# Understanding and addressing Android VPN vulnerabilities

## White paper

Driving Trust
www.insidesecure.com

Enterprise Security
& Secure Access
inside SECURE

# Table of contents

## Introduction

In early 2014, mobile data security specialists discovered vulnerabilities in the Android mobile operating system, which affects the natively installed VPN client and exposes data and communications to interception. The concept of the VPN boundary (as described by the IeTF and required by the US department of defense) is the fundamental element in this vulnerability and when implemented properly the solution to this problem.

This paper is intended for a technical audience looking to better understand their current risks related to this disclosure including:

- CISO's and Enterprise Network Security professionals
- Network security services providers
- Security Analysts
- Mobile Device OEM's
- Mobile Device Management and managed security services

It provides an analysis of the root cause of the Android VPN vulnerabilities, the risks of continued use of the native client and why use of mobile devices with the INSIDE Secure's QuickSec Mobile VPN client provides VPN security and enforcement as required.

## Native Android VPN vulnerabilities

The Cyber Security Lab of Ben Gurion University revealed vulnerabilities in the native VPN client on Android devices [1] that:

"*enables malicious apps to bypass active VPN configuration (no ROOT permissions required) and redirect secure data communications to a different network address. These communications are captured in CLeAR TeXT (no encryption), leaving the information completely exposed. This redirection can take place while leaving the user completely oblivious, believing the data is encrypted and secure*."

The description above indicates that the affected traffic was been made to bypass the VPN connection. In other terms, the native Android VPN client did not enforce the VPN boundary.

## The principle of VPN boundary

The principle of VPN boundary is one of the key concepts of the VPN security concept and it is well explained in RFC 4301, "Security Architecture for the Internet Protocol "[2]. This IeTF specification is focused on IPsec, but its principles are in fact applicable to any types of VPNs.

A VPN "*creates a boundary between unprotected and protected interfaces, for a host or a network... Traffic traversing the boundary is subject to the access controls specified by the user or administrator*"[2]. The rules of the traffic handling are specified in a security policy. The security policy "*must be consulted during the processing of all traffic (inbound and outbound), including traffic not protected by IPsec, that traverses the IPsec boundary.*"[2]

Unprotected interfaces (WiFi, 3G and LTe Internet, for example) of the VPN host are connected to public networks that are not trusted. Protected traffic sent out from an unprotected interface must be protected by the VPN. All traffic received from an unprotected interface must be processed by the VPN.

The above requirement is clearly expressed in STIG guidelines [3]: "*it is imperative that all inbound and outbound traffic traverse only the IPSec tunnels […] the external interface must not receive any traffic that is not secured by an IPSec tunnel or other provisioned WAN links connected to the*

*central or remote site. This not only ensures that inbound and outbound traffic does not bypass the enclave's perimeter defense, but also eliminates any backdoor connection*."

To be compliant to this requirement, a VPN client must control all packets sent and received in order to enforce the security policy of the VPN host.

## Security risks if VPN boundary is not enforced

Failure to enforce the VPN boundary means that an attacker may impose backdoors that allow packets to bypass the security policy of the VPN.

Let's first consider the scenario where incoming packets bypass the VPN client.

### Packet attack on the same network

An attacker on the same network can exploit the weakness by sending malicious/malformed packets to an application on the mobile device. Since the packets can be made to bypass the security policy (VPN boundary) they will end up at the targeted mobile application. The source IP address of the fraudulent attack packet indicates that it was received through a VPN tunnel. For the receiving application on the device, it appears to be coming from a trusted network. As the sender authenticity cannot be trusted, an important VPN principle is violated.

This scenario is not theoretical and it has been demonstrated in practice with a downloadable VPN client.

Let's now consider two scenarios where outgoing packets bypass the VPN client:

### A malicious application establishing a split tunnel

The application sending the packet may act maliciously and address packets directly to an external interface, thus bypassing the VPN. This allows an application to implement "a split tunnel" VPN configuration (even if the security policy prohibits split-tunneling).

When successful, this allows a malicious application or an attacker to access the protected network by routing the data through this application.

The US department of defense recommendations [4] and many carriers require that split tunneling should be disabled. This requirement cannot be satisfied without a VPN solution that can effectively enforce the VPN boundary.

### Malware intercepting confidential date

The application may believe that its traffic is protected (meaning directed to the VPN) but a malware running on the same device may be able to redirect the traffic to an unprotected interface. This allows the malware to intercept confidential traffic.

This attack has been demonstrated in practice by the Cyber Security Lab of Ben Gurion University, and it applies to all traffic going through the VPN. Intercepting application traffic shows that the VPN boundary principle is not properly enforced.

### Summary of the risks

In summary, the enforcement of VPN boundary is critical. Without a proper VPN boundary enforcement:

- Sender authentication cannot be trusted
- Split tunneling cannot be enforced
- Confidential data sent by a valid application can be intercepted

## Quicksec VPN client implementation

After analyzing, studying and replicating the vulnerability and its implications, we can confirm that QuickSec VPN Client for Android is not affected by this flaw.

The QuickSec VPN Client provides two levels of protections against the demonstrated attack:

- QuickSec VPN Client monitors that no redirection takes place and is able to take corrective actions.
- QuickSec VPN Client includes a security module that enforces the VPN security policy for all inbound and outbound traffic. Any packet attempting to bypass the VPN is discarded by the security module.

QuickSec VPN client for Android is designed for demanding customers who require conformance with requirements from both carriers and national regulators (such as the US department of defense). When designing and implementing the QuickSec VPN Client for Android, INSIDE Secure has spent considerable effort in implementing a proper VPN boundary and reviewing the design against the various requirements set.

A thoroughly secure implementation requires deep integration with the Android platform, and can practically only be achieved in cooperation with Android OEMs. This has lead to the QuickSec VPN client being pre-installed by the device manufacturer, rather than being deployed over the “normal” mobile application store distribution.

QuickSec VPN already ships as a pre-installed VPN client on many leading Android devices.

To verify if the QuickSec VPN client is installed on a device, one should check the VPN menu “about” section. If it indicates that it is coming from INSIDE Secure or on older models from AuthenTec, the VPN client is not affected by this security flaw.

## Conclusion

Implementing a secure VPN on an Android device is a complex task that requires deep modifications within the software platform of the device. In close cooperation with the leading Android OEMs and dozens of man years of investment, INSIDE Secure has developed a VPN client that meets the most stringent security requirements of carriers, businesses, and governments.

In addition to guaranteeing the integrity of the VPN boundary and the STIG compliance, QuickSec VPN Client includes a FIPS-validated cryptographic library and offers support of the Suite B cryptographic specification. Its VPN Management API allows easy MDM integration. QuickSec® VPN Client has been interoperability tested with all major IPsec gateways from enterprise and carriers and fully supports IPv6 along IPv4.

QuickSec VPN is the leading IPsec VPN client for Android OEMs and has been shipped pre-installed on many popular Android devices and is currently available on over 100 million devices.

## References

[1] VPN Related Vulnerability Discovered on an Android device - Disclosure Report:

http://cyber.bgu.ac.il/blog/vpn-related-vulnerability-discovered-android-device-disclosure-report

[2] RFC 4301, Security Architecture for the Internet Protocol:

http://tools.ietf.org/html/rfc4301

[3] IPSeC VPN Gateway STIG, Version 1, Release 9:

https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=423

[4] dod Wireless Smartphone Security Requirements Matrix, Version 3.5: www.dla.mil/issuances/documents/i8130.01.pdf

## About INSIDE Secure

INSIDE Secure (NYSE INSD.PA) is a major provider of security technologies that include (VPN, DRM, FIPS certified crypto, payments, secure elements and TrustZone enabled software. INSIDE offers a complete portfolio of IPsec products: QuickSec Mobile VPN Client, QuickSec IPsec Toolkit and HW IP acceleration for IPsec.

The INSIDE Secure team (originally part of SSH, then SafeNet and AuthenTec) has worked with VPN technology since 1988 when they release of the world's first VPN product for X.25. They become a founding members of the VPN Consortium in 1999. Since then the team has been responsible for many industry first VPN developments including release of the first IPSec client (1997), first IKEv2 toolkit, first MOBIKE enabled toolkit. INSIDE Secure continues to work with industry partners and customers to stay at the forefront of VPN security.

For more information visit:

http://www.insidesecure.com/eng/Products/Security-Solutions-for-Android/QuickSec-Mobile-VPN-Client-for-Android

**INSIDE Secure**

Arteparc Bachasson • Bât. A
Rue de la carrière de Bachasson
CS 70025 • 13590 MEYREUIL • France

Tél: + 33 (0)4 42 90 59 05
Fax: + 33 (0)4 42 37 01 98



www.insidesecure.com

Driving Trust