iOS VPN Security

BSides Ljubljana – 10th March 2018

Obligatory $whoami

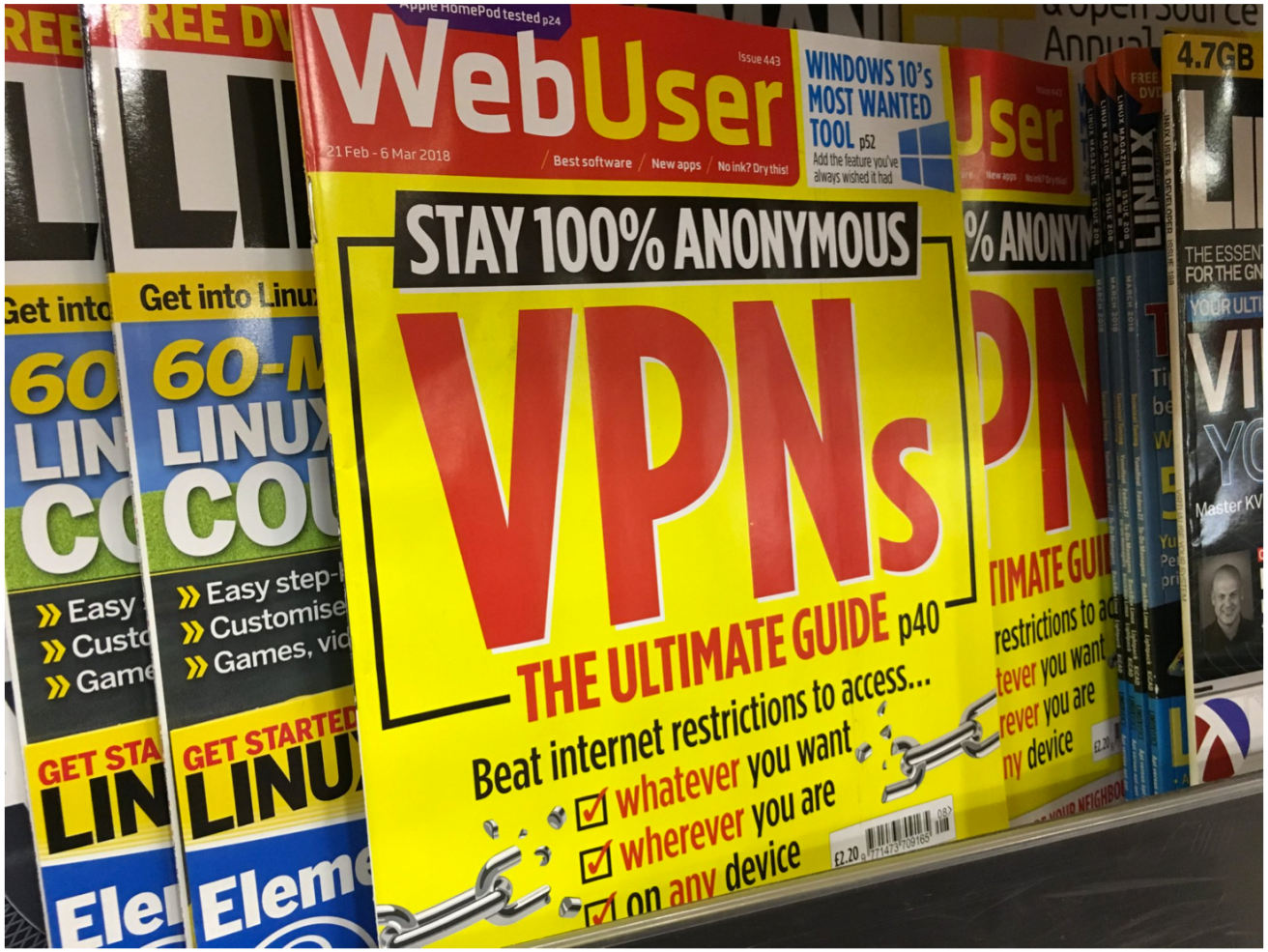
- Jack Wilson
- 4th year student
  - BSc (Hons) Ethical Hacking (Dundee, Scotland)
  - @AbertayHackers
- Intern Security Consultant
  - Views my own etc.
- Interested in privacy + red/blue team stuff

Shameless plug: Securi-Tay

- 2018.securi-tay.co.uk
- 18th/19th May (rescheduled due to weather)
- Largest student-organized conference in Europe
- Up to 350 attendees
- ~20 talks
- After party with sponsored bar
- There's a pig

Why VPN Security?

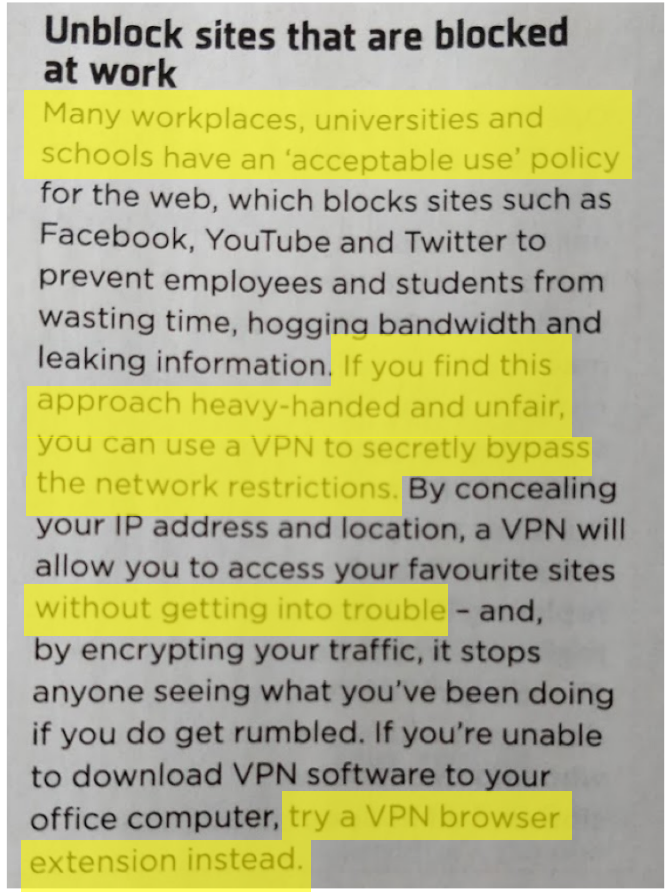
Why VPN Security?



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 "100% Anonymity" 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.

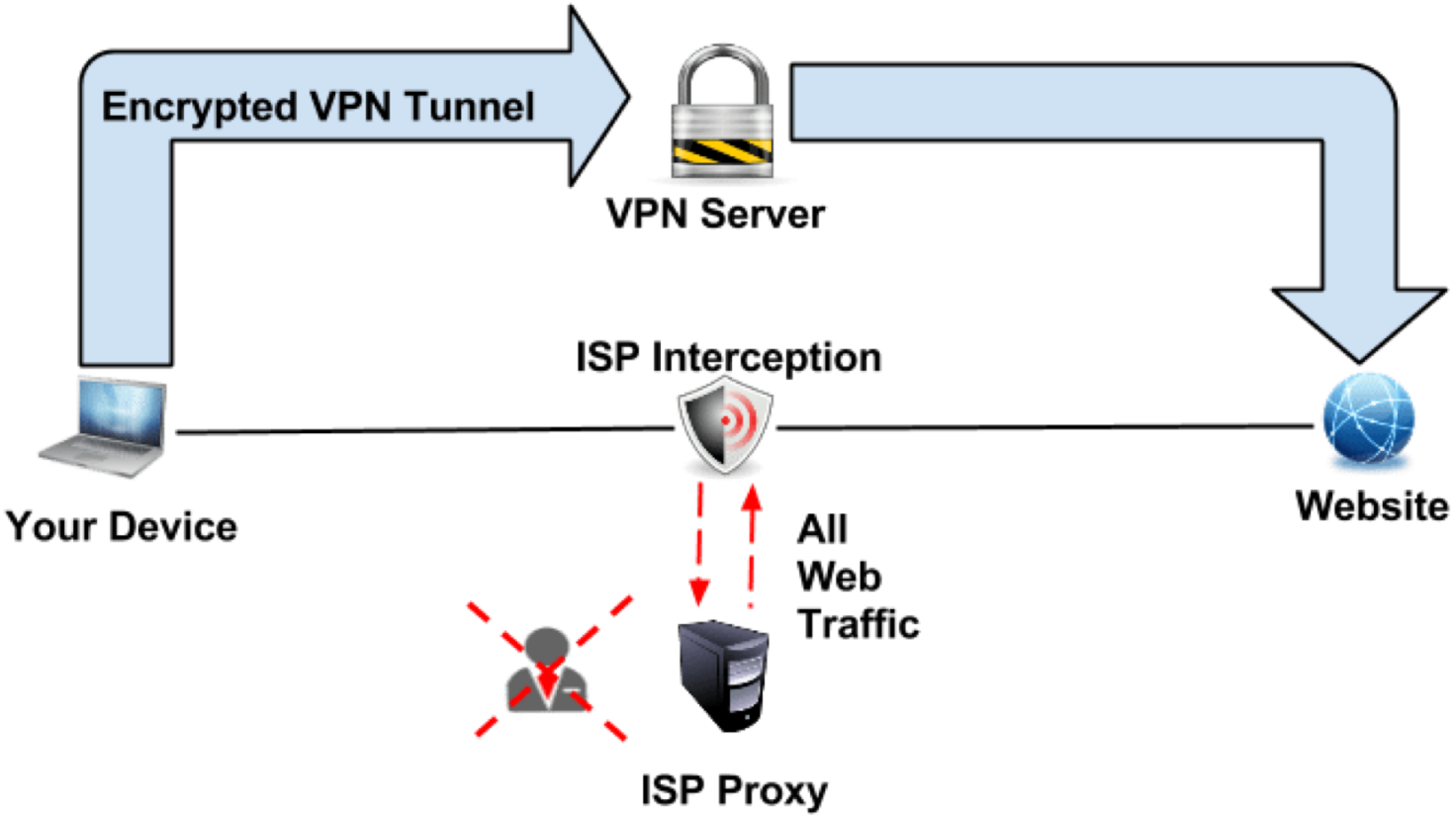
But why iOS?

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 makes research/testing an absolute nightmare

Threat Models

- Why you SHOULD use a VPN
  - Security on public Wi-Fi
  - Avoiding ISP tracking
    - We'll go into this later
  - You want to appear somewhere you're not/avoid geo-restrictions
  - You want to avoid websites/advertisers tracking you (kind of)
- Why you SHOULDN'T use a VPN
  - To avoid governments
    - I don't doubt governments are sitting on VPN o-day's
  - To be anonymous
    - Privacy != Anonymity
    - "If your threat model includes the NSA, do not use the internet" –The Grugq

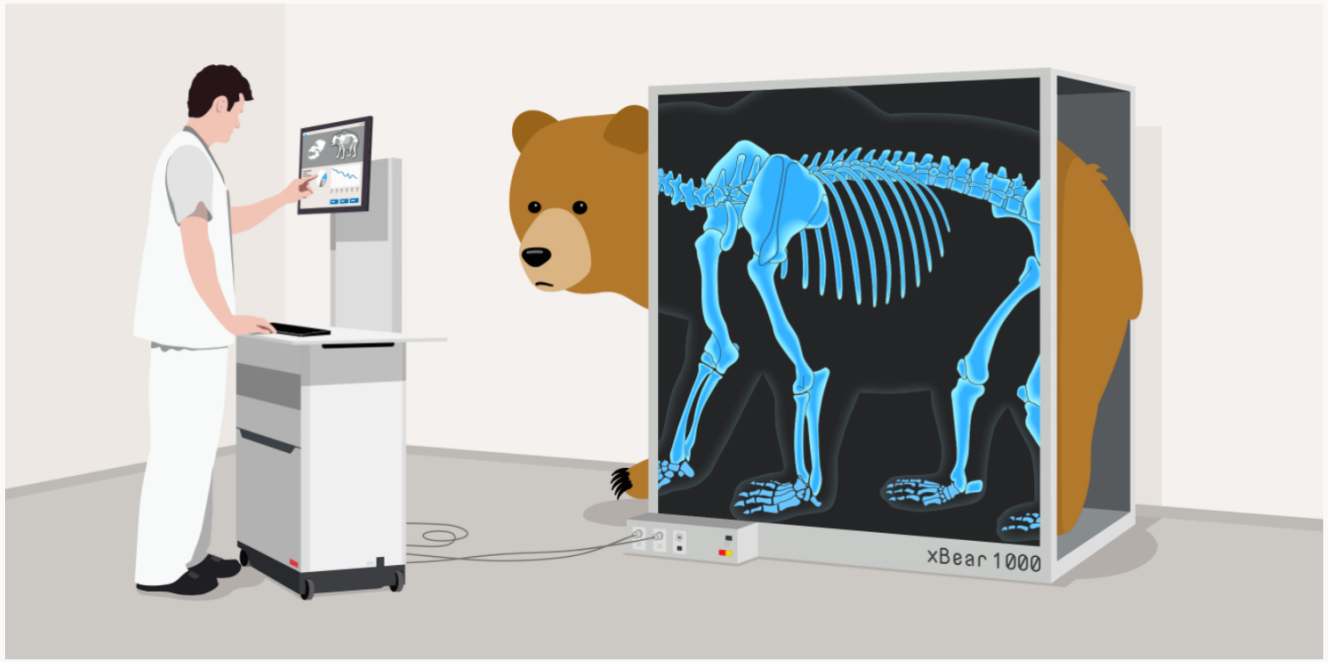
Trust

- 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?

Trust

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 provider catches a stalker

Hola uses user devices as VPN 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

Hot off the press

McAfee acquires VPN company TunnelBear

*Posted 20 hours ago by **Romain Dillet** (@romaindillet)*

Security giant McAfee is acquiring Canadian VPN provider TunnelBear. Terms of the deal haven't been disclosed. McAfee said that it plans to integrate TunnelBear's technologies into the company's own VPN product, Safe Connect.

Other stuff 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.)

- Via Kenn White (@kennwhite)
- https://twitter.com/kennwhite/status/570062025641951232

The Dissertation

Take a heap of iOS VPN clients and test for:

- Sending traffic over HTTP
- DNS Leak
- Transmission of PII
- Using insecure/outdated tunnelling protocols
- Using Non-Unique Pre-Shared Keys
- Asking for unnecessary permissions
- Malvertising
- Other weird stuff stupid developers do

*Disclaimer: I don't think all developers are stupid

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…

```
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
```

You'd be wrong

```
▼ 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?

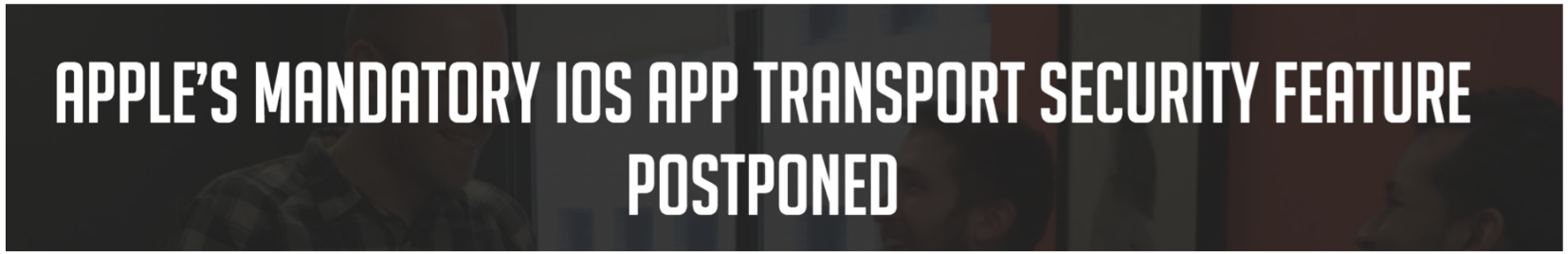
How can this be fixed on a larger scale?

SECURITY

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

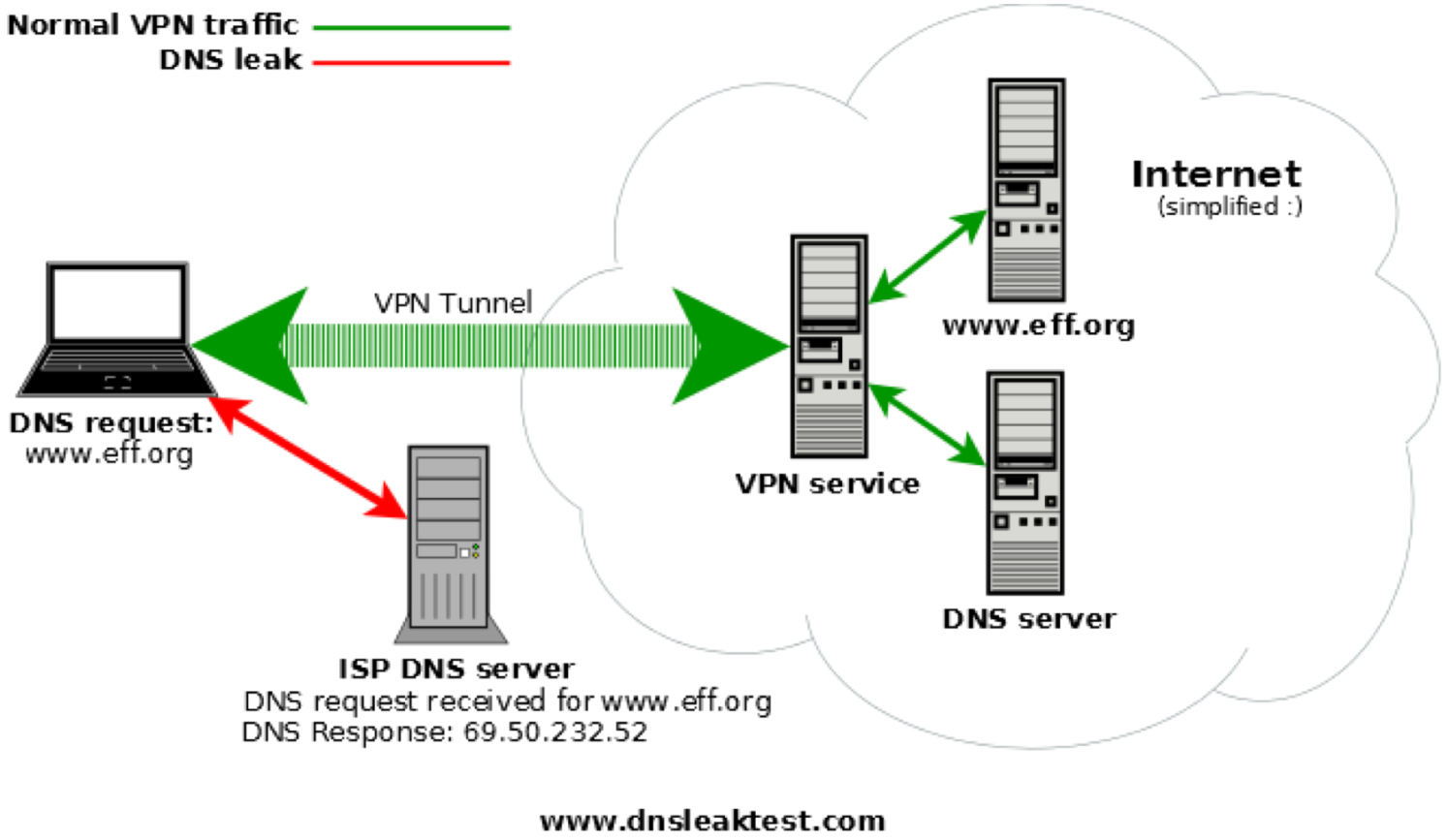
At a session at the 2016 WWDC, Apple revealed that it would be requiring all iOS apps to use HTTPS connections through an existing feature called App Transport Security by the end of the year.

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



¯_(ツ)_/¯

DNS Leak


Normal VPN traffic
DNS leak
Internet
(simplified :)
www.eff.org
VPN Tunnel
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

Why this is bad

- It 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, secure DNS provider
    - Trust means a different thing to different people
  - 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

Transmission of PII

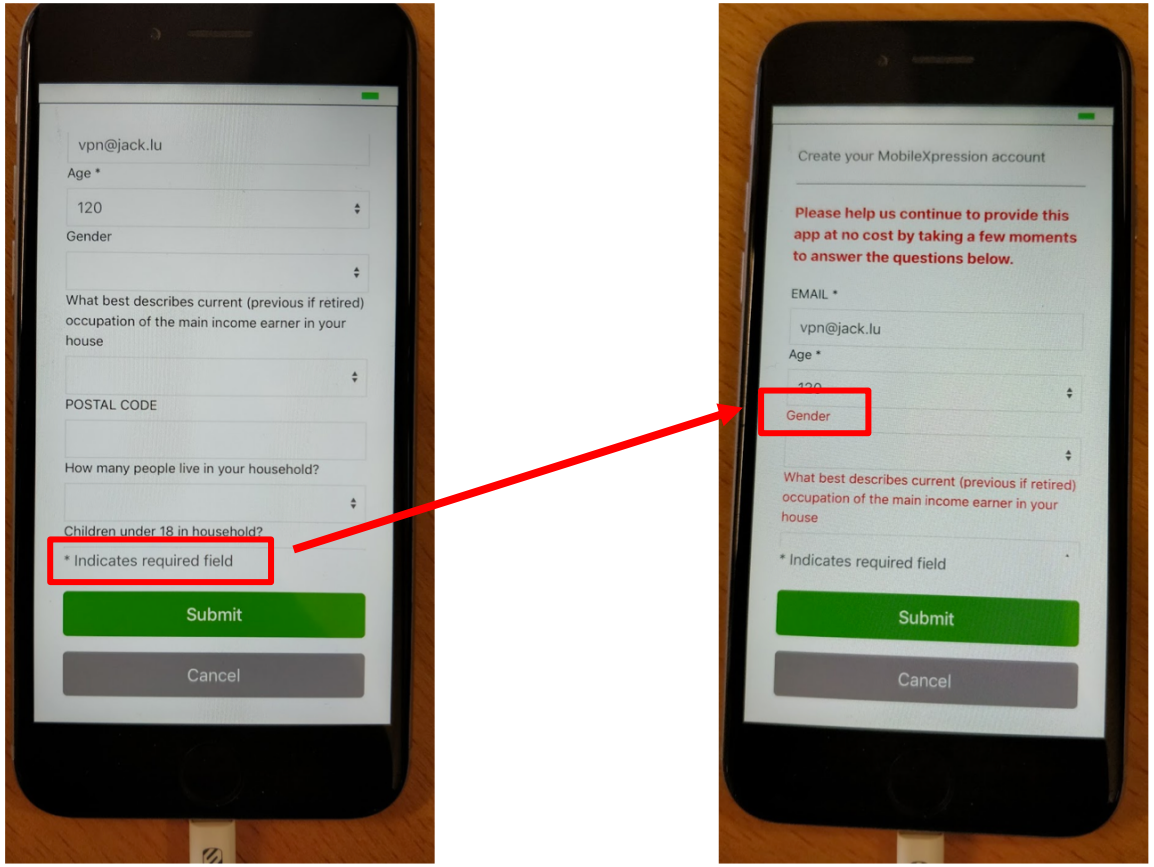
- Determining what information apps are sending that could uniquely identify a person/device
  - Install Burp certificate on phone?
  - TLS/SSL downgrade attacks?
- If all the goodies so far are in plain text what is hiding under encryption?
  - I've not looked too much at this yet

What is PII?

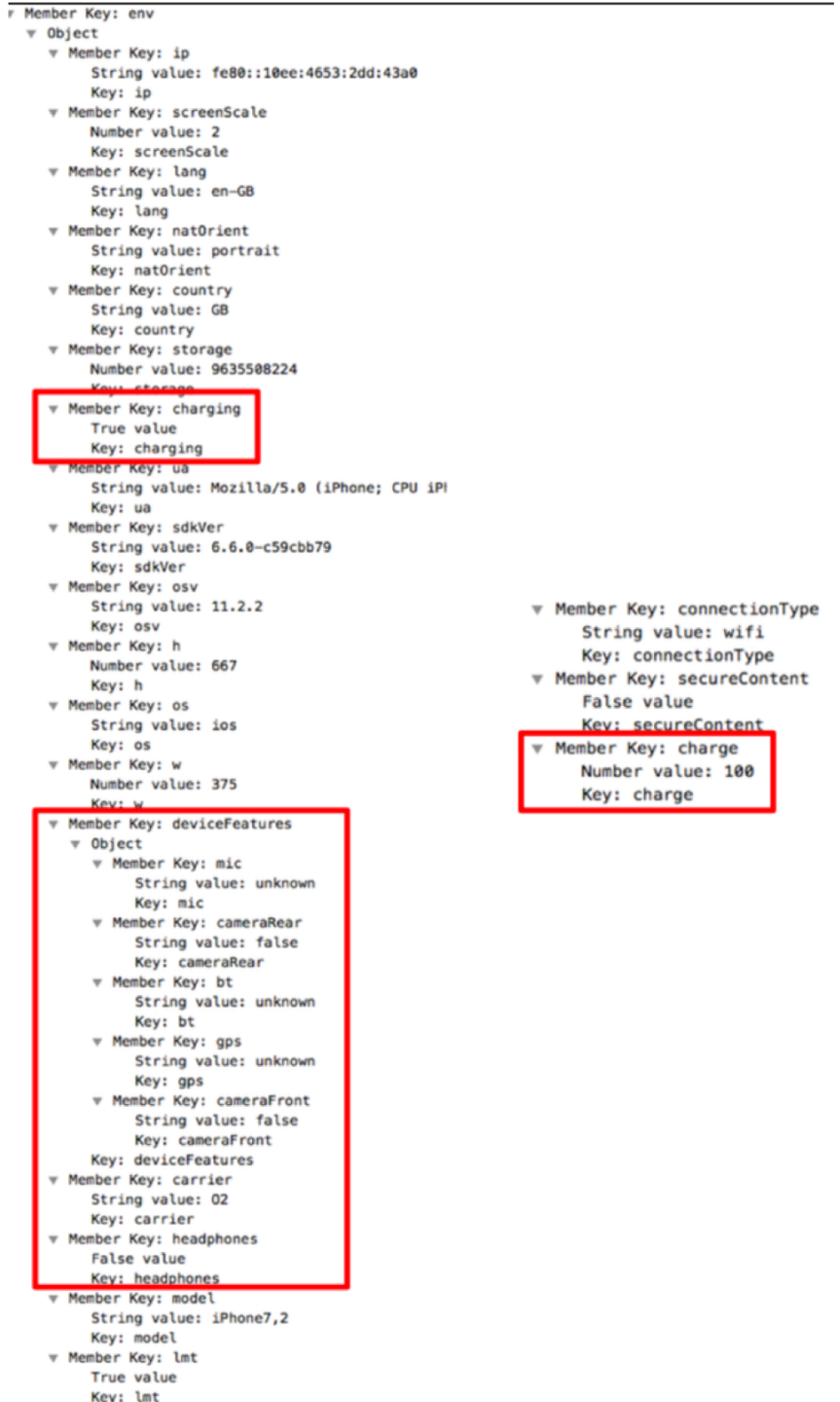
- Personally-Identifiable Information
  - **Anything** that can be used to identify someone/something
- Device Identifier
  - IMEI
  - IP Address
  - Device Serial Number
- User Identifier
  - Name
  - Banking Details
  - Date of Birth
  - Contact Information (Phone Number/Email etc.)
- Location Data
  - Home/Work Address
  - GPS Location
- Credentials
  - Username
  - Email address (again)
  - Password

How can this be fixed?

- Developers: Don't be greedy, only take what you need
  - There's no need for a VPN app to require my age, gender, postcode and how many people live in my house
  - I wish I was kidding



Greedy developers (cont.)



Non-Unique Pre-Shared Keys

- A pre-shared key is required to authenticate to some VPN services
- Similar to how you connect to your home WiFi
- If an adversary knows the PSK they could theoretically impersonate the VPN server and decrypt/eavesdrop connection

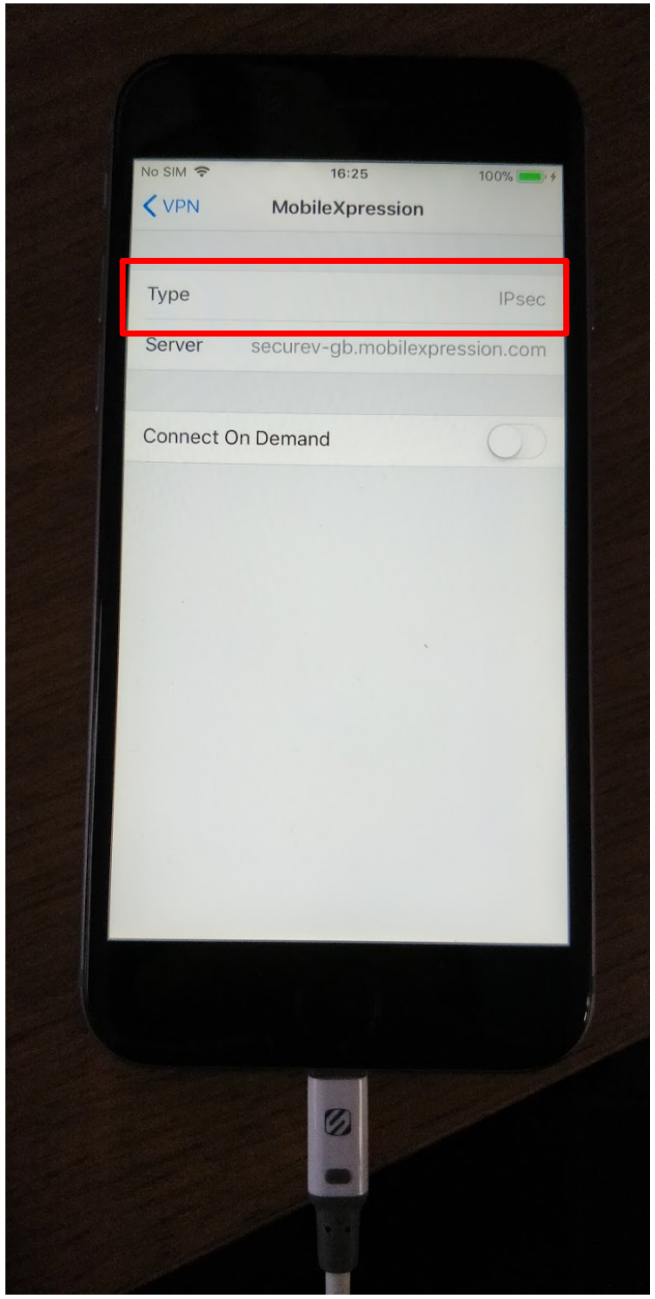
Tunnelling Protocols

- Apple support the following protocols:
  - IKEv2 (with IPSec)
    - Good, secure, fast
  - L2TP over IPSec
    - May be compromised by the NSA
    - Let's not go down the Snowden rabbithole…
  - SSL VPN
    - Light, clientless (works in a browser)
  - PPTP (Deprecated in iOS 10)
    - Insecure, weak encryption

- All apps tested apps (so far) appear to be using IPSec or IKEv2

Tunnelling Protocols

- How to analyse protocols?
  - Some VPN's documentation refers to protocols used/offered
  - VPN config settings within iOS (sometimes) gives this information
  - Not consistent or guaranteed to be accurate



Bro? Bro!

Bro

- Bro Network Security Monitor
  - A very powerful tool
  - Comes with analysers for protocols
  - Open source
  - A royal PITA to get working

Permissions

- Are apps asking for permissions they don't necessarily need?
  - E.g. contacts, camera roll, GPS etc.
  - No evidence of this (so far) in preliminary testing

Malvertising

- Are the third-party ad libraries some developers use known to display malicious adverts?
  - Cryptocurrency miners
  - "Your iPhone has (6) viruses, click here to fix"
- A bit tricky to test in the restricted iOS ecosystem
  - Can't just rip apart an APK
  - Possibly determine ad networks from Wireshark data?

Malvertising on iOS pushes eyebrow-raising VPN app

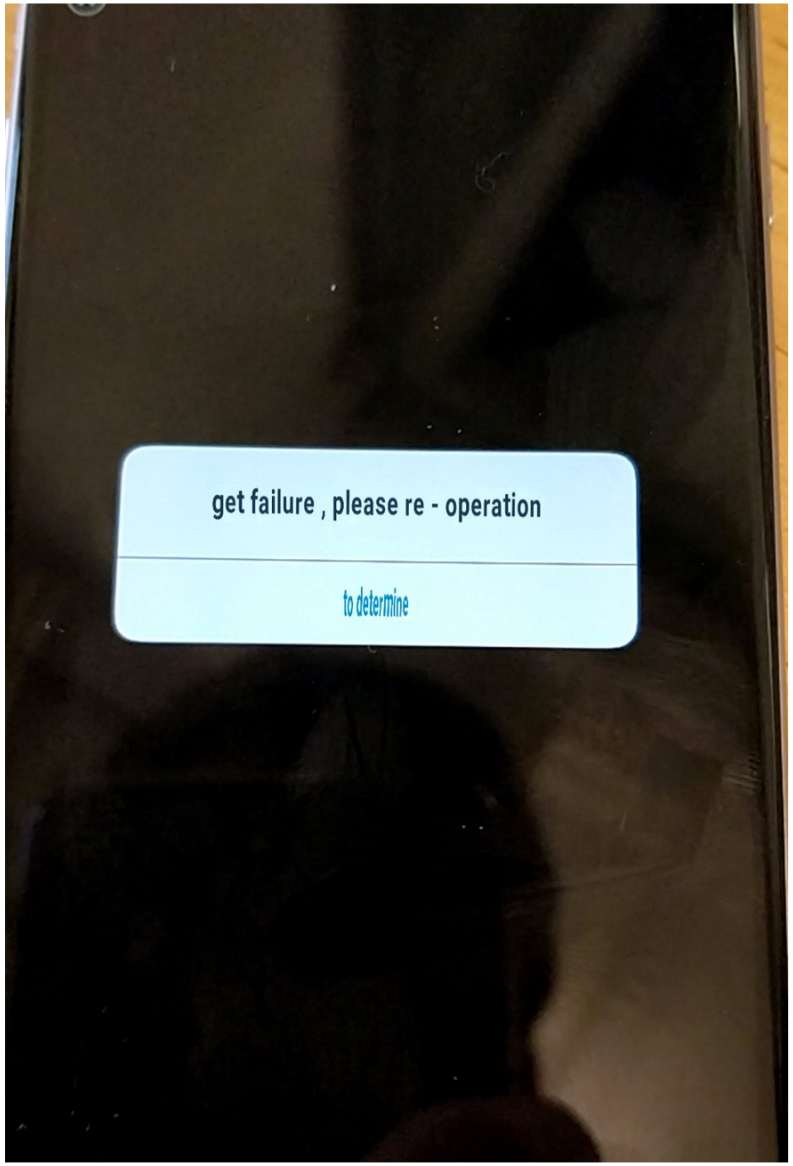
Posted: April 6, 2017 by Jérôme Segura

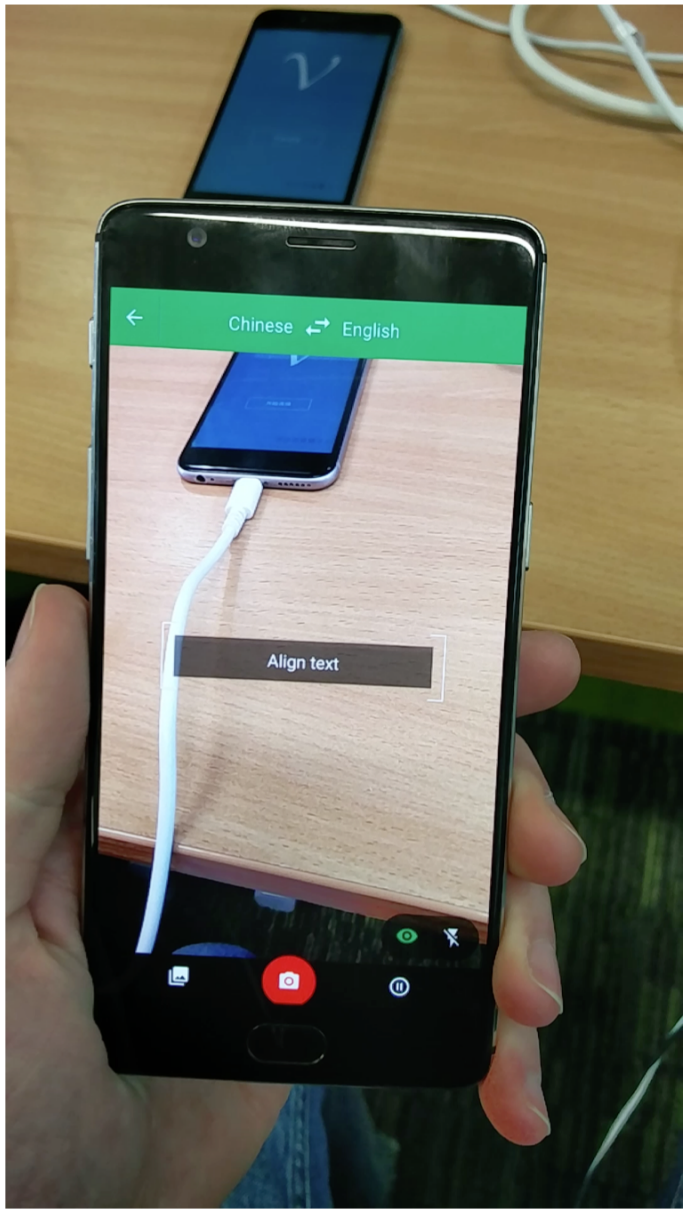
There is a preconceived idea that malvertising mostly affects the Windows platform. Certainly, when it comes to malicious adverts, Internet Explorer is a prime target for malware infections. However, malvertising can produce different outcomes adapted to the device the user is running.

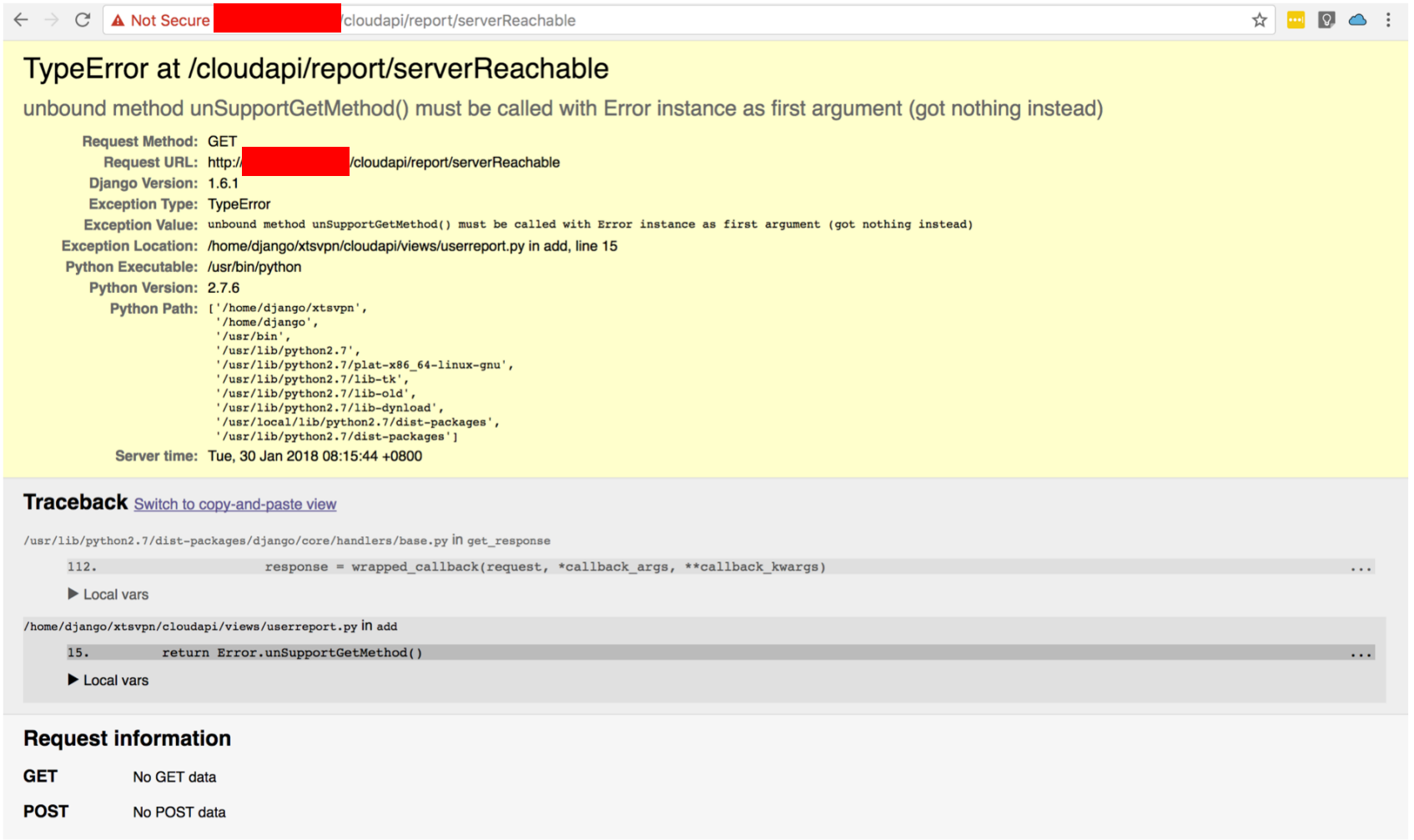
Case in point, we discovered this scareware campaign that pushes a 'free' VPN app called *My Mobile Secure* to iOS users via rogue ads on popular Torrent sites. The page plays an ear-piercing beeping sound and claims your device is infected with viruses.

"We have detected that your Mobile Safari is (45.4%) DAMAGED by BROWSER TROJAN VIRUSES picked up while surfing recent corrupted sites."

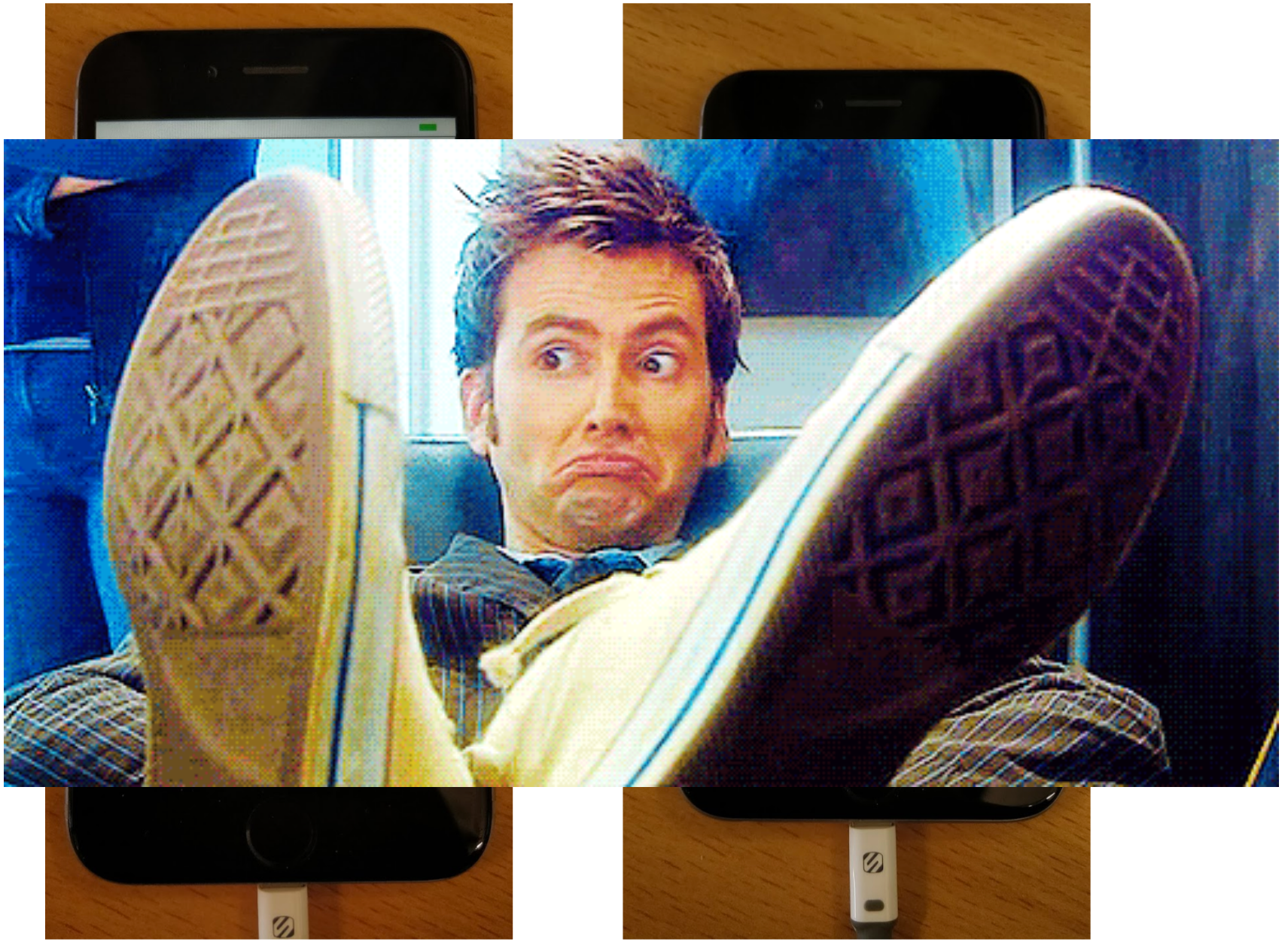
Other weird findings


get failure , please re - operation
to determine


Chinese
English
Align text



Django 1.6.1 was released December 2013.
CVE's for XSS, CSRF, DoS…



```
GET /downloads/config/whalevpn_config.zip HTTP/1.1
```

Hot(ish) off the press!

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

- Hotspot Shield
- 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

h/t @0x0304 for sending the article

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

Cryptostorm

- Disclaimer: I haven't looked into this a lot, but from looking at their website they seem to be doing things right
- VPN provider
- Bare metal servers
- Self-compiled, gr-sec hardened kernel
  - Access control and memory-corruption prevention
- Open source
- Primarily based in Iceland but generally decentralized as a company
- Token-based authentication for 'anonymity'
- Blockchain-based DNS (using DNScurve for encryption)

Results

Let’s see some statistics

29 apps tested (so far)

- Note: Most apps work, a couple are broken
- 75% leak DNS
  - Almost all of these use Google DNS (8.8.8.8)
- 77% send any traffic over HTTP
  - Majority of these apps send confidential data over HTTP
  - Usernames, passwords etc.
- 2 apps were fully in Chinese
- A few apps were shut down by the Chinese government
- 1 app charged me £28 for a free trial
  - Symantec
- 1 VPN server was hosted on the same server as an Italian Hotel's website

Game Plan

- Look more into Algo/Cryptostorm
- Test a well-renowned app for a good baseline standard
  - VyprVPN/NordVPN/PIA etc.
- Test more apps for a larger set of results
- Test more for TLS interception/PSK stuff
- Write 10,000 word dissertation
- Write guidance for devs
- Responsible disclosure
- 52 days and counting…

Questions/ Comments/ Feedback?

- Now
- Chat to me if you see me
- Afterparty
- Twitter (@iJackWilson)

- Dissertation journal/proposal available at bit.ly/JacksDJ
- These slides + other work at www.jack.lu/blog

IT DEPENDS