



Cellcrypt Security Brief

JULY 2010

*An Introduction to Cell Phone
Voice Call Interception and Security*



Table of Contents

Cell phone voice calls are vulnerable.....	2
Multiple Interception Threats.....	3
Increasing Evidence of Problem.....	5
Practical Advice.....	6
Appendix: GSM Cracking.....	7
Relevant Articles.....	9
About Cellcrypt.....	10

Cell phone voice calls are vulnerable

High profile attacks on voice calls have highlighted the well-documented gaps in security within cellular phone networks. Barriers exist to prevent most opportunistic snoopers but professionals with insider access or specialist equipment can overcome these with concerted effort.

Cell phone usage has grown rapidly since the first cell phone call in 1973 to be the most pervasive communications technology in the world with over 4 billion users. Before second generation (2G) cellular networks arrived in 1988, communications were analogue and not encrypted meaning that interception was easy for anyone using a radio scanner.

Since digital technology was introduced with 2G networks it has been much more difficult to intercept calls due to digital encoding and data compression as well as call encryption. However, over time researchers, hackers and criminals have developed more sophisticated attack methods and leveraged the vast increase in computing power since 1988 to exploit weaknesses in cellular call architecture.

Eavesdropping cell phone calls splits into two main challenges: physically intercepting the call, and then cracking or bypassing any encryption that protects the call.

Because a call is routed over a number of different network segments as it travels between caller and receiver, a cell phone voice call is vulnerable to interception at a number of different points and by a number of different methods, for example: on the device via malware or physical bugs, at the air interface between cell phone and base station tower by sophisticated radio interception equipment or in the carrier's internal network using fixed line interception equipment.

This fixed line interception equipment could be operated by the carrier itself as telecommunications operators have lawful intercept capabilities (often mandated by national security legislation) to aid criminal investigations and counter terrorism and one method of attack is to subvert this lawful intercept equipment.

Because the network segments that a call traverses may be owned by different operators, sometimes in different countries and subject to locally defined security policies, it is challenging for a mobile service provider to guarantee call protection over the entire route taken by the call. Many nation states are perceived to intercept calls as standard policy and it is not clear to callers how their calls are routed through multiple countries. Cell phone calls, particularly when made internationally, require callers to trust many organizations and networks that they do not know and are unable to assess for security risks.

Although encryption promises to keep calls confidential standard cellular calls suffer from a variety of encryption implementation weaknesses including encryption not being turned on at all along major segments of the call route, weak encryption algorithms being used and vulnerabilities in key management.

These inherent vulnerabilities mean that for the security-minded, the only way for callers to have assurance that their voice communication is safe from eavesdropping is to use their own end-to-end encryption system. This encrypts a call on the caller's handset and transmits it to the receiver's handset where it is decrypted. Assuming keys remain secret and encryption is high-strength, even if the call is intercepted, it cannot be listened to.

By using end-to-end encryption users can communicate securely over any network infrastructure, even if perceived as insecure, with the call's content being protected from attack between caller and receiver, allowing them to discuss sensitive and confidential information without the risk of it being compromised.

Multiple Interception Threats

There are several methods of cellular voice call interception, with techniques and equipment improving all the time. There is a mature commercial industry dedicated to lawful surveillance and counter surveillance solutions used by government, military and law enforcement agencies. Although these systems require government licenses to operate, inevitably some technology and research is subverted for illegal use by criminal organizations, researchers and hackers.

As the cost and technical complexity of radio wave interception reduces and becomes more accessible to more people a new dimension of threat appears, in addition to individuals being actively targeted, in which multiple calls in a certain location are randomly captured and recorded for subsequent analysis. This harvesting of calls may become prevalent around financial districts, celebrity neighborhoods, political and business conferences, international hotel districts or any densely populated area that may yield conversations containing confidential data.

DEC 2009 UPDATE: Cellular encryption cracked

In 2009, a team of independent researchers published a 'codebook' that enables the encryption in GSM, used in 80% of mobile phone calls globally to be cracked using off-the-shelf computers. This pre-computed codebook is freely available on the Internet and requires no more than a normal laptop and a widely available programmable radio system for individuals to intercept and crack GSM calls.

The security in 3G is much stronger and was considered unbreakable until January 2010 when a leading cryptographer published a paper that details an attack that cracks the encryption in less than 2 hours using a standard PC – although it is expected that it will be some years before equipment is available to eavesdrop 3G calls in the real world.

Below are the most common methods of eavesdropping calls.

Active attacks

This attack uses a radio scanner to intercept and manipulate the radio signal between the cell phone and the cellular base station tower.

It exploits a particular weakness of some cellular systems whereby cell phones do not check the authenticity of base stations that they connect with. Because cell phones continually scan radio waves and switch to base stations with the strongest signals, it is easy for a scanner that impersonates a base station to cause all cell phones in an area log on to it simply by transmitting the strongest signal.

Once a scanner has control of a connected cell phone, then it can manipulate communications in several different ways. First and most simply, it can redirect outgoing calls from the cell phone through its own communication channel and record the call. However, because the cell phone is not registered with an authentic base station it is actually offline and no incoming calls can be received (an incoming caller will typically be diverted to standard voicemail or get a "phone unavailable" message).

Second, it can perform a man-in-the-middle attack where two independent connections are made, one with the cell phone (whilst impersonating the base station) and another one with the base station (whilst impersonating the cell phone). By relaying all messages and calls between each, it can eavesdrop calls while simultaneously making both cell phone and base station believe that they are directly connected. Because the cell phone is connected to an authentic base station (albeit through a fake intermediary one), both outgoing and incoming calls can be made and eavesdropped.

If encryption is being used then this attack is able to instruct the phone to turn its encryption off, thereby bypassing the normal encryption between the phone and the base station. The unencrypted call is then readily eavesdropped.

This method is called an active attack because it actively interferes with the radio signals and can be detected by mobile operators if the right detection equipment is installed.

Although, 3G systems use mutual authentication (the 3G cell phone checks that the 3G base station is authentic before logging on so cannot be exploited in the same way), 3G systems also interoperate with GSM systems to maximize network coverage so a fake GSM base station can still have a 3G handset connect to it.

Passive attacks

This method also intercepts the radio signal between the cell phone and the base station but simply decodes the signals without needing to interfere with them. This makes the attack particularly dangerous because its activity is impossible to detect. Passive scanners contain advanced processing software that can be run on a laptop and a programmable radio receiver and antenna. Without disturbing the normal operations of the cellular network, the passive scanner listens to the radio waves of the cell phone call and processes them. Depending on the sophistication of equipment used, individual calls can be targeted or multiple calls harvested.

If a call is encrypted then passive scanners must decrypt it, depending on the encryption algorithm is used. The GSM encryption standard is A5 with several flavors: A5/0 is no encryption at all, A5/1 is used in 2G calls, A5/2 is a cryptographically weaker and cracked version of A5/1 so not often used; and A5/3 is used in 3G.

A5/1 has been cracked and a “lookup table” of keys which enables high speed decryption has been pre-computed in a large rainbow table (codebook) that has been freely published on the internet by hackers. In 2010 the encryption algorithm that underpins A5/3 was theoretically cracked using a technique that for the first time can be practically implemented and starts the countdown towards likely commercial availability of 3G passive interception equipment, expected in 2011.

Insider attacks

A common method of interception bypasses the need to intercept radio waves at all and exploits the internal infrastructure of the telecommunication companies themselves. This often proves to be the most vulnerable segment of the call route because any deployed call encryption is only between the handset and the base station and the call is decrypted and transmitted internally within the carrier as plaintext data. Additionally, internal systems – including lawful intercept systems – used to monitor and manage the calls may be subverted to illegally intercept calls.

The perpetrators of insider attacks are authorized staff who have been bribed, threatened, coerced or placed within the company specifically to make such an attack.

In device attacks

Another method of interception that bypasses the call entirely is by placing a listening device (hardware or software) in the cell phone, which monitors the microphone and speaker, and records or forwards the call to the eavesdropper.

This technique is more complex for attackers in that they must have physical access to the device to place the bug. For software this involves secretly installing unauthorized software on the device and can be foiled by reasonable simple device security measures such as using a PIN password to access the phone or authorize software installations. More sophisticated prevention includes installing anti-malware software or, for organizations using device management technology to enforce corporate security policies.

Increasing evidence of problem

Publicity of cell phone interception cases has become more and more frequent recently and has revealed an increasing number of threat-sources as well as volume of interception instances, and expose how vulnerabilities have been attacked. Attacks have come from industrial espionage by competitors and foreign governments, criminals, and investigative journalism. Recent examples include:

- **In 2010**, a technician who worked in a Lebanese mobile phone operator was arrested for being an Israeli spy and giving access to phone calls for 14 years.
- **In 2010**, Romanian law enforcement authorities arrested 50 people for allegedly using off-the-shelf software to monitor other people's cell phone communications.
- **In 2010**, Indian parliament disrupted by politicians protesting at alleged government-sponsored cell phone wiretapping
- **In 2010**, industrial espionage of international commercial operations. Pirelli accused of tapping Michelin & Yokahoma via insider attack at Telecom Italia
- **In 2010**, Mexican spy center discovered, including equipped mobile van unit, alleged to be used for intercepting politicians, businessmen and journalists
- **In 2010**, ex-mistress of captain of England football team sues against alleged cell phone interception
- **In 2010**, Computer Weekly reported a YouTube video that shows interception equipment performing a GSM interception using open source software on a laptop and a radio receiver bought on the internet for under \$1,500. A second video demonstrates the same interception but with software running on an Android cell phone instead of a laptop.
- **In 2009**, the New York Times and Financial Times reported that an international group of security researchers had released a codebook of pre-computed keys that enables decryption of GSM calls, and the blueprint to build a low-cost GSM interception kit.
- **In 2009**, in the same month it was reported that the encryption algorithm for 3G networks had been successfully cracked using a technique that, for the first time, can be practically implemented starting, the countdown towards likely commercial availability of 3G interception equipment, expected by mid-2011.
- **In 2008**, Anthony Pellicano "P.I. to the stars" was jailed for three and a half years for wiretapping activities that he performed on demand against a large number of celebrities and C-level executives. FBI found recordings of conversations that stretched back almost ten years.
- **In 2008**, it was found that journalists at the British tabloid News of the World routinely hired private investigators to break into voice mailboxes of various celebrities, businessmen and dignitaries. Not all espionage is concerned about blackmail, corporate secrets or matters of national security - in this case it was about having exclusive news information.
- **In 2005**, the annual report to the US Congress on Foreign Economic Collection and Industrial Espionage stated that 108 countries were involved in collection efforts against sensitive and protected US technologies. It is risks such as these that have brought about the stack of legislation and best practice that guides company and agency responses. For example, the information standard ISO 27002 specifically mentions using encryption to secure sensitive information carried between mobile devices.
- **From 2004 to 2005**, Greek government communications were the target of sophisticated tapping operation that compromised the cell phone calls of the Prime Minister, the Minister of Defense, the Minister of Justice and the Head of the Greek Intelligence Service. Eavesdropping went on for months during the Athens Olympics and was only discovered accidentally, during an unrelated investigation into the performance of the mobile network. Calls were not intercepted over the air. Instead, the attackers wiretapped government officials using the lawful interception capabilities built into the network.

Practical advice

While enforcement of a corporate voice security policy through processes and technology is essential for mitigating risk, individual awareness and management of threats and vulnerabilities is a simple and effective step towards this goal.

Some basic steps to protect voice calls on your cell phone are:

- **Never assume that calls are secure** unless you have deliberately implemented suitable security measures to protect your specific calls end to end. This includes VoIP calls.
- **Keep your phone safe and do not leave it unattended** in the same way as your bankcard. Skilled attackers can take just a few moments to install a malicious program, compromise the security of the SIM card or install a special battery with a bug in it, all of which can be used later to intercept or decrypt calls.
- **Use and protect your phone and voicemail PINs** in the same way as your bankcard PIN. Never leave confidential messages in voicemails or sent as texts. Received texts on a phone in particular are rarely encrypted and cell phone voicemails can be accessed from any phone with the PIN.
- **Be vigilant to prevent malicious use of your phone.** Be wary of downloads, SMS/ MMS texts, emails, system messages or events on your phone that you did not ask for, initiate or expect (even from known contacts as malware can utilize address book information). Cancel, remove or destroy them without actioning them. Turn off Bluetooth, infrared and Wi-Fi if you are not using them and turn off the phone or set it to flight mode if you don't need it. Remove the battery as an extreme precaution. Install the latest patches for the operating system of your phone and use anti-malware software. Regularly check that the phone's configuration and settings have not changed. Check for irregular battery usage and irregular activities on the phone bill. Simplify device settings and minimize use of add-on applications, plug-ins, and internet access.
- **Check your signal and force the phone to use 3G where possible:** calls on newer technologies like 3G or LTE are more secure than 2G but be aware that the phone often is configured to fall back to 2G when 3G is unavailable. Also, a 3G call can be eavesdropped if connected to a GSM base station and an encrypted 3G call can be recorded and decrypted later after intercepting a 2G call on the same handset, because of a known key vulnerability.
- **Use voice call encryption software on your phone,** it works everywhere your phone does and it is as simple to use as making a normal phone call. Ensure it uses end-to-end encryption and you trust the key management.

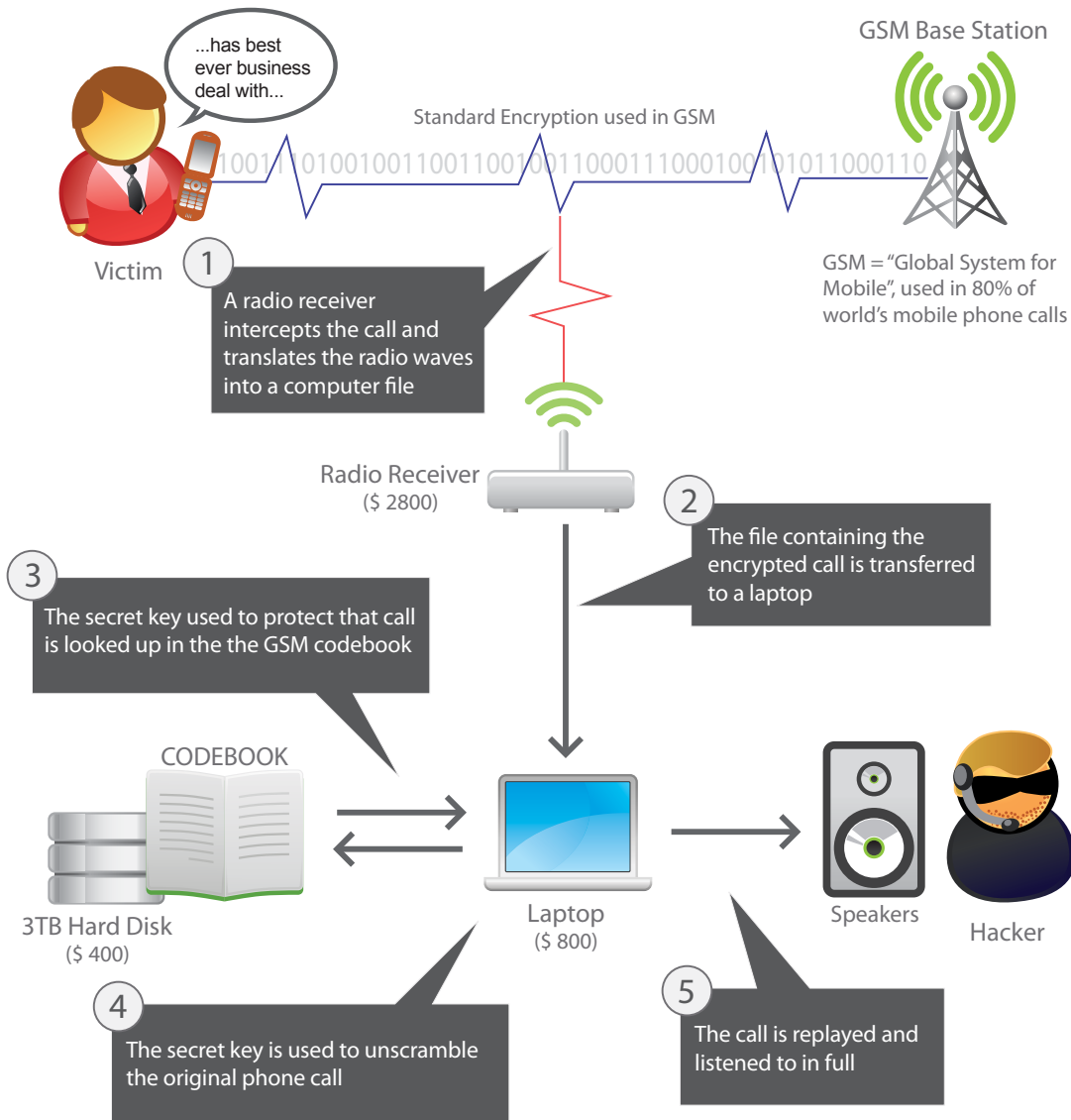
If you have no alternative (such as using encryption software) and urgently need to discuss confidential matters over a cell phone, it is recommended that you:

- Buy/rent a phone with pre-paid calling plan for temporary use
- Chose a location where you can't be overheard
- Cover your mouth so you can't be lip read
- Talk quietly and be brief
- Use code words, or obfuscate information. Often the value of confidential information decreases rapidly with time so delayed information may be useless to an attacker
- Split information across different communication channels (e.g. voice, emails and text messages etc. so information is incomplete and meaningless on its own)

Appendix: GSM Cracking

In December 2009, The New York Times reported that GSM cell phone conversations – used by 80% of cell phones – could be cracked using low-cost equipment, following the publication of a GSM codebook by a security researcher.

GSM MOBILE PHONE CALL INTERCEPTION AND CRACKING



© Cellcrypt 2010

What happened?

On 27th December 2009 at the 26th Chaos Communication Congress (26C3) in Berlin, the security researcher Karsten Nohl announced that a GSM codebook – a large lookup table of GSM encryption keys – had been computed successfully and was freely available on the Internet. This follows Nohl's presentation at the HAR 2009 conference in August where the project was first announced.

Why is this important?

The GSM codebook cracks standard encryption used in GSM calls enabling them to be listened to. This is the first time a GSM codebook has been made publicly available. There is no other standard encryption option on GSM making 80% of all cell phones vulnerable.

What else does an attacker need to do to listen to GSM calls?

In addition to the GSM codebook, an attacker would need equipment to intercept and process GSM radio waves, and methods to target cell phone callers. The GSM Association reports that this is very difficult to achieve. However, Nohl disputed this and at 26C3 specified all the equipment required: costing less than \$2,000 and readily available on the internet, this included OpenBTS open source software for radio capture and processing, a laptop with additional mass storage devices and two USRP2 radio receiver cards.

This equipment was demonstrated publicly by Chris Paget, Nohl's colleague, at the RSA security conference in San Francisco in 2010, where calls made between attendees' GSM handsets were intercepted and recorded. One demonstration (captured on a video available on YouTube) shows a call interception between a BlackBerry Bold and an iPhone. Another demonstration (also on YouTube) shows the interception software being run on an Android smartphone instead of a laptop.

To target a specific phone call, the attacker needs to know the IMEI number (International Mobile Equipment Identity number, unique serial number) of the phone, which identifies the call over the airwaves. This can be obtained directly from the phone for example by entering '#06#' into the phone (requires physical access), sending an SMS (requires the phone number), using malware, or by observing a caller and matching call patterns (requires visual proximity or access to phone log).

Are all my phone calls now at risk?

No, this threat currently only affects GSM calls, not 3G or CDMA. In addition, the current technical immaturity of the equipment means that any attack is most likely to be carried out by professional organizations against specific targets for specific gain, rather than untargeted random attacks by casual users.

However, as the equipment becomes commercialized (by 2011) it is anticipated by security experts that its cost (under US \$5,000) will lead to equipment becoming more accessible to more professional organizations, and also casual hackers, so making the likelihood of attacks greater. In addition, the equipment developers indicate that because it is based on a software radio, it is relatively easy to reconfigure the radio to process other cellular systems such as 3G, CDMA.

Relevant Articles

BBC: Call to check on mobile network security

BBC: Secret Mobile Phone Codes Cracked

Boston Globe: Guide to Breaking Cell Phone Security Revealed

BusinessWeek: Guide to Breaking Cell Phone Security Revealed

Channel 4: Mobile Phone Code Cracked

Chicago Tribune: Group Posts Way to Crack Encryption of Cell Phones

CNBC: Guide to Breaking Cell Phone Security Revealed

Financial Times: Secret Mobile Phone Code Cracked

Financial Times: Security Fear as Mobile Phone Code Is Cracked

Forbes: Guide to Breaking Cell Phone Security Revealed

Fox News: Hacker Cracks Security Code That Protects Cell Phone Calls

International Herald Tribune: Cellphone Encryption Code Is Divulged

MSNBC: Guide to Breaking Cell Phone Security Revealed

New York Times: Cellphone Encryption Code Is Divulged

New York Times: Guide to Breaking Cell Phone Security Revealed

The Daily Telegraph: Mobile Phone Security Codes Cracked

The Guardian: Mobile Phone Security Cracked, Says German Hacker

Washington Post: Hacker Builds \$1,500 Cell-Phone Tapping Device

Washington Post: Guide to Breaking Cell Phone Security Revealed

Note: URL links correct as of August 1st 2010

Additional Background

Nohl's 26C3 presentation "GSM: SRSLY":

- 26C3 Slides
- 26C3 Video
- 26C3 website

Nohl's HAR 2009 presentation "Cracking A5 GSM encryption":

- HAR 2009 Slides
- HAR 2009 Video *(If your media player doesn't open, use the open source VLC [available here](#))*
- HAR 2009 website

Paget's interception videos:

- Live interception at Defcon 2010
- Live interception at RSA 1 2010
- Live interception at RSA 2 2010
- Scmoocoon interview 2010

Equipment resources:

- GSM Codebook tables
- The OpenBTS Project
- USRP2 Radio Receiver Cards

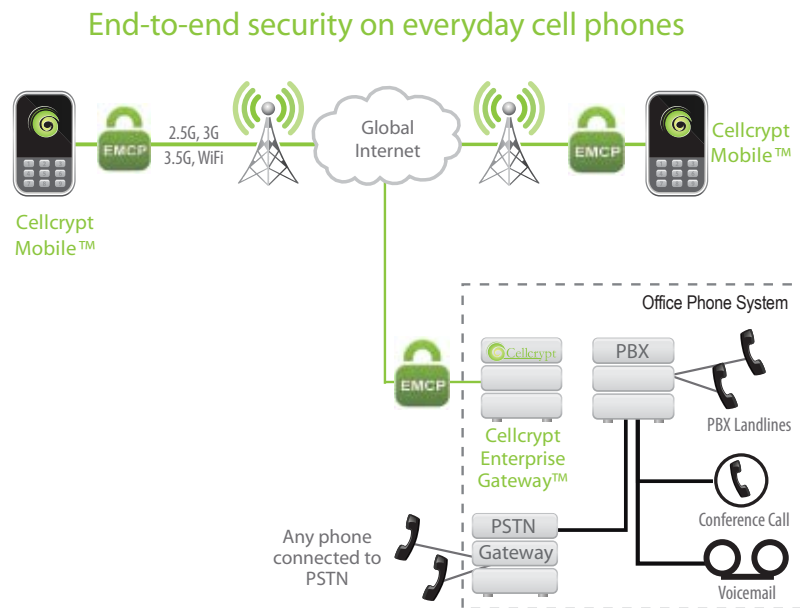
About Cellcrypt

Cellcrypt encrypts voice calls on smartphones like BlackBerry and Nokia to deliver government-grade security in an easy-to-use application that makes secure calling as simple as making a normal phone call.

Utilizing the IP data channel it provides unparalleled voice quality over wireless networks including cellular, Wi-Fi and satellite.

Cellcrypt enables secure calls to mobiles and, via a PBX, to office phone systems, and supports standard PBX features such as voicemail, conference calling and dial-through to the public telephone network.

Cellcrypt's end-to-end encryption is validated to the FIPS 140-2 standard approved by the US National Institute of Standards and Technology. By providing end-to-end encryption, Cellcrypt protects against the risk of call interception over multiple segment of the call path between callers, which includes the wireless network between cell phone and base stations, fixed lines within and between carrier networks and Internet backhaul.



Major features of the Cellcrypt solutions include:

- **Security:** end-to-end encryption validated to FIPS 140-2 security standard, approved by the US National Institute of Standards and Technology, and using open standard algorithms including the DoD-approved 256bit AES. Key pair storage is on each endpoint device not a central server.
- **Simple to use and manage:** no specialist equipment required, standard mobile application installs over-the-air and is as simple as making a normal cell phone call.
- **Device Support:** BlackBerry and Nokia smartphones.
- **Performance:** utilizing IP, supports cellular (2G/3G GSM/CDMA) Wi-Fi® and satellite networks with unparalleled encrypted voice quality and performance.
- **Office telephony integration:** supports calling between cell phones and, via a PBX, to office phone systems.

Cellcrypt solutions are used routinely by governments, enterprises and senior-level executives worldwide. For more information please visit <http://www.cellcrypt.com>.

North America

One Freedom Square
11951 Freedom Drive,
Reston, VA 20190
United States
Tel: +1 703 251 4887

530 Lytton Avenue
Palo Alto, CA 94301
United States
Tel: +1 650 617 3219

Latin America

7791 NW 46 St, Suite 104
Miami, FL 33166
United States
Tel: +1 786 999 8425

Europe & Asia Pacific

222 Regent Street
London, W1B 5TR
United Kingdom
Tel: +44 (0) 2070 995 999

Middle East & Africa

JLT Lake Plaza
Unit 1504, P.O. Box 38255
Dubai, UAE
Tel: +971 (0)4390 2908

info@cellcrypt.com
www.cellcrypt.com

