

Comms: GSM encryption no longer secure

In the last days of 2009, just as everyone was packing up and preparing for a New Year's party, a piece of news should have gained priority but slipped under the radar, picked up by bloggers and a few speciality magazines, it gained virtually no mainstream coverage; and far from being a major topic of conversation in the restaurants, bars and parties it never made it into the public consciousness. It should.

Intelligence agencies and industrial spies know that cell-phones are not inherently secure. The encrypted signal operates only during the transmissions between the cell and the phone. Between cell and network, the signal is carried openly, just like a normal phone conversation, and across the network it is carried normally, too. That includes where the network is carried over the internet.

But it's the fact that, unless you are habitually stationary in one cell, anyone wanting to listen into your calls would have to follow you around a large and complex network, tapping into a succession of lines to catch even the shortest snippet of your conversation; and if you were roaming, he would have to tap into the networks of all available operators.

So the nature of the network provides a de facto security; leaving GSM digital to cope with the comms between cell and handset.

GSM was introduced with, amongst other things, promises of security. A number of cases, including the infamous Squidgygate, had arisen with unencrypted phones before GSM and devices for identifying and listening into mobile phone signals were widely available. But GSM, now two decades old, is decaying technology: its encryption level is just 64-Bit. There is a higher encryption level available: but at 128-bit, that's already sub-standard by encryption standards.

The system has been the target of many criminals but on 28 December reports began to circulate that the code had been cracked and that a copy of the necessary algorithm had been posted on the internet. Two weeks later, reports emerged of a second crack.

The first instance resulted from a brute force attack on the code by a German, Kartsen Nohl. Nohl says that his group wants to force GSM manufacturers to increase their security, and that that his actions proved that the system is insecure. However, the GSM Association said that it frequently hears claims of such hacks and had not see the research and so could not validate the claims. The algorithm later appeared on the internet, and further information was revealed showing that

calls could be intercepted, monitored and recorded on equipment that is both readily available and relatively inexpensive: around USD10,000.

In mid January, a paper published by the International Association for Cryptologic Research claimed that Israeli researchers had broken the cypher. Their approach was much simpler: having identified the crack, they were able to use an ordinary laptop. "We simulated the attack in less than two hours on a single PC, and experimentally verified its correctness and complexity."

There have been many allegations that various intelligence agencies have cracked the GSM code.

The importance of the hacks is that now the tap can take place in the space between handset and cell. And that means that the previous idea of using a phone in a moving car, and so jumping from cell to cell, will not work. Nor with the simple expedient of crossing the street where tower blocks often mean changing cells over very small distances on the ground. Even moving from one side of an office building to the other will often result in a change in cell.

So, in theory, it's goodbye to all of those calls taking instructions on deals in meetings held in the other side's offices; it's goodbye to discussions of commercially important matters even where care is taken not to be overheard.

But in truth, many people freely reveal all manner of information on commuter trains and planes; some serious conversations can be heard in airport queues, especially from those who have an innate need to sound important.

The reality is that the most likely use, in the short term at least, for this information will be from those hoping to replicate the scandal of Squidgygate by finding a public figure with his pants down, to coin a phrase.

But the GSM industry does need to deal with its ageing systems.

In the meantime, those who need security can get it - at a price. Phones providing end-to-end

encryption (which convert the voice to encrypted code before passing it to the mobile-phone's comms chip) are readily available. But they are useless unless the other party has matching technology.

One of the reasons that GSM encryption remained at 64-bit was because of restrictions on the use and, especially, export of "strong encryption." At one stage, France banned any and all encryption greater than 64-bit.

But strong encryption, as it is defined now, still requires export licences from many countries. For example, a company marketing end-to-end security and handset verification has prominent notice on its website: "Due to the high level of encryption this equipment requires an export licence for sale outside of the EU."

Such equipment is not new: Rohde & Schwarz, a German comms company, released a modified Siemens S35i model phone in 2001, that the company said "uses a combination of asymmetric 1-024-bit and symmetric 128-bit encryption for a high level of security."

But the problem is also addressed by software that can be downloaded and installed on your phone, encrypting SMS and voice for as little as USD400 per phone. Again, all users must use the same software.

The requirement that all users must have compatible crypto-systems removes the ubiquity of the mobile, and so all the methods can be bypassed, so allowing calls to non-compatible third parties.