Sysadministrivia

Linux, Lagers, and Late Nights

S3E16: "When a VPN is Not a VPN"

Posted 2018-10-08 03:59
Modified 2019-05-29 18:29
Comments 2

Navigation

Previous Episode	Next Episode
S3E15: "YUMmy"	S3E17: "China Dentata"

Log

Recorded (UTC)	Aired (UTC)	Editor
2018-09-27 02:37:45	2018-10-07 16:02:18	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`257dc37a64d263d0635e26975a47e6c196a3a67a61f9a92843cc20fc572efee7`	click	click
OGG	`35fee323616e999efcb2120b5c428d3c01652de9e0fb3ac03b80f6f642acc99d`	click	click

Quicklisten:

We mostly talk (argue) about WireGuard, the pseudo-VPN that maintainers are trying to get mainlined into the kernel.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- The first officially registered GDPR notice has been issued in the UK.
- The White House is considering an investigation (with the possibility of an antitrust lawsuit as a result) of Google and Facebook.
- A massive WordPress compromise campaign (better source) is causing installations to redirect to a tech support scam.
- Georgia (the US state, not the country) had its entirely-digital voting system criticized by a judge for not taking appropriate precautionary measures.
- A flaw was discovered in Bash's tab-completion.
- CentOS/RHEL and Debian are still susceptible to Mutagen Astronomy.

Notes

Starts at **19m2s**.

I was drinking Hell or High Watermelon. Paden was drinking Diet Dr. Pepper. Jthan was drinking Red Stripe.

- We review WireGuard!
  - Linus Torvalds, at least, thinks the code is clean.
  - If you're setting up a permanent, robust installation, you'll probably want to read the following:
    - The DO guide that Jthan followed
    - Arch's WireGuard guide
    - A quick primer
    - Using WireGuard with two NAT networks
    - Another NAT resource
  - I see a lot of comparison to OpenVPN ("The code is cleaner than OpenVPN", "It's easier to audit than OpenVPN", "It's easier to set up than OpenVPN", etc.)
    - OK, but WireGuard is **not** a VPN. OpenVPN is. WireGuard has roughly <= 10% of the functionality that OpenVPN does.
    - WireGuard is, more accurately, merely a **peer-to-peer tunnel**; it'd be MUCH more appropriate to compare it to (for instance) CJDNS or Lantern, both of which have existed for longer than WireGuard.
  - Jthan wonders when we'll see a full security audit.
  - Jthan asks "What are some example use cases that make this an ideal solution?"
    - I counter with "If you have to *come up* with ideal use cases… you shouldn't use it. You look for solutions to a problem, not problems for a solution."
  - I hate it still.
    - NAT traversal ugly and ungraceful, even for a dedicated "server/client" model, which it doesn't really have anyway…
    - I hate the decentralized/peer-based model.

    - There's no authority for access, no hierarchy.
    - I can't see a valid use case for it **except** just a couple of friends who want to play Starcraft I together with the same CD key or something (i.e. entirely flat casual end-user simulated LAN environment). A Heroku replacement or whatever.
    - It feels the exact same as CJDNS.
        - Except CJDNS does more.
    - There's no automatic address provisioning i.e. via DHCP (because it's a layer-3, not a layer-2, see this for good discussion on this), there's no way to automatically assign IP addresses or manage an address pool. Addressing conflicts ahoy, good luck debugging those with the exact type of people WireGuard is designed for (namely, newbies/people lacking the wherewithal to turn up a full, proper VPN solution).
    - it **will not work** in double-NATted environments (i.e. nested NAT, one NAT behind another) without port-forwarding at least one of them, even for clients only. (OpenVPN, for instance, handles this fine.)
        - This setup is not uncommon for VM labs and apartment Internet access in Eastern EU, for instance.

- Jthan found it MUCH easier than OpenVPN to set up (I didn't).
    - He thinks it'd be useful for bridging remote sites (but that's what a real VPN is for. ;)
- Paden did some speed testing and found that speeds were roughly the same, but had greater variance on WireGuard. The latency, however, had a huge hit (and this can, of course, vary depending on the location of your peer).
    - He also didn't like how bare the Arch package was; he felt that the /etc/wireguard directory (and perhaps some stock/default configs) should have been provided.
- It seemed worrying to me – since there's no CA/PKI structure, if you wipe/overwrite your key (and aren't using persisting configuration/keeping the keys in the configuration), all your peers will need to re-add your public key.

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(59m54s)**

Twitter has been caught leaking DMs via their API.

Errata

- For some reason, I always pronounce "spermatozoan" as "sperm-O-tah-zoh-an".
    - Which is wrong. :P
- WireGuard is, apparently, indeed now cross-platform.
- Linus is indeed Finnish, and you should probably check this out.
- The protégé for the Linux kernel is Gregory Kroah-Hartman. Dunno where I got Peter/Paul from.
- I mention Syncthing.
- A listener named Jon has let us know below in the comments that the BBC uses Wireguard for parts of their production process.
    - I continue my personal journal to try to find a valid use case for Wireguard that isn't satisfied by another existing technology. The BBC's use case doesn't require encryption at all, but it seems they did not disable encryption for their OpenVPN trials (which should have yielded an even smaller processing resource footprint than Wireguard, at that point) or use a plain packet tunneling method such as GRE.
- On May 28, 2019 we received an email from a Brian Mullan letting us know that there is a configuration utility for WireGuard. It supposedly is developed by the WireGuard team. While it does make things easier, I still find a lot of my criticism valid – namely, that nobody that can/would use it can come up with a valid use case where something else wouldn't be better suited for. To each their own, though.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	uRLauB	Phillip Gross	click	CC-BY 4.0
Outro	CNN	Semaphore	click	CC-BY 4.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories Season Three

Comments

1. 2018-10-13 07:10 (1176 days ago)

   Please excuse my brevity, but I'm writing this from my phone and am supposed to be somewhere else :)

   The BBC recently produced a piece on why they selected Wireguard for their Outside Broadcast units.

   https://www.bbc.co.uk/rd/blog/2018-09-vpn-throughput-ip-broadcasting

2. 2018-10-13 07:49 (1176 days ago)

   hey, Jon – thanks for reaching out! your brevity is of course excused. :)

   that's definitely an interesting note! i'm still confused as to why they'd use OpenVPN **or** Wireguard instead of just straight GRE tunneling! (or a non-encrypted OpenVPN, which should have even less latency/overhead than Wireguard.) they aren't exactly running something that needs encryption, you know?

   regardless, thanks! i'll add it to the show's errata.