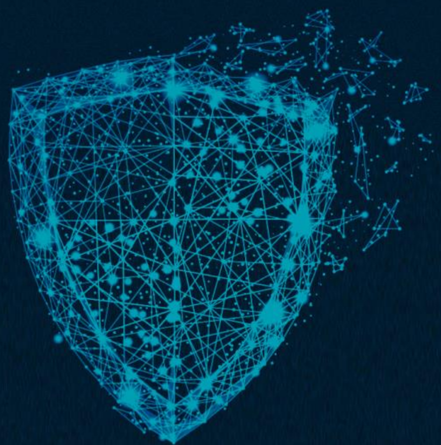
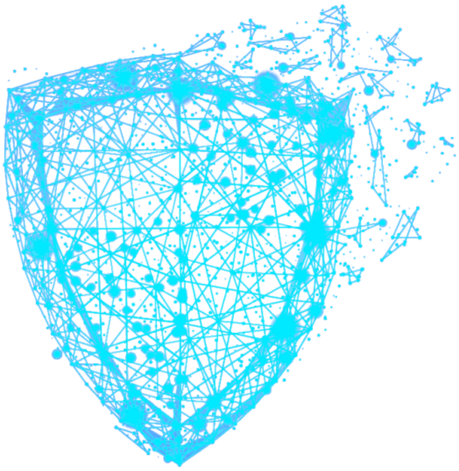
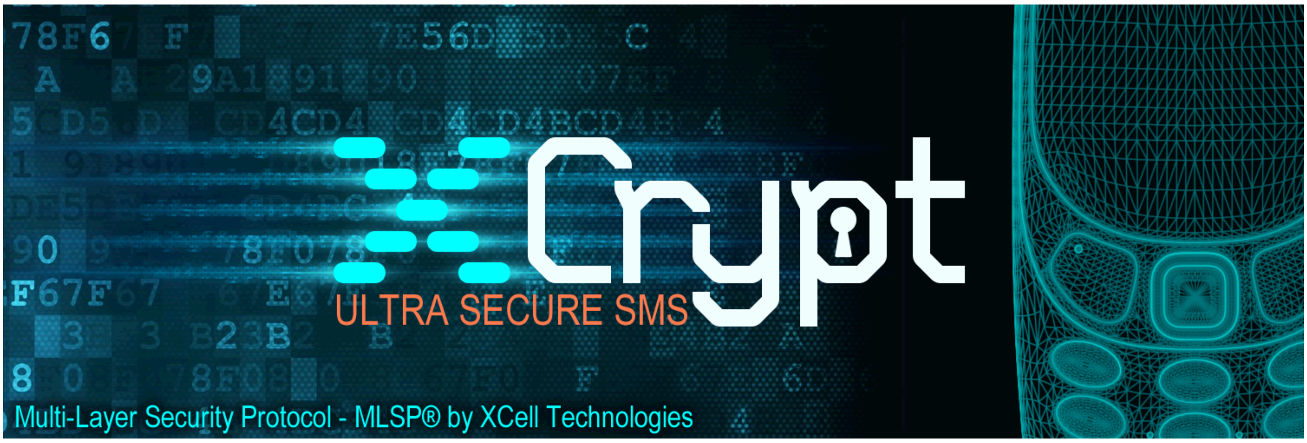
ULTRA SECURE SMS
MULTI-LAYER SECURITY PROTOCOL - MLSP®



x-cellular.com

Contents





WHEN ENCRYPTION IS NOT ENOUGH: ULTRA SECURE MESSAGING

- SMS ENCRYPTION REDEFINED -

A revolutionary innovation: Multi-Layer Security Protocol - MLSP® by XCell Technologies

Real end-to-end encryption and protection

Introduction

If you are either super important, super paranoid or a super spy, there are times when you need to be able to use a cell phone and not leave a trace or any chance to anyone to intercept your calls and text messages, including law enforcement and intelligence agencies.

Secure = encryption? Well, think again...

Nowadays, interception issue affects most of the people, even if they are not aware of it. Not to mention so called “off air GSM interception systems” or also known as “IMSI-catchers”, "GSM Interceptors" or "StingRays", it has been known since 2014 that using the legacy SS7 (Signaling System No. 7) protocol SMS based traffic text messages can be easily intercepted by using diameter based networks independently of device or OS type. Signaling System No. 7 vulnerabilities are easy to be exploited even by hackers, being a 50-year old protocol that is probably part of a majority of cell phones and text messages in the world.

Generally speaking, most of aware users regarding cell phone interception by above technologies, believe that using encryption solutions will secure their calls and text messages. It is encryption a real solution? Let's see...

Law enforcement, homeland security and other related actors have plenty of methods to intercept messages and read text content, even when using encryption. Ranging from SS7 exploit, encryption backdoors or intentionally weaken popular encryption algorithms to lawful hacking that circumvent encryption and hi-tech decryption technology, all are there at their fingertips.

Encryption will not protect your privacy. At all

Recent headlines warn that the government now has greater authority to hack your coell phones, in and outside the US. Changes to federal criminal court procedures known as Rule 41 are to blame; they vastly expand how and whom the FBI can legally hack cell phones. But just like the NSA's hacking operations, FBI hacking isn't new. In fact, the bureau has a long history of surreptitiously hacking us, going back two decades.

That history is almost impossible to document, however, because the phone hacking happens mostly in secret. Search warrants granting permission to hack get issued using vague, obtuse language that hides what's really happening, and defense attorneys rarely challenge the hacking tools and techniques in court. There's also no public accounting of how often the government hacks phones. Although federal and state judges have to submit a report to Congress tracking the number and nature of wiretap requests they process each year, no similar requirement exists for hacking tools. As a result, little is known about the invasive tools the bureau, and other law enforcement agencies, use or how they use them. But occasionally, tidbits of information do leak out in court cases and news stories.

When a password is just not enough to protect your privacy

In November 11, 2016, Federal Bureau of Investigation (FBI) General Counsel James Baker reported that for fiscal year 2016, the FBI had encountered passcodes on 2,095 of the 6,814 mobile devices examined by its forensic laboratories. They were able to break into 1,210 of the locked phones, leaving 885 that could not be accessed.

In the 2017 fiscal year, Wray advises the FBI was able to access data stored in 7,775 devices "using appropriate and available technical tools," having the legal authority to do so. "Each one of those nearly 78-hundred devices is tied to a specific subject, a specific defendant, a specific victim, a specific threat".

Insisting the FBI is "on the front line fighting cyber crime and economic espionage," Wray adds that "Information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep the American people safe."

The National Security Agency had, in secret, worked to undermine certain popular encryption algorithms. In addition to direct attempts to break encryption with mathematical methods, an NSA project code-named Bullrun included efforts to influence or control international cryptography standards, and even to collaborate with private companies to ensure the NSA could decode their encryption.

This came to light when former NSA contractor Edward Snowden revealed a massive trove of files about U.S. government spying in 2013 and reignited the debate about what abilities and powers the government should have to read encrypted material.

Backdoors provided for law enforcement

Encryption backdoors remain largely viewed as weakening everyone's protections all the time for the sake of some people's protections on rare occasions. As a result, workarounds like the FBI found are likely to be the most common approach going forward. Indeed, in recent years, law enforcement agencies have greatly expanded their hacking capabilities.

Many reputable encryption developers and companies have chosen to retain the ability to read and use their customers' content, or perhaps they decided there is not a sufficient business case to add end-to-end encryption or user-controlled encryption. Their users' encrypted content is more readily available to law enforcement because they hold the decryption keys. The same companies offer their services in a way that encryption does not preclude their ability to hand over the content to law enforcement in response to a warrant. Are those services as secure?

Lawful hacking

Most of national security agencies had been shown to have immense surveillance capabilities actively deployed on a mass scale, especially in those countries where the functions of law enforcement and national security overlapped. Beside encryption master-key and built-in backdoors that provide law enforcement exceptional access to anyone secrets and privacy, they now have unprecedented access to information through open-source intelligence, collection of metadata, sophisticated traffic analysis tools and data analysis algorithms. Many local and international laws are mandating insecurity by requiring government access to all data and communications that permits lawful hacking (otherwise known as encryption circumvention). We see this, for example, in the joint statement of Europol and ENISA in 2016, where they say:

"Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible. … For the investigation and disruption of crimes, it is important to use all possible and lawfully permitted means to get access to any relevant information, even if the suspect encrypted it. To achieve this, it would be worthwhile to collect and share best practices to circumvent encryption already in use in some jurisdictions. …"

In this regard, the European Commission announced on 18 October 2017, as part of its anti-terrorism package, that it would "support Europol to develop further its decryption capability".

A lawful hacking approach starts to look like a viable option as it turns out that it is not so easy to create encrypted protocols, platforms or services without any weaknesses. (See, for example, the recently unveiled weakness in the Wi-Fi encryption protocol WPA2, known as Key Reinstallation Attack (KRACK), and the Infineon crypto chip key generation bug). The presence of weaknesses means there may be a way in for law enforcement without the need for the decryption keys. However, often, exploiting security weaknesses requires a more targeted approach, as well as more sophisticated technical resources, which smaller law enforcement agencies may not have. Also, any security weakness that law enforcement could use, if discovered, could be potentially exploited by cyber criminals or other state actors.

We also see in the UK the emerging idea that the use of encryption should be an aggravating factor in sentencing for terrorist offences. While this idea is now focused on terrorism, it might be later applied to other criminal offences. This is alarming.

Encryption vendors and law enforcement work together to solve access "problem". One suggested fix is one-way information sharing where vendors make law enforcement aware of unpatched exploits, allowing the government (and anyone else who discovers it) to use these vulnerabilities to gain access to communications and data. It's a horrible suggestion - one that puts vendors in the liability line of fire and encourages continued weakening of device and software security.

Several individuals with backgrounds in security and systems have begun to explore possible technical mechanisms to provide government exceptional access. Three individuals presented their ideas to the committee.

- Ernie Brickell, former chief security architect, Intel Corporation, described ways that protected partitions, a security feature provided by future microprocessor architectures, could be used to provide law enforcement access to devices in their physical possession, provide remote access by law enforcement, or provide key escrowed cryptography for use by applications and nonescrowed cryptography for a set of "allowed" applications.

- Ray Ozzie, former chief technical officer and former chief software architect, Microsoft Corporation, argued that if a user trusts a vendor to update software, the user should be able to trust the vendor to manage keys that can provide exceptional access. He proposed that this extension of the trust model used for software updates could be used to provide government exceptional access to unlock mobile devices. Ozzie also provided the committee with materials describing how this approach could be extended to real-time communications such as messaging.

- Stefan Savage, professor of computer science and engineering, University of California, San Diego, described how phone unlock keys could be stored in hardware and made available via an internal hardware interface together with a "proof-of-effort" lock that together would require physical possession and a time delay before law enforcement could unlock a device.

Mobile threats

Mobile threats can be commonly divided into three groups: Communication related, Device related and User actions related:

> Communication related threats are mostly the product of communication interception. Simple tactical solutions, pretending to be legitimate cellular-base-stations, can be used to intercept exchanged communication over a regular cellular network. Data communication can also be intercepted over WiFi networks using simple "Man in the middle" techniques.
>
> Device related threats are reflected by the amount of information kept on the device as well as the ability of installed applications to access that information. Be it a legitimate application that is granted with access to sensitive information, a rogue by nature application that is downloaded from unknown sources, or a Trojan horse that was specifically engineered to steal information, all have a huge effect on the ability to secure both private as well as corporate related data.
>
> Last but not least are the users themselves. Users are usually reluctant to give away their mobile freedom, usability and functionality for better, higher level of security. Therefore, mobile security through restrictions is often not effective as users generate and require access to large amounts of

information, applications of all sorts and kinds as well as extensive social media activities without understanding or sometimes even care about the security implications associated with those actions. Counting on users to do the right security savvy thing or make the right security savvy decision when handling new and exciting mobile functionalities or content, would, in most cases lead to a security disaster. End users education is no less important as most users are not even aware of the threats they are exposing themselves to. Smartphones have changed our world for the better but also created many security challenges. It is time for innovative solutions to step up their mobile security game.

Our approach regarding SMS encryption and protection

At XCell Technologies we are serious about mobile security, bringing you the most advanced SMS security solutions. Concerns about government mass surveillance and their ability to decrypt anything by using given master-keys, backdoors, lawful hacking or effective decryption solutions were the factors driving us to develop a brand new and 100% secure SMS communications which use not only strong military grade encryption but adding a new security layer by exploiting GSM network via MLSP®, to make sure there is no way to intercept text messages or metadata, even in encrypted mode. All above overleap existing commercial-encrypted apps, services, devices, and also law enforcement access to your sensitive info.

GSM provides by default only a basic range of security features to ensure adequate protection for both the operator and customer. Over the lifetime of a system threat and technology change, and so the security is periodically reviewed and changed here on XCell Technologies, and then applied on our products.

Taking advantage on GSM network architecture and SMS Transport Protocol, our SMS encryption technology is capable to send/receive encrypted and non-interceptable messages.

Our SMS encryption application called XCrypt use a groundbreaking multi-layer technology to protect SMS from being intercepted and decrypted. As a unique encryption application, beside strong military grade encryption, XCrypt use a brand new patented technology in order to send/receive encrypted messages: discrete GSM channels or Multi-Layer Security Protocol®. That will protect not just encrypted text messages but also metadata which is not encrypted.

XCrypt concept. An insight into techniques used for 100% secure text messages

Definitions

"A-Party" phone is the sender phone which send encrypted messages via MLSP®
"B-Party" phone is the receiver phone that will decrypt and display received message.
Plain text message: a standard text message that can be read by anyone. Can be intercepted and read with no effort.
Encrypted message: an encrypted text message that can be read only by using the right password. Can be easily intercepted in encrypted mode but cannot be read. A password is required in order to read the message.
Metadata: data about data. SMS metadata is not encrypted because is not contained by the encrypted text itself, but law enforcement agencies are collecting unencrypted metadata to characterize the encrypted data. SMS metadata contain data about sender, receiver, message encoding (UTF8, UnicodeX etc.), date/time and length.
Non-interceptable message: a text message (plain text or encrypted) which cannot be intercepted by any means.
Real end-to-end encryption: no Internet and 3rd party servers involved.
XCrypt: software application that use MLSP® in order to send/receive ultra-secure messages.

MLSP®

Multi-Layer Security Protocol - MLSP® consist in:

1. **Physical layer:** encrypted text message.

The phone will encrypt text messages by using following protocols:

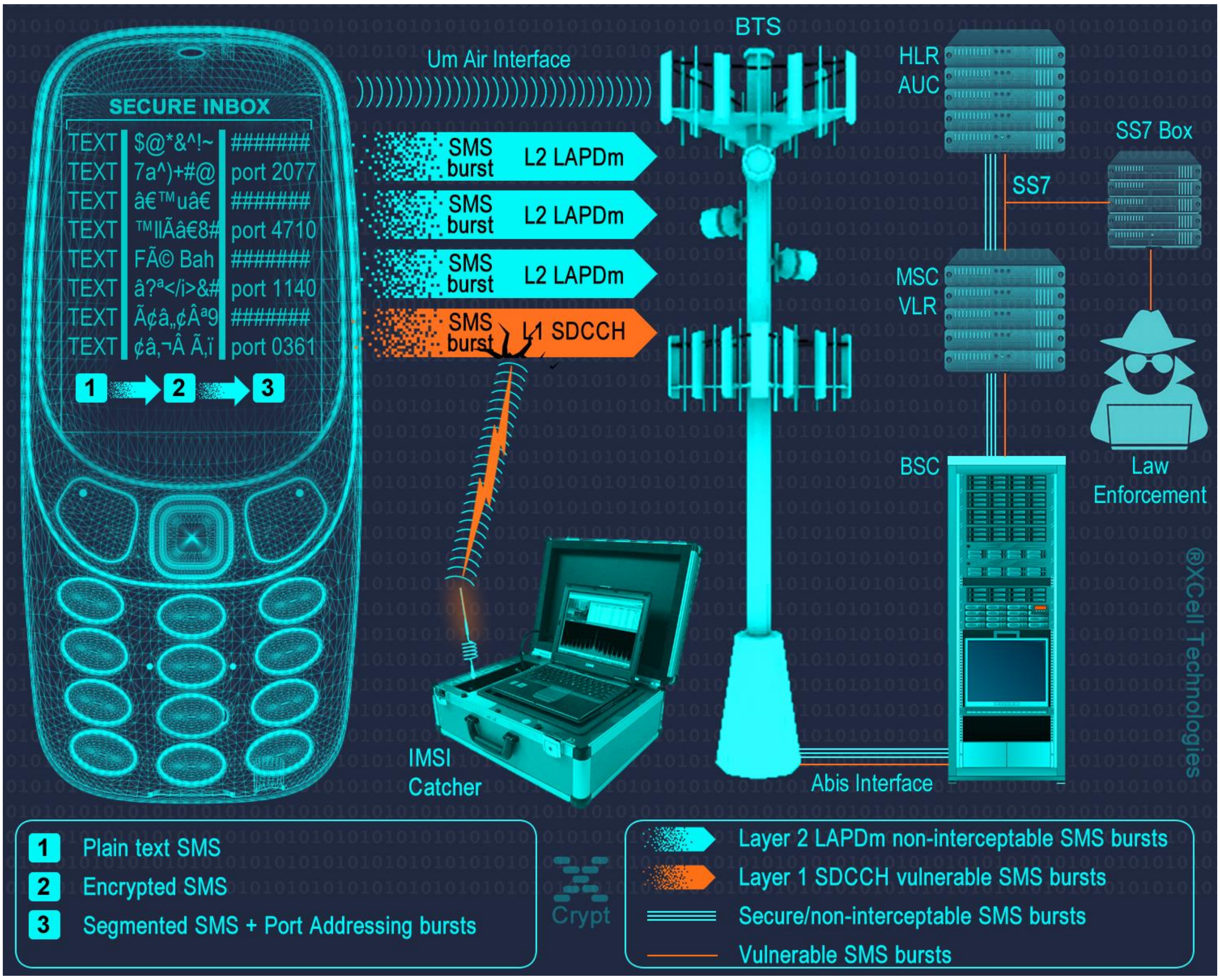
- RSA
- AES 256
- Elliptic Curve (ECIES) 256
- SHA256
- Protected by ITSEC Evaluation level 3

2. Multi-layer routing and transport protocol. Encrypted SMS data is randomly segmented and distributed in bursts by Application Port Addressing Technology, via discrete GSM channels which usually are not "listened" by mobile interception systems (IMSI Catchers, GSM Interceptors or StingRays), both in air interface (UM Interface in terms of GSM networks) and Abis, A and C-G mobile network interfaces. This way, SMS data which is usually sent over GSM Layer 1 (and widely intercepted on Layer 1) will be sent by using a combination of GSM Layer 1 and GSM Layer 2 (LAPDm). By consequence, no mobile interception systems (as GSM Interceptors) and lawful

interception systems (SS7 interception also known as network switch based interception or interception by the help of network operator) will be able to intercept the whole message but only a few bursts which are encrypted anyway.

3. Metadata protection. Regular SMS metadata is not saved in a separate file (called a metadata file). XCrypt separate metadata and the data it describes (SMS encrypted text), sending metadata file in bursts over the network, by the same Port Addressing technology. Metadata is of little value without the data file (SMS) it relates too. At the same time, metadata makes the data more usable and therefore, more valuable. An encrypted text message with separate metadata file will reveal nothing about SMS sender and receiver.

How does it work



1. **Phone level**

At phone level XCrypt use a technology called port directed SMS, which is widely implemented in J2ME MIDP on mobile devices. The concept is basically that when an user send an encrypted SMS message to "B-Party" phone, a particular port number will be specified along with encrypted message, so only the device which is "listening" on that particular port will be able to receive an encrypted message. When a message is received on a port that the application is listening on, the message gets directly routed to secure Inbox instead of going to the standard message Inbox.

XCrypt will locally encrypt text messages at military level, then by message segmentation and Port Addressing will send randomly splitted bursts (bit streams) along with certain port address data by adding redundant bits to information binary string, to "B-Party" phone. Along with encrypted split message, the application on "A-Party" phone will send Port Addressing data, which will trigger opening certain Port Address on "B-Party" phone. This way, encrypted message will go through, avoiding standard phone Inbox and arriving directly on secure Inbox.

All this steps are transparent on receiving ("B-Party") phone, which also require user interaction which have to allow message to be routed to secure Inbox and decrypted by inserting the right password.

On "B-Party" phone, by port destination address, encrypted bursts will be selectively received, concatenated, decrypted and displayed only on "B-Party" phone which use the same XCrypt application that "listen" on certain receiving ports.

If on the "B-Party" (destination phone) is not also installed XCrypt app, then received message will not be delivered nor displayed by the phone (not even in encrypted/unreadable mode) due to Port Addressing technology which filter messages by port address.

When encrypting SMS, metadata file will be generated separately from text message and not as an integral part of the message as regular SMS do. Metadata file will be then truncated and sent in bursts over GSM network, by Port Addressing technology. This way no metadata can be intercepted by SS7 means.

At this level, handset vulnerability refer to forensic grade hardware and software that intend to extract system files and private data off the phone, including decrypted messages stored on XCrypt secure Inbox. XCell phones are protected against forensic procedures by USB volatile filters which does not permit any unauthorised USB connection, triggering motherboard self-nuke. Moreover, XCrypt run on Sandbox partition which is 100% encrypted and protected against file extraction by self-delete mechanism.

2. Um level

Um interface (the radio link between the cellular network and the subscriber handset) is the most vulnerable and exploited part of the GSM network by MItM attacks (IMSI Catchers, GSM Interceptors and StingRays), since no network operator help or target consent is needed. XCrypt will make use of GSM network architecture and SMS Transport Protocol in order to protect (already) encrypted messages to be intercepted even in encrypted mode. After encryption, the modulation signal has a carrier wave using GMSK (Gaussian Minimum Shift Keying) modulation. GMSK is a two-state modulation based on the frequency keying stroke.

On Um interface XCrypt will use MLSP® technology: encrypted message bursts are not sent only on usuall L1 SMS channels - SDCCH (Standalone Dedicated Control CHannel) signaling channels, but also on other available channels which are not subject of SMS interception, forcing Signaling Layer 2 (data link layer based on LAPDm protocol) for SMS Transport.

Since GSM Interceptors are "listening" only SDCCH physical channels in order to intercept text messages, will catch only a few encrypted bursts sent over SDCCH but not the whole encrypted message which is split and sent over multi-channel by MLSP® technology.

Same for metadata file: is sent over the network in bursts, separately from encrypted message body. No metadata extraction is possible at this level.

3. Core network level

The four-layer transport protocol stack of SMS (application, transfer, relay, and link) is used at this level and the transfer layer of this stack is the one which secure text message. GSM core network consist in Mobile switching center (MSC), Home location register (HLR), Authentication center (AuC), Visitor location register (VLR) and Equipment identity register (EIR), which are all vulnerable to network switch based interception, also known as SS7 interception or lawful interception. This kind of interception can be successfully performed only by law enforcement and homeland security agencies, by the help of network provider that allow monitoring hardware installation (SS7 boxes) at their core network based on Communications Assistance for Law Enforcement Act (CALEA). CALEA's purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance, allowing federal agencies to selectively wiretap any telephone traffic. CALEA covers mass surveillance of communications rather than just tapping specific lines and not all CALEA-based access requires a warrant. Generally, lawful Interception implementation is similar to the implementation of conference call. While A and B are talking with each other, C can join the call and listen silently.

At this network level, the main security vulnerability consist in lawful interception. XCrypt is taking advantage on GSM core network, sending both encrypted and non-interceptable text messages by using MLSP® technology. Core network protocols cannot be enforced as Um interface can. Actually there is no need to manipulate those protocols and transfer layers as long as message bursts that transit this part of the mobile network can be logically concatenated (fit together) by Port Addressing and decrypted only by "B-Party" phone which run the same XCrypt application and by knowing the right password. By consequence, no text messages can be entirely intercepted by a third party that use CALEA - lawful interception. A few encrypted SMS bursts which are eventually intercepted by SS7 cannot lead by any means to SMS interception. Thus no private data will be collected by this method, phone user privacy being preserved peer-to-peer from "A-Party" to "B-Party" phone.

Let's face it: most of nowadays encryption solutions are taking care only on text itself, neglecting message metadata which are still sent on plain text over the network, due to network requirements. Law enforcement and other actors are taking advantage on this, collecting unencrypted metadata to characterize the encrypted data, metadata being this way a valuable source of information for them.

By using MLSP® technology on both Um and Core network levels, collecting unencrypted message metadata is not possible, thus no way to extract any additional info beside encrypted message.

It has long been said that it doesn’t matter how secure your organization, or personal information and assets, are if you connect them with third parties that are less secure. So take note: servers are third parties.

A real end-to-end encryption require no third parties involved on the way from "A-Party" to "B-Party" phone.

For maximum level of security and privacy, XCrypt does not require any Internet connection, third party servers or monthly subscriptions. All processes and protocols run locally on the phones (on Sandbox partition) providing this way not just a real end-to-end unbreakable encryption, but also non-interceptable messages by the reasons explained above.

Holistic

XCrypt address the whole breadth of threats and attack vectors, providing the enterprise and private individuals with a holistic approach to the whole range of SMS security issues.

Flexible

With the ongoing fast changes in the mobile domain together with the growing security challenges those changes bring, XCrypt provide flexibility and robustness to address rapid changes in interception technology.

Usable

Balancing security and usability is a key success factor. Security by restrictions usually drives the common user (who usually cares more about his convenience than the security risks his actions create) to seek the required functionality elsewhere and carry two devices – one is restricted and the other is usable. This creates a whole new spectrum of security challenges since the user is now in charge of using the right device at the right time. The challenge here was to create a solution that is both usable as well as secured. XCrypt is our comprehensive answer.

Transparent

Since the user is the weakest link in any security structure, XCrypt generated security have been transparently implemented into the mobile device, protecting the end-user at all times without the need for any end-user decision making or specific interaction.

Up-to-Date

Multi-Layer Security Protocol (MLSP®), the security solution used by XCrypt has been designed with the ever changing SMS security threats landscape in mind, having the the ability to quickly adjust to known and unknown threats. The infamous “cat and mouse” security game, in which an identified vulnerability is patched just for another vulnerability to appear has been replaced with a flexible, fast moving, intelligent mechanism.

Organizations and private individuals have to rethink their mobile security strategy and realize that one-size-fits-all mobile security structures may not be suitable for some of the most sensitive functions. Organizations should also aim to provide employees with a security solution that offers the optimal balance between ultimate freedom-of-use and robust protection instead of applying security by restriction. XCrypt is just the right answer.

XCrypt has been already implemented as standard on XCell Basic v3 Stealth Phones, both on Basic and Advanced versions.

x-cellular.com