Secret mobile phone code cracked
By Maija Palmer, technology correspondent
Published: December 29 2009 15:11 | Last updated: December 29 2009 16:17

Computer hackers this week said they had cracked and published the secret code that protects 80 per cent of the world’s mobile phones. The move will leave more than 3bn people vulnerable to having their calls intercepted, and could force mobile phone operators into a costly upgrade of their networks.

Karsten Nohl, a German encryption expert, said he had organised the hack to demonstrate the weaknesses of the security measures protecting the global system for mobile communication (GSM) and to push mobile operators to improve their systems.

“This shows that existing GSM security is inadequate,” Mr Nohl told an audience of about 600 people at the Chaos Communication Congress in Berlin, a four-day conference of computer hackers.

“We have given up hope that network operators will move to improve security on their own, but we are hoping that with this added attention, there will be increased demand from customers for them to do this,” he told the Financial Times.

“This vulnerability should have been fixed 15 years ago. People should now try it out at home and see how vulnerable their calls are.”

Mr Nohl was due to run a practical demonstration of the code book at the conference on Wednesday, but has postponed it while he takes advice from lawyers on whether the exercise would be legal. However, the code is already being widely circulated on the internet.

Mr Nohl, a widely consulted cryptography expert with a doctorate in computer engineering from the University of Virginia, waged a similar campaign this year which caused the DECT Forum, a standards group based in Bern, to upgrade the security algorithm for 800m cordless home phones.

The hacked GSM code could compromise more than 3bn people in 212 countries. It does not affect 3G phone calls, however, which are protected by a different security code.

The GSM Association, the industry body for mobile phone operators, which devised the A5/1 encryption algorithm 21 years ago, said they were monitoring the situation closely.

“We are concerned but we don’t believe it will result in widespread eavesdropping tomorrow, or next week or next month,” said James Moran, security director of the GSMA.

“The reality is that a practical attack is beyond the capabilities of the vast majority of people,” he said.

However, security experts disagreed, saying that cracking the code significantly lowered the bar for intercepting calls.

“A year ago it would have required equipment costing hundreds of thousands of dollars, and serious expertise to listen in to a call,” said Simon Bransfield-Garth, chief executive of Cellcrypt, a mobile phone encryption company.

“Today it is going to require $1,500 of network equipment and a computer. It is getting down to a mainstream price tag and moving to the point when it will be straightforward to do,” he continued.

“A skilled computer engineer can now build this,” said Mr Nohl.

Mr Moran said that if the hack was thought to pose a serious practical threat, the GSM Association could force all GSM operators to upgrade their security systems to use a stronger form of encryption.

The GSMA has done this once before, in 2004, when security flaws were discovered in another security code, known as A5/2, and operators across Latin America, Asia and Africa were forced to upgrade their networks.

A security upgrade could prove very costly, however, as some operators would have to replace their old base stations completely, Mr Moran said. The A5/2 upgrade, for example, took about 18 months.

A decision on whether to upgrade to a stronger code could be taken at the next meeting of the GSMA security group in February.