster than OpenVpn
- implementation OpenSwan

OpenVPN

- Developed by OpenVPN technologies but not RFC Standard
- Uses OpenSSL library for encryption & supports 3DES AES RC5 blowfish et.al. Using SSL/TLS for Key exchange
- No known major vulnerabilities
- Easy to use and configurable can run any port and UDP TCP
- Not included in any OS but easy to install

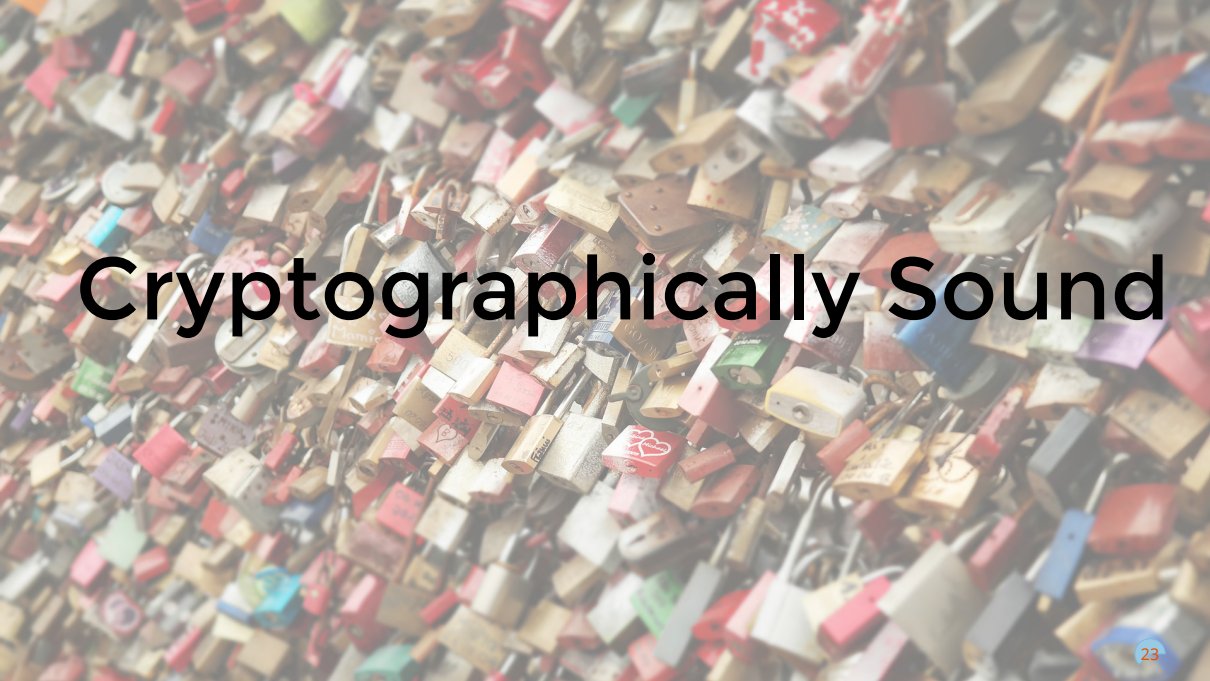
Wireguard

- Very fast with low overhead using Standardized sauce
- Standardized Encryption
  - ChaCha20 for symmetric encryption (RFC7539)
  - Curve25519 for ECDH
  - Blake2 hashing (RFC 7693)
  - SipHash24 hashtable keys
  - HKDF key derivation (RFC5869)
  - UDP based handshake & key exchange with perfect forward secrecy protects against impersonation and replay attacks

Wireguard (cont.)

- No known major vulnerabilities but is new has been 3rd party audited
- Uses UDP and configurable to any port but may suffer from traffic shaping more easily
- In tree support in Kernel 5.6 but other OS require installation of Client App.

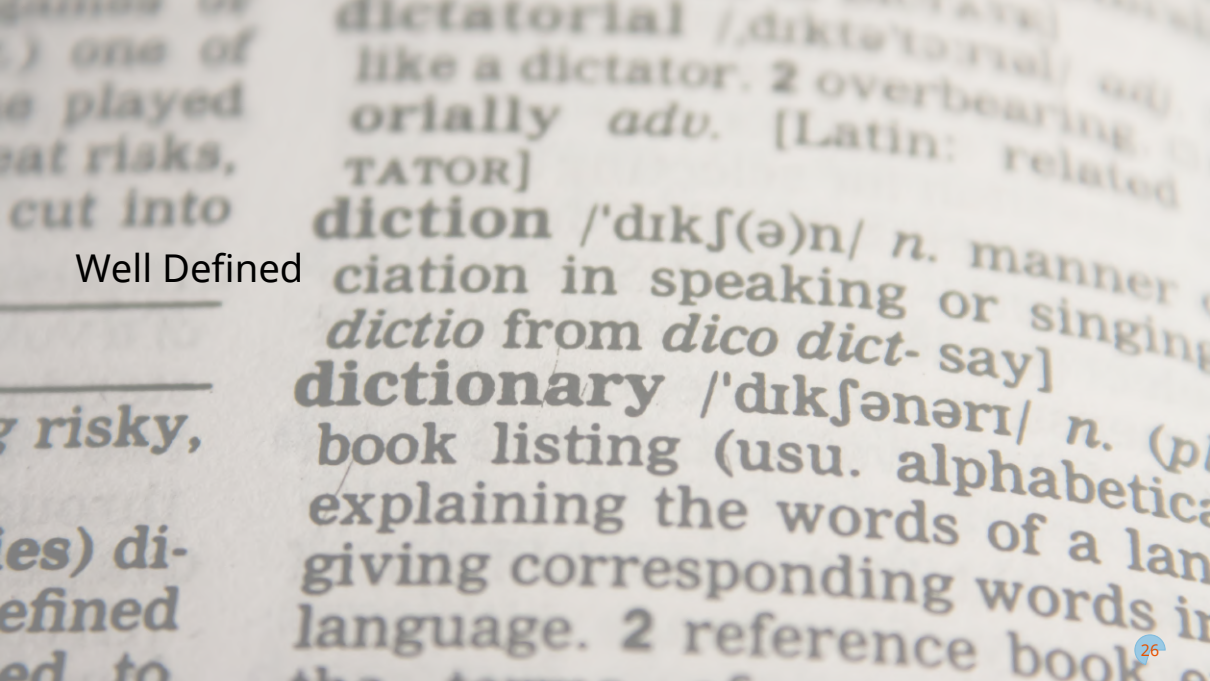
Simple, easy to use



Cryptographically Sound

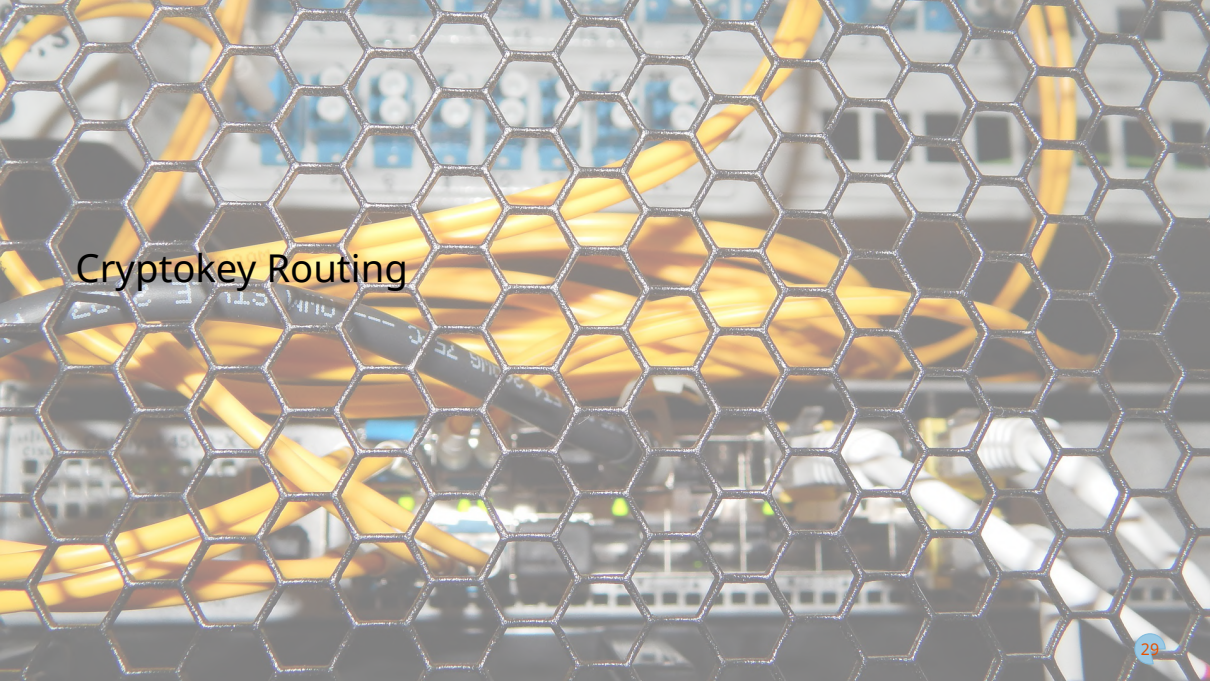

Minimal Attack Surface


High Performance


Well Defined
dictatorial
like a dictator. 2 overbearing
orially adv. [Latin: related
TATOR]
diction /'dɪkʃ(ə)n/ n. manner
ciation in speaking or singing
dictio from dico dict- say]
dictionary /'dɪkʃənərɪ/ n.
book listing (usu. alphabetica
explaining the words of a lan
giving corresponding words in
language. 2 reference book
risky,
es) di-
efined

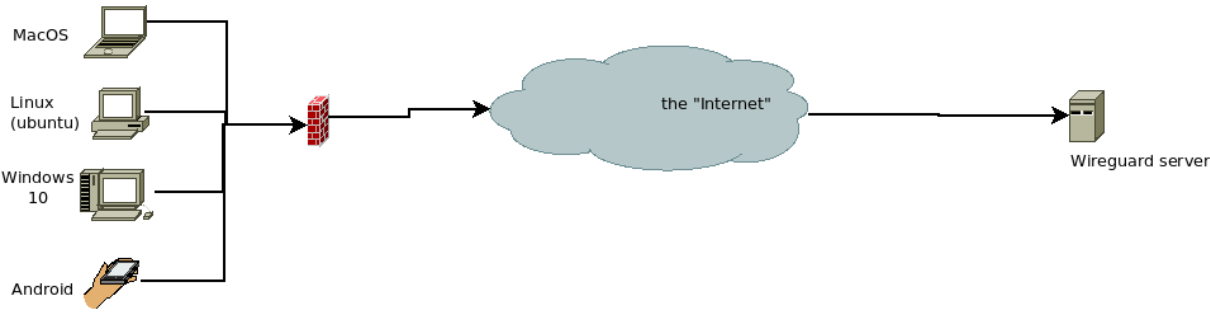
They even have a 20 page TEXwhitepaper...

How it works


Cryptokey Routing

Built in Roaming

Ready for containers


MacOS
Linux
(ubuntu)
Windows
10
Android
the "Internet"
Wireguard server

Demo 0: Install Wireguard on Rasbery Pi

Install Wireguard on Rasbery Pi (cont)

- see `https://wireguard.how/server/raspbian/`

Demo 1: Install Wireguard on Ubuntu 20.04

Demo 2: Install Wireguard on MacOS

Demo 3: Install Wireguard on Android

References

- Comparison of VPN Protocols https://www.ivpn.net/pptp-vs-ipsec-ikev2-vs-openvpn-vs-wireguard
- NSA Crack of PPTP: https://hacker10.com/internet-anonymity/secret-documents-show-the-nsa-is-spying-on-vpn-users/
- NSA IPSEC: https://www.forbes.com/sites/thomasbrewster/2016/08/19/cisco-nsa-vpn-hack-shadow-brokers-leak/
- Set Up Wireguard https://www.linode.com/docs/networking/vpn/set-up-wireguard-vpn-on-ubuntu/