



[Print this article](#) | [Close this window](#)

Eavesdrop fears as mobile phone security codes cracked

Asher Moses

December 30, 2009 - 11:29AM

Billions of mobile phone users around the world are at risk of having their calls intercepted and recorded after hackers broke the encryption used to protect 80 per cent of the world's mobiles.

People regularly trading in confidential information, such as Government officials and executives, would be the most likely eavesdropping targets but virtually anyone with enough skills and determination could harness the research for nefarious means, security experts warn.

German computer engineer Karsten Nohl told a hacker conference in Berlin that he and his team decoded the GSM (Global System for Mobile Communication) encryption algorithm to draw attention to gaping security holes in the technology and drive mobile operators to patch them.

About 80 per cent - or 3.5 billion - of the world's mobiles are based on GSM, which is over 20 years old.

In Australia, virtually every mobile phone uses GSM or a variation of it after Telstra shut down its ageing CDMA network, Telsyte research director Warren Chaisatien said.

Nohl, who has published the secret GSM encryption code online, told the Chaos Communication Congress this week that a skilled eavesdropper using basic equipment and free software could be recording phone calls within 15 minutes, [The Guardian reported](#).

"This shows that existing GSM security is inadequate," Nohl, 28, said, insisting his work was purely academic.

"We are trying to push operators to adopt better security measures for mobile phone calls."

Security experts including mobile encryption firm Cellcrypt said it would be largely skilled hackers and well-funded criminals who would have access to the technology and expertise required to intercept calls..

However, Cellcrypt's Ian Meakin [told the BBC](#) that Nohl's work was still a "massive worry".

"It lowers the bar for people and organisations to crack GSM calls. It inadvertently puts these tools and techniques in the hands of criminals," Meakin said.

The GSM Association, which devised the algorithm, said Nohl's work was illegal and admitted intercepting calls using his method was "theoretically possible but practically unlikely". It said it was taking the security threat very seriously.

Nohl claims he consulted lawyers before publishing his findings and insists he is operating within the law. But he conceded the data he produced could be used for illegitimate purposes, such as to create a phone tapping device.

"What he is doing would be illegal in Britain and the United States. To do this while supposedly being concerned about privacy is beyond me," GSM association spokeswoman Claire Cranton [told The New York Times](#).

Nohl is developing a solid reputation in the hacker community after a similar campaign last year that led to an update to the security protecting millions of cordless home phones.

Several hacker groups had earlier signalled their intentions to crack the GSM algorithm, which protects calls by scrambling the communications link between the radio base station and handset.

Serious security flaws in the technology were discovered and exposed as early as 1994.

A newer, more secure version of the algorithm has been developed by the GSM Association but it has not yet been implemented by most mobile mobile network operators around the world.

This story was found at: <http://www.smh.com.au/technology/security/eavesdrop-fears-as-mobile-phone-security-codes-cracked-20091230-lj90.html>