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

Muhammad Ikram (UNSW, Data61, CSIRO)
Narseo Vallina-Rodriguez (ICSI, IMDEA Networks)
Suranga Seneviratne (Data61, CSIRO)
Mohamed Ali Kaafar (Data61, CSIRO)
Vern Paxson (UC Berkeley, ICSI)
Typical VPN Use Cases

- Geo-filtered content
- Anti-surveillance
- Censorship
- Untrusted networks
Android VPN API

• Available since Android $\geq 4.0$ (Ice Cream Sandwich)
• Highly sensitive API

+ Protected by BIND_VPN_SERVICE
+ Requires user’s direct action

- Users may not understand VPN technology
- Lack of apps’ vetting process
**Privacy and Security Risks of Android VPN Permission-enabled Apps**

Muhammad Ikram

---

### SuperVPN - Free VPN Client

<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 11, 2016</td>
<td>10,000,000 - 50,000,000</td>
<td>2.0.1</td>
</tr>
</tbody>
</table>

**Requires Android**

4.0.3 and up

**Content Rating**

Everyone

**Permissions**

View details

---

**Great App!! Works Perfectly in China**

Thanks for creating an awesome app. Using your

**Nooooo, Why? Ouch, ouch, ouch...**

Worked okay at first, but now my internet won't work
Are VPN Android apps trustworthy?
Approach

1. Static Analysis

2. Network Measurements
Some salient results

- Malware presence
- Traffic leak
- Javascript injection and TLS interception

2 apps inject JavaScript code
4 apps implement TLS interception
Agenda

• VPN App Detection and Methodology

• Passive Analysis

• Network Measurements

• Summary

• Developer’s feedback
Methodology

Google Play Crawl (1.4M+ Apps)

Executables and metadata (apps description, reviews, etc)

Static Analysis

Network Measurements

VPN App Detection and Classification

Privacy and Security Risks of Android VPN Permission-enabled Apps | Muhammad Ikram
## Identified VPN App

<table>
<thead>
<tr>
<th>App Category</th>
<th># of apps found</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free VPN apps with Free services</td>
<td>130</td>
</tr>
<tr>
<td>Free VPN apps with Premium services</td>
<td>153</td>
</tr>
</tbody>
</table>

---

10  Privacy and Security Risks of Android VPN Permission-enabled Apps  |  Muhammad Ikram
Analyzed VPN Apps - Evolution

Android 4.0 release date

Estimated Release Date
User installs and ratings

- 37% of apps > 500K installs
- 55% of apps > 4-star rating
Static Analysis
67% of Android VPN apps claim privacy and security enhancement features
Access to Sensitive Data and Resources

- 82% of the VPN apps request sensitive permissions
  - READ_LOGS (14%)
  - READ_SMS (6%)
  - READ_CONTACTS (6%)
  - WRITE_SMS (4%)

Limitation: is the use of those permissions legitimate?
3rd-party Tracking Libraries

- 67% of VPN apps include 3rd-party tracking libraries

<table>
<thead>
<tr>
<th># Trackers</th>
<th>VPN Apps</th>
<th>Free non-VPN Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Premium</td>
<td>Free</td>
</tr>
<tr>
<td>0</td>
<td>65%</td>
<td>28%</td>
</tr>
<tr>
<td>1</td>
<td>13%</td>
<td>10%</td>
</tr>
<tr>
<td>2</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>3</td>
<td>12%</td>
<td>25%</td>
</tr>
<tr>
<td>4</td>
<td>2%</td>
<td>8%</td>
</tr>
<tr>
<td>&gt;5</td>
<td>5%</td>
<td>18%</td>
</tr>
</tbody>
</table>
Malware Presence

- **Scanner**: VirusTotal aggregator

- **AV-rank**: number of AV tools reporting malware

- 38% of VPN apps contain malware with 4% having AV-rank $\geq 5$

### Table: Malware Presence

<table>
<thead>
<tr>
<th>#</th>
<th>App ID</th>
<th>Class</th>
<th>Rating</th>
<th># Installs</th>
<th>AV-rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OkVpn [35]</td>
<td>Prem.</td>
<td>4.2</td>
<td>1K</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>EasyVpn [15]</td>
<td>Prem.</td>
<td>4.0</td>
<td>50K</td>
<td>22</td>
</tr>
<tr>
<td>3</td>
<td>SuperVPN [52]</td>
<td>Free</td>
<td>3.9</td>
<td>10K</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>Betternet [19]</td>
<td>Free</td>
<td>4.3</td>
<td>5M</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>CrossVpn [7]</td>
<td>Free</td>
<td>4.2</td>
<td>100K</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Archie VPN [4]</td>
<td>Free</td>
<td>4.3</td>
<td>10K</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>HatVPN [22]</td>
<td>Free</td>
<td>4.0</td>
<td>5K</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>sFly Network Booster [48]</td>
<td>Prem.</td>
<td>4.3</td>
<td>1K</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>One Click VPN [36]</td>
<td>Free</td>
<td>4.3</td>
<td>1M</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>Fast Secure Payment [17]</td>
<td>Prem.</td>
<td>4.1</td>
<td>5K</td>
<td>5</td>
</tr>
</tbody>
</table>
Network Measurements
Testbed

Traffic manipulations

1. Local interception
2. Cloud-based forwarding
3. Cooperative forwarding

Testing device

Dedicated VPN Server

Forwarded user traffic

Dual-stack WiFi AP

Packet capture

Participating devices

WWW

Testing servers

Cloud-based forwarding

Dotted lines represent untunneled traffic/leaks.

Traffic manipulations

Local interception

VPN Tunnel

Testing Traffic/Leaks

Testing device

Dotted lines represent untunneled traffic/leaks.

Cloud-based forwarding

Dotted lines represent untunneled traffic/leaks.

Cooperative forwarding

Dotted lines represent untunneled traffic/leaks.
Forwarding models

• Tested manually each vantage point reported in the app

• 18% of apps do not inform about the terminating end-point

• 4% of VPN apps intercept traffic

• 16% use vantage points hosted on residential networks (Spamhaus PBL)

VPN - Hola Free VPN
Installs 10,000,000 - 50,000,000

Welcome to a Better Internet!
** Hola works by sharing the idle resources of its users for the benefit of all **
• Access sites blocked by your country through an innovative peer to peer network
• Accelerates browsing by choosing the closest and fastest sources
DNS and IPv6 Leakages

- 18% of apps do not use encrypted tunnels
- 84% of VPN apps leak IPv6 traffic
- 66% of VPN apps leaks DNS queries

Users can be potentially subject to in-path modification, profiling, redirection, and censorship.
Adblocking and JavaScript Injection

- DOM-based analysis
- Top 30 Alexa sites, reference website and seven e-commerce sites
TLS Interception

- Analysed certificates from 60 websites/domains
- Apps compromise root store

<table>
<thead>
<tr>
<th>Domain(port)</th>
<th>Neopard</th>
<th>DashVPN</th>
<th>DashNet</th>
<th>Packet Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazon.com</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>gmail.com</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>orcart.facebook.com (8883)</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>bankofamerica.com</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>hsbc.com</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps

Muhammad Ikram¹,², Narseo Vallina-Rodriguez³, Suranga Seneviratne¹, Mohamed Ali Kaafar¹, Vern Paxson³,⁴
¹Data61, CSIRO   ²UNSW   ³ICSI   ⁴UC Berkeley

ABSTRACT

Millions of users worldwide resort to mobile VPN clients to either circumvent censorship or to access geo-blocked content, and more generally for privacy and security purposes. In practice, however, users have little if any guarantees about to request the BIND_VPN_SERVICE permission (for simplicity, the “VPN permission”) to create such clients.

Android’s official documentation highlights the serious security concerns that the VPN permission raises: it allows an app to intercept and take full control over a user’s traffic [60]. Moreover, as an entitlement over the VPN service
“And isn’t it ironic?”

• Do users care?

• Manually analysed negative reviews (4.5K) (1- and 2-Stars)

• < 1% of the negative reviews raised privacy and security concerns
Summary

• 38% of apps have malware presence

• 67% of apps have at least one third-party tracking library

• 66% of VPN apps have DNS leakages and 84% have IPv6 Leakages

• 2 VPN apps perform JS-injection for ads, tracking, and redirections

• 4 VPN apps perform TLS interception
Developer Feedback and Reactions

“... Appflood [third-party library] was the best choice to monetize the app”.

Now: ads- and tracking free app

Confirmed JS-Injections for tracking users and showing their own advertisements

Now: status quo
Developer Feedback and Reactions

“... we will promise these problems never occur again.”

November 2015

October 2016

29 Privacy and Security Risks of Android VPN Permission-enabled Apps | Muhammad Ikram