

Montreal Gazette

Hacking most cellphones is cheap, easy; Less than \$100, takes 20 seconds. Pair of researchers demonstrate how widely used GSM networks are vulnerable

Thu Dec 30 2010
Page: B3
Section: Business
Byline: JASON MAGDER
Source: The Gazette

Most of the world's cellphones can be hacked and their phone calls recorded using less than \$100 of equipment, a pair of researchers have found.

The pair, Sylvain Munaut and Karsten Nohl, demonstrated to the Chaos Computer Club Congress in Berlin, Germany, on Tuesday how they intercepted phone calls and SMS messages using four phones they bought for less than \$15 each, and a laptop. The pair said most phone networks working on the GSM standard are vulnerable. The GSM network is used by 80 per cent of the world's phones, including Rogers Communications Inc., which has the largest market share in Canada, and Fido.

Speaking for Rogers, Sebastien Bouchard said he wasn't sure if customers were affected by this vulnerability. He said, however, that Rogers works closely with the world GSM association to protect the privacy of its customers.

Bell Canada Enterprises and Telus Corporation use different technology, the HSPA+ network. Bell spokesperson Marie-Eve Francoeur said that network isn't affected by the vulnerabilities of GSM software. She said, however, that Bell is concerned with security and reviews its procedures continuously.

The pair showed how they could send a ghost text message to a target phone, that the phone would not see, but the phone would transmit its identification number to the sender.

The whole process takes about 20 seconds, the researchers bragged, and afterwards, phone conversations and SMS messages could be recorded and later decrypted.

Munaut and Nohl are outspoken in the area of GSM network security. Both have been developing and pushing for worldwide adoption of an open-source GSM software, which they say would be more secure than current software, since it would be scrutinized by a much larger group.

Nohl told the conference that GSM phone software is 20 years old and out of date, "with lots of private data and not a lot of security." He said in that time computing power has evolved much, while GSM security has remained virtually unchanged.

This is not the first time GSM phone security has been put under the microscope. Until recently, however, it was believed that hacking into GSM

phones was a complicated, and expensive proposition, with equipment costing more than \$50,000 to perform the task. Nohl and Munaut argue their experiment shows anyone with a little computer savviness can eavesdrop and record conversations.

The pair says most cellular networks have very little security around the data that gets sent and received by phones, and this is akin to operating a computer on the Internet without using any kind of firewall security.

They said upgrading networks to protect against this vulnerability is fairly simple.

jmagder@montrealgazette.com

[Twitter.com/jasonmagder](https://twitter.com/jasonmagder)