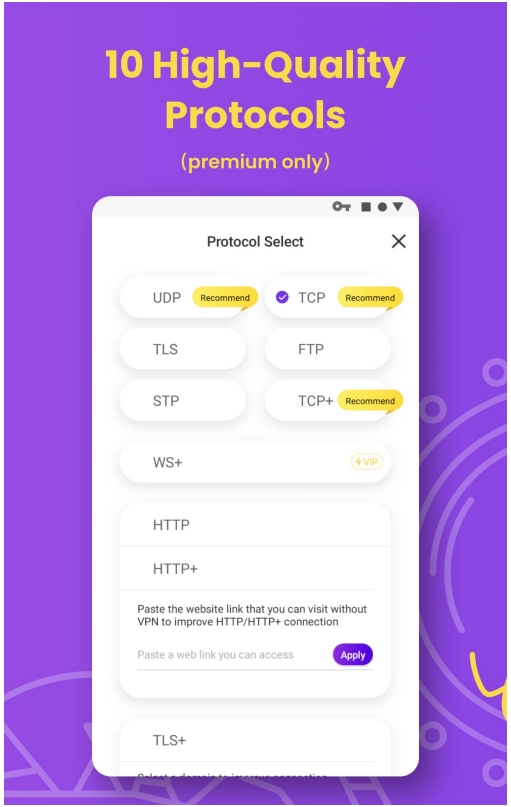
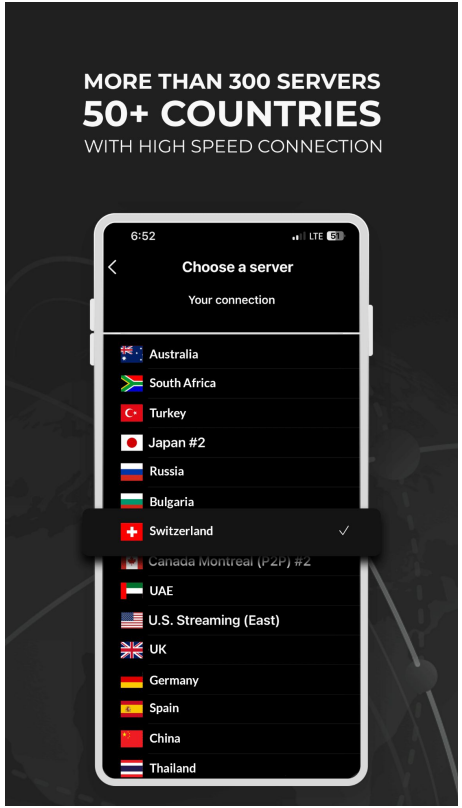
MVPNalyzer: An Investigative Framework for Auditing the Security & Privacy of Mobile VPNs

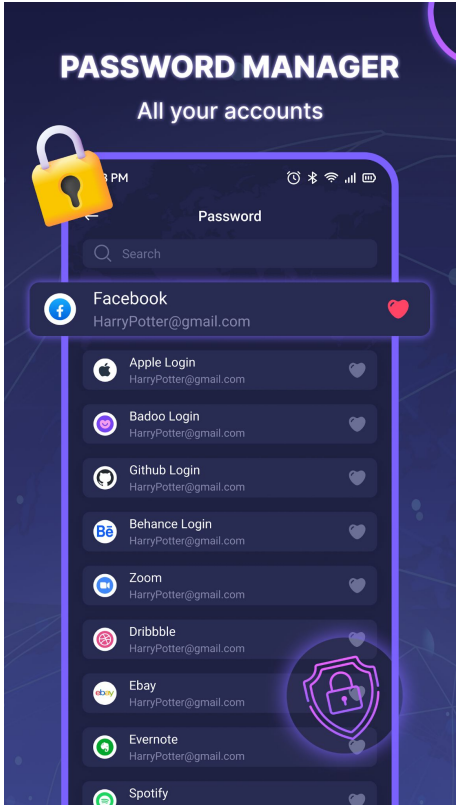
Wayne Wang*, **Aaron Ortwein***, Enrique Sobrados*†,
Robert Stanley, Piyush Kumar Sharma, Afsah Anwar†, Roya Ensafi

University of Michigan, †University of New Mexico

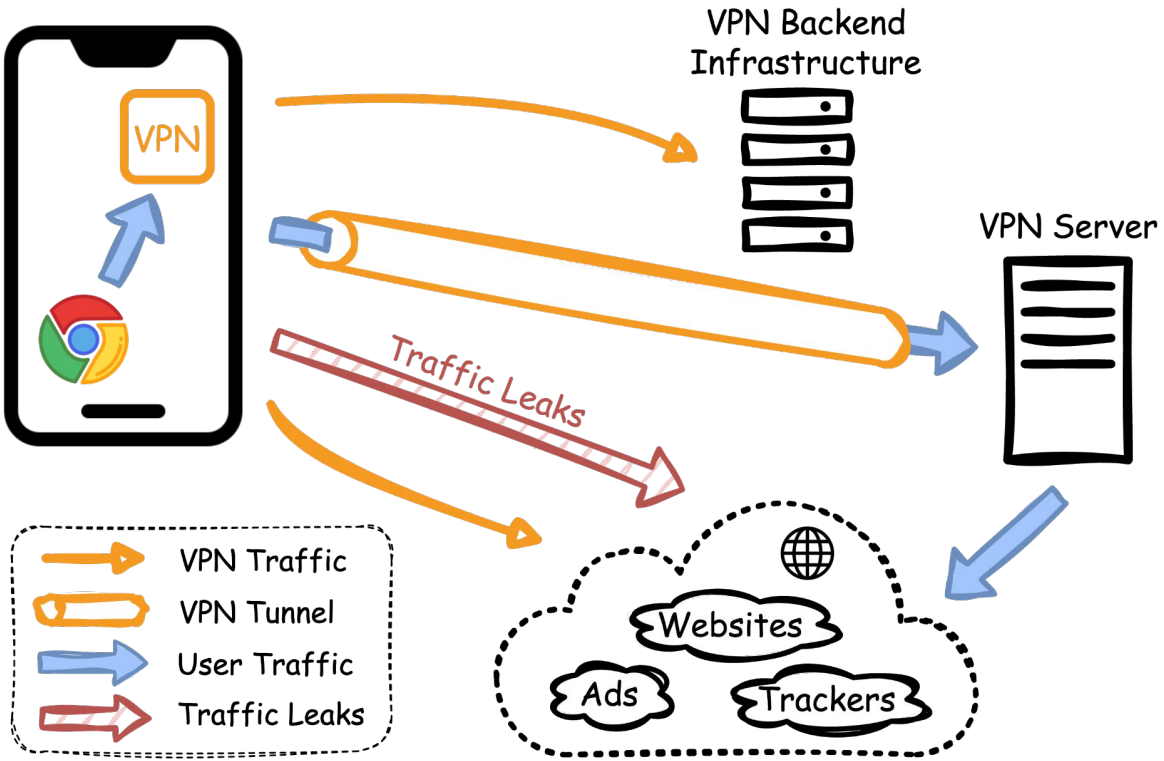
Advertising & Marketing, Perfected to a Science







VPNs as a Secure Tunnel for Communications



Censored Planet

VPNs as a Secure Tunnel for Communications

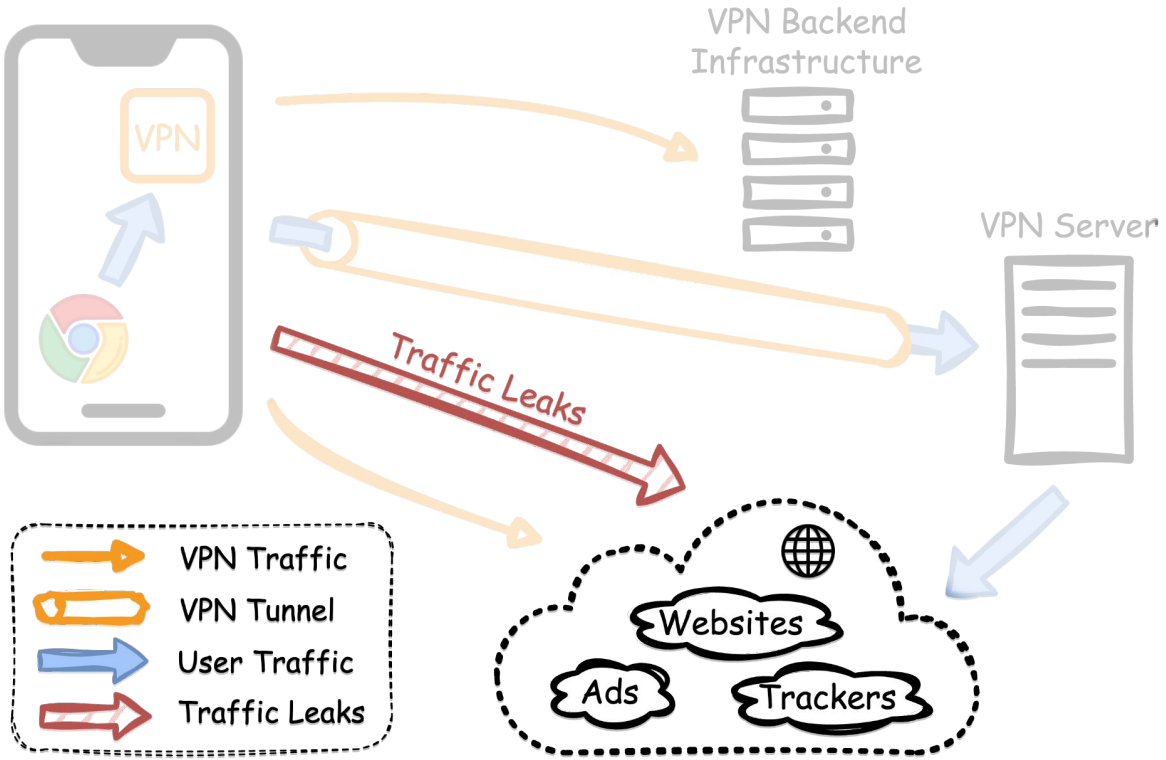
Traffic Leaks

Vasile C. Perta*, Marco V. Barbera, Gareth Tyson, Hamed Haddadi[1], and Alessandro Mei[2]

A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients

Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables

Nian Xue, *New York University*; Yashaswi Malla, Zihang Xia, Christina Pöpper, *New York University Abu Dhabi*; Mathy Vanhoef, *imec-DistriNet, KU Leuven*



Censored Planet

VPNs as a Secure Tunnel for Communications

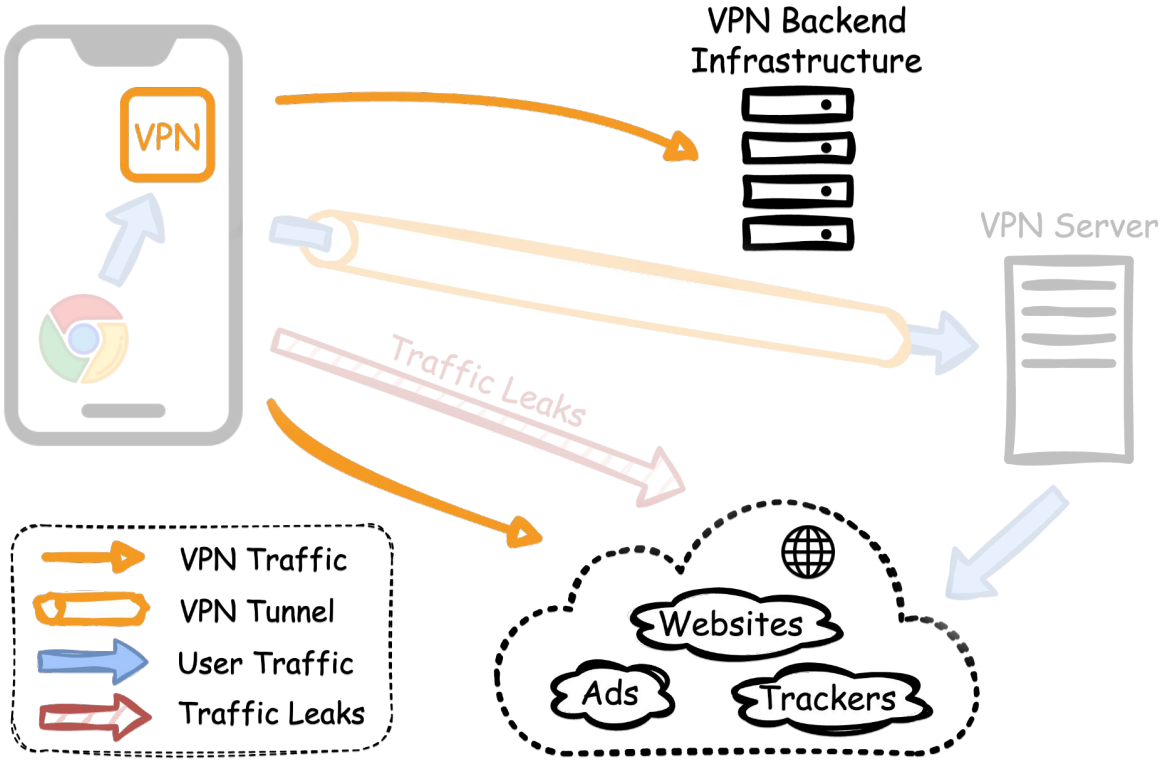
Cleartext

Investigation into the Security and Privacy of iOS VPN Applications

Jack Wilson
Division of Cybersecurity
Abertay University
Dundee, UK
hi@jack.lu

David McLuskie
Division of Cybersecurity
Abertay University
Dundee, UK
d.mcluskie@abertay.ac.uk

Ethan Bayne
Division of Cybersecurity
Abertay University
Dundee, UK
e.bayne@abertay.ac.uk



Censored Planet

VPNs as a Secure Tunnel for Communications

Server-Side Vulnerabilities

Back to School: On the (In)Security of Academic VPNs

Ka Lok Wu[†] Man Hong Hue[†,‡,1] Ngai Man Poon[†] Kin Man Leung[§]
Wai Yin Po[†] Kin Ting Wong[†] Sze Ho Hui[†] Sze Yiu Chau[†,2]

[†] *The Chinese University of Hong Kong*
[‡] *Georgia Institute of Technology*
[§] *The University of British Columbia*

Attacking Connection Tracking Frameworks as used by Virtual Private Networks

Benjamin Mixon-Baca
ASU/Breakpointing Bad
bmixonba@asu.edu

Jeffrey Knockel
Citizen Lab, University of Toronto

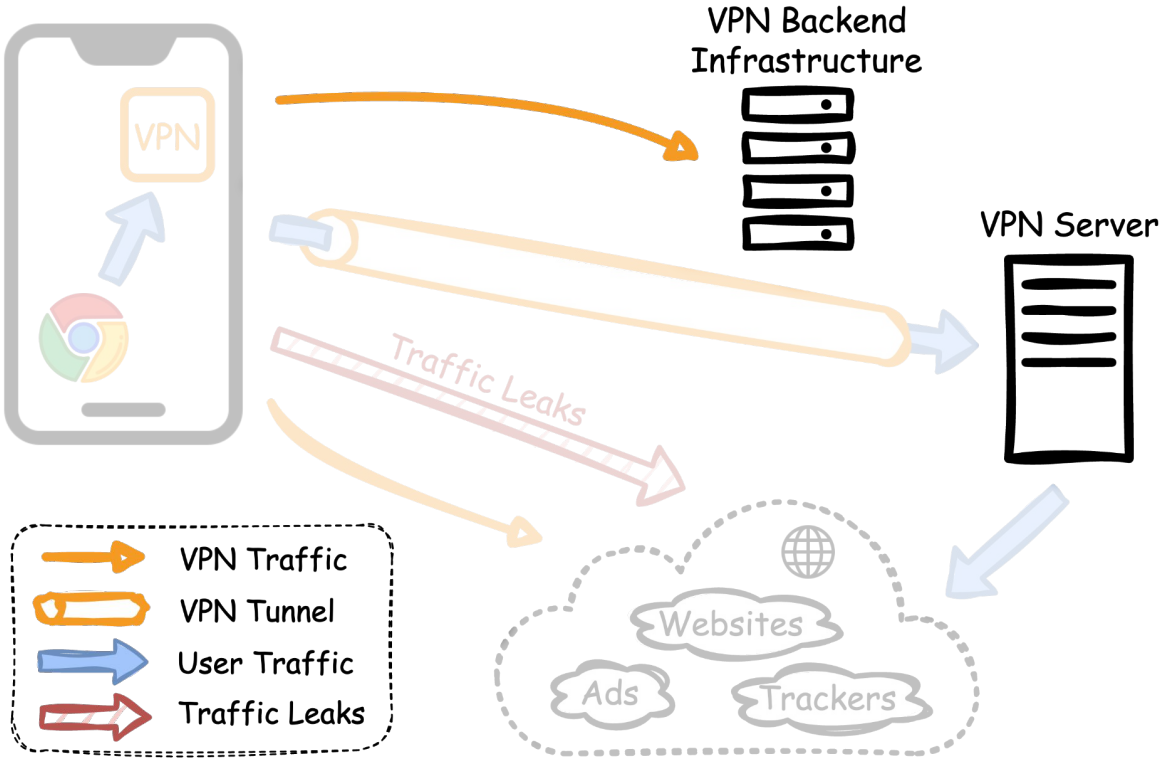
Diwen Xue
University of Michigan

Tarun Ayyagari
Arizona State University

Deepak Kapur
University of New Mexico

Roya Ensafi
University of Michigan

Jedidiah R. Crandall
ASU/Breakpointing Bad



Censored Planet

VPNs as a Secure Tunnel for Communications

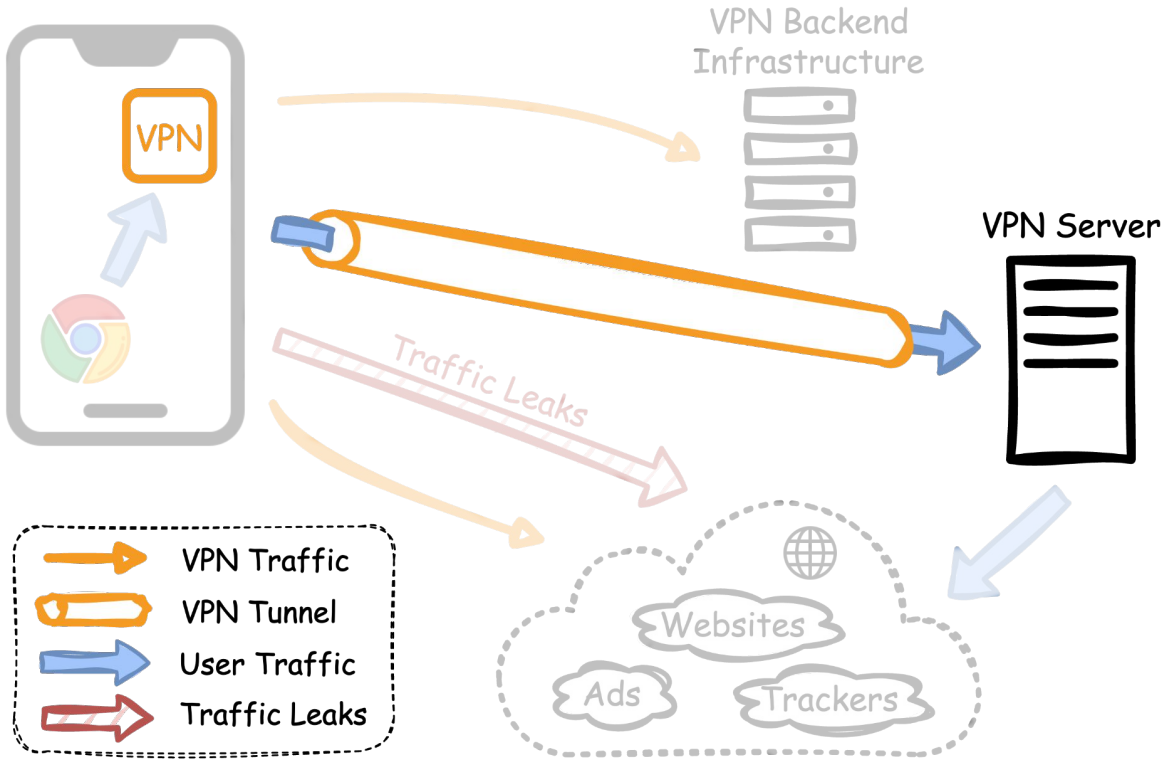
Tunnel Security

OpenVPN is Open to VPN Fingerprinting

Diwen Xue* Reethika Ramesh* Arham Jain* Michalis Kallitsis†
J. Alex Halderman* Jedidiah R. Crandall‡ Roya Ensafi*
*University of Michigan †Merit Network, Inc.
‡ Arizona State University/Breakpointing Bad

Oh-Pwn-VPN! Security Analysis of OpenVPN-based Android Apps *

Qi Zhang, Juanru Li, Yuanyuan Zhang(✉), Hui Wang, and Dawu Gu
Shanghai Jiao Tong University, Shanghai, China



Censored Planet

VPNs as a Secure Tunnel for Communications

Multidimensional

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

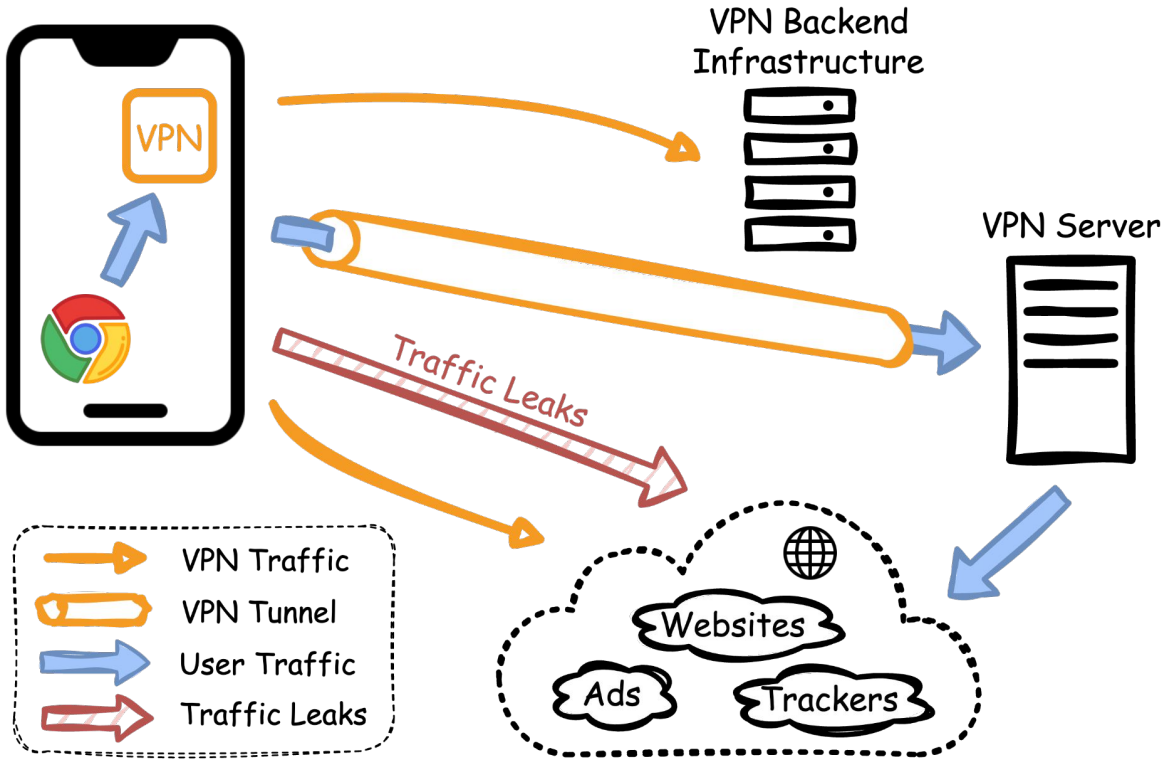
Muhammad Ikram[1,2], Narseo Vallina-Rodriguez[3], Suranga Seneviratne[1], Mohamed Ali Kaafar[1], Vern Paxson[3,4]
[1]Data61, CSIRO [2]UNSW [3]ICSI [4]UC Berkeley

An Empirical Analysis of the Commercial VPN Ecosystem

Mohammad Taha Khan* UIC
Joe DeBlasio* UC San Diego
Geoffrey M. Voelker UC San Diego
Alex C. Snoeren UC San Diego
Chris Kanich UIC
Narseo Vallina-Rodriguez IMDEA Networks Institute ICSI

VPNalyzer: Systematic Investigation of the VPN Ecosystem

Reethika Ramesh University of Michigan reethika@umich.edu
Leonid Evdokimov Independent leon@darkk.net.ru
Diwen Xue University of Michigan diwenx@umich.edu
Roya Ensafi University of Michigan ensafi@umich.edu



VPNs as a Secure Tunnel for Communications

Multidimensional

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

2016 Mobile

...na-Rodriguez[3], Suranga Seneviratne[1], ...afar[1], Vern Paxson[3,4]

...Data61, CSIRO UNSW [3]ICSI [4]UC Berkeley

An Empirical Analysis of the Commercial VPN Ecosystem

Mohammad Taha Khan* UIC

Joe DeBlasio* UC San Diego

Geoffrey M. Voelker UC San Diego

2018 Desktop

...anich ...C

Narseo Vallina-Rodriguez IMDEA Networks Institute ICSI

VPNalyzer: Systematic Investigation of the VPN Ecosystem

2022 Desktop

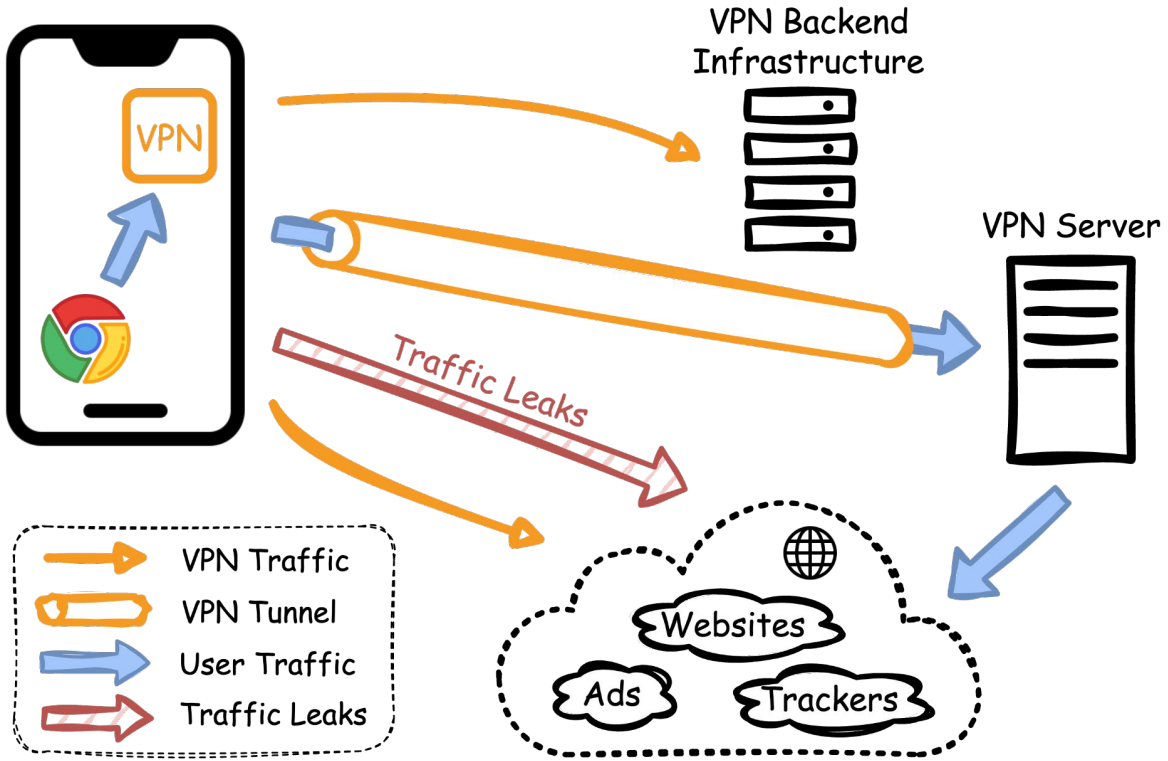
...reethika@umich.edu

Diwen Xue University of Michigan diwenx@umich.edu

...leon@darkk.net.ru

Roya Ensafi University of Michigan ensafi@umich.edu

Mobile now accounts for ~60% of all Internet traffic!



Investigating Mobile VPNs Raises New Challenges

Authenticity vs. Observability

- ➔ User devices elicit genuine behavior
- ➔ But they lack root or debugging access necessary for analysis
- ➔ Apps often resist analysis

Investigating Mobile VPNs Raises New Challenges

Authenticity vs. Observability

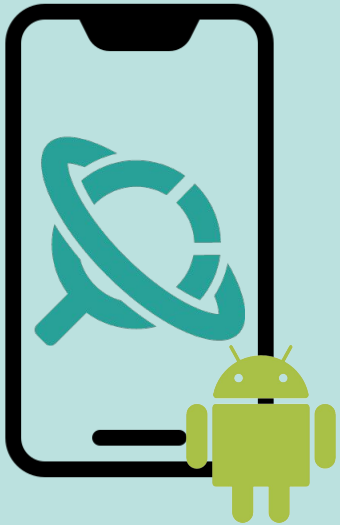
- ➔ User devices elicit genuine behavior
- ➔ But they lack root or debugging access necessary for analysis
- ➔ Apps often resist analysis

Scalability

- ➔ Large space of apps and configurations to test
- ➔ Analysis techniques must generalize to diverse apps
- ➔ **Only one VPN may be active at a time**
- ➔ **Meaningful evaluation requires legitimate app interaction**

Key Questions for Auditing VPNs

1. Does the VPN **transmit cleartext traffic** (e.g., HTTP)?
2. Does the VPN **leak** which **websites** the user is visiting?
3. Does the VPN **make an effort to obfuscate itself** from network adversaries?
4. Does the VPN engage in **user tracking** or **device fingerprinting**?
5. Does the VPN **properly configure its tunnel** protocol?

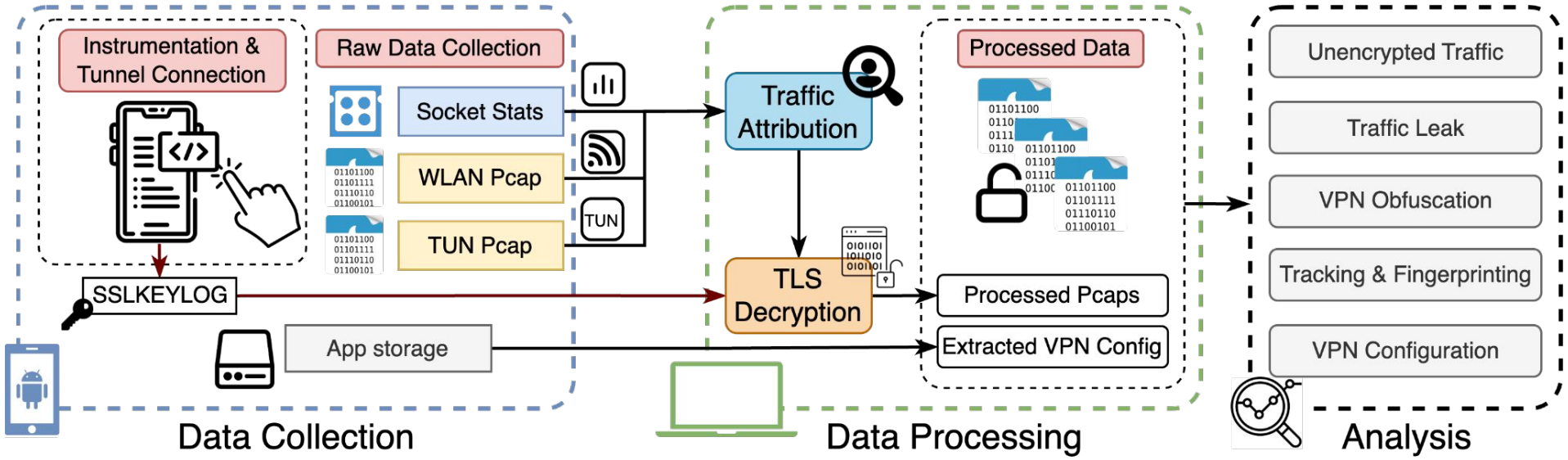


We built MVPNalyzer

to overcome these challenges &
answer these key questions

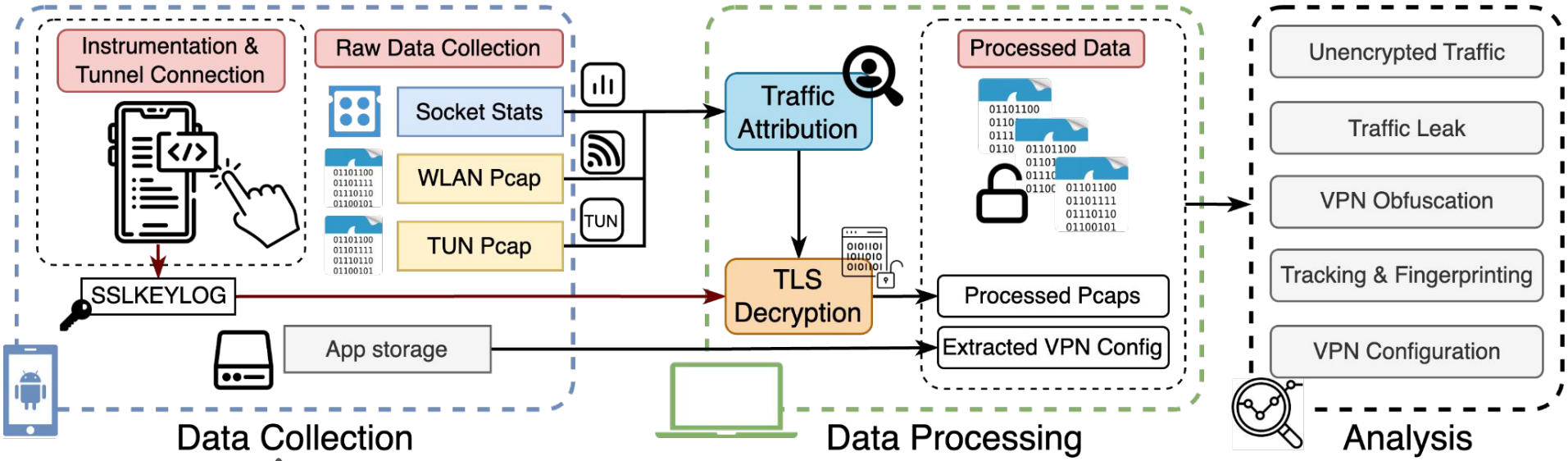
Censored Planet

MVPNalyzer System Architecture



Censored Planet

MVPNalyzer System Architecture



Automated Instrumentation → Manual Tunnel Connection → Automated Traffic Generation

Censored Planet

Measurement Setup

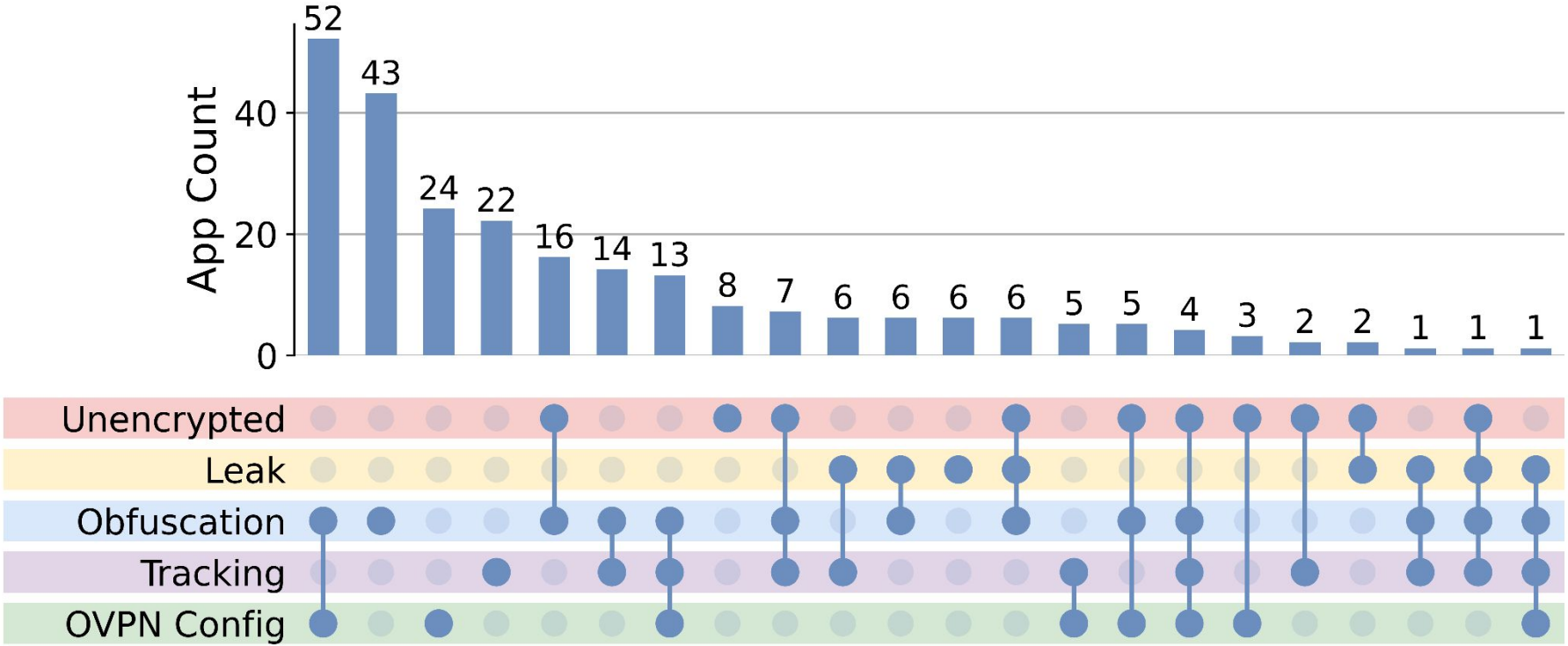
- We tested 281 **operational free** VPNs collected from 40 Google Play searches
- Each app was tested in its **default configuration**
- All apps were tested on **Android 14**

Google Play Store Search Terms		
VPN	VPN app	Secure VPN
Fast VPN	Free VPN	Unlimited VPN
VPN proxy	VPN for privacy	VPN with no logs
VPN with split tunneling	VPN for streaming	VPN for gaming
VPN with kill switch	VPN with multiple servers	VPN with encryption
VPN for Android	VPN for public Wi-Fi	VPN for travel
VPN for torrenting	VPN for school	VPN for work
High-speed VPN	Low-latency VPN	Reliable VPN
Best free VPN	Premium VPN	Cheap VPN
Trial VPN	VPN for Netflix	VPN for sports streaming
VPN for YouTube	Private VPN	Anonymous VPN
VPN with strong encryption	Fast free VPN	Secure private VPN
Best VPN for streaming	Unlimited free VPN	No-logs secure VPN
VPN and proxy tools		

Censored Planet

Findings - Overview

These apps combine for 2.4 billion installs!

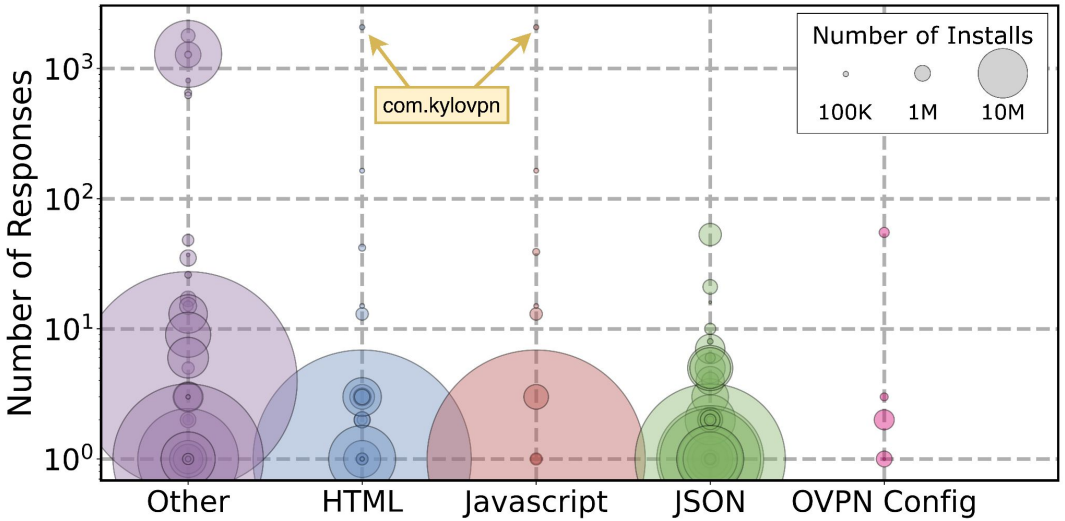


Censored Planet

Findings - Cleartext Traffic

61 apps **exchange cleartext** traffic

- ↪ 105 of 604 requested URLs are likely **VPN infrastructure**
- ↪ 5 apps transmit **OpenVPN configuration files**
- ↪ Apps are also vulnerable to **ad and JavaScript injections**



Censored Planet

Findings - Traffic Leaks

29 apps **leak** virtually **all websites visited**

- ↪ 24 leak DNS queries
- ↪ 6 do not tunnel browser traffic
- ↪ 4 tunnel browser traffic in unencrypted tunnel

DNS leaks may be misconfiguration, while other leaks suggest app may not be a real VPN

Leak Type	Apps
DNS Leak (24)	Java VPN, Noon VPN, AM TUNNEL LITE VPN, AM TUNNEL PRO, MahsaNG, GoFly VPN, Ostrich VPN, NewNode VPN, Cookie, Delight VPN, Phone Guardian, RoboProxy, Kylo Vpn, LVCHA VPN, XY VPN, Take Off, Tesla Proxy Pro, Global VPN, Air Net VPN, FoxoVPN, Bolt VPN, Free VPN, Siam VPN, Nine Tail VPN
Traffic Leak (6)	Java VPN, Noon VPN, NewNode VPN, Phone Guardian, Unicorn HTTPS, Free VPN
Unencrypted Tunnel (4)	Geo Tunnel, Raytunnel, Rosa VPN, V2net

Censored Planet

Findings - Obfuscation

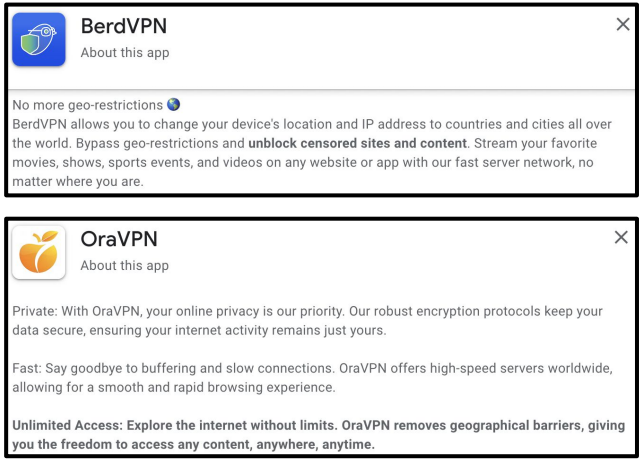
169 VPNs are **trivially detected** using **standard** Deep Packet Inspection

- ↪ 117 by **protocol**
- ↪ 54 by **port**
- ↪ 101 by **traffic to VPN-related domains**

110 of them claim to **circumvent censorship** or **provide unrestricted Internet**

dns.qry.name contains "vpn" || tls.handshake.extensions_server_name contains "vpn" || openvpn

No.	Time	Source	Destination	Protocol	Src Port	Dest Port	Len	Info
…		35.3.252.15	10.10.10.10	DNS	54866	53	…	Standard query 0x0458 A fast-vpn.fun
…		10.10.10.10	35.3.252.15	DNS	53	54866	…	Standard query response 0x0458 A fast-vpn.fun
…		35.3.252.15	80.209.231.41	TLSv1.3	49326	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	49330	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	41854	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	39914	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	39922	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	39934	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	80.209.231.41	TLSv1.3	39938	443	…	Client Hello (SNI=fast-vpn.fun)
…		35.3.252.15	195.201.42.224	OpenVPN	37058	1194	…	MessageType: P_CONTROL_HARD_RESET_CLIENT_V2
…		195.201.42.224	35.3.252.15	OpenVPN	1194	37058	…	MessageType: P_CONTROL_HARD_RESET_SERVER_V2
…		35.3.252.15	195.201.42.224	OpenVPN	37058	1194	…	MessageType: P_ACK_V1



Censored Planet

Findings - Tracking and Fingerprinting

Many apps **violate privacy** by **actively facilitating tracking**

- ↪ 76 transmit the **uniquely-identifying** Advertising Identifier
- ↪ 42 transmit relatively **fine-grained location** data
- ↪ 200+ transmit coarse-grained device attributes

Category	Attribute	App Count	Example
Device	AdID	76	{“adid”: “...”}
	Make	176	{“make”: “OnePlus”}
	Model	210	{“model”: “CPH2513”}
	OS Type	209	{“os”: “android”}
	OS Version	177	{“osv”: “14”}
	Android API Level	184	{“android_api_level”: “34”}
	Display	28	{“screen_size”: “1080x2400”}
Location	Coordinates	1	{“lon”: “-00.0000000”}
	IP	38	{“ip”: “x.x.x.x”}
	City	3	{“city”: “xxxxxx”}
	Country	130	{“country”: “US”}
	Timezone	12	{“timezone”: “est”}
Language	Language	191	{“language_code”: “en-US”}

Findings - OpenVPN Configuration

Only 1 of 108 examined OpenVPN apps **follows best practices**

- ↪ Most common issue is **lack of multi-factor authentication**
- ↪ Most severe issue is **disabling encryption** and **data integrity checks**

Category	Check	Apps	Unique Apps	Combined Installs
Insecure Cryptography	Weak Cipher Msg Auth	20 9	20 (18.5%)	40M+
Weak Authentication	Uname/Passwd Client Cert	22 74	96 (89%)	728M+
Deprecated Directives	Compression Others	12 6	12 (11%)	513M+
Hardening Options	ID Verify HMAC TLS	38 56	61 (56.4%)	601M+

Censored Planet

Recommendations for Google

Cleartext Prevention

(1) Remove or reject apps that enable cleartext

```
<?xml version="1.0" encoding="utf-8"?>
<manifest>
    <application android:usesCleartextTraffic="true">
    </application>
</manifest>
```

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
    </base-config>
</network-security-config>
```

(2) Sockets check network traffic for encryption

```
public @NonNull Builder detectCleartextNetwork() {
    return enable(DETECT_VM_CLEARTEXT_NETWORK);
}
```

Censored Planet

Recommendations for Google

Cleartext Prevention

(1) Remove or reject apps that enable cleartext

```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest>
    <application android:usesCleartextTraffic="true">
    </application>
</manifest>
```

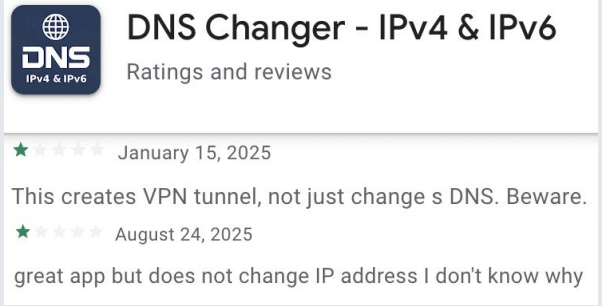
```xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
    </base-config>
</network-security-config>
```

(2) Sockets check network traffic for encryption

```
public @NonNull Builder detectCleartextNetwork() {
    return enable(DETECT_VM_CLEARTEXT_NETWORK);
}
```

Separate VPNs & Network Tools

Clearly separate VPNs from other non-VPN networking tools



Censored Planet

Recommendations for Google

Cleartext Prevention

(1) Remove or reject apps that enable cleartext

```
<?xml version="1.0" encoding="utf-8"?>
<manifest>
    <application android:usesCleartextTraffic="true">
    </application>
</manifest>
```

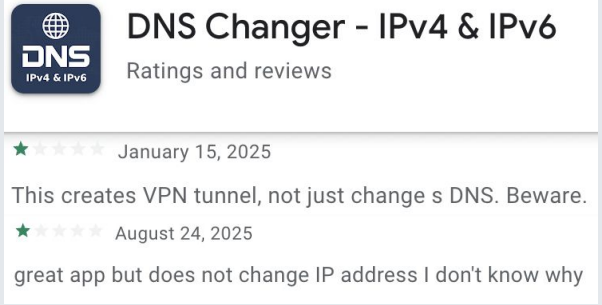
```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
    </base-config>
</network-security-config>
```

(2) Sockets check network traffic for encryption

```
public @NonNull Builder detectCleartextNetwork() {
    return enable(DETECT_VM_CLEARTEXT_NETWORK);
}
```

Separate VPNs & Network Tools

Clearly separate VPNs from other non-VPN networking tools



Improved Auditing

Perform independent auditing *before* distribution

- ↪ Data Safety is self-reported
- ↪ Verification badge is eligibility-based and paid

To be considered for the "Verified" badge, your VPN app needs to:

- Complete a Mobile Application Security Assessment (MASA) Level 2 validation
- Have an Organization developer account type
- Meet target API level requirements for Google Play apps
- Have at least 10,000 installs and 250 reviews
- Be published on Google Play for at least 90 days
- Submit a Data Safety section declaration, opting into:
  - Independent security review, under 'Additional badges'
  - Encryption in transit

MVPNalyzer: An Investigative Framework for Auditing the Security & Privacy of Mobile VPNs

Wayne Wang*, **Aaron Ortwein***, Enrique Sobrados*†,
Robert Stanley, Piyush Kumar Sharma, Afsah Anwar†, Roya Ensafi

University of Michigan, †University of New Mexico