Whitepaper

The Case for Secure Communications

The tapping of voice communications has occurred virtually as long as electronic communication has been in existence. In the early days of electronic communications, and prior to the implementation of digital technology, tapping a phone was very easy. One simply needed access to the physical wiring where a listening device could be connected. Today's communications landscape has migrated to mostly wireless communications. This doesn't mean that communications are more secure. In fact, it means that the attack surface has become much larger. Wireless traffic has the potential to be captured, listened to and even hijacked without any indication to those on either end of a call. The good news is that these communications can be protected with solutions that encrypt and secure voice and messaging communications so that even if its captured, it will reveal no usable information.

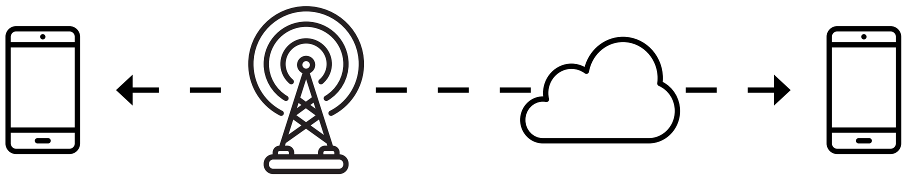
Why do we care?

Information is probably the world's most valuable commodity today and can be used to determine social habits, marketing demographics, intelligence, trends and location to name a few. There is also a wide range of data that is protected by laws such as HIPPA, FCRA, ECPA, COPA, FISMA, FTCA, FERPA, GLBA and PCI to name a few. Additionally, agencies and enterprises want to protect their IP, trade secrets, intelligence and personal information as well. Bad actors don't really follow the rules and the first step of almost every data breach is some form of social engineering or surveillance where personal information is collected and used to perform a larger targeted breach. The bottom line is that even the smallest bits of information collected from calls can be pieced together and significantly increase safety, liability, economic, and privacy risk.

Types of surveillance

There can be lawful reasons to conduct surveillance on someone's communications. When conducted in the United States, surveillance requires a warrant, issued by a judge after law providing sufficient grounds for the action. Warranted surveillance of cellular traffic involves the use IMSI catchers that enable surveillance by appearing as a valid cellular service provider which can capture and pass information without detection. The capture of communications outside of legally warranted surveillance is strictly illegal. This doesn't mean that communications are protected from illegal entities and bad foreign actors intercepting voice and messaging communications. In fact, a Department of Homeland Security (DHS) open letter to Senator Ron Wyden (D-OR) states that "the use of IMSI catchers by malicious actors to track and monitor cellular users is unlawful and threatens the security of communications, resulting in safety, economic, and privacy risks" and that "the malicious use of IMSI catchers is a real and growing risk". A recent study found more than 40 rogue cell towers in use in the Washington, D.C. area. Additionally, the attack surface is extended to TCP/IP networks, cellular infrastructure, and mobile devices themselves.

Commonly used attack vectors



Attack on Integrity of Device

Attack on Air Interface

Attack on Country’s Gateway

Attack on Integrity of Device

Attack During Network Transmission

IMSI International Mobile Subscriber Identity (IMSI) catchers enable surveillance by appearing as a valid cellular service

MITM Man-in-the-middle attacks are possible on certain wi-fi routers, mi-fi networks, or any use of unsecured TCP/IP networks

SS7 A Signal System 7 (SS7) vulnerability allows third party actors to enable the theft of data, eavesdropping of calls, interception of text messaging and location tracking

Mobile Devices Lack of password, no encryption, connection to public Wi-Fi, no VPN

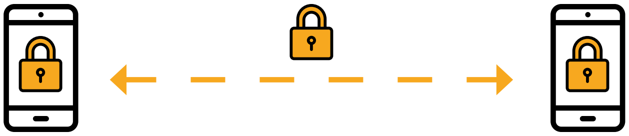
Operational Security

When it comes to operational security, agencies need to be aware of that there is an extremely wide range of information being discussed over voice and text messaging that are not secured. Although any one conversation may not contain sensitive information, there could be information discussed that when combined with multiple conversations over time, or when combined with external information, could become sensitive or even classified. Personal discussions with colleagues, friends and family can help bad actors and foreign elements glean enough personal information to identify areas that could be used for coercion, to gain access to systems and to identify employees as targets for further surveillance. Agencies and organizations should do everything possible to ensure the safety and security of their personnel and the content of discussions that may involve work and/or personal information, in the workplace, at home and especially while travelling abroad. In a public travel alert, the FBI stated that "everyone travelling abroad should assume that their calls, messaging and internet traffic are being compromised".

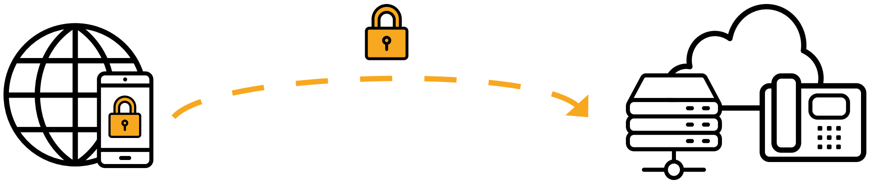
What can be done to protect voice and text messaging on mobile devices?

The first step to securing voice and text is to reduce the attack surface that is exposed. It is a pretty safe assumption that telecommunications networks in the United States are far more secure than those in use in many foreign countries, especially China, Russia, the Middle East and several third-world nations. This doesn't mean that calls in the United States are secure, these calls are also susceptible to attack and eavesdropping especially near government building, military bases, airports, hotels, coffee shops and other areas where one might set up a rogue tower or access point. Strong voice and messaging encryption should be employed on mobile devices to ensure that intercepted calls are private and secure.

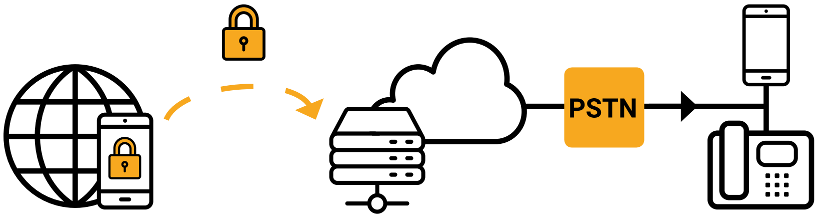
Use Cases



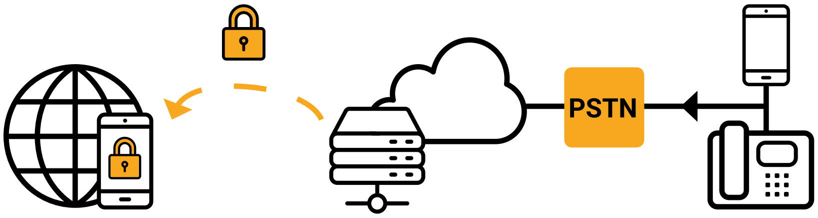
Mobile to Mobile: From SecuSUITE for Government-enabled mobile device to SecuSUITE for Government-enabled mobile device.



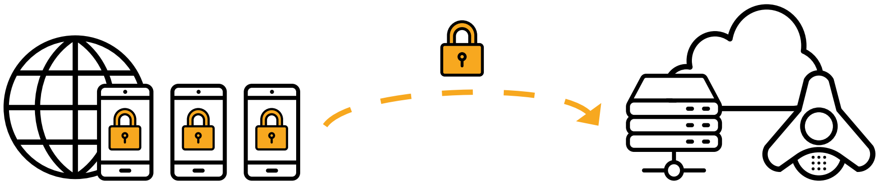
Secure Landing: From a SecuSUITE for Government-enabled mobile device to a landline within the agency network.



Break-out: From a SecuSUITE for Government-enabled mobile device to the user's home network and from there to external mobile or landlines via PSTN extension.



Break-In: From any mobile or landline on the user's home network to a SecuSUITE for Government-enabled mobile device..

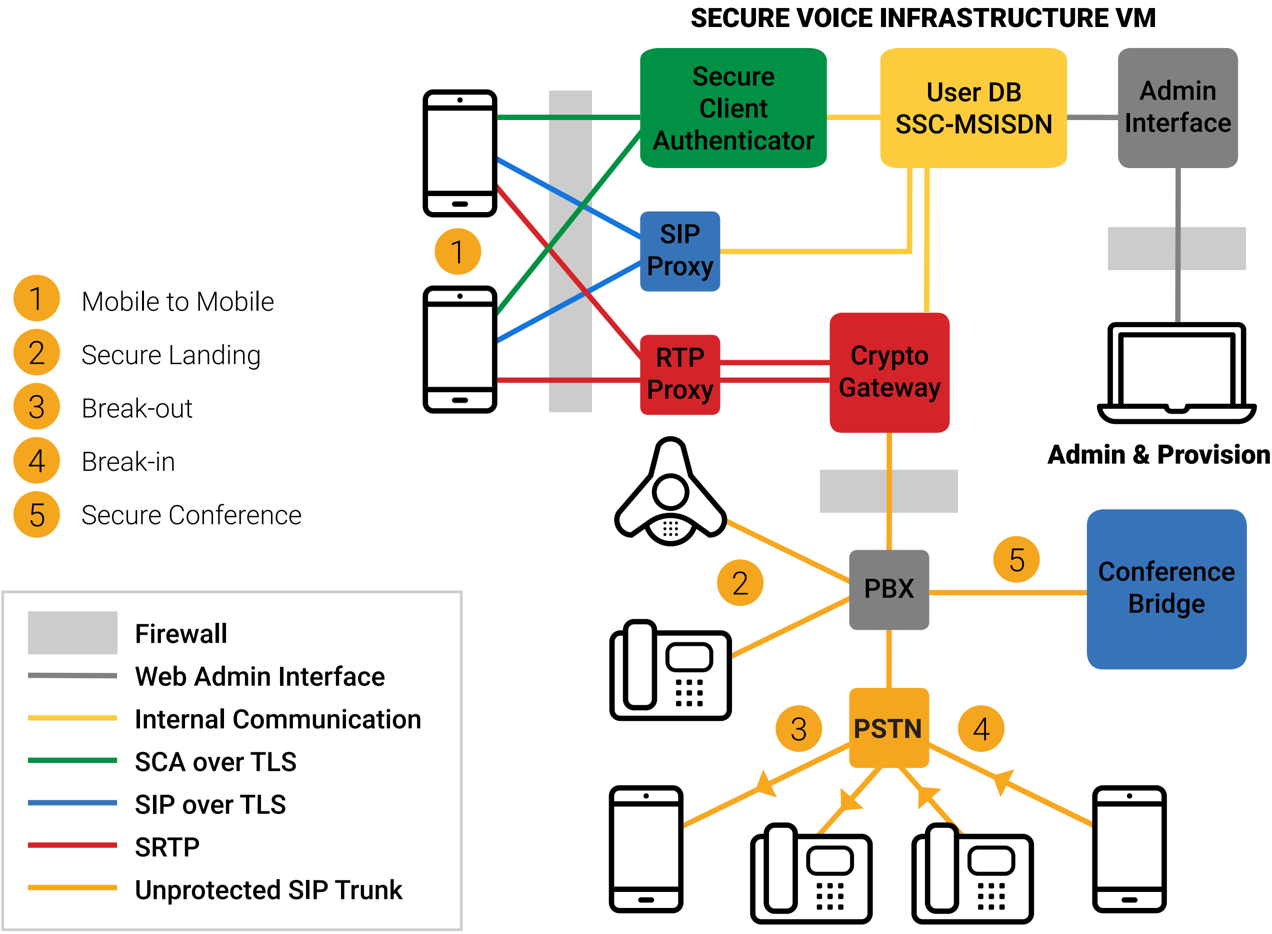


Secure Conferencing: From a SecuSUITE for Government-enabled mobile device to a secure conference bridge.

Solution Architecture

The implemented solution for secure voice and text messaging should be easy to set up, easy to use and easy to maintain. SecuSUITE for Government is intuitive with the look and feel of the native phone application that users employ every day on their iOS and Android devices. This means users can focus on communicating instead of on learning a new way to make calls or send text messages.

The SecuSUITE solution can be installed on-premise, in a data center, or in-the cloud. Soon, BlackBerry will be offering a subscription cloud based secure voice and text messaging service hosted in a FEDRAMP certified data center for sensitive but unclassified use for our federal civilian and DoD customers.
The SecuSUITE architecture ensures that communications are as secure as possible. Every call securely negotiates a fresh pair of SRTP session keys during call establishment at the beginning of each call taking place in less than 2 seconds! The encryption methodology uses ephemeral-static ECDH with S/MIME enveloped data to protect the SRTP key. After key exchange (during secure call setup) SecuSUITE implements two separate SRTP session keys, one for uplink and one for downlink resulting in, End-2-End encrypted voice and messaging over SRTP.



Certifications

To ensure the highest level of security for any application, the most stringent certifications should be sought and obtained. SecuSUITE for Government secure voice and text communication components have been tested and approved for use on U.S. Government devices up to, and including, the secret level. The software for the client and the server have been evaluated and certified to be compliant with the Common Criteria protection profile for VOIP applications and SIP servers, respectively. Additionally, the SecuSUITE client and Server have earned NIAP certification and have been placed on the NSA Commercial Solutions for Classified Program (CSfC) component list of products certified for use on classified systems.

SecuSUITE Roll-Out

Once set-up of the back-end is complete, users are provisioned through a 5 five step process that is fast and easy. Users are enrolled into the SecuSUITE for Government system via the Administrator portal which generates an invitation that the user can receive via email. The email contains a download link for the SecuSUITE application for the user's device and an activation key. Once the application is installed, the user enters the activation key and authenticates with the SecuSUITE for Government server. During the enrollment process, the client is properly configured and receives all required certificates for securing the communications towards the SecuGATE infrastructure as well as for securing the end-to-end voice communication. Once the enrollment process is complete (usually within a minute or two), the device is ready to make secure calls with other SecuSUITE for Government users.

5 Steps to Roll-Out SecuSUITE for Government

1. On-Premise Install

Licences purchased and servers set up on-premise[1]

2. Admin Set-up

Customer admin enrolls users via portal

- Name
- Email
- Mobile number

3. Activation

User receives activation key.

- App download link
- Activation key
- App pushed via MDM (Optional)

4. Download

User enters activation key

5. Roll-Out complete

SecuSUITE for Government is ready for use

[1] Cloud deployments also available.

Summary

In today's environment where information is key to every aspect of our daily business and personal life, agencies need to ensure that great care is taken to protect and ensure the safety and security of their personnel and the content of discussions that may involve work and/or personal information. Hackers, scammers and state sponsored actors are actively involved in gathering information by any means possible, including implementing rogue cell towers, using public Wi-Fi and various social engineering methods. The risk significantly increases when employees are traveling or using free public Wi-Fi. SecuSUITE for Government provides an encrypted solution that ensures communications are secure and easy to use. Is your agency doing all it can to protect its information and its employees?