iOS VPN Security

Jack Wilson

Obligatory $whoami

- 4th year student
- Intern Security Consultant @ SBRC
- I got to a lot of conferences
  - Ask me about the Blackhat scholarship
- You've probably seen me in the corner of the Hacklab cursing idiot iOS developers
  - This talk is why

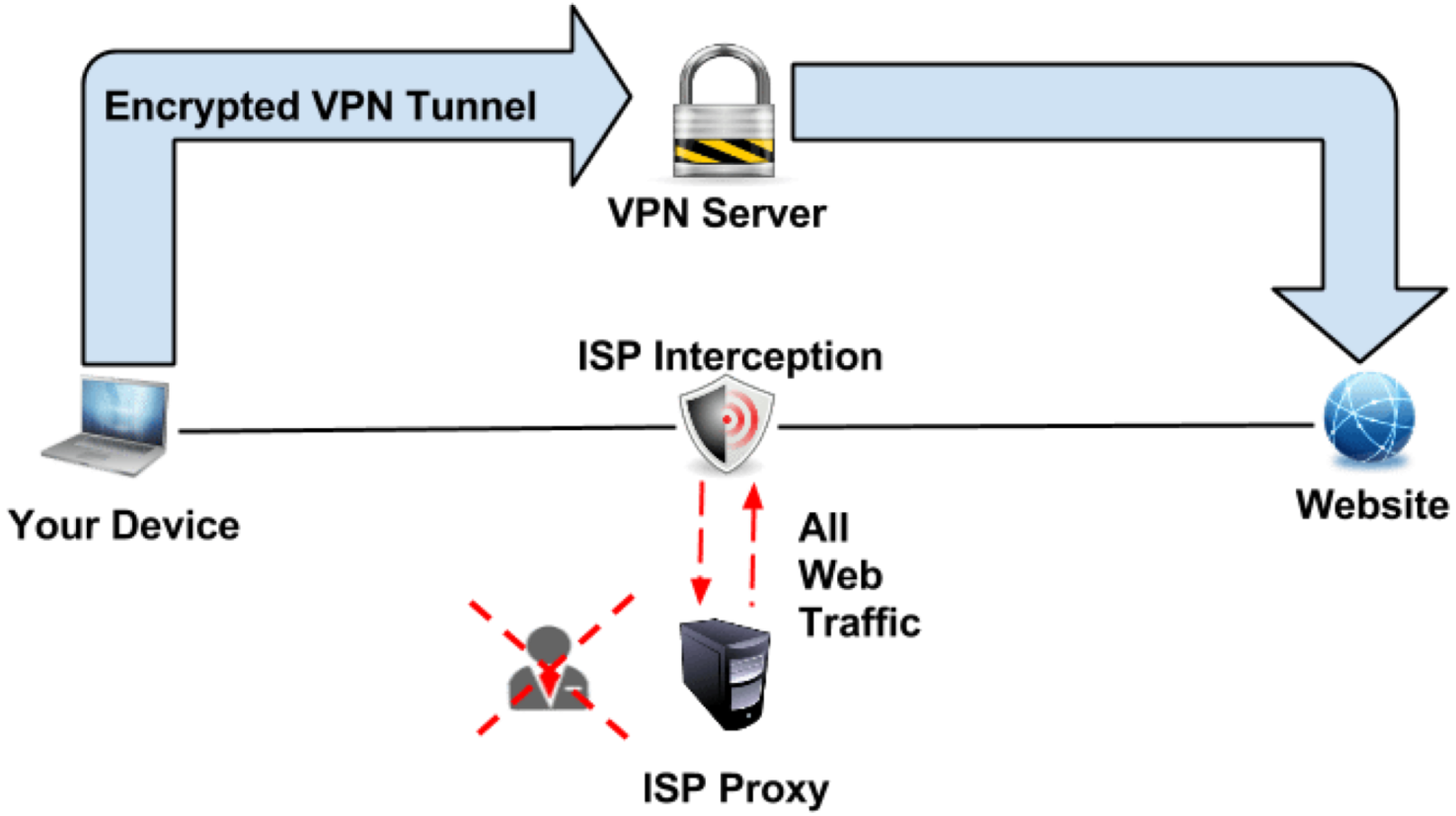
Why iOS VPN Security?

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?



- Fun fact: Did you know it's against the acceptable usage policy to use a VPN on eduroam?

Threat Models

- Why you SHOULD use a VPN
  - Security on public Wi-Fi
  - Avoid 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
  - To be anonymous
    - Privacy != Anonymity
    - "If your threat model (sec.) includes the NSA, do not use the internet" –The Grugq

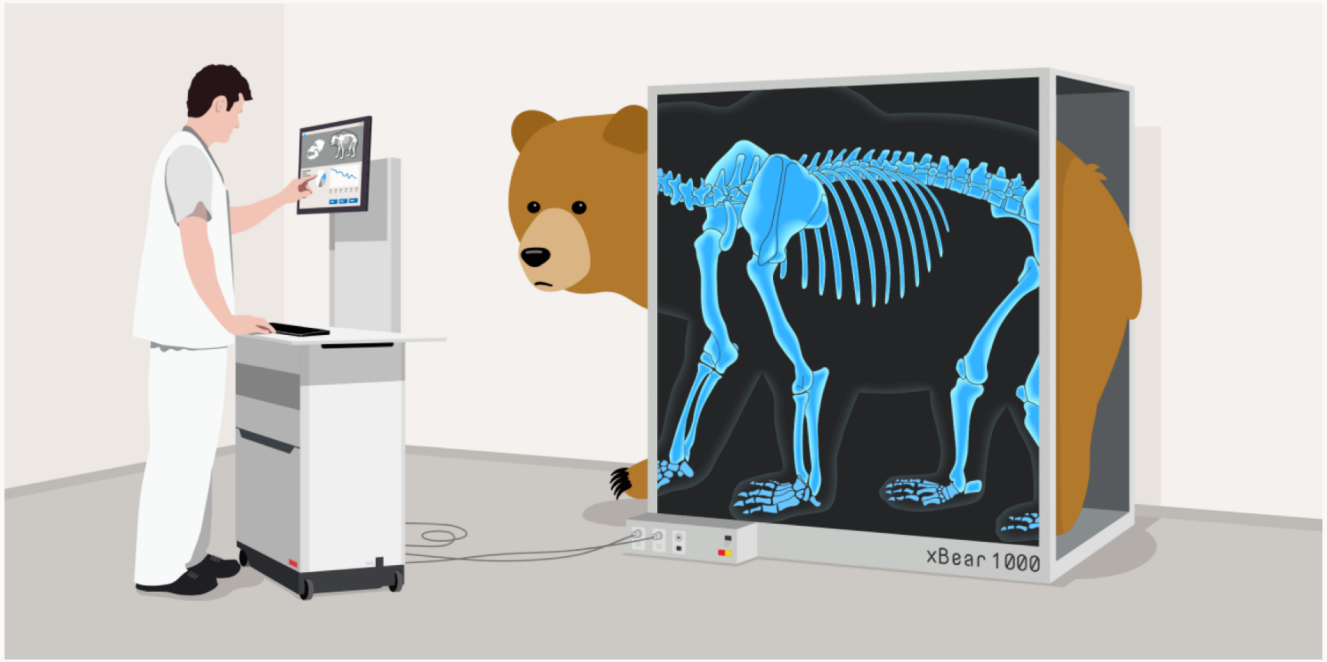
Trust

- 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

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
- 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
```

You'd be wrong

```
&pass=7c6a180b36896a0a8c02787eeafb0e4c
```

```
▼ <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?

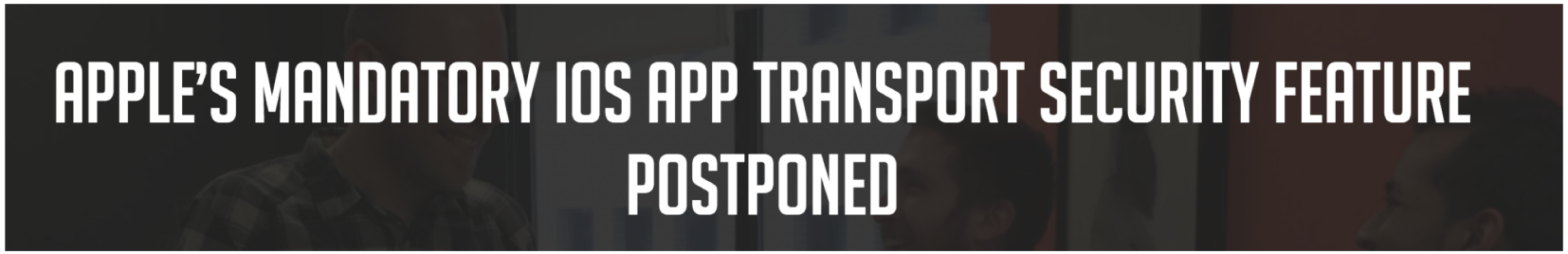
How can this be fixed on a larger scale?

SECURITY

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

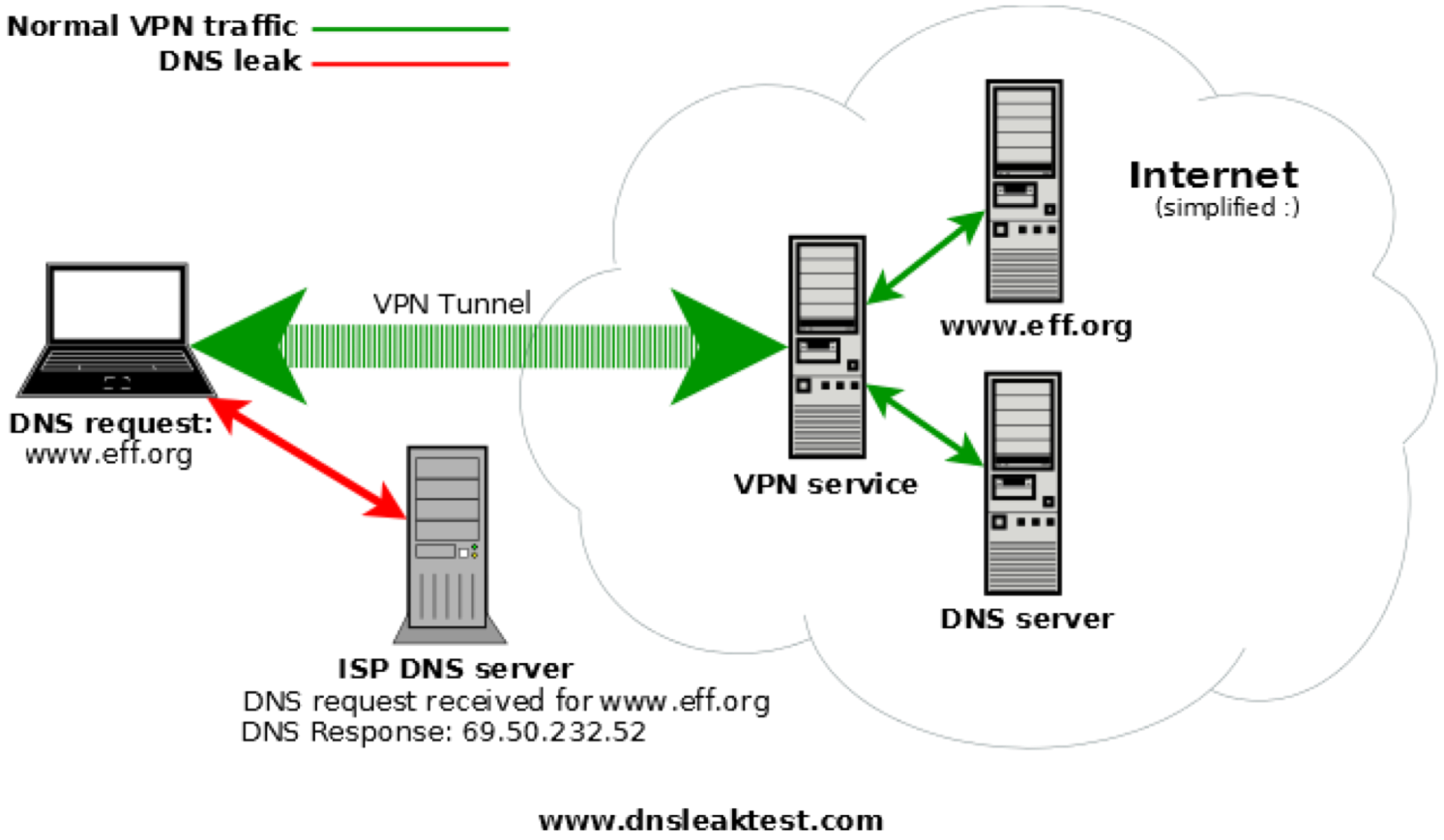
At a session at the 2016 WWDC, Apple revealed that it would be requiring all iOS apps to use HTTPS connections through an existing feature called App Transport Security by the end of the year.

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
  - Not an ISP or Google
- DNSSEC
  - Verifies correct DNS server is responding to requests to prevent poisoning attacks
- 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

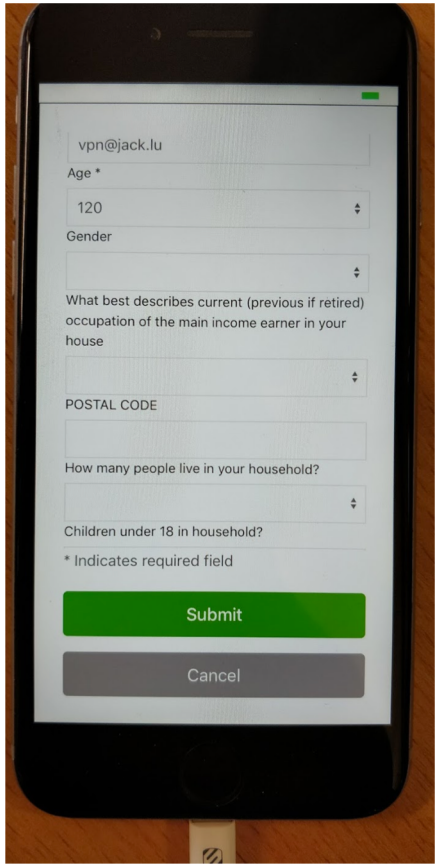
- Determining what information apps are sending that could uniquely identify a person/device
  - Install Burp certificate on phone?
  - TLS/SSL downgrade attacks?
- If all the goodies so far are in plain text what is hiding under encryption? 🤔
  - I've not looked too much at this yet

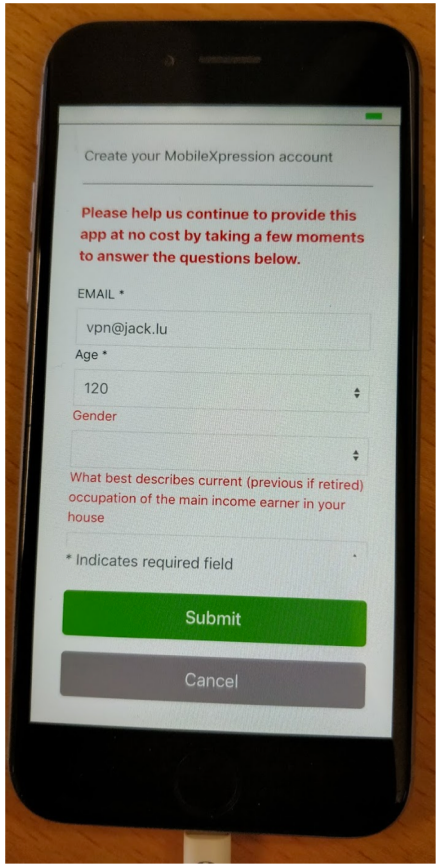
What is PII?

- 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





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
  - SSL VPN
    - Light, clientless (works in a browser)
  - PPTP (Deprecated in iOS 10)
    - Insecure, weak encryption

Tunnelling Protocols

- How to analyse protocols?
  - Some VPN's documentation refers to protocols used/offered
  - Not consistent or guaranteed to be accurate

Bro? Bro!

Bro

- Bro Network Security Monitor
  - A very powerful tool
  - Comes with analysers for protocols
  - Also 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

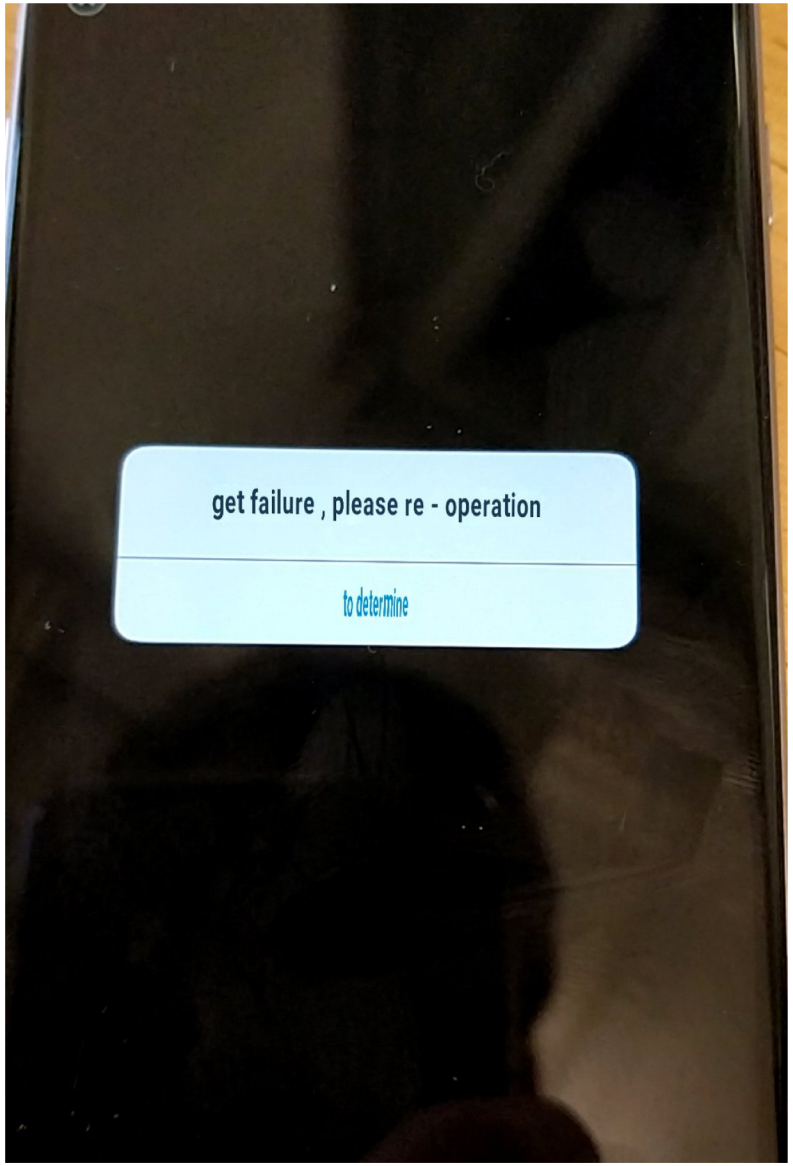
Posted: April 6, 2017 by Jérôme Segura

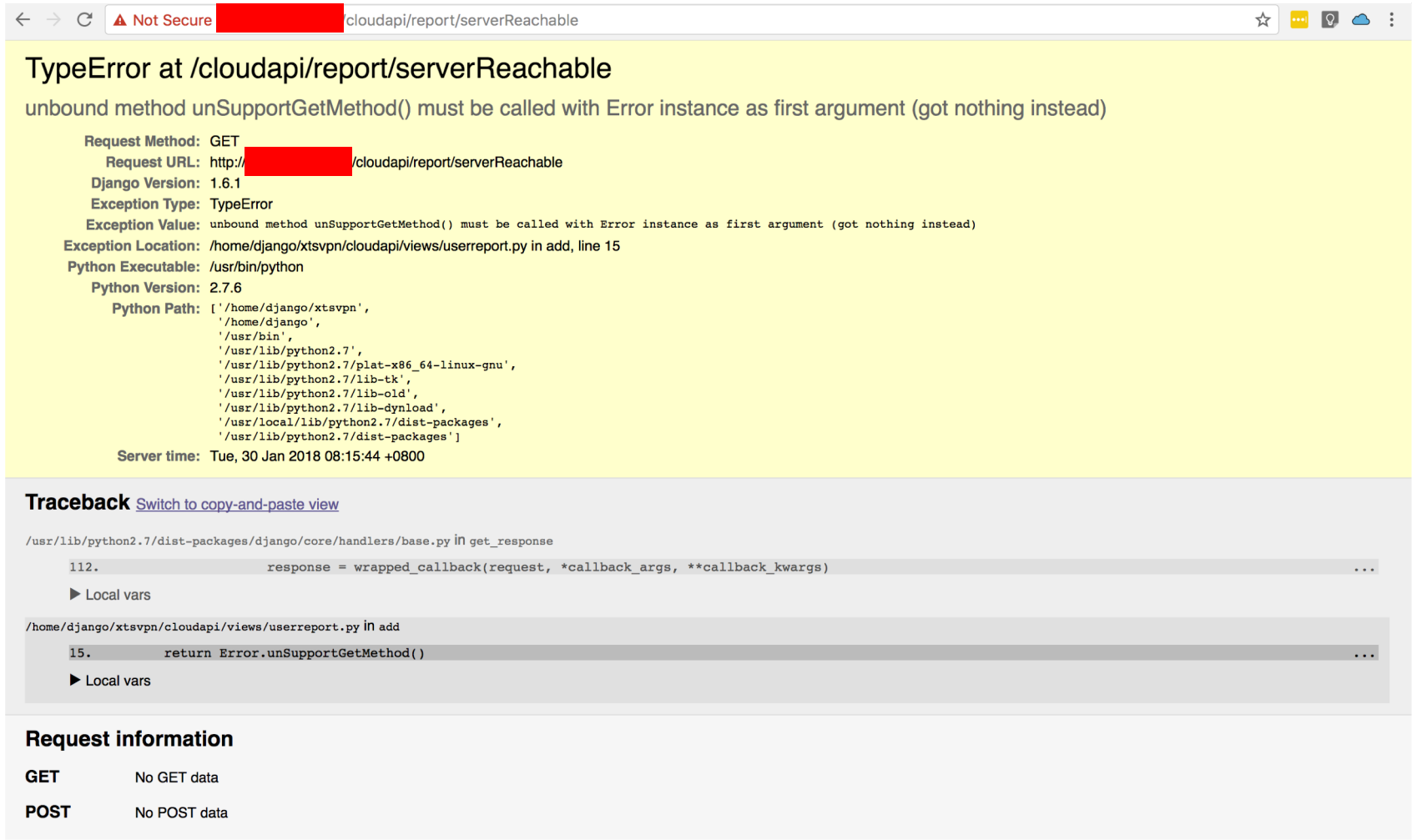
There is a preconceived idea that malvertising mostly affects the Windows platform. Certainly, when it comes to malicious adverts, Internet Explorer is a prime target for malware infections. However, malvertising can produce different outcomes adapted to the device the user is running.

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.

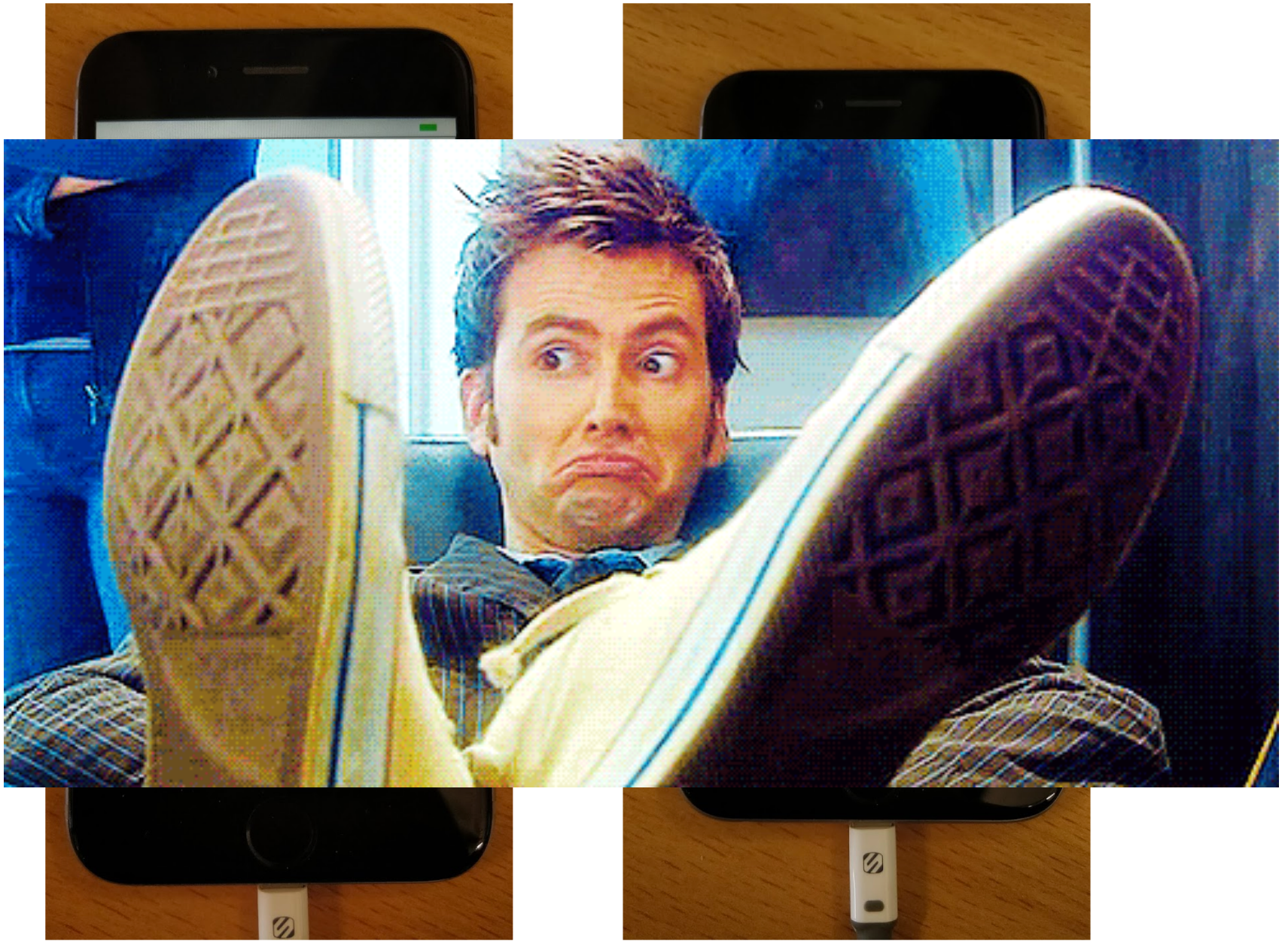
"We have detected that your Mobile Safari is (45.4%) DAMAGED by BROWSER TROJAN VIRUSES picked up while surfing recent corrupted sites."

Other weird findings


get failure , please re - operation
to determine



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



Hot 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 Mikey for sending the article

Algo?

- Roll your own VPN
  - Works 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

Let’s see some statistics

17 apps tested (so far)

- Note: Some apps work, some are broken
- 100% leak DNS
- 80% send any traffic over HTTP
  - 57% 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
- Test a well-renowned app for a good baseline standard
- Test more apps for a larger set of results
- Test more for TLS interception/tunnelling protocol/PSK stuff
- Write dissertation
- Write guidance for devs

Questions?

- Now
- Pub
- Twitter (@iJackWilson)
- Slack (@jack)

- Dissertation journal/proposal available at bit.ly/JacksDJ
- Other work at www.jack.lu/blog