DHS Science and Technology Directorate

Homeland Security
Science and Technology

MOBILE COMMUNICATIONS AT RISK

Standard mobile telephone calls and text messages are subject to eavesdropping using Access-as-a-Service capabilities available to nation-state and non-state actors.

Gaining unauthorized access to the core Signaling System Seven (SS7) or Diameter or 5G network is a growing risk since there are tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage. For example, SS7 is used worldwide to route phone calls as well as SMS text messages and can be exploited to allow Man-in-the-Middle (MITM) intercepts of voice and text messages.

Low-cost, secure voice and messaging applications that use—but do not rely on—commercial networks are needed that work with Android, iOS, and Windows 10 platforms and also integrate into conferencing bridges and managed address books (with selectable viewing/user privileges).

SECURING VOICE COMMUNICATIONS

This Secure and Resilient Mobile Network Infrastructure (SRMNI) R&D project will develop and refine the following two major software solutions for secure voice and text communications:

- GovSecure, a centrally managed sensitive but unclassified (SBU) voice and text capability for iOS, Android, and Windows platforms that provides secure, untraceable calls over internet protocols (IP) (not Voice Over IP [VoIP]), and
- EchoPTT Pro, a serverless Push-To-Talk VOIP application for Android, with AES256 encryption on all traffic as well as X.509 certificate-based mutual authentication and encryption on unicast interlinks crossing private and/or public networks.

Historically, secure communications require the use of specialized encryption hardware and software. This combination has an exceptionally long development/approval timeline, is not very mobile or lightweight, and is not adaptive to the ever-changing mobile phone environment.

GovSecure Server and Group Infrastructure

MANAGED SECURITY

Through the GovSecure solution, central management, control and easy administration is implemented without specialized hardware or requiring a recall of the equipment.

Also, there will be no need for controlled cryptologic item storage, safeguard or protection protocols normally associated with secure telecommunications equipment.

GovSecure and Echo PTT Pro will help deliver secure communications that provide their users the following three benefits:

- Flexibility—The solutions will work with a wide range of mobile devices and operating systems.
- Agility—The solutions can be remotely installed and secured on the fly.
- Confidence—Each solution's secure communications capability can be removed as fast as it is added via a centrally managed server.

UPCOMING MILESTONES

- GovSecure for iOS and Android apps that will be available in app stores. Windows 10 version is being developed.
- EchoPTT Pro for Android is being tested.
- Training videos and manuals for GovSecure and EchoPTT Pro are being developed.

SRMNI R&D PERFORMER

4K Solutions, LLC, Midland, Georgia