

# 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

A red fire extinguisher is the central focus, resting on a horizontal metal bar of a stand. The background is a blurred workshop with various tools and machinery. The lighting is somewhat dim, creating a moody atmosphere. The fire extinguisher has a red body and a white nozzle with a red handle.

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...



An empty classroom with rows of wooden chairs. In the background, there is a blackboard, a wooden podium, and a door. The text "The show must go on" is overlaid in the center.

**The show must go on**



**Networking is  
important**



Especially in 2020

# What are my options?





**PPTP**



**OpenVPN**

A knight in full plate armor, including a helmet with a visor and chainmail coif. The knight wears a red surcoat over a black tunic. The shield is white with a red horizontal stripe. The knight holds a spear in the right hand and a sword in the left. The background is a stone wall.

**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.)

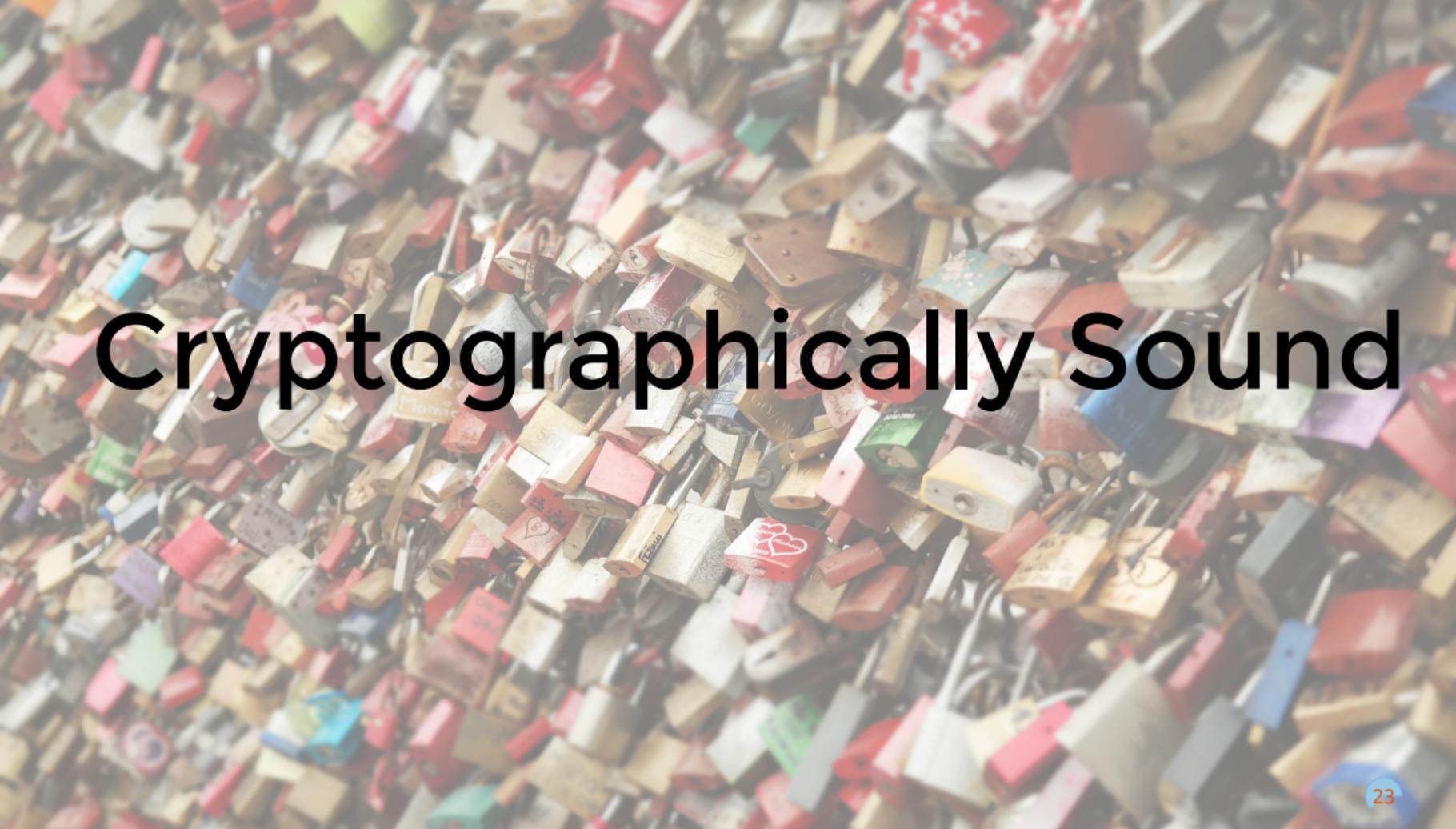
- No known major vulnerabilities but is new has been 3rd party audited
- Uses UDP and configurable to any port but may suffer from traffic shaping more easily
- In tree support in Kernel 5.6 but other OS require installation of Client App.

T<sup>5</sup> A<sup>2</sup> K<sup>2</sup> E<sup>1</sup>

Simple, easy to use

I<sup>2</sup> T<sup>5</sup>

E<sup>1</sup> A<sup>2</sup> S<sup>7</sup> Y<sup>9</sup>



# Cryptographically Sound



## Minimal Attack Surface

A close-up photograph of a high-performance engine. The image shows a polished aluminum intake manifold with four large, curved headers. The headers are connected to the engine block with brass fittings. Several red spark plug boots are visible, attached to the engine. The overall appearance is clean and well-maintained, suggesting a high-performance or racing engine.

High Performance

Well Defined

dictatorial /ˌdɪktəˈtɔːriəl/ *adv.*  
like a dictator. 2 overbearing.  
orally *adv.* [Latin: related  
TATOR]

**diction** /ˈdɪkʃ(ə)n/ *n.* manner  
ciation in speaking or singing  
*dictio* from *dico dict-* say]

**dictionary** /ˈdɪkʃənəri/ *n.* (pl  
book listing (usu. alphabetical  
explaining the words of a lan  
giving corresponding words in  
language. 2 reference book

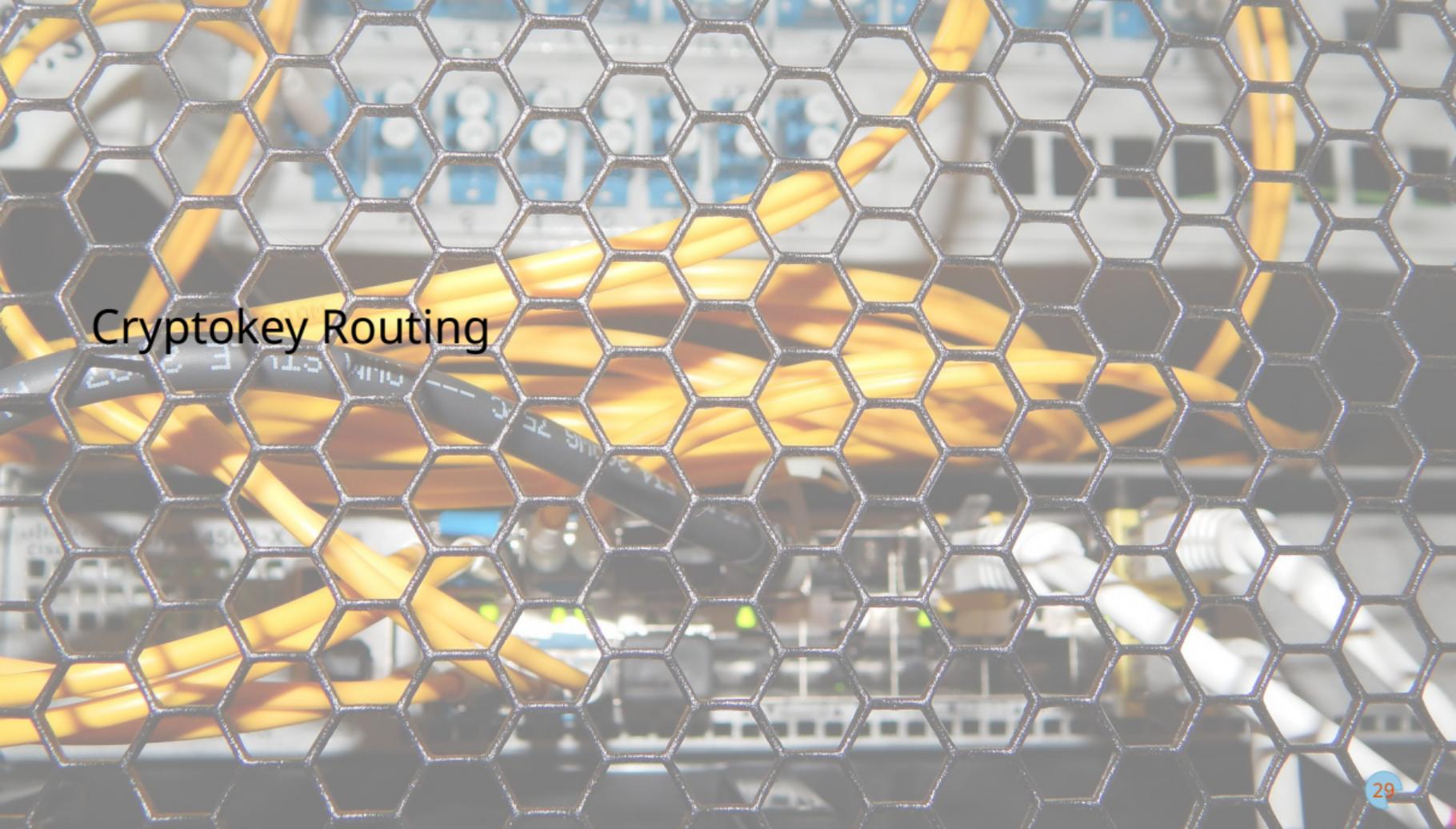
They even have a 20 page T<sub>E</sub>Xwhitepaper...



# How it works

WHO  
WHEN  
WHERE  
How  
?  
WHAT  
WHY



The background of the slide is a photograph of a server room. In the foreground, there is a silver metal mesh with a hexagonal pattern. Behind the mesh, several thick yellow cables are visible, some of which are plugged into server racks. The server racks are white and have various ports and lights. The overall scene is brightly lit, with some green indicator lights visible on the server racks.

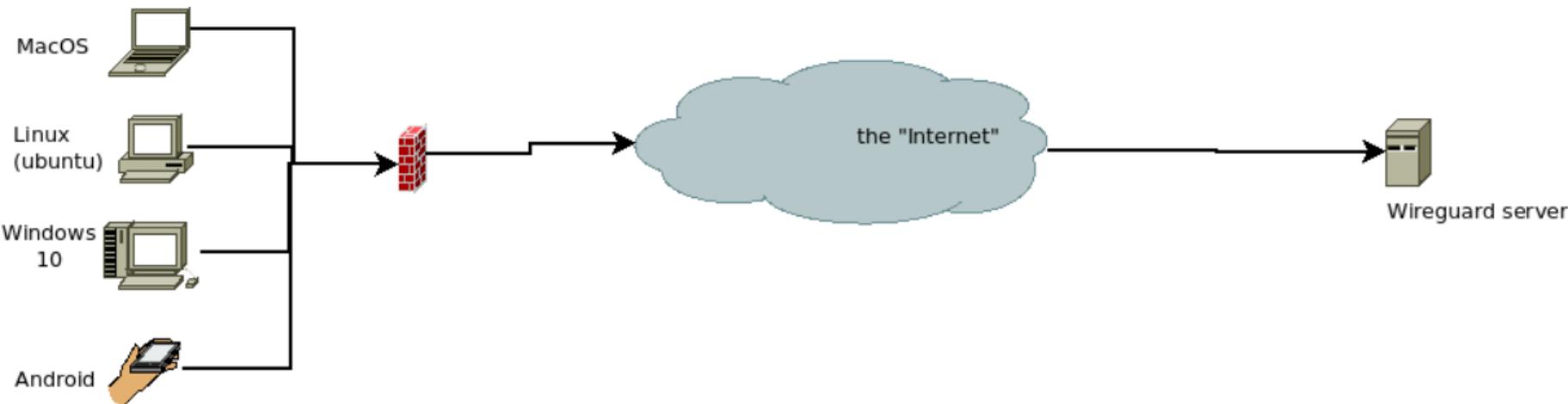
# Cryptokey Routing

# Built in Roaming



# Ready for containers





A top-down view of a wooden table with various items. In the center is a round pie on a yellow plate, with a hand reaching towards it. To the right is a white oval plate with several pastries, one with a red jam filling. In the top right is a pie with a red filling on a metal tray. In the bottom center is a silver teapot, a black mug, and a red mug. On the left is a white rectangular plate with a long, thin object (possibly a sandwich or roll) and a butter knife. A blue and white checkered cloth is partially visible on the left side of the table.

## Demo 0: Install Wireguard on Rasbery Pi

## Install Wireguard on Rasbery Pi (cont)

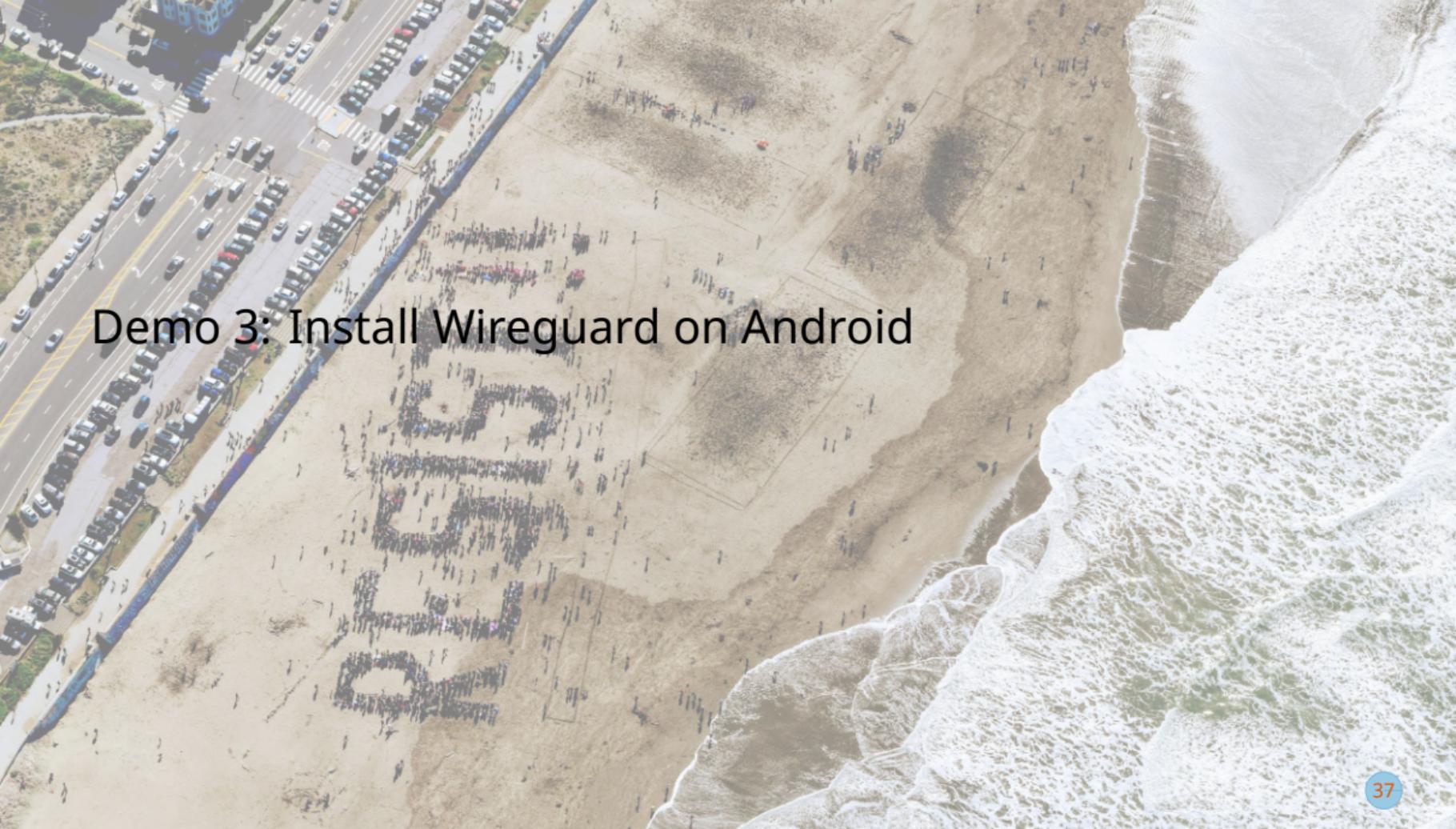
- see <https://wireguard.how/server/raspbian/>

A black and white photograph of a large, dense crowd of people, likely at a protest or demonstration. Many individuals are holding up their smartphones to take pictures or videos. Some people are holding up signs, though the text on them is mostly illegible. The crowd is diverse in age and appearance, and the overall atmosphere appears to be one of active participation and public expression.

## Demo 1: Install Wireguard on Ubuntu 20.04



## Demo 2: Install Wireguard on MacOS

An aerial photograph of a crowded beach. On the left, a multi-lane road is filled with cars, with a large parking lot adjacent to it. The beach itself is wide and sandy, with many people scattered across it. In the foreground, the ocean waves are breaking, creating white foam. The overall scene is busy and scenic.

## 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/>