IOS VPN SECURITY

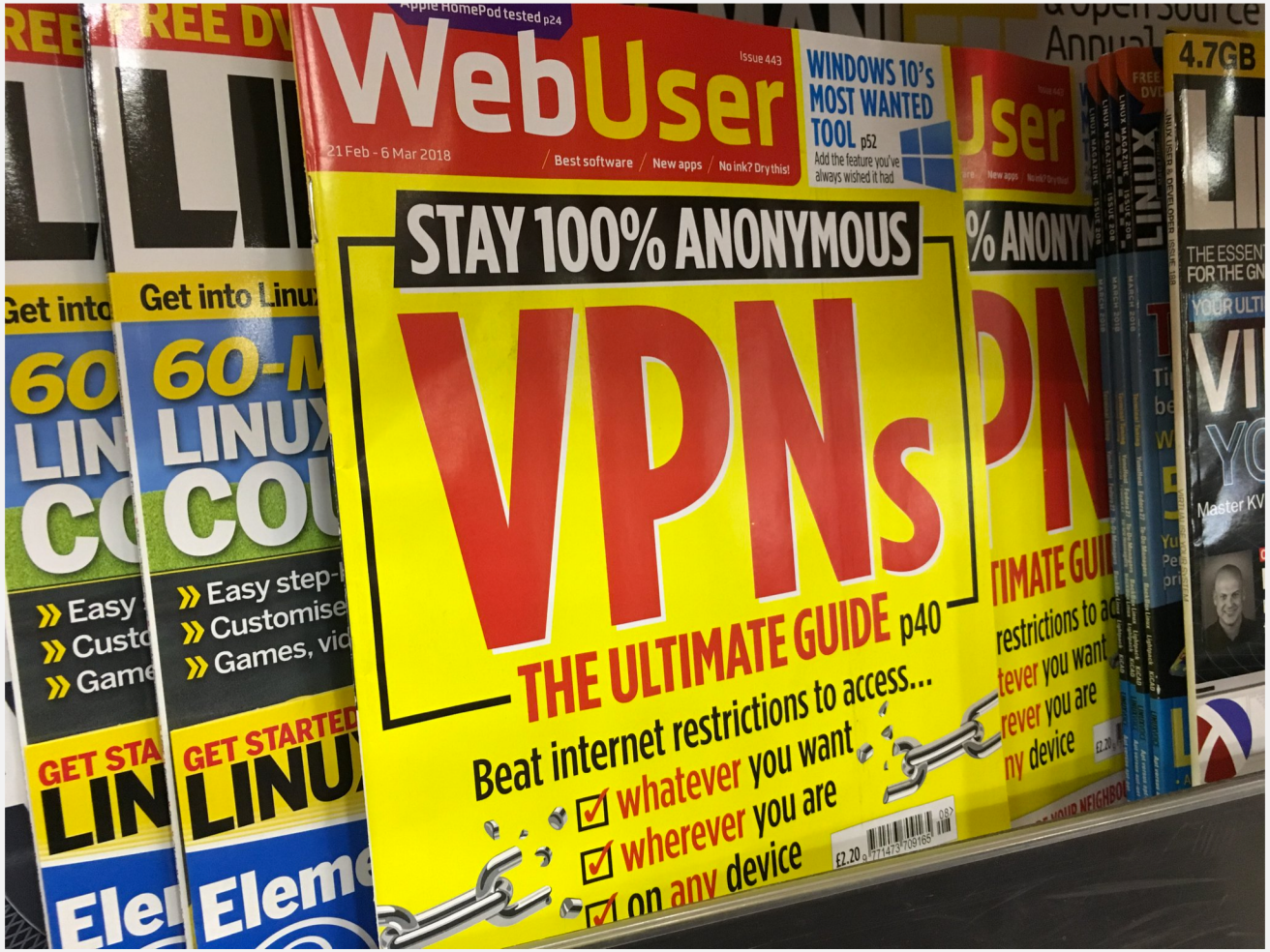
Securi-Tay 2018

QUICK DISCLAIMER

- I'm not a dev
- I'm not a lawyer
- Compared to most people in this room I'm also not the most experienced

WHY VPN SECURITY?

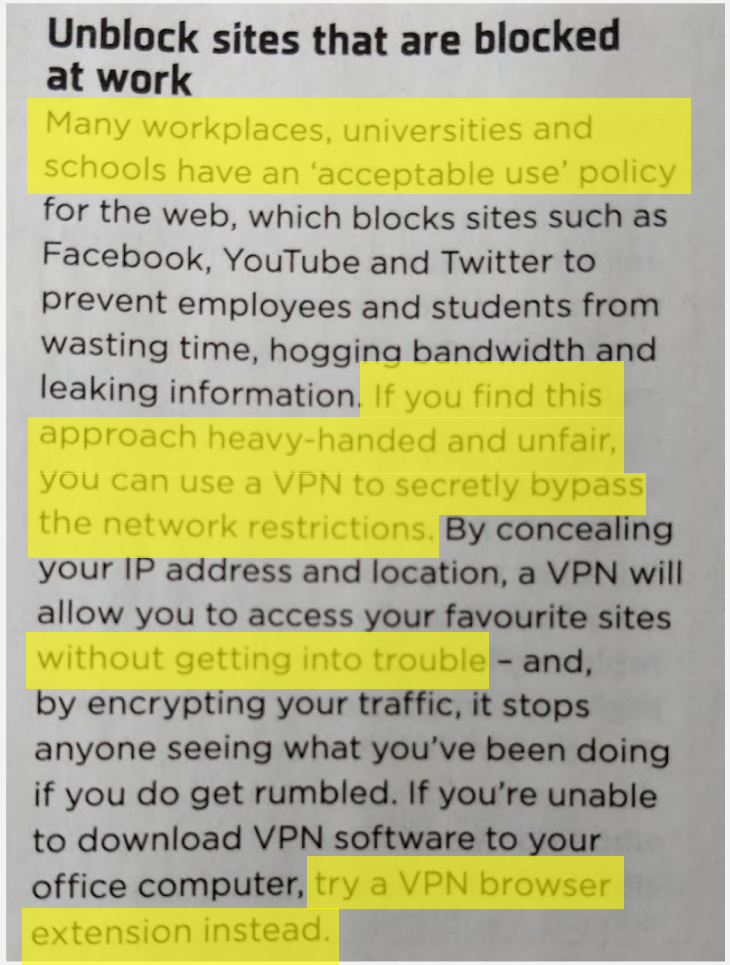
WHY VPN SECURITY?



- h/t @neil_neilzone

NOTES FROM THE ARTICLE

- This is a wider issue, I'm only picking on this article as it's recent
- The general advice is ok
- The "Stay 100% Anonymous" claim is garbage
- The image (right) is terrible advice



Unblock sites that are blocked at work

Many workplaces, universities and schools have an 'acceptable use' policy for the web, which blocks sites such as Facebook, YouTube and Twitter to prevent employees and students from wasting time, hogging bandwidth and leaking information. If you find this approach heavy-handed and unfair, you can use a VPN to secretly bypass the network restrictions. By concealing your IP address and location, a VPN will allow you to access your favourite sites without getting into trouble – and, by encrypting your traffic, it stops anyone seeing what you've been doing if you do get rumbled. If you're unable to download VPN software to your office computer, try a VPN browser extension instead.

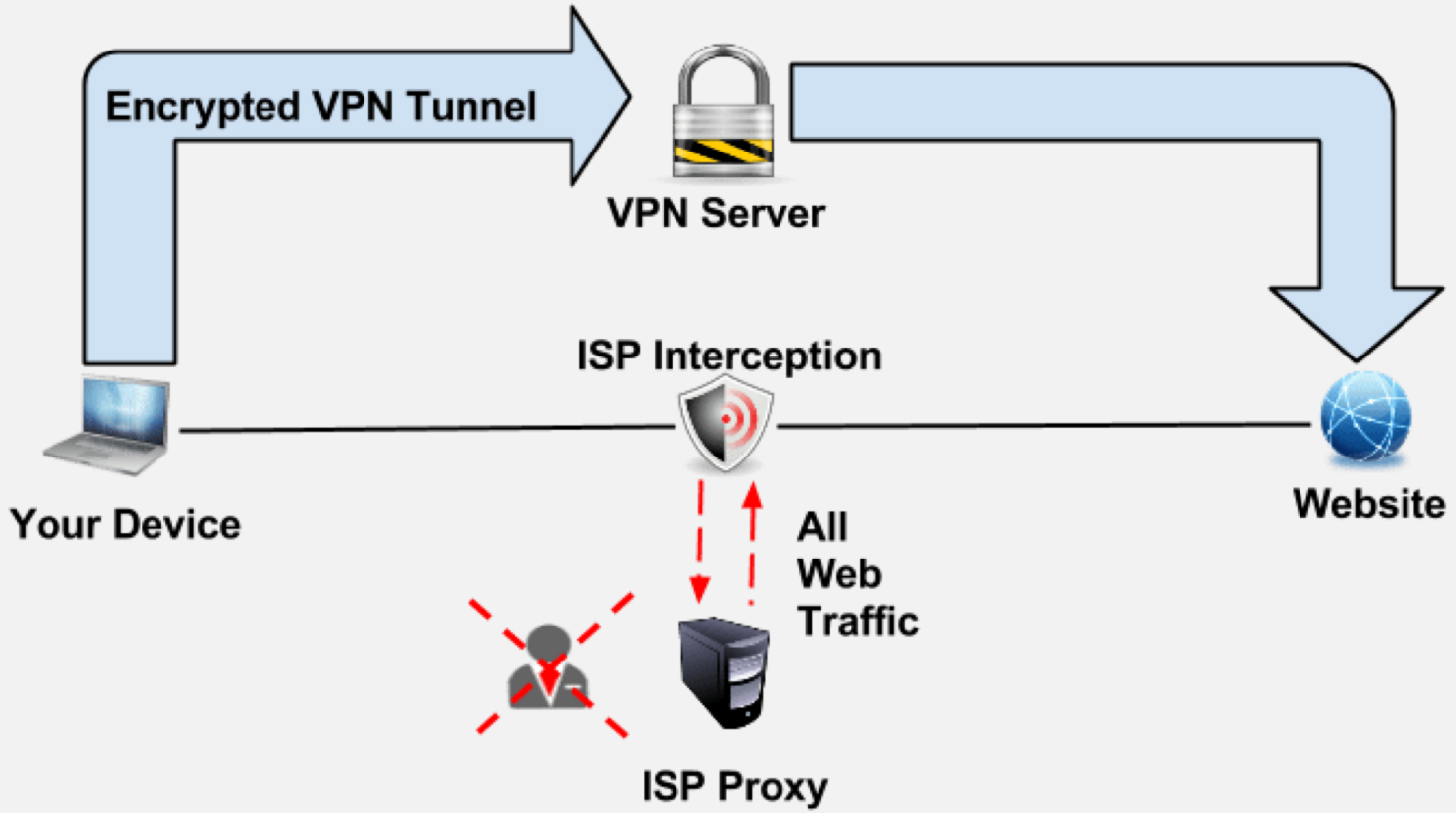
BUT WHY IOS?

ANDROID WAS ALREADY DONE

An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps

Muhammad Ikram[1,2], Narseo Vallina-Rodriguez[3], Suranga Seneviratne[1],
Mohamed Ali Kaafar[1], Vern Paxson[3,4]
[1]Data61, CSIRO [2]UNSW [3]ICSI [4]UC Berkeley

BASICS FIRST: WHAT IS A VPN?



- It's against the acceptable usage policy to use a VPN on eduroam
- This made research/testing a nightmare

THREAT MODELS

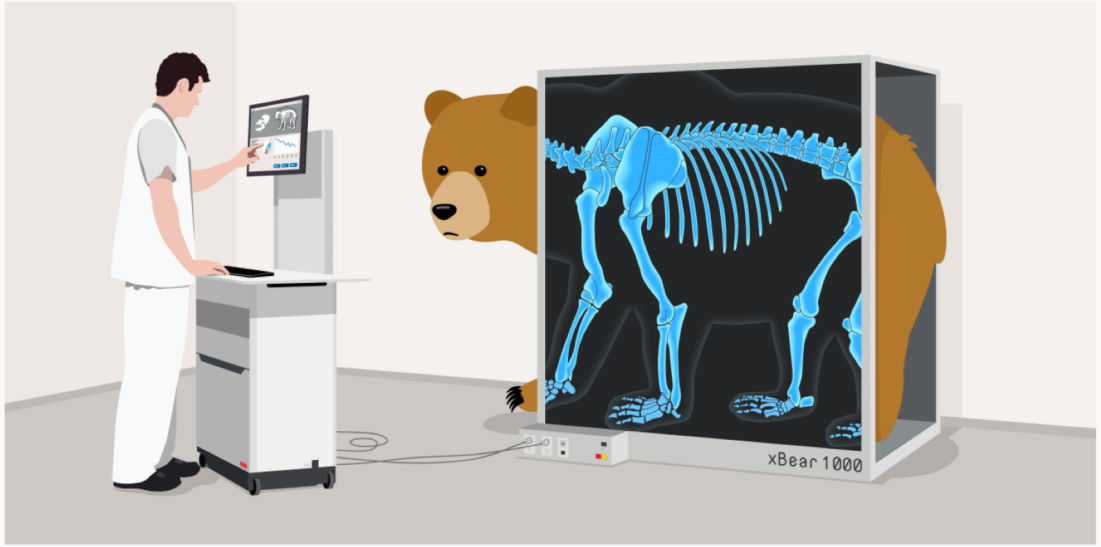
- Why you SHOULD use a VPN
  - Security on public WiFi
  - Avoiding ISP tracking
  - Appearing somewhere you're not/avoiding geo-restrictions
  - You want to avoid websites/advertisers tracking you (kind of)
- Why you SHOULDN'T use a VPN
  - To avoid governments
    - "If your threat model includes the NSA, do not use the internet" –The Grugq
  - To be anonymous
    - Privacy != Anonymity

TRUST

- Picking a VPN provider involves a lot of trust
  - Will they (at least try) to keep your data safe/secure?
  - Will they stick to the claims in their privacy statement?
  - Are they truly the “No logging” VPN service that they advertise?
  - Will they sell your data?
  - Will the fiddle with your traffic?

A VPN simply moves trust from your ISP to the VPN provider

TUNNELBEAR AUDIT



Share this post

TunnelBear Completes Industry-First Consumer VPN Public Security Audit

Consumers and experts alike have good reason to question the security claims of the VPN industry. Over the last few years, many less reputable VPN companies have abused users' trust by selling their bandwidth, their browsing data, offering poor security or even embedding malware.

“NO LOGS” VPN SERVICE CATCHES A STALKER

HOLA USES USER DEVICES AS ENDPOINTS

Hola Better Internet Sells Your Bandwidth, Turning Its VPN into a Botnet

Alan Henry
5/28/15 3:15pm • Filed to: PRIVACY

88 8

The botnet claim part is debatable, but the exit node part is an issue

via https://lifehacker.com/hola-better-internet-sells-your-bandwidth-turning-its-1707496872

FACEBOOK BUYS VPN SERVICE FOR ANALYTICS

Facebook's Onavo Gives Social-Media Firm Inside Peek at Rivals' Users

Information from data-security app shows company what people do on their phones beyond suite of firm's apps

When an Onavo Protect user opens a mobile app or website, Onavo redirects the traffic to Facebook's servers and the action is logged in a database, according to Onavo's website and the people familiar with the system. Facebook's product teams can analyze the aggregated data to get detailed information on things such as which apps people generally are using, how frequently, for how long, and whether more women than men use an app in a specific country. If data inside an app isn't encrypted, the information can be as specific as the number of photos the average user likes or posts in a week.

via https://www.wsj.com/articles/facebooks-onavo-gives-social-media-firm-inside-peek-at-rivals-users-1502622003

OTHER THINGS TO LOOK FOR

- Self-hosted infrastructure VS third –party
- Mitigations to SSL/TLS downgrade attacks
- Uptime guarantee
- Policies around staff access/customer confidentiality
- Log longevity/destruction
- Server security (hardening/encryption/patching etc.)
- Customer password storage (plain text vs bcrypt etc.)
- Country of incorporation

via Kenn White (@kennwhite)

https://twitter.com/kennwhite/status/570062025641951232

THE DISSERTATION

TAKE A BUNCH OF IOS VPN CLIENTS AND TEST FOR:

- Sending traffic over HTTP
- Sending PII over HTTP
- DNS Leak
- Tunnelling protocol implementation
- Unnecessary(ish) permissions
- Other weird stuff developers do

WHAT'S THE POINT?

- To get an overview of the state of iOS VPN security within the free/cheap market
  - Realistically, most non-technical consumers will look at this price range
- To write guidance for developers
- Possibly some responsible disclosure

TESTING CRITERIA EXPLAINED

HTTP

- Web traffic (unencrypted)
- PCAP using RVI
- Analyse PCAPS
  - Automation ❤️
  - grep -i –a –f wordlist.txt ${SEARCHTERM} | grep –ivf exclusions.txt || echo “No keyword matches” >&2
- You’d think encrypting passwords is simple…

UNFORTUNATELY NOT

```
GET /lygamesService.asmx/TollUserReg?apikey=lygames_0953&uuid=CADF4902-5C7F-428E-BF9A-98BEFA172682&name=&mail=junk@jack.lu&pass=7c6a180b36896a0a8c02787eeafb0e4c&source=SDNEW560 HTTP/1.1
```

```
&pass=7c6a180b36896a0a8c02787eeafb0e4c
```

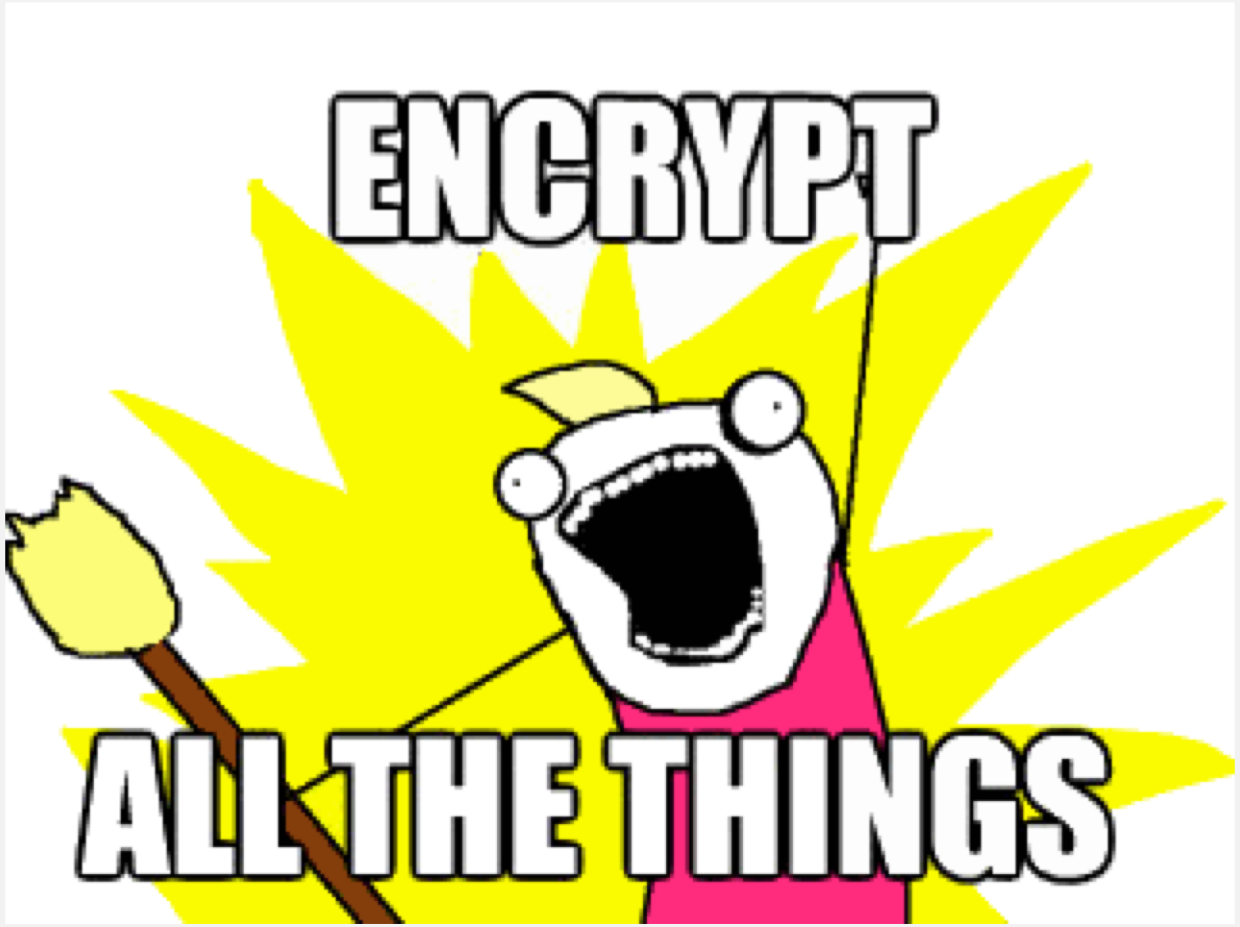
```
▼ Member Key: username
    String value: 58554cb5ad71e8977c06a94c2bd2a99a
    Key: username
▼ Member Key: password
    String value: iMEGODmd
    Key: password
```

```
▼ <name>
    user
  </name>
▼ <value>
  ▼ <string>
      junk@jack.lu
    </string>
  </value>
</member>
<member>
▼ <name>
    password
  </name>
▼ <value>
  ▼ <string>
      password
    </string>
  </value>
</member>
```

```
{
  "user_name" : "3CD2E3CE-8C17-4C32-97C4-DD53A3D4A14B",
  "user_passwd" : "3CD2E3CE-8C17-4C32-97C4-DD53A3D4A14B"
}HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 23 Jan 2018 14:36:58 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Transfer-Encoding: chunked

{"psk":"Z6utCz93PG","remote_id":"abcedf.com","local_id":"test@abcedf.com","eap_user":"user1","eap_passwd":"rj0T6ID62j"
```

HOW CAN THIS BE FIXED?



HOW CAN THIS BE FIXED?

- Encrypt everything!
- Certs are free from Let's Encrypt
- Harder when reliant on third-parties (e.g. advertising)
  - User privacy vs 💰 💰 💰

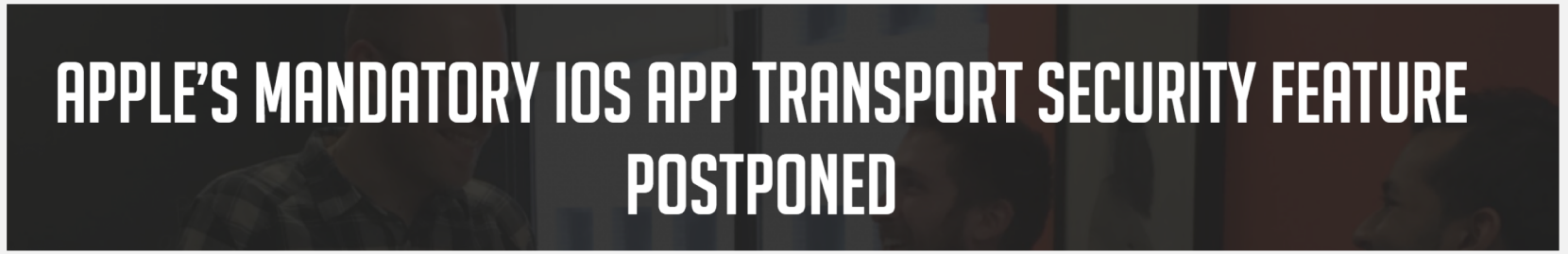
HOW CAN THIS BE FIXED ON A LARGER SCALE?

SECURITY

WWDC 2016: Apple to require HTTPS encryption on all iOS apps by 2017

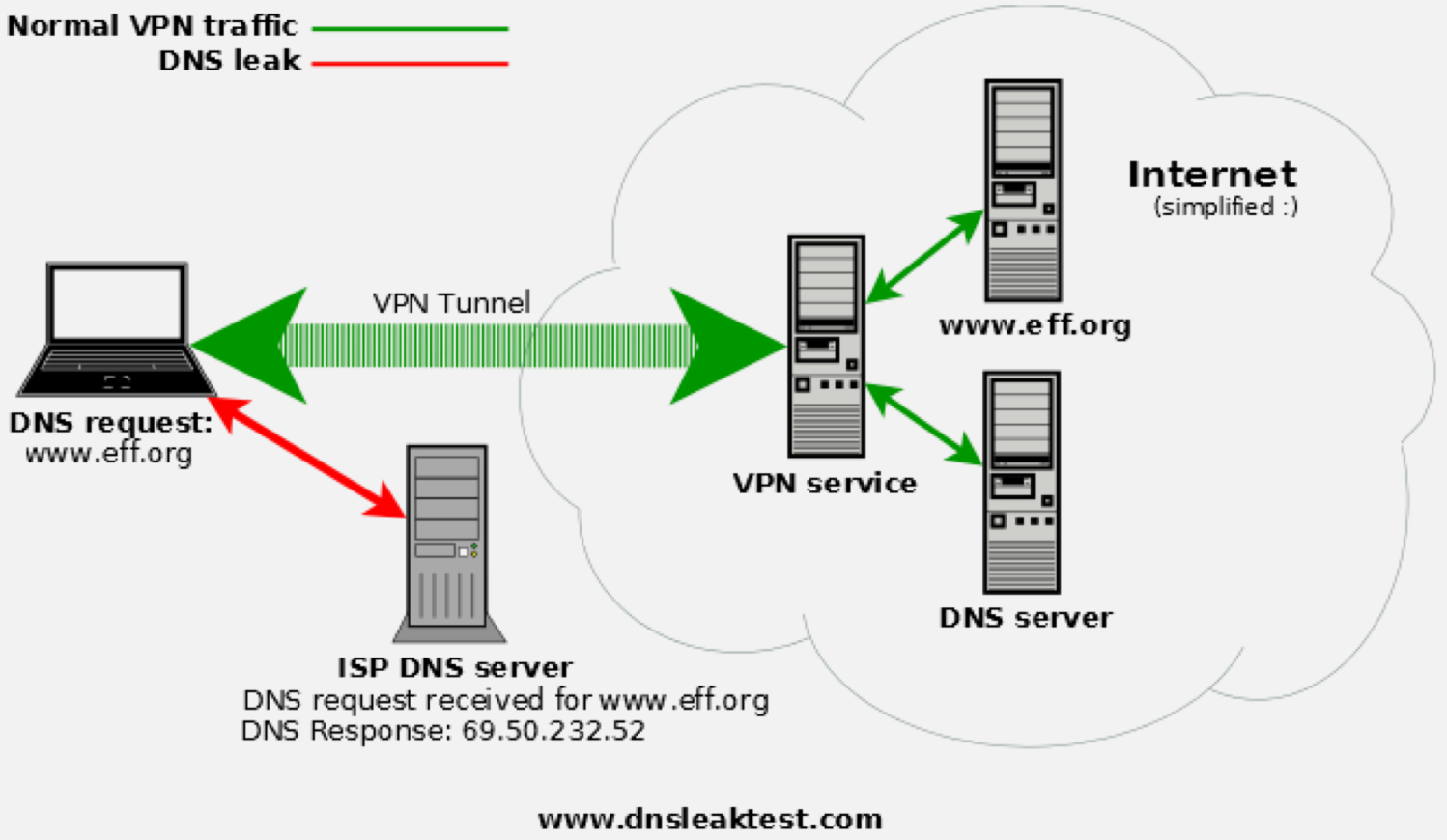
At a session at the 2016 WWDC, Apple revealed that it would be requiring all iOS apps to use HTTPS connections through an existing feature called App Transport Security by the end of the year.

By Conner Forrest | June 15, 2016, 2:14 PM PST



¯_(ツ)_/¯

DNS LEAKAGE


Normal VPN traffic
DNS leak
Internet
(simplified :)
VPN Tunnel
www.eff.org
DNS request:
www.eff.org
VPN service
DNS server
ISP DNS server
DNS request received for www.eff.org
DNS Response: 69.50.232.52
www.dnsleaktest.com

DNS LEAKAGE

- Tested by running an extended test on dnsleaktest.com while VPN is active
- A DNS gives whoever is receiving the DNS requests the ability to monitor which sites you visit
  - Your ISP, Google, etc.
  - Not ideal if you want to avoid tracking

HOW CAN THIS BE FIXED?

- In a perfect world?
  - VPN providers running their own DNS
- A bare minimum
  - Using a 'trusted' and/or 'secure' DNS provider
    - Trust means a different thing to different people
    - Quad1 or Quad9?
  - Probably not an ISP or Google
- DNSSEC(?)
  - Verifies correct DNS server is responding to requests to prevent poisoning attacks
  - There is some debate on the effectiveness of DNSSEC
- Honourable mention: DNS over TLS
  - Encrypts DNS traffic (when not using a VPN)
  - Avoids anyone sniffing traffic from viewing your DNS requests

TUNNELLING PROTOCOLS

- Apple support three protocols on iOS 10+
  - IKEv2 (with IPSec)
    - Good, secure, fast
    - IPv6 support
    - Stability between network changes
  - L2TP over IPSec
    - *Possibly* compromised by the NSA
  - SSL VPN
    - Lightweight, clientless
    - Works in a browser

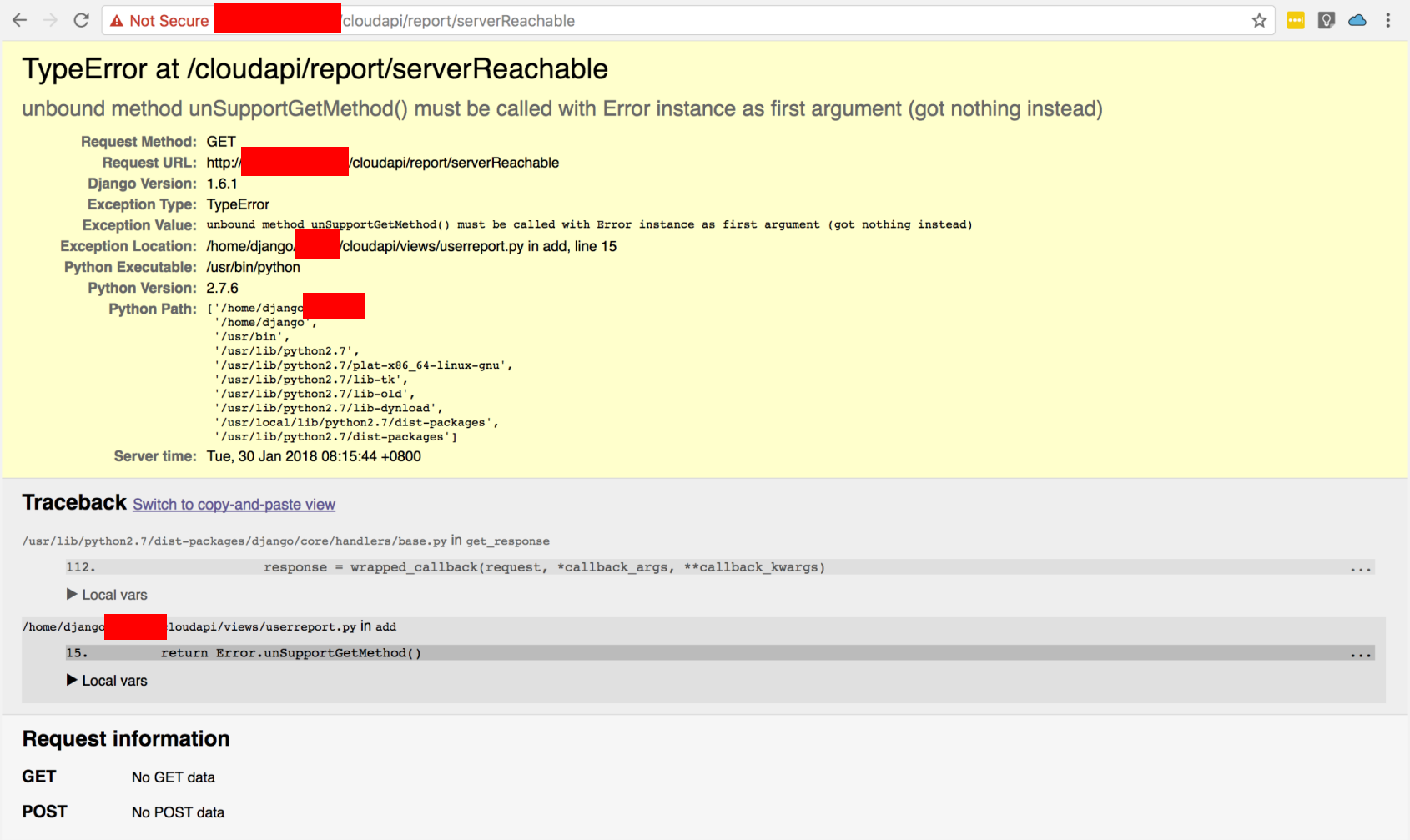
TESTING FOR PROTOCOL IMPLEMENTATION

- Some VPN's documentation/websites refer to protocol support
- VPN config settings on iOS (sometimes) gave this away
- Further verification was done using:
  - Bro (Network Security Monitor)
  - PCAP Analysis

PERMISSIONS

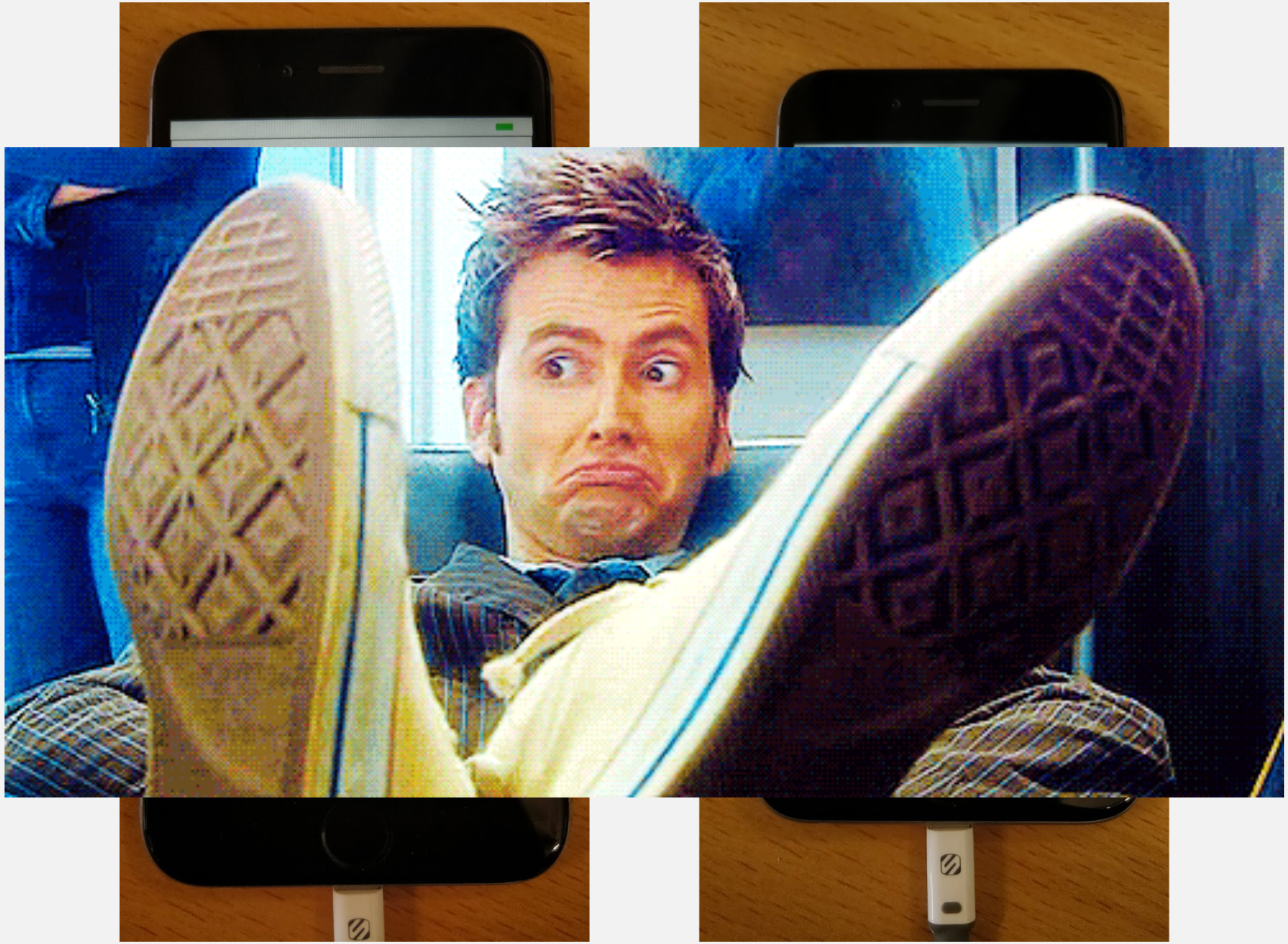
- Are apps asking for permissions they don't necessarily need?
  - E.g. contacts, camera roll, GPS etc.
- Tested by interacting with app and recording permissions that were requested

OTHER WEIRD FINDINGS



Django 1.6.1 was released December 2013

CVE's for XSS, CSRF, DoS…




GET /downloads/config/ _config.zip HTTP/1.1

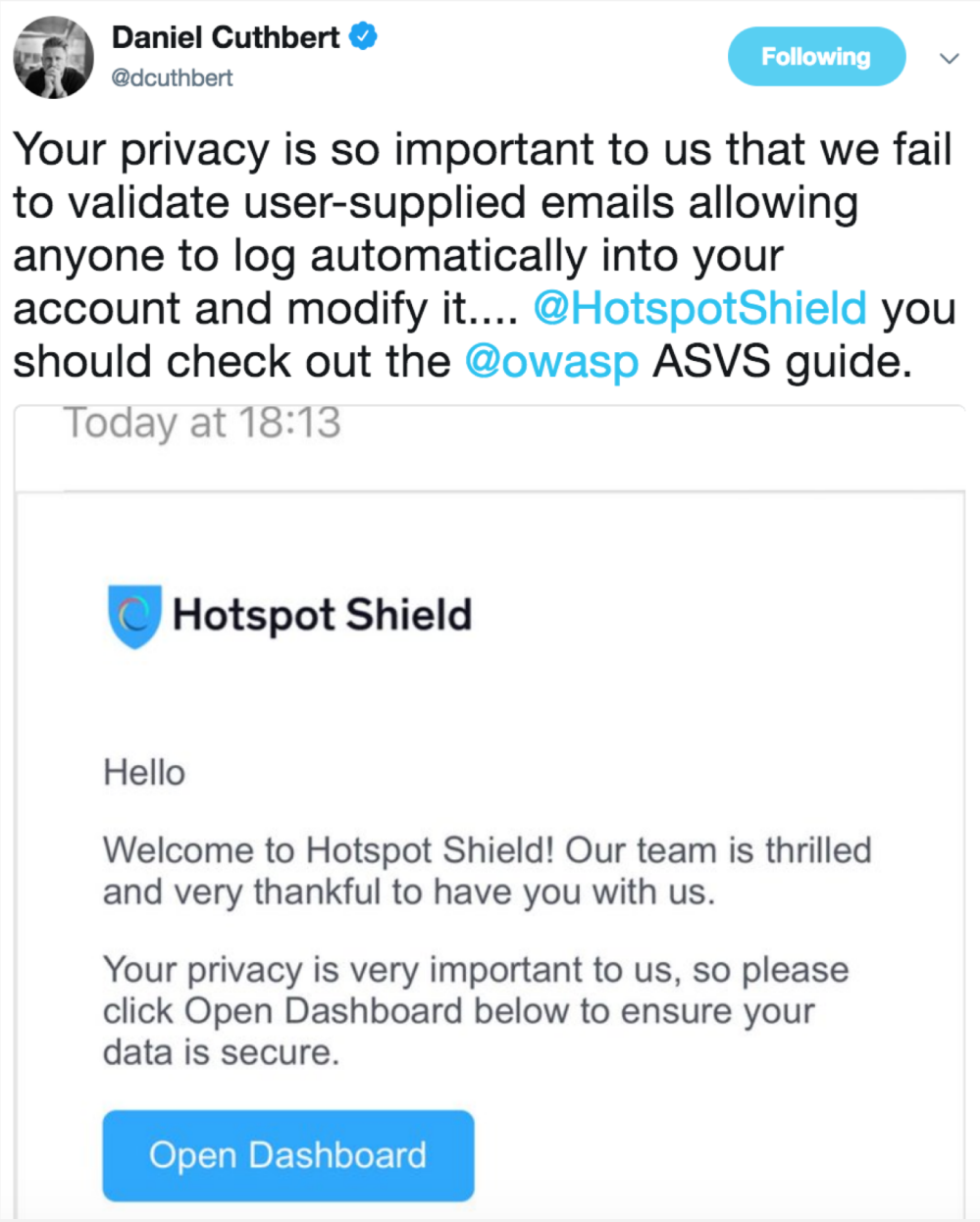
HOTSPOT SHIELD

A flaw in Hotspot Shield can expose VPN users, locations

The virtual private network says it provides a way to browse the web "anonymously and privately," but a security researcher has released code that could identify users' names and locations.

By Zack Whittaker for Zero Day | February 6, 2018 -- 20:00 GMT (20:00 GMT) | Topic: Security

- 9M+ installs across every platform worldwide
- Runs a web server on localhost that hosts JSON endpoints
- Including source IP, WiFi SSID and country
- SSID + wigle.net = profit?
- Researcher also developed a PoC for RCE


Daniel Cuthbert
@dcuthbert
Following
Your privacy is so important to us that we fail to validate user-supplied emails allowing anyone to log automatically into your account and modify it.... @HotspotShield you should check out the @owasp ASVS guide.
Today at 18:13
Hotspot Shield
Hello
Welcome to Hotspot Shield! Our team is thrilled and very thankful to have you with us.
Your privacy is very important to us, so please click Open Dashboard below to ensure your data is secure.
Open Dashboard

OTHER ALTERNATIVES?

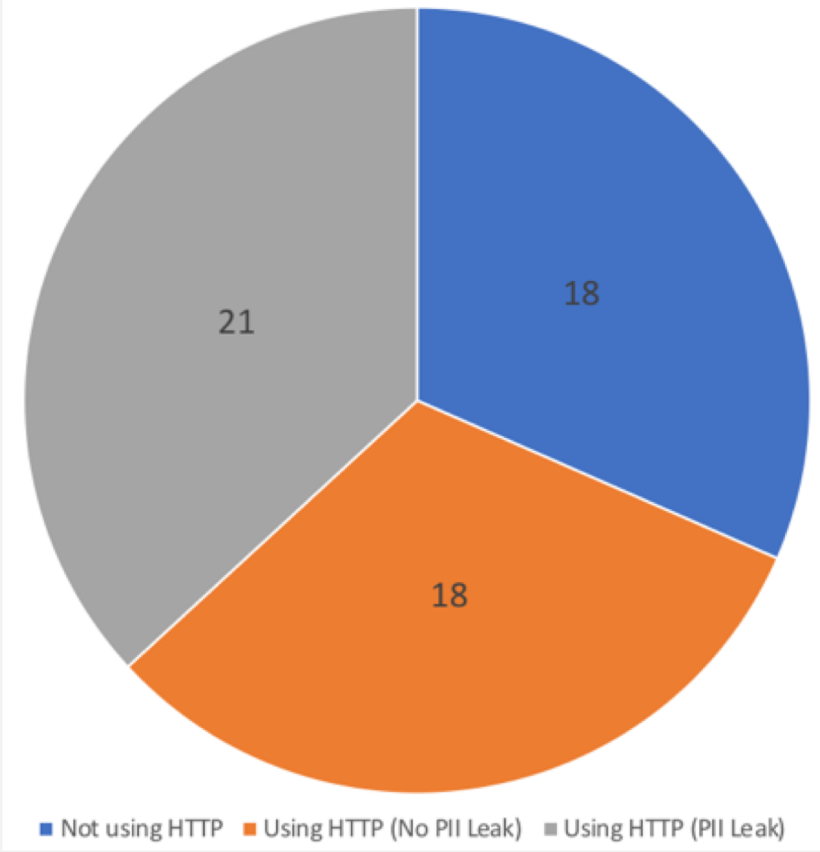
ALGO

- Roll your own VPN
  - Works well with DO, AWS, Azure, Google Compute Engine
  - Only supports IKEv2
  - Works well natively on Apple
  - A bit janky on Android/Windows
  - Built-in ad-blocking
  - Cheapest DO droplet is $5/month

RESULTS:
57 APPS TESTED

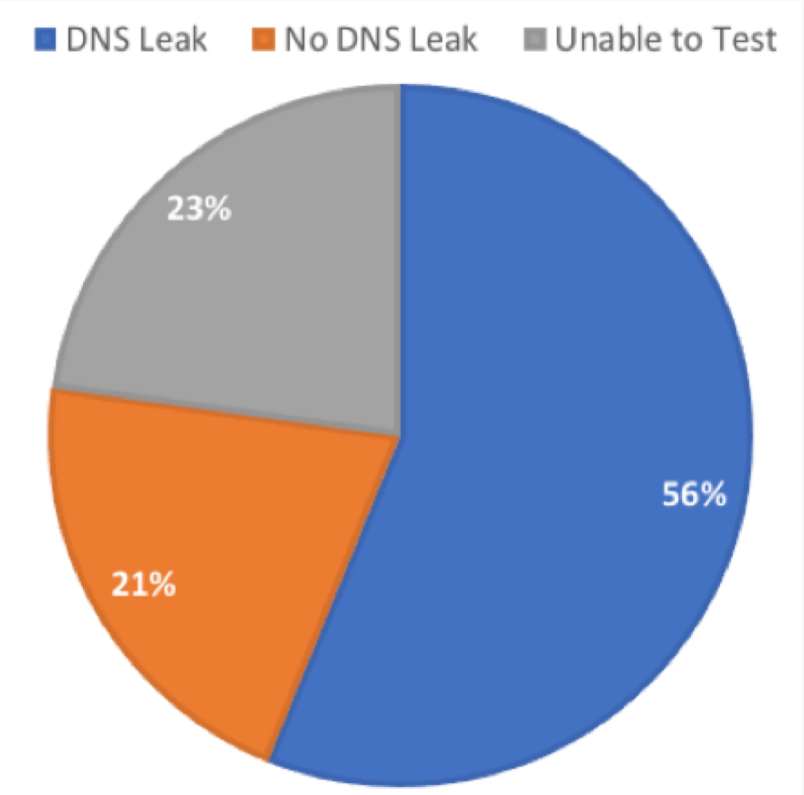
HTTP

- 39/57 apps were using HTTP
- 21/39 were leaking PII over HTTP
  - Email, password, GPS, source IP, UDID etc.



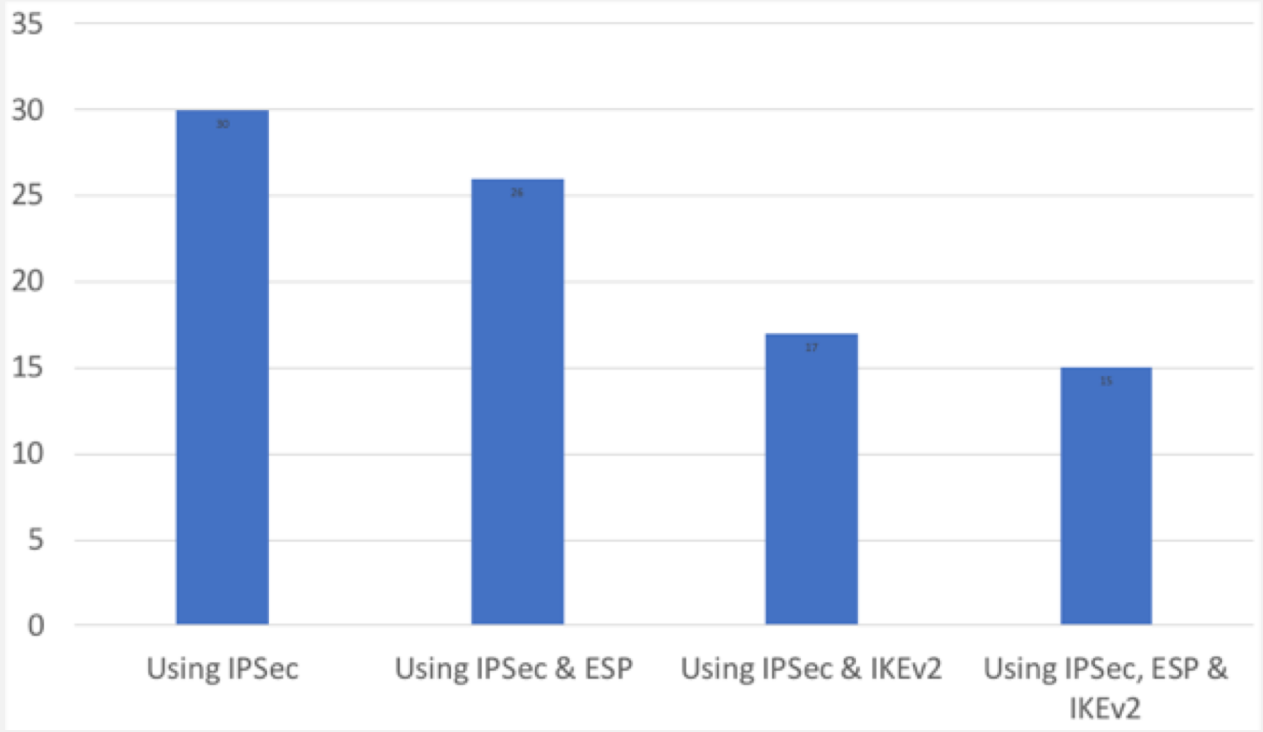
DNS LEAKAGE

- Not all apps could be tested
- 32/44 (73%) leaked DNS
  - Primarily to Google DNS



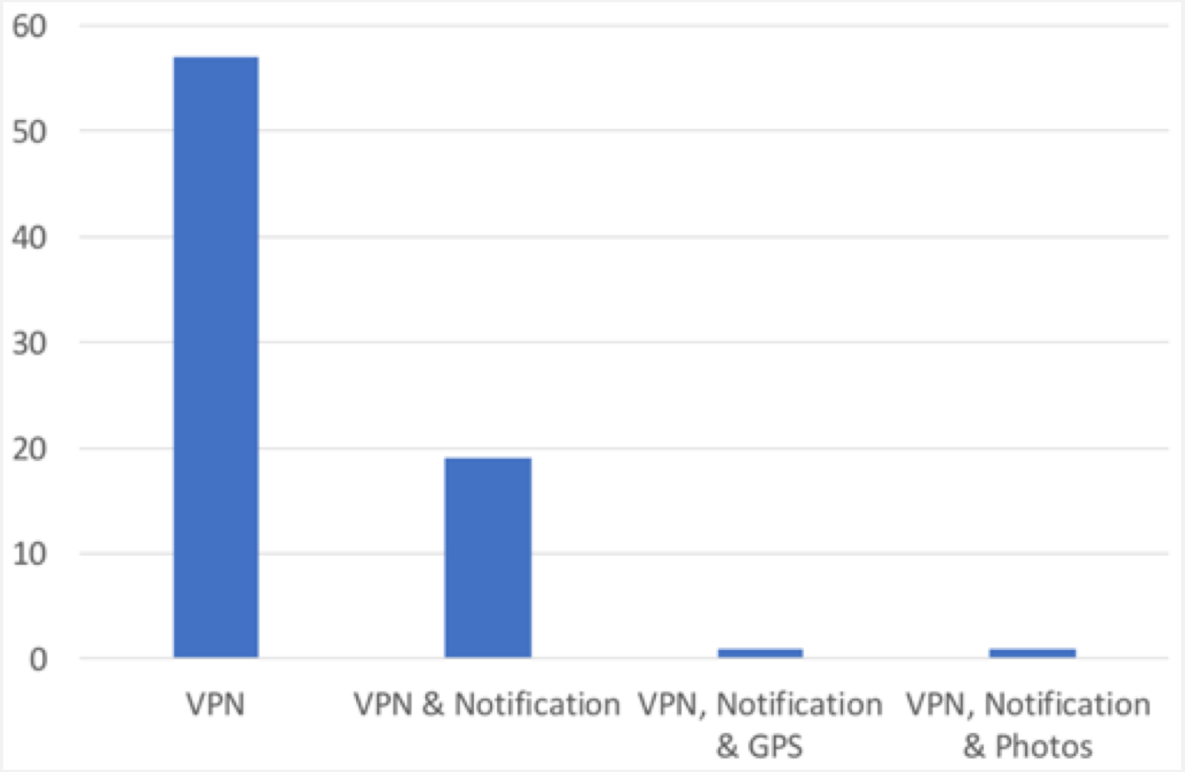
TUNNELLING PROTOCOLS

- 30/57 apps were using IPSec
- Even less were using IPSec with IKEv2 and/or ESP



PERMISSIONS

- Majority of apps only requested the expected permissions
  - VPN + Notification
- One app required access to camera roll
- One app also required GPS



WERE ANY APPS ACTUALLY GOOD?

- Yes!
- All below apps did **not** use HTTP or leak DNS
  - SecureVPN (IPSec with ESP)
  - VPN Unlimited (IPSec with IKEv2 and ESP)
  - ~~Onavo (IPSec with ESP)~~
  - Cyberghost VPN (IPSec with IKEv2 and ESP)
  - iBVPN – (IPSec with IKEv2 and ESP)

TL;DR: WHAT CAN DEVS DO BETTER?

- Encrypt everything
- Don't take unnecessary data
  - "Data that doesn't exist can't be stolen/misused"
- Don't request unnecessary permissions
- Route all traffic through the VPN tunnel
  - Including DNS and IPv6
- Use IPSec with IKEv2 and ESP

QUESTIONS/COMMENTS/FEEDBACK

- Now
- Afterparty
- Twitter (@iJackWilson)

- Dissertation available at jack.lu/s/Dissertation.pdf
- Other work at www.jack.lu/blog