ENGINEERING

SECUREIO

Accelerate Fielding of CSfC Android End-User Device Apps By Offloading TLS Encryption Functionality

THE CHALLENGE

The National Security Agency's (NSA's) Commercial Solutions for Classified (CSfC) program enables CSfC-compliant commercial products to be used in layered solutions for protecting classified information. The Mobile Access Capability Package (MACP) addresses composition of secure mobile solutions.

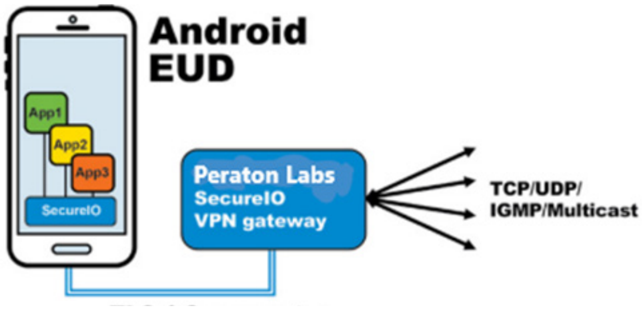
MACP requires individual testing and approval by the National Information Assurance Partnership (NIAP) for each app implementing Transport Layer Security (TLS) for use on a CSfC EUD. Since Android CSfC EUDs typically use TLS-encrypted app traffic inside an IPSec tunnel, each such app is subject to separate NIAP testing and NSA review.

NIAP testing and certification can be a long and expensive process, representing a high barrier to entry for new apps on CSfC EUDs, especially government off-the-shelf (GOTS) apps. The time required to approve, test and field TLS apps for CSfC-compliant Android devices needs to be dramatically reduced in order to help ensure that warfighters have the best technology in their hands as soon as possible.

THE SOLUTION

Peraton Labs' SecureIO suite provides a NIAP-approved common, shared TLS encryption function that can be used by every TLS app running on Android CSfC EUDs. The SecureIO Android service eliminates the need for apps to implement their own transport security, enabling a wide variety of new apps to be quickly deployed on NSA MACP-compliant Android EUDs.

Since the SecureIO suite is separate from upper layers, new upper layers can be added or existing upper layers can be modified without requiring SecureIO suite modification or re-approval. An application programming interface (API) for applications makes integration straightforward and painless.

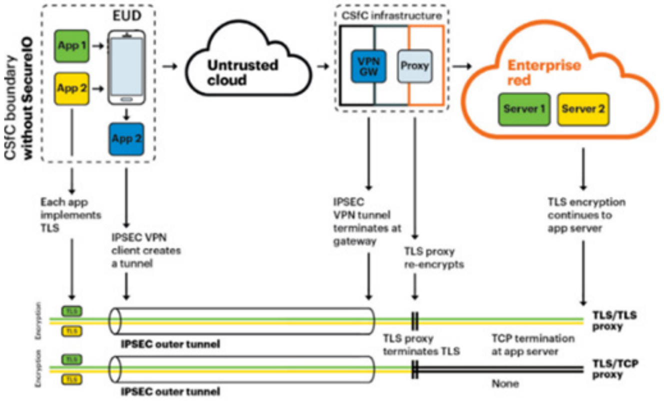


VALUE AND BENEFITS

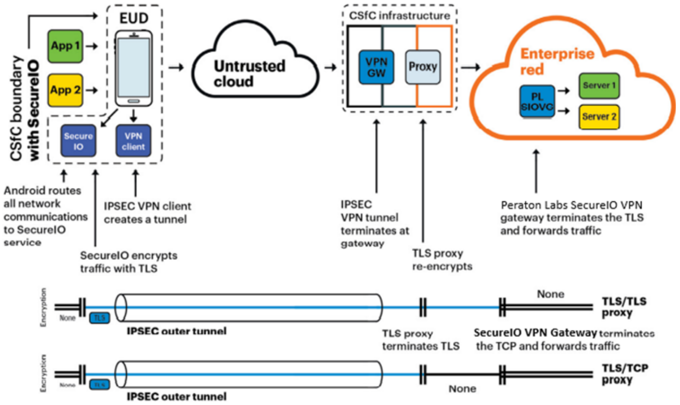
- Eliminates the requirement for NIAP testing and NSA review of each Android app on CSfC devices, because apps use a common, shared, NIAP-approved TLS encryption function
- New apps, including GOTS apps, can be rapidly and inexpensively fielded
- API provides quick and seamless integration
- SecureIO suite consists of SecureIO VPN Gateway and SecureIO Android components
- SecureIO is NIAP-approved and listed on the NSA's CSfC Components List

SECUREIO VPN GATEWAY (SIOVG) FEATURES

- Provides the anchor point for secure services
- Allows Android connection termination in TCP, or TLS, or Websocket
- Provides IP Forwarding Services for UDP, TCP, Multicast, and IGMP
- Provides a DHCP pool, route setting, and ARP Proxy for Android TLV TUN
- Can reside on a VM (on a Type-1 cluster)



Without SecureIO: Apps are within the CSfC boundry. Each app must implement TLS and be tested and approved for NIAP compliance


CSfC boundary with SecureIO
EUD
App 1
App 2
Secure IO
VPN client
Untrusted cloud
CSfC infrastructure
VPN GW
Proxy
Enterprise red
PL SIOVG
Server 1
Server 2
Android routes all network communications to SecureIO service
IPSEC VPN client creates a tunnel
SecureIO encrypts traffic with TLS
IPSEC VPN tunnel terminates at gateway
TLS proxy re-encrypts
Peraton Labs SecureIO VPN gateway terminates the TLS and forwards traffic
Encryption
None
TLS
IPSEC outer tunnel
None
TLS/TLS proxy
TLS proxy terminates TLS
SecureIO VPN Gateway terminates the TCP and forwards traffic
TLS/TCP proxy

With SecureIO: Apps are outside CSfC boundary and communicate locally with SecureIO, which encrypts all communications with TLS

SECUREIO ANDROID COMPONENTS FEATURES

- Standard Android software, compliant with VPN framework
- Implements Android VPN API
- Implements KNOX Extensions
- Exposes a standard TUN interface when configured as a VPN
- Offers UDP, TCP, IGMP, and Multicast interfaces
- Imports certificates from Android Key Chain and grants access
- Creates TLS or Websocket+TLS profiles
- Manages cipher suites
- Performs SAN/SNI checks using TLS server hostname
- Performs certificate validation, OCSP, and CRL checking
- Provides a statistics manager
- Monitors activity
- Runs as a service, auto-started by upper layer
- Requires no user interaction

For more information on the SecureIO product suite see SecureIO - Peraton Labs or contact the Peraton Labs CSfC experts: trusted.csfc@mail.peratonlabs.com.