

## Mobile-phone snooping fears

Any good hacker can exploit GSM security flaws.

Tue, Jan 19, 2010  
my paper

By KENNY CHEE

CONCERNS over mobile phone security have been growing since a code book - which can crack the standard encryption that protects most cellphone calls - was posted online late last month.

This means that criminals, terrorists or anyone can download the code book from the Internet, and use it to listen in on mobile-phone calls or intercept text messages.

But Singapore seems safe from such attacks on mobile communication for now.

The three telecommunication companies here - SingTel, M1 and StarHub - said that they have had no known cases of eavesdropping or message interception.

The Ministry of Home Affairs also said that police have not received any reports of communications being intercepted via this method.

The Infocomm Development Authority of Singapore (IDA) said that "the unauthorised interception of any radio communication that is not meant for general reception is an offence".

Flouting the rules draws a fine of up to \$10,000 and/or a jail term of up to three years.

"IDA will continue to ensure that operators take the necessary measures to maintain the integrity and security of their mobile networks in Singapore," said its spokesman. The New York Times reported that the code book for eavesdropping on mobile-phone calls consists of binary numbers that can decipher the standard encryption code that keeps the calls and text messages of over 80 per cent of global cellphone users safe from snooping.

The 21-year-old encryption code, part of the global system for mobile communications (GSM), was established by the GSM Association, which represents mobile operators and related companies globally.

German computer engineer Karsten Nohl, who devised the code book with a team of more than 20 people, told The New York Times that his group's work "shows that existing GSM security is inadequate".

He added that his group is trying to goad the world's wireless operators into using better security.

The GSM Association said that there is minimal immediate risk posed by the code book. It noted that similar claims of cracking the code have been made in the past 10 years.

It told The Financial Times code book, but added that a practical attack "is beyond the capabilities of the vast majority of people".

Telcos here said that they will work with the association to keep phone networks safe.

Security experts agreed that current methods for deciphering GSM mobile-phone calls are not practical for widespread use, even with the release of the code book. Still, its existence poses security concerns.

Professor Rohan Gunaratna, who heads the Nanyang Technological University's International Centre for Political Violence and Terrorism Research, said that the code book poses no immediate threat, as many criminals and terrorists "lack the capability" to monitor phone communications.

But a determined group could build this capability over time unless phone networks are upgraded to address this issue, he said.

He added that he was confident that the Government would take measures to prevent organisations from

breaking into communication networks, to maintain business confidence.

Mr Stan Schatt, vice-president of enterprise communications and security at market-research firm ABI Research, said that security services can protect conversations to some extent, but "very large companies, whose executives tend to talk to each other in public areas about very sensitive information" should be concerned about the code book.

He added that the GSM Association might not have upgraded the encryption on GSM networks all these years because of "inertia, expense and other practical concerns".

Mr David Rottmayer, vicepresident of technology at training, consulting and research firm Telefocal Asia, said "GSM is not secure and never has been".

He said that while the security code was not officially published, it has "serious flaws... which any good hacker can exploit with a handset and some basic software".

Mr Paul Ducklin, head of technology for the Asia-Pacific at security firm Sophos, said the code book shows that GSM encryption is not secure against attackers with a limited budget, much less modern-day terrorists.

He estimates that it can cost as little as US\$5,000 (S\$6,950) to put together a device for decrypting GSM calls.

The GSM security issue may be addressed next month as the GSM Association's security group will decide if GSM networks need to be upgraded, said the Financial Times.

**kennyc@sph.com.sg**

**mypaper** 

For more my paper stories [click here](#).

[an error occurred while processing this directive]

Copyright ©2007 Singapore Press Holdings Ltd. Co. Regn. No. 198402868E. All rights reserved.

[Privacy Statement](#) [Conditions of Access](#) [Advertise](#)