DHS Science and Technology Directorate

Homeland Security
Science and Technology

IMPROVE MOBILE COMMUNICATIONS SECURITY

Mobile communications are known to be vulnerable to various forms of attack, yet communication of voice and data over wireless is ubiquitous. In addition, changes in work patterns resulting from COVID-19 have exacerbated the potential risks associated with entire organizations working virtually over mobile networks, bringing the security of mobile voice and data communications to the forefront.

In light of acknowledged cyber-threats and to protect government interests, federal agencies handling sensitive but unclassified information also require more secure voice and data communications.

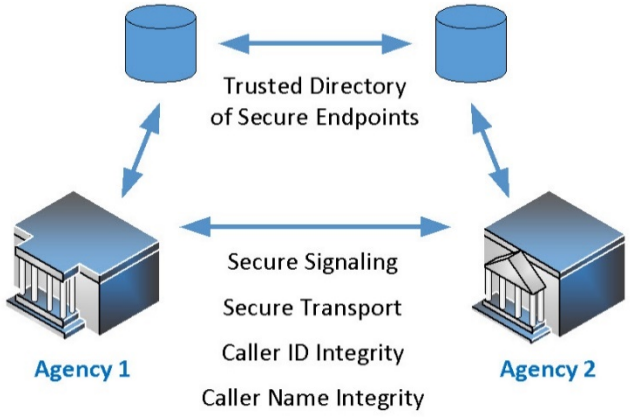
CREATING A SECURE VOICE NETWORK

Using existing commercial voice systems from leading service providers and enterprise equipment manufacturers, the Texas A&M Internet 2 Technology Evaluation Center (ITEC), in partnership with Columbia University and Texas A&M University at Commerce, is developing a testbed for full-function secured and interoperable voice and data services. The research-and-development project is part of S&T's Secure and Resilient Mobile Network Infrastructure (SRMNI) Project.

The ITEC team is defining, implementing, and testing a secure voice network that can support landline-to-landline, landline-to-mobile, and mobile-to-mobile secure communications within and between government agencies. The planned network will use existing technologies and work with legacy and emerging voice networks such as 5G to validate caller identities and establish secure connections, enabling agencies operating in sensitive areas to do so with secure communications. The testbed will include premise-based systems, cloud-based systems, and Mission Critical Push to Talk.

A SOLUTION FOR MOST TECHS & BRANDS

The testbed will create a "cookbook" for use by agencies to implement the secure voice architecture developed. The secure voice architecture will benefit several key customer types: federal agencies, government contractors,



Secure Voice Architecture

and state and local public safety agencies. Users of the secure voice architecture will benefit from secure voice communications, both in content and signaling, and protection from robocalls and "phishing" attacks through caller ID and caller name integrity.

All technologies proposed in this architecture are based on open standards, and most are standard-system capabilities. The remaining standards-based technologies are available as open-source, low-cost, or no-cost solutions. The encryption of Session Initiation Protocol data uses standard features for signaling and media using Internet Engineering Task Force Requests for Comment for Transport Layer Security and Secure Real-time Transport Protocol. These use the same proven secure authentication tools used today for secure web and banking applications.

UPCOMING MILESTONES

- Transport Layer Configuration Definitions – June 2021
- Call Routing Configurations – August 2021

SRMNI R&D PERFORMER

Texas A&M University ITEC, College Station, Texas.