Cellcrypt
Government Grade Encryption for Mobile Calls Over Satellite
Protect Mobile Telephone Calls Over Satellite Using Government Grade Encryption

Running the Cellcrypt App on Standard Smartphones Gives BGAN Users Strong End-to-end Protection

The mobile phone is an indispensable communications tool for government officials across the world, and much of the business that is conducted over these phones is sensitive. The most sensitive conversations relating to defence, public order and national security are conducted using specialist communications systems which incorporate high grade encryption. However, because such systems are expensive, with significant management overheads, and their use is generally restricted to personnel with security clearances, the vast majority of government conversations are carried out using over standard commercial telephone networks. Despite a range of built-in security measures, such networks are vulnerable to interception. However, interception can be defeated by adding an extra layer of end-to-end encryption, where the call is encrypted by the caller and only decrypted by the recipient. This functionality is now available in the form of an app that can be downloaded and run on a standard smartphone, and which will work on both cellular and satellite networks.

The Challenge

It is commonly thought that the protection provided to 3G mobile telephone calls cannot be defeated. However, while it is undoubtedly much harder to intercept and exploit digital communications than analogue calls there are nevertheless important vulnerabilities which can be, and are, exploited. Digital call encryption is hard to overcome by an attacker. In the absence of end-to-end encryption, however, confidentiality relies on the right level of protection being used at every step along the communications chain between callers. In practice, there are frequently implementation weaknesses, including encryption not being turned on at all along some segments of the call route, weak encryption algorithms being used, and vulnerabilities in key management. Furthermore, a single call may involve multiple service providers, and cross telecommunications infrastructures in several countries, operated by a mix of different companies and subcontractors. It is thus impossible for one service provider to guarantee end-to-end call security using the existing global public telecommunications infrastructure.

Government telephone calls are, of course, an attractive target for a range of individuals and organisations. Hostile intelligence services are likely to be the most dangerous and technologically capable threat, but they are by no means the only one. Terrorists, organised criminals, activists, disgruntled government employees and even journalists all have the motivation, opportunity and capability to inflict real damage in the context of a system without true end-to-end security. Perhaps the most insidious threat exists within the carrier network itself, where the call is often not encrypted, and listening devices can be installed or calls intercepted, often through an insider attack where an employee is bribed, coerced or otherwise induced to perform the attack.

It is of course possible to use high grade encryption, of the kind used to secure military battlefield communications. This approach, however, involves so many constraints and overheads that it is rarely practical for anything but the most sensitive applications, for it requires specialised equipment which must be stored under secure conditions and may only be handled by specially cleared personnel. There is a clear requirement, therefore, for a more affordable, straightforward and easy to use means of protecting mobile telephone communications which can be deployed to normal users, requiring none of the special clearances and management overheads of high-grade military crypto.
The Solution
In order to satisfy its government customers’ requirement for confidentiality when using their mobile phones over satellite networks, Inmarsat Global Government has identified a simple and practical method of making secure calls, and sending secure texts, over satellite. Cellcrypt Mobile is an easy to use, next generation software solution for voice encryption that runs on standard cellphones and uses Internet Protocol networks to deliver unparalleled voice quality, high-strength security and low voice delay.

The solution is to connect the smartphone to the Inmarsat BGAN terminal by Wi-Fi, either using a wireless router, or directly, in the case of Wi-Fi enabled terminals (such as the Hughes 9201 or 9202, or the Cobham 700). The Cellcrypt app is then downloaded from the iTunes store or the Android, Nokia, BlackBerry equivalents. Once the app is activated, it can immediately be used to make calls to other smartphones running Cellcrypt or, via a Cellcrypt Gateway, to a subscriber operating through a PABX.

Cellcrypt establishes high-performance encrypted voice calls between trusted wireless devices using the Encrypted Mobile Content Protocol, a set of standards-based protocols for optimizing delivery of encrypted real-time content between cell phones over low-bandwidth wireless networks. Cellcrypt’s products are certified to the US FIPS 140-2 standard, approved by the US National Institute of Standards and Technology. Voice calls are double-wrapped for added security: voice calls are first encrypted using RC4-256 bit and then encrypted again using AES-256 bit.

Applications

Overseas Government Offices
Government personnel operating overseas can use secure communications while avoiding local untrusted communications networks. They can do so discreetly, using standard, unmodified smartphones.

Military Welfare Calls
Soldiers, sailors and airmen deployed to operational theatres can safely call their families at home using normal cell phones while sharing a satellite connection, without compromising their security.

Disaster Recovery
Cellcrypt and BGAN together enable secure communications even when normal terrestrial communications infrastructure has been disabled or destroyed.

We connect those who protect