

The activities of parts of the British Press have drawn attention to the problem of Phone Hacking. While in most cases voice mail was the target, the subsequent debate has uncovered a much wider and potentially more serious set of threats. This application note outlines those threats and shows how phones can be protected.

### The Problem

While the activities of some of the UK Press have focused attention on the security weaknesses of mobile phones, the reality is that most of the phone hacking reported to date has been confined to voice mail hacking. If a hacker successfully attacks your voice mail, all of the messages in your mailbox are compromised.

While this is a significant problem, a much more serious issue is the threat of call interception and monitoring. When one of the many techniques for GSM call interception was demonstrated to Chris Bryant, a British MP active in the debate on phone hacking, he made the following statement in Parliament:

**13 July 2011, Chris Bryant (Rhondda) (Lab):**

*Yesterday afternoon we heard that the man who is in charge of counter-terrorism in the Metropolitan police is 99% certain that his phone was hacked. An hour later, I was shown a piece of kit that costs about £1,500 and is readily available on the internet. It effectively sets up an illegal mobile phone mast through which it is possible to listen to any conversation held by anyone on a mobile phone within three miles. <sup>[1]</sup>*

The system that was demonstrated to Chris Bryant was based on an open-source software project<sup>[2]</sup>. This project has built a low-cost GSM base station using a commercially available software controlled radio system<sup>[3]</sup>. The radio connects to a laptop via a USB cable. The complete system is small enough to be packaged into a briefcase. To monitor a GSM call, the system is configured to operate as a base station on the appropriate network. Any nearby phones will join the base station if that station broadcasts the strongest available signal. The open-source software will handle the GSM call, including processing the encryption built in to the GSM protocols. It is then a simple matter to forward that call over a VoIP connection, recording it along the way.

Another method of intercepting calls was devised by Karsten Nohl<sup>[4]</sup>. Karsten, a researcher formerly at the University of Virginia, has generated a code book that allows a GSM call to be passively monitored and captured and then decrypted.

Other researchers have found weaknesses in the design of a femtocell, which in the UK is supplied by Vodafone<sup>[5]</sup>. These weaknesses enable the femtocell to be modified so that any phone within range will connect to it and calls can be recorded. Vodafone have issued a statement claiming that the vulnerability has been fixed, but the researchers point out that the fix does not address the core problem.

To demonstrate the ease with which these techniques can be adapted, researchers in the USA have built their own flying surveillance drone using readily available components<sup>[6]</sup>.

These examples show that there is a genuine risk that calls made on mobile phones can be intercepted and monitored. There are a number of techniques that allow an eavesdropper to monitor calls between the handset and the operator's base station or to subvert the network by running a fake base station. This means that even if calls are made on a trusted operator's network there can be no guarantee of the call's security. The risk magnifies when

phones are roaming and calls are made on networks that are not necessarily trusted. This is a particular problem in the government and defence sectors and for commercial organisations conducting business in certain overseas territories.

### *The Solution*

The mobile operators cannot solve this problem. They have to support dated technologies which are burdened with the vulnerabilities that enable call monitoring and interception. Even if they could change technology overnight, there is still a risk that a rogue employee with a mobile operator could monitor calls or that an overseas operator may be pressured to provide access to calls.

Fortunately Voice over IP (VoIP) technology can provide a solution. VoIP applications are available for most smart-phones and use the mobile data channel or a WiFi network to make voice calls. Obviously just switching to VoIP does not solve the problem, as mobile data channels can be monitored as easily as voice and monitoring WiFi is even easier. The benefit that VoIP brings is that it is easy to add effective call encryption. Also, as the VoIP application and therefore the encryption is completely under your control, secure end-to-end encryption can be established from the mobile handset to a trusted point in your network or to a trusted hosted service. Better still; a secure VoIP based phone service can be extended to include not only mobile devices, but desk phones within your office. This means that sensitive calls, for example from an office-based CFO to a CEO in an overseas hotel room can be protected with robust and effective encryption.

A secure VoIP system for mobile phones requires two components:

- A suitable VoIP app with built-in encryption for your smart phone. Apps are available for all major smart phones. The choice will depend on the type of phone in use, your requirements and planned usage.
- A security gateway to accept secure connections from phones, to route calls between phones and to provide the necessary encryption/decryption services. This gateway may be located in your office and linked to your existing phone system, or you may prefer to use a trusted hosted provider.

The UM Labs *SIP Security Controller* provides the secure gateway functions. This product is in use in a number of large scale encryption projects for both mobile and fixed line phones. UM Labs can also advise on the choice of smart phone app, selecting specialist product from one of our partners or an openly available app.

For more information on the security threats, for details on the technologies used to prevent phone hacking or for an assessment of how secure mobile communication can protect your business, please contact UM Labs.

**Email:** crypto@um-labs.com

**Phone:** +44 20 3021 3200 (UK)  
+1 202 470 1684 (USA)

**Web:** www.um-labs.com

## References

1. <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110713/debtext/110713-0001.htm#11071354001743>
2. <http://openbts.sourceforge.net>
3. <http://www.ettus.com>
4. [http://news.cnet.com/8301-27080\\_3-10423219-245.html](http://news.cnet.com/8301-27080_3-10423219-245.html)
5. <http://thcorg.blogspot.com/2011/07/vodafone-hacked-root-password-published.html>
6. <http://blogs.forbes.com/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/>