DC4420 - 31ST JULY 2018

VPN'S & YOU

OBLIGATORY $WHOAMI

- Jack Wilson
  - Scot in London
- BSc (Hons) Ethical Hacking graduate
  - Abertay University, Dundee
- Associate Security Consultant @ Gotham Digital Science
- Likes privacy and offensive security

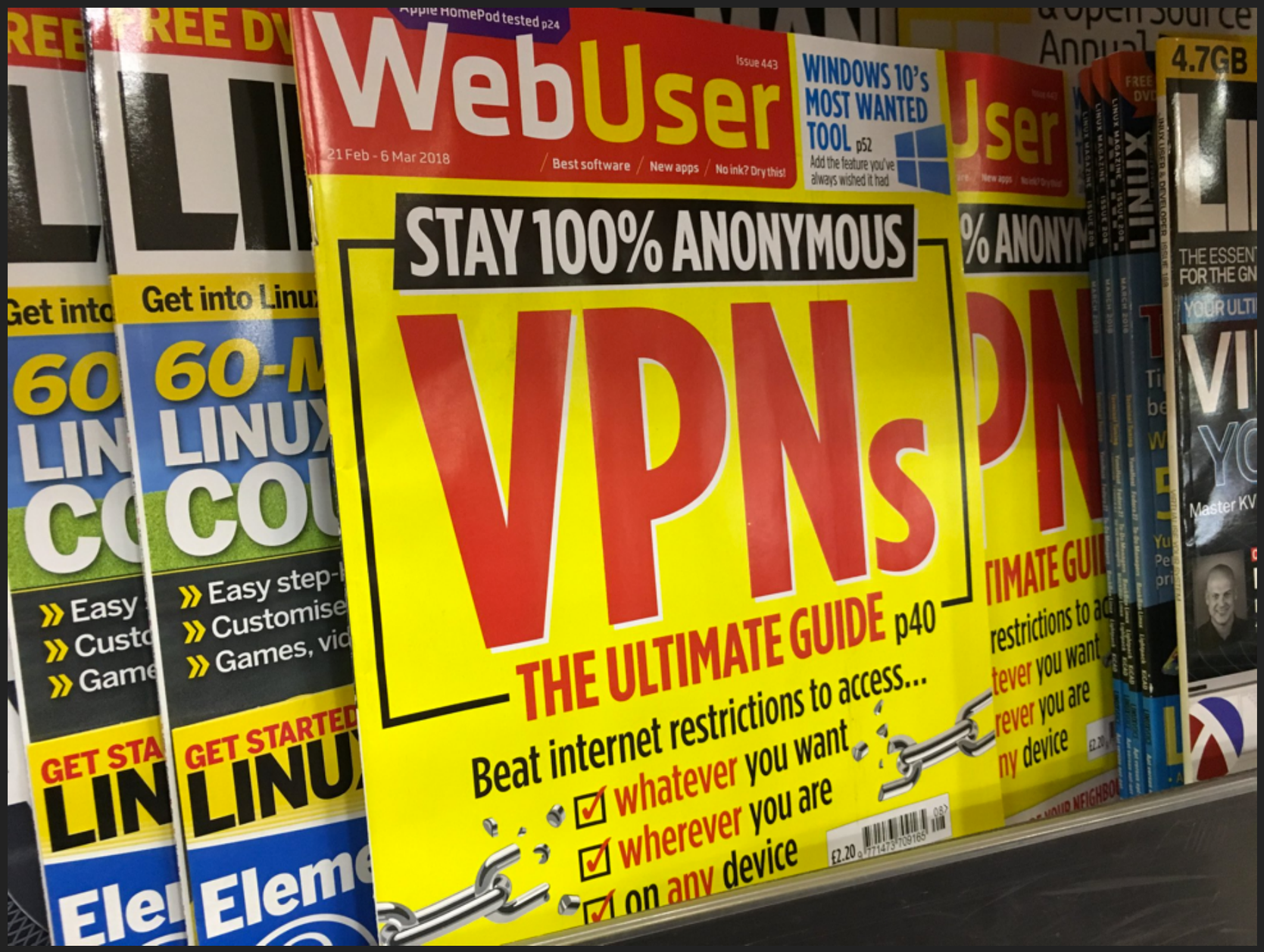
QUICK DISCLAIMER(S)

- I'm not a dev
- I'm not a lawyer
- I'm not the most experienced in the room
  - pls no low-level TCP/IP questions
- Opinions are my own, etc.

WHY VPN SECURITY?

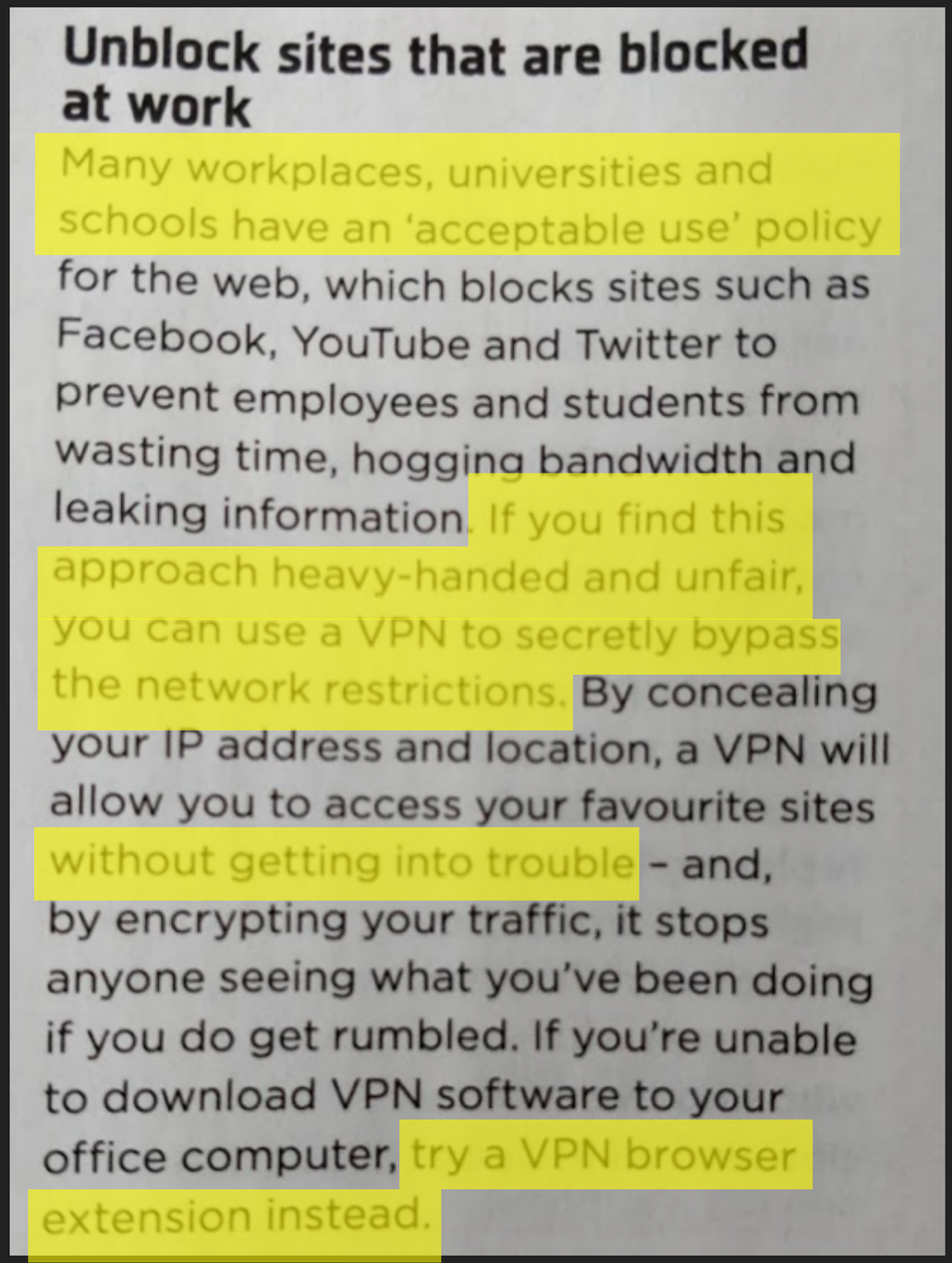
WHY VPN SECURITY?

h/t @Neil_Neilzone



NOTES FROM THE ARTICLE

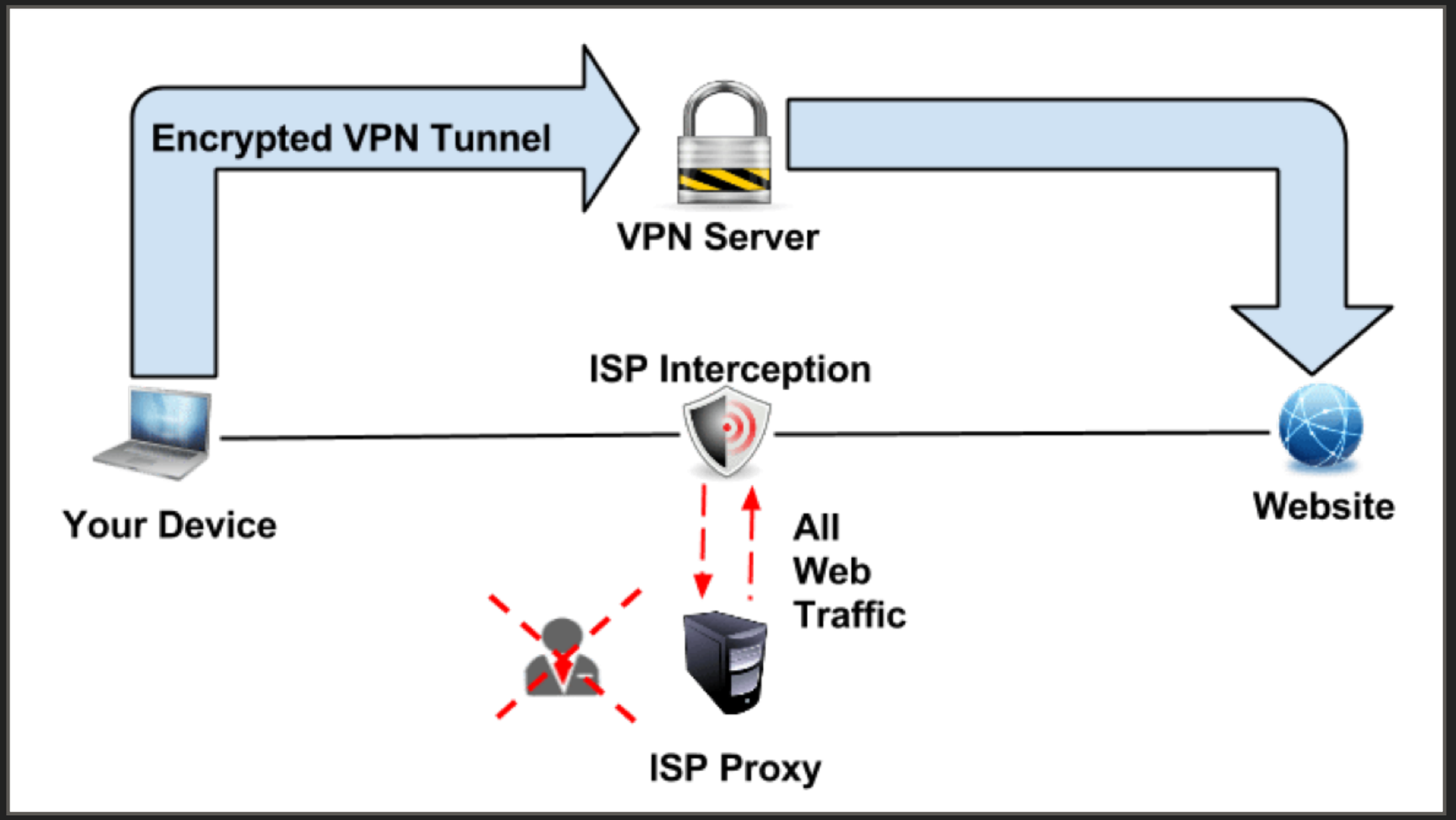
- This issue is wider than one article
- This article is (fairly) recent
- The “Stay 100% Anonymous” claim is garbage
- The image (right) is terrible advice



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.

BASICS FIRST: WHAT IS A VPN?



THREAT MODELS

WHY YOU SHOULD USE A VPN

- Security on public WiFi
- Avoiding tracking by ISP's
- Avoiding geo-restrictions/appearing somewhere you are not (kind of)
  - Netflix has decent VPN detection, Chinese gov doesn't
- Avoiding advertisers tracking you (kind of)
  - 🍪

WHY YOU SHOULDN'T USE A VPN

- To do illegal stuff
  - VPN providers can and (sometimes) will work with law enforcement
- 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 logs” VPN service that they claim
- Will they sell your data?
- Will they fiddle with your traffic?

OTHER THINGS TO LOOK FOR

- Self-hosted vs third-party infrastructure
- 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 (plaintext vs crypt etc.)
- Country of incorporation (legal jurisdiction)

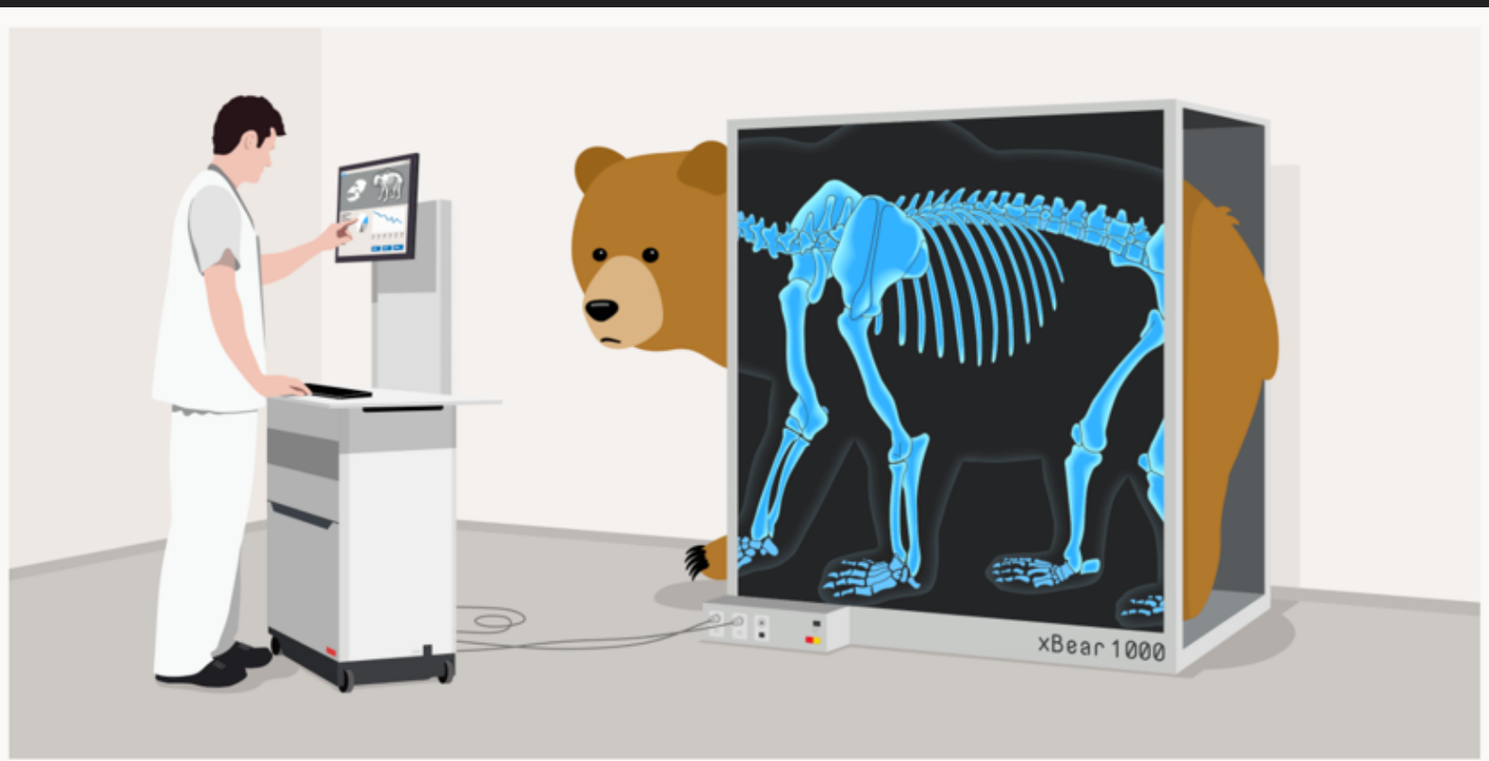
via Kenn White (@kennwhite)

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

A VPN SIMPLY MOVES TRUST FROM YOUR ISP TO THE VPN PROVIDER

VPN PROVIDER TRUST EXAMPLES

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.

MCAFEE BUYS TUNNELBEAR

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.

NEWSLET

The Daily Cr
Get the top te
to your inbox

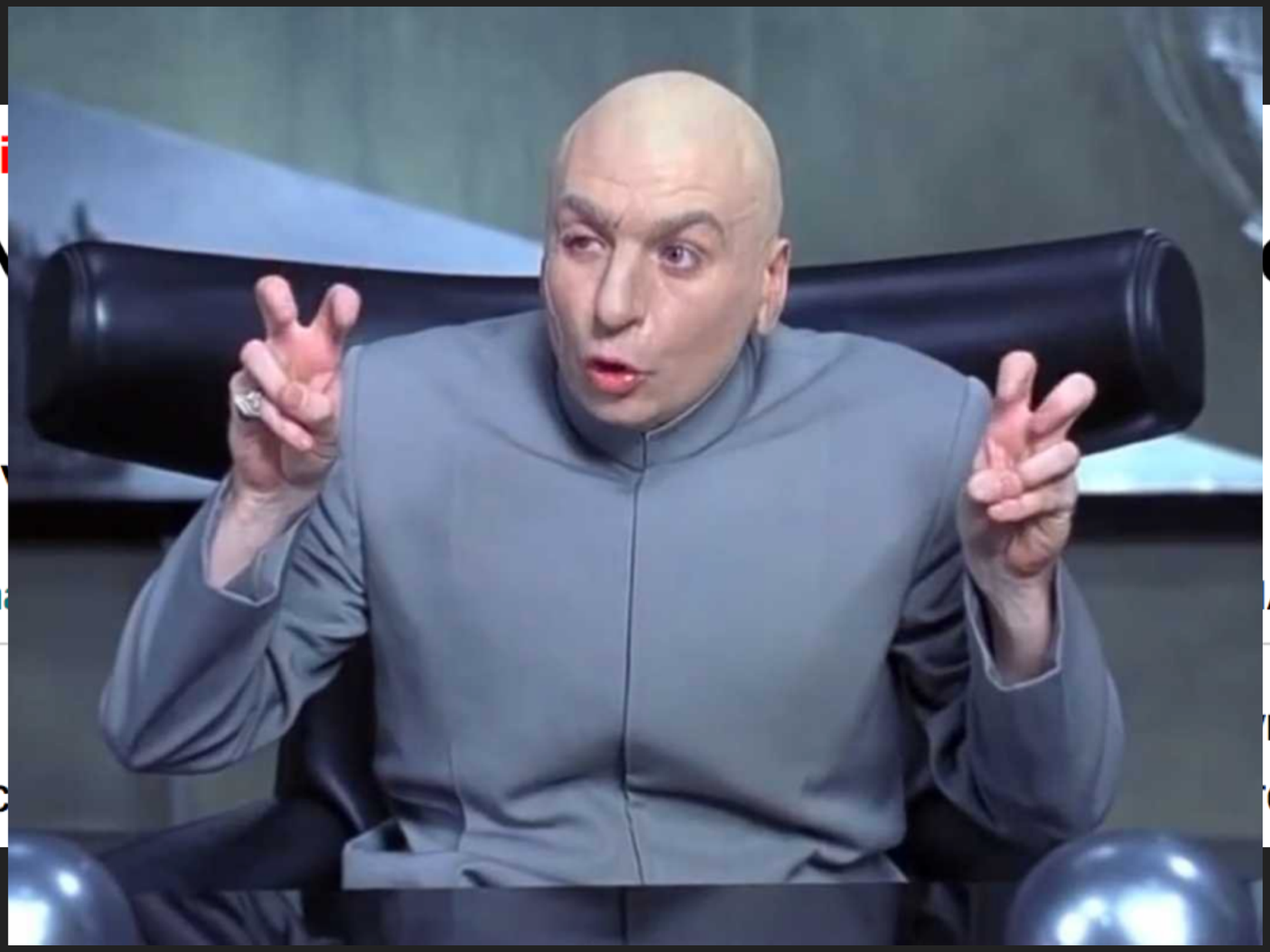
TC Weekly R
Get a weekly
stories

Crunchbase
The latest sta

Enter your email

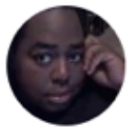
protected by
Privacy · Terms

"NO LOGS" VPN SERVICE CATCHES A STALKER



VPN P2P NETWORK?

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 part is debatable, but the exit node part is an issue

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

VERIZON VPN?

Verizon's Safe Wi-Fi is an ad-blocking VPN that costs only $3.99 a month

By Shannon Liao | @Shannon_Liao | Jul 27, 2018, 3:40pm EDT

- "The Safe Wi-Fi app includes McAfee software which allows the security functions of the Safe Wi-Fi app to operate on Your device"
- Privacy policy redirects to McAfee privacy policy
- Collects *a lot* of user data

Source: https://twitter.com/Cauchon/status/1022985740077039616

We may also collect other information from or about you, such as information about what products you purchased, your interests, demographic information, photographs and videos, and biometric data such as fingerprints or voice prints. You may also provide us with additional data.

We automatically collect information about your interactions with the Services as well as devices on which the Services are installed. In some cases, we automatically collect information about other devices connected to the same network as the device on which the Services are installed.

For example, we may collect and use the following:

- Information about the products you looked at or searched for and the Services you used, including time spent and other statistical information;
- Details about your computers, devices, applications, and networks, including internet protocol (IP) address, cookie identifiers, mobile carrier, Bluetooth device IDs, mobile device ID, mobile advertising identifiers, MAC address, IMEI, Advertiser IDs, and other device identifiers that are automatically assigned to your computer or device when you access the Internet, browser type and language, language preferences, battery level, on/off status, geo-location information, hardware type, operating system, Internet service provider, pages that you visit before and after using the Services, the date and time of your visit, the amount of time you spend on each page, information about the links you click and pages you view within the Services, and other actions taken through use of the Services such as preferences. We may collect this information through our Services or through other methods of web analysis; and

Contact us

Feedback

We may also collect other information from or about you, such as information about what products you purchased, your interests, demographic information, photographs and videos, and biometric data such as fingerprints or voice prints. You may also provide us with additional data.

What's the moral of the story?

Privacy policies can be as important as technical spec

THE DISSERTATION

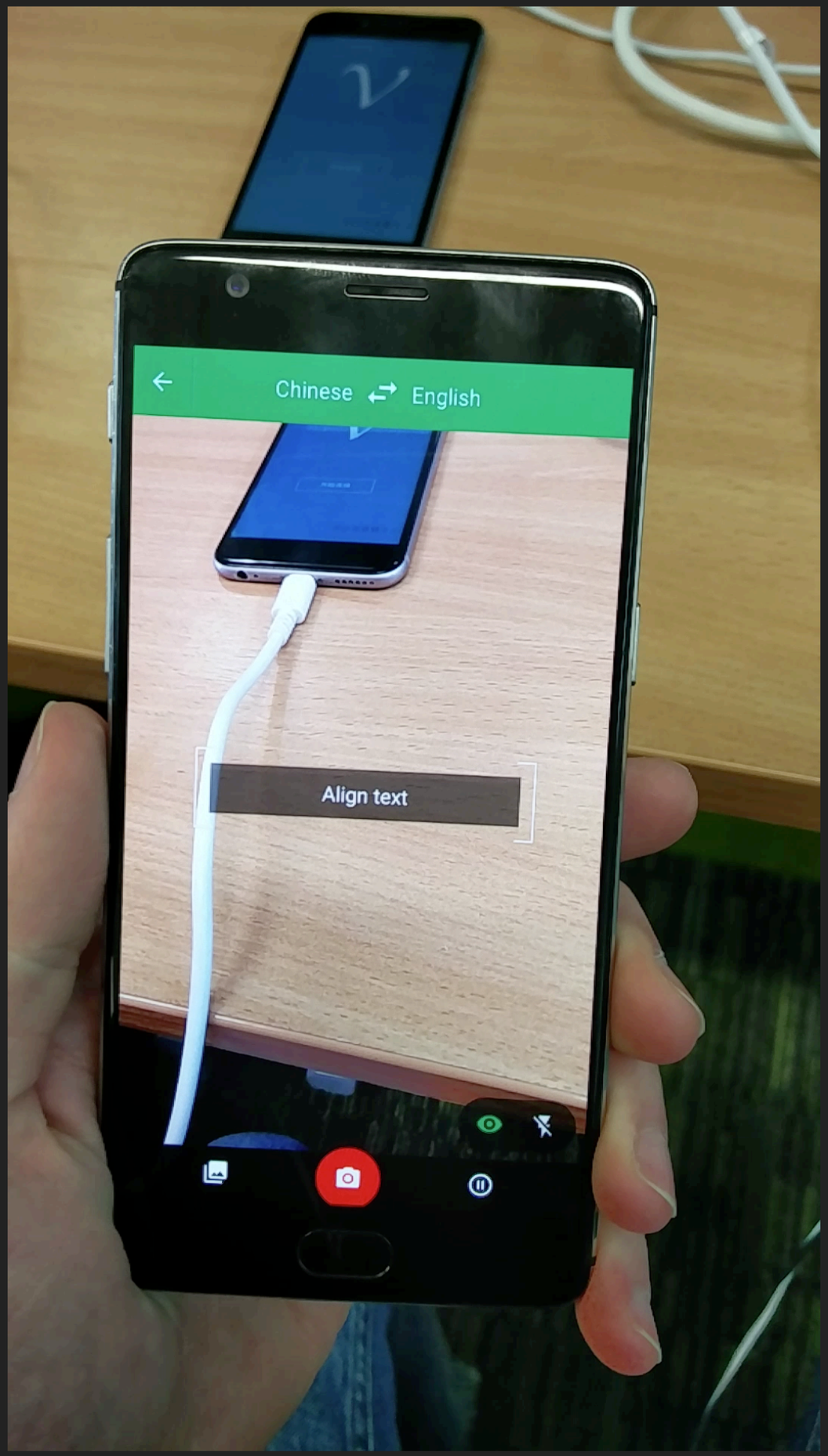
TAKE A BUNCH OF IOS VPN CLIENTS AND TEST FOR:

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

WHAT'S THE POINT?

- Get an overview of the state of security within the free/ cheap market
  - Most consumers will look at this price range
- To write guidance for developers

THE TESTING CRITERIA


Chinese
English
Align text

HTTP

- Unencrypted web traffic
- 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
```

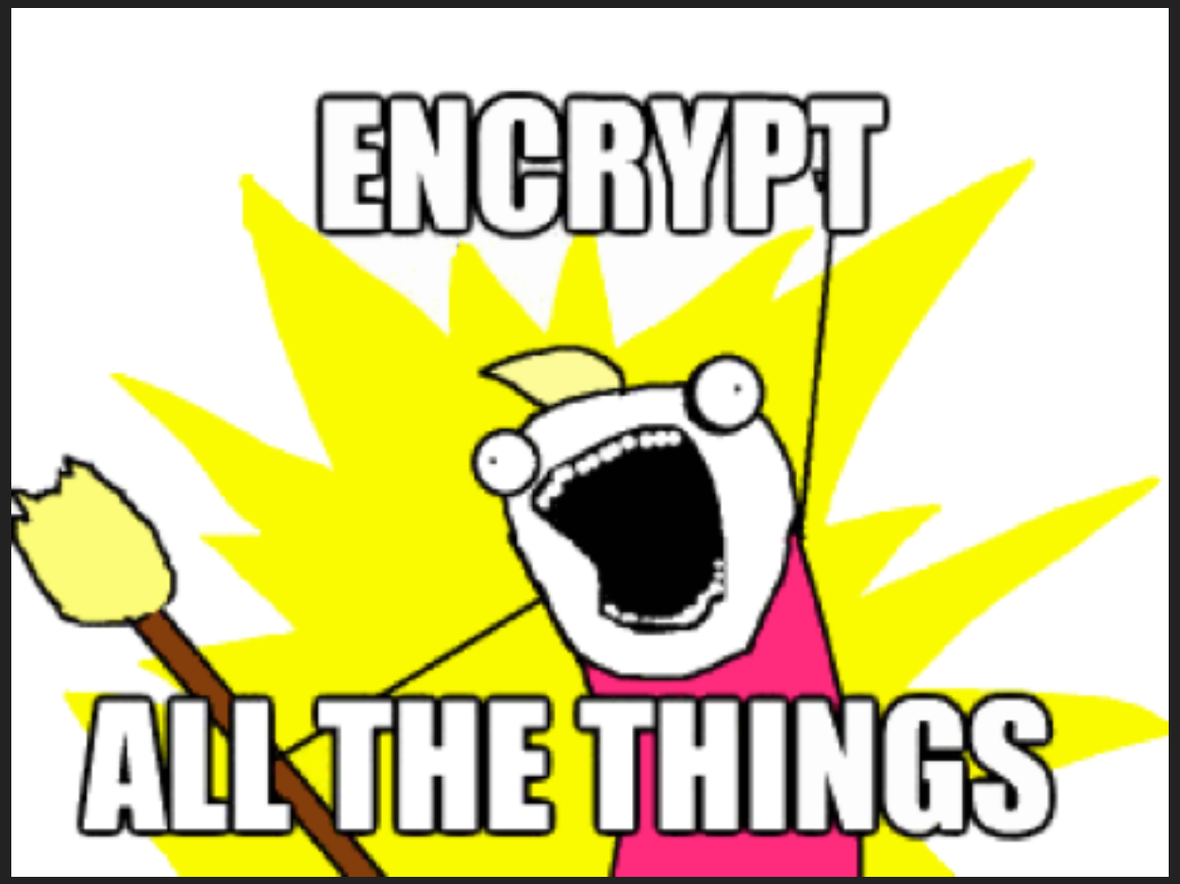
```
▼ Member Key: username
    String value: 58554cb5ad71e8977c06a94c2bd2a99a
    Key: username
▼ Member Key: password
    String value: iMEGODmd
    Key: password
```

```
▼ <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-partied (e.g. advertising)
  - User privacy vs 💰 💰 💰

HOW CAN THIS BE FIXED ON A LARGER SCALE?

SECURITY

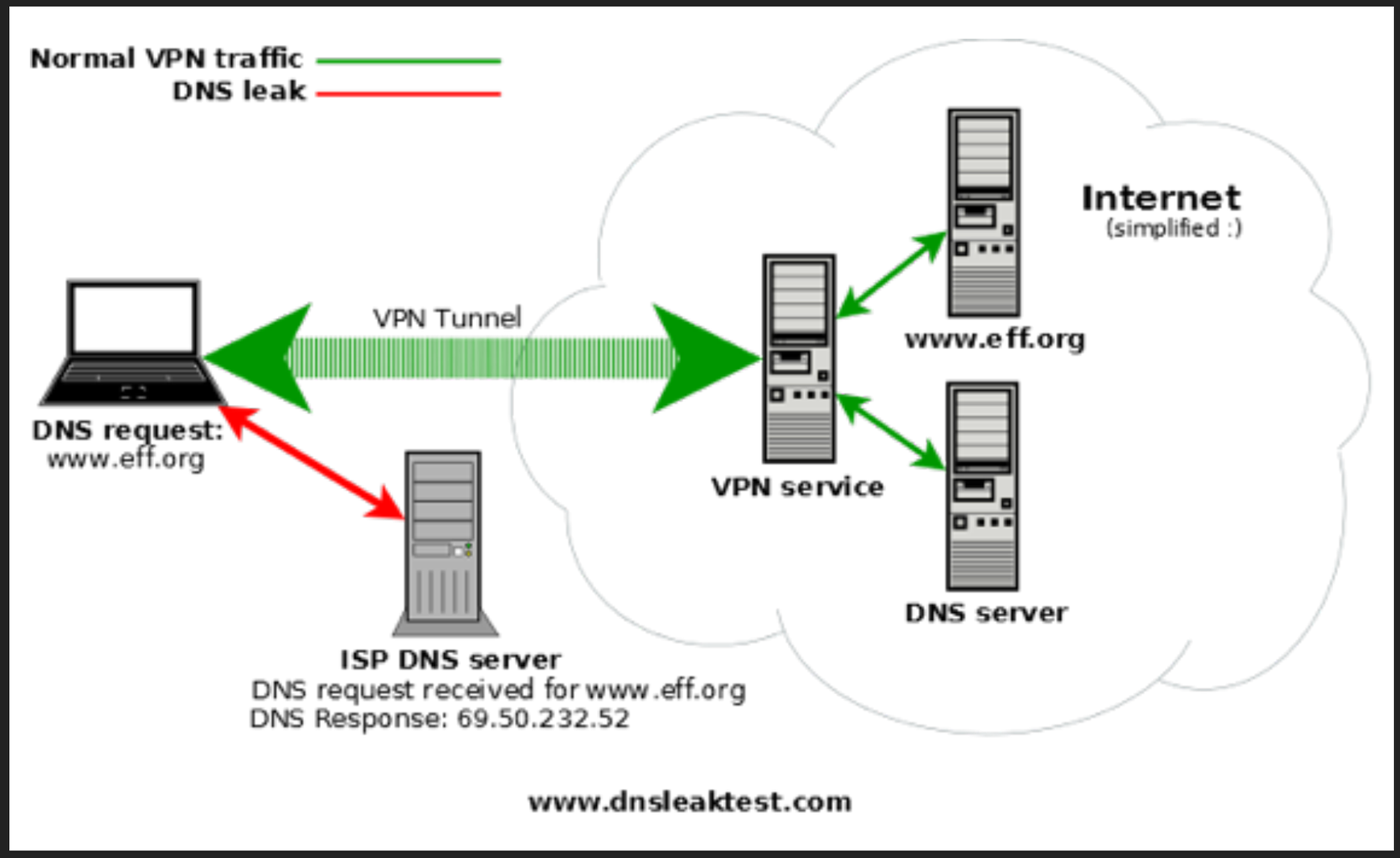
WWDC 2016: Apple to require HTTPS encryption on all iOS apps by 2017

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, 12:14 PM PST

APPLE'S MANDATORY IOS APP TRANSPORT SECURITY FEATURE POSTPONED

DNS LEAKAGE


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

DNS LEAKAGE

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

HOW CAN THIS BE FIXED?

- In a perfect world?
  - VPN providers running their own DNS
  - This would centralise trust
- At a minimum
  - Using a ‘trusted’ and/or ‘secure’ DNS provider
  - This will mean different things to different people
  - Probably not your ISP or Google
  - Quad1 or Quad9?
- Honourable mention: DNS over TLS
  - Encrypts DNS traffic (with/without VPN)
  - Avoids anyone sniffing traffic from viewing your DNS requests

TUNNELLING PROTOCOLS

- Apple support three protocols on iOS 10+
  - IKEv2 (with IPSec)
    - Secure, fast
    - IPv6 support
    - Stability between network changes
  - L2TP over IPSec
    - *Possibly* compromised by the NSA
  - SSL VPN
    - Browser-based
    - Not really used for consumer VPN's, more for business use

TESTING FOR PROTOCOL IMPLEMENTATION

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

PERMISSIONS

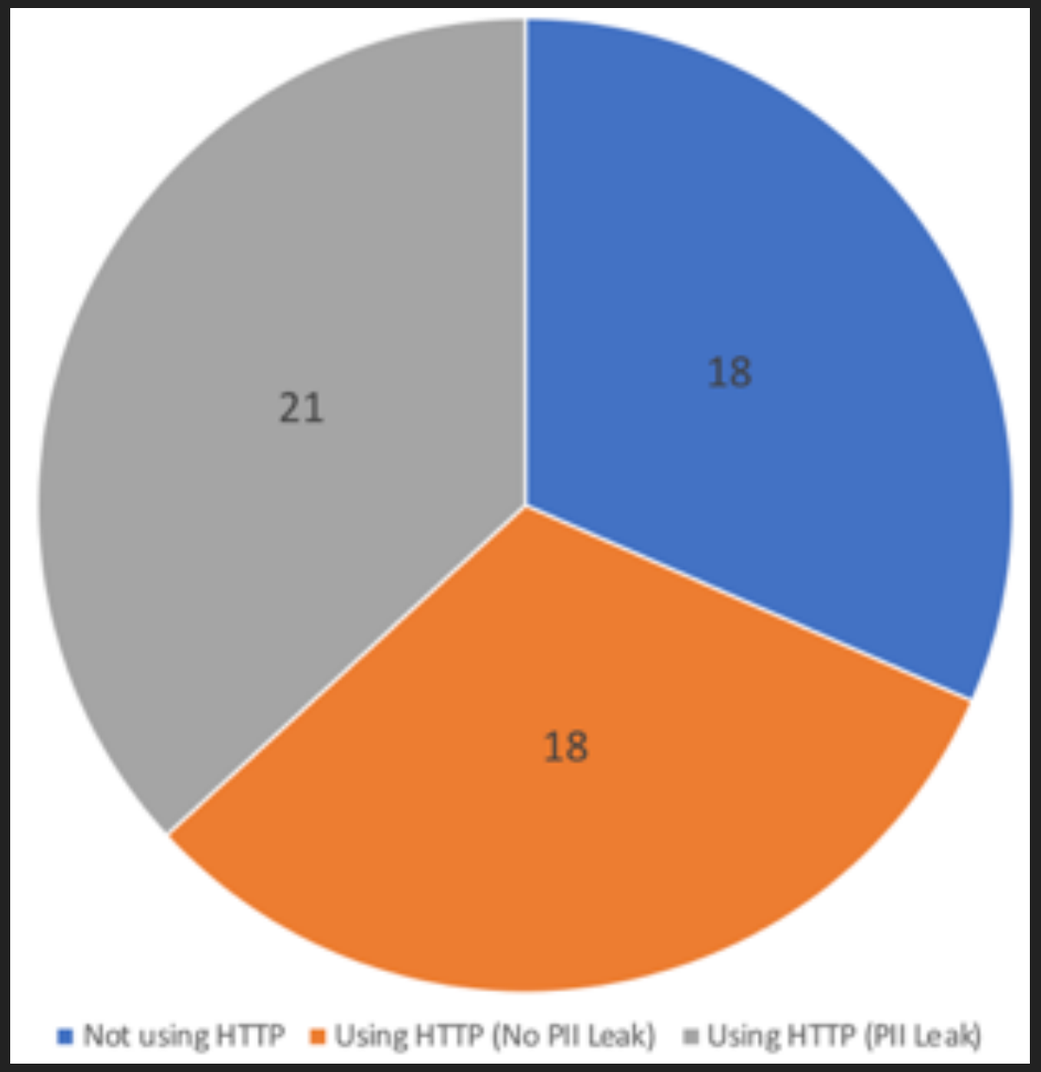
- Are apps asking for permissions they don’t necessarily need?
  - E.g. contacts, camera roll, GPS etc.
- Tested by interacting with app and recording permissions that were requested

57 APPS TESTED

RESULTS

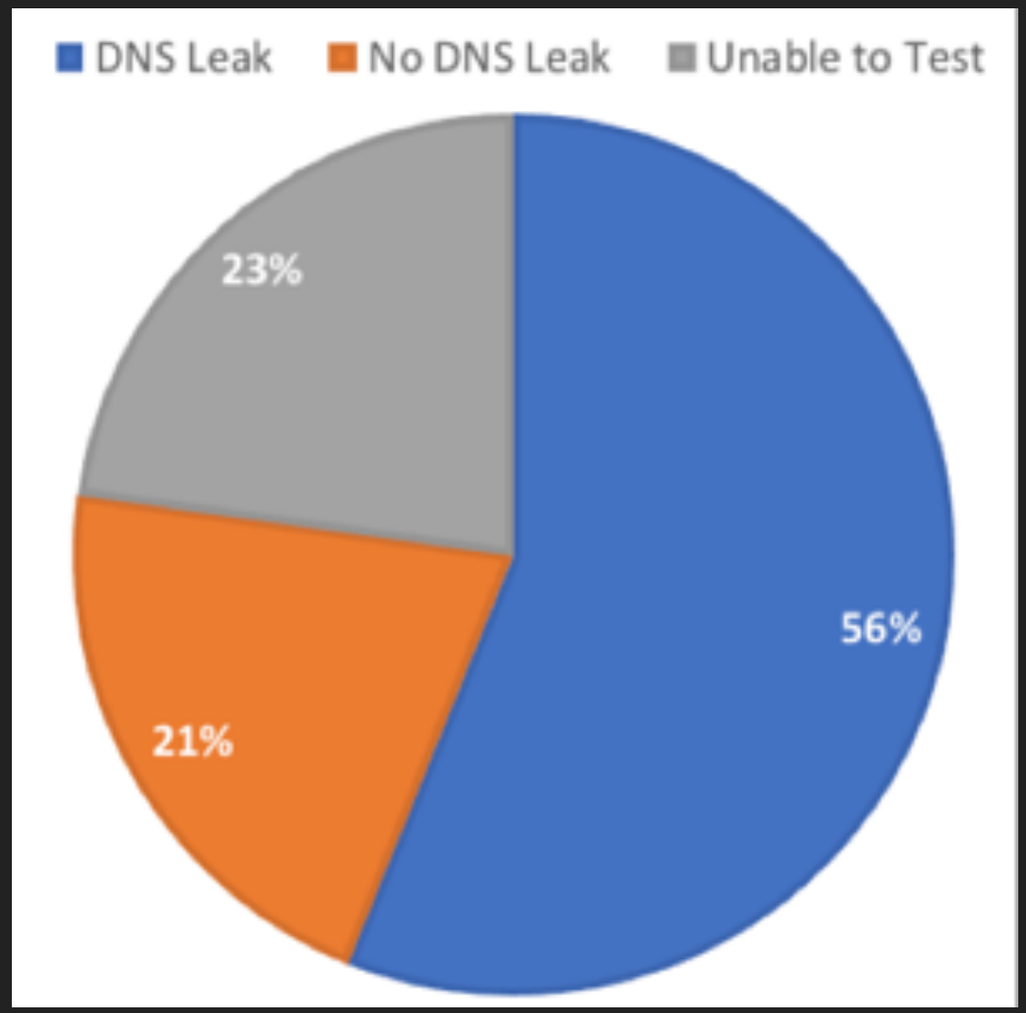
HTTP

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



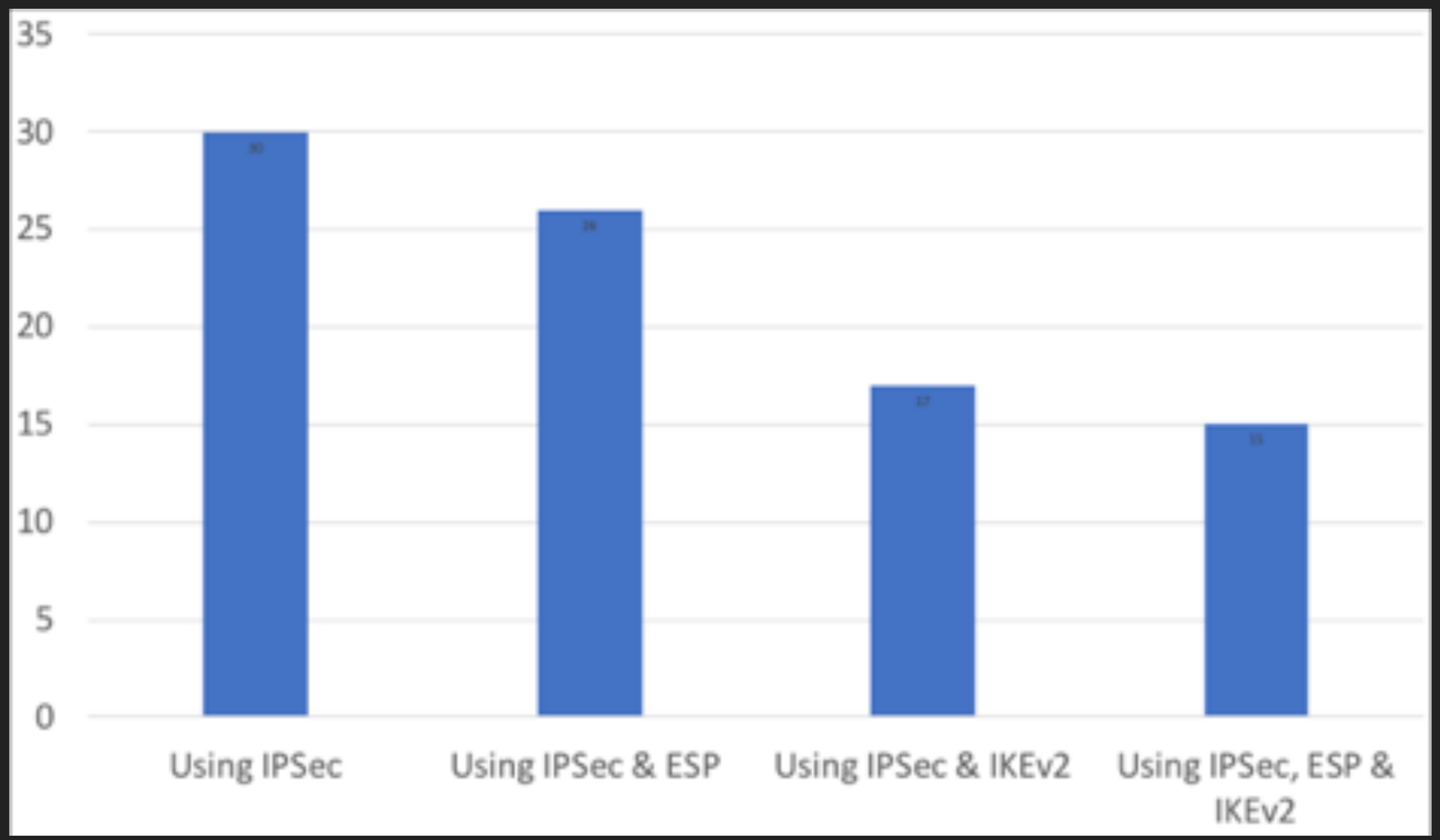
DNS LEAKAGE

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



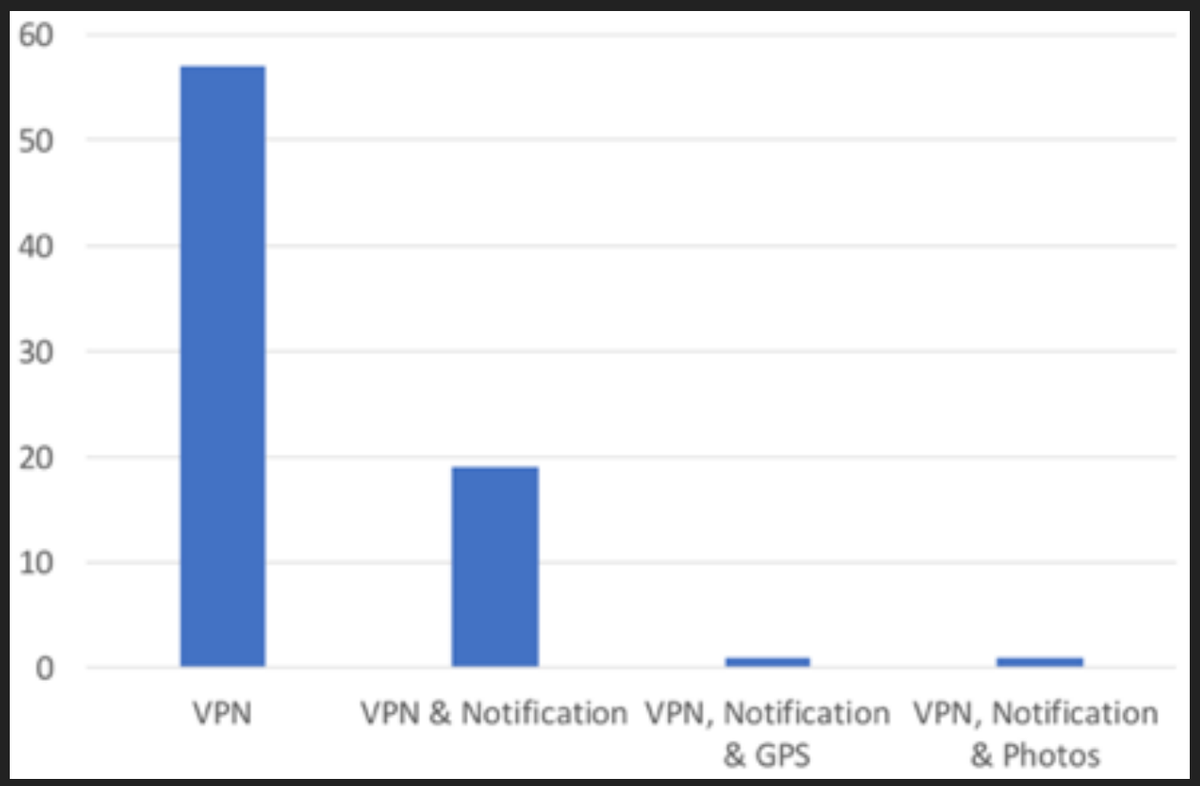
TUNNELLING PROTOCOLS

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

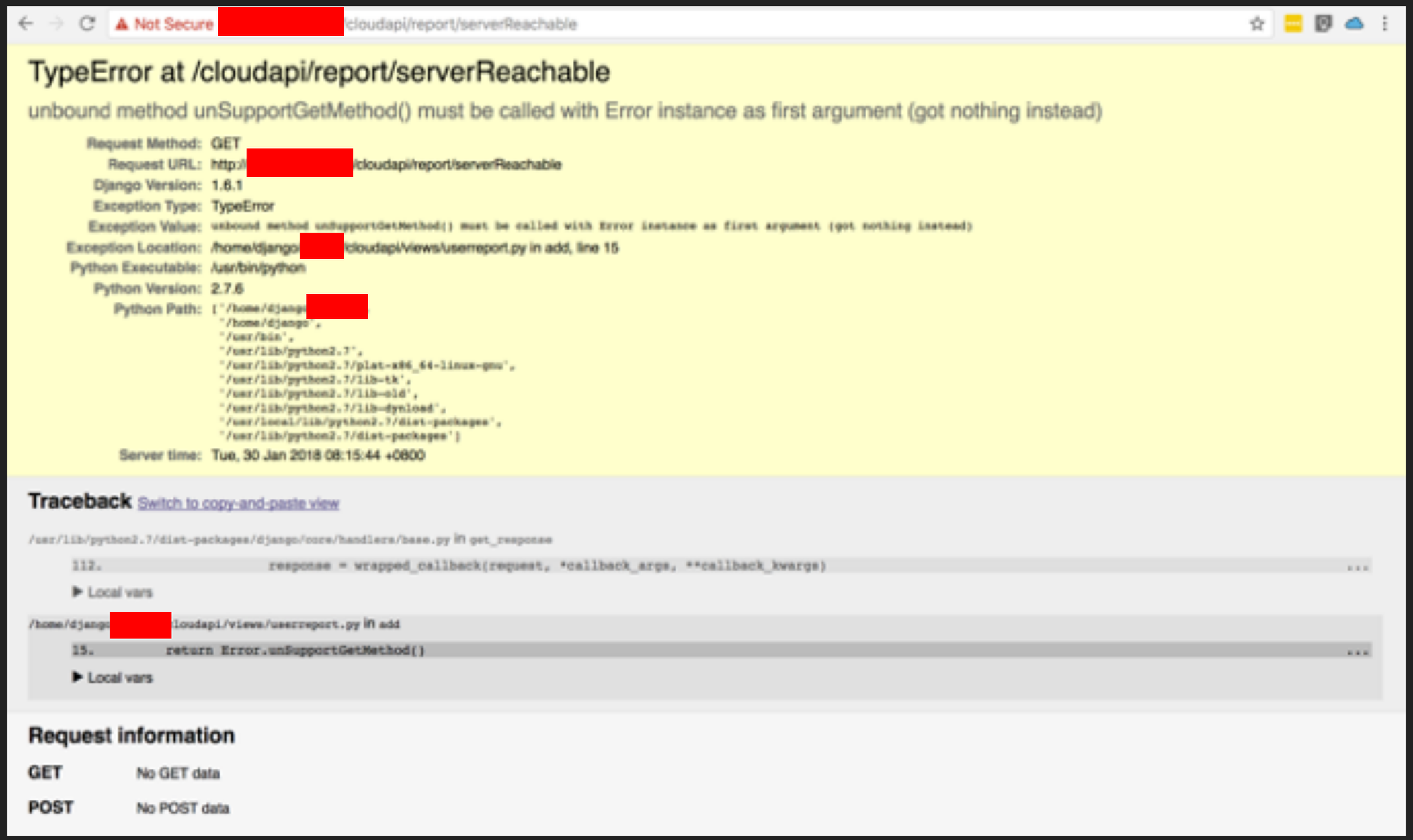


PERMISSIONS

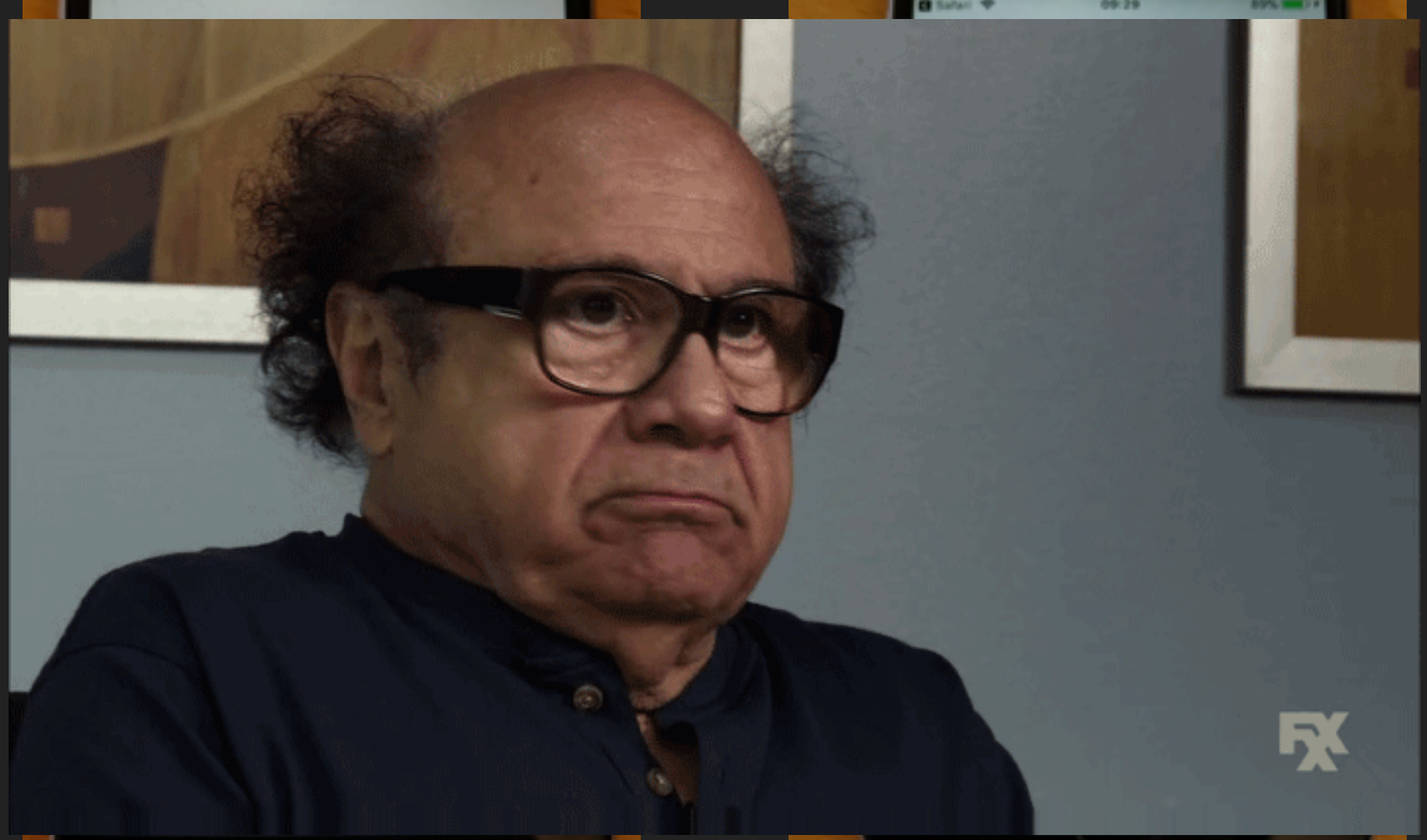
- Majority of apps only requested the expected permissions
  - VPN + Notification
- One app required access to the camera roll
- One app also required GPS access



OTHER WEIRD FINDINGS



- Django 1.6.1 was released in December 2013
- CVE’s for XSS, CSRF, DoS…


FX


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

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)
- As a reminder - security/privacy can go past the technicalities

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 Windows/Android
  - Build in ad-blocking (DNS resolver)
  - From ~$5/month

ALGO – THE GOOD AND THE BAD

👍

- Well hardened default config
- Less config required than deploying an OpenVPN instance
  - Give VPS API key to (Ansible) script and go
- Open source

👎

- Will require maintenance on the deployed server
- Substantially reduced anonymity factor

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 VPN tunnel
  - Including DNS and IPv6
- Use IPSec with IKEv2 and ESP

@iJackWilson | www.jack.lu | hi@jack.lu

THANKS FOR LISTENING!

QUESTIONS/COMMENTS?