GSM system about to be compromised

December 8 2009, by Lin Edwards

GSM logo

(PhysOrg.com) -- Research scientists in California and elsewhere are deliberately setting out to compromise the mobile phone system used by around three billion people. The system uses Global System for Mobile communications (GSM) encryption technology to prevent eavesdropping.

Karsten Nohl, a research scientist at a Californian security research firm H4RDW4RE, and a member of the Chaos Computer Club (CCC) in Germany, is behind the effort to crack the A5/1 encryption technology used by GSM, and he plans to release the keys publically on the Internet by the end of the year.

Every phone using GSM has its own secret key, which is recognized by the network. When a call is made the secret key is used to create a session key that is then used to encrypt the phone call. It is the session key that Nohl plans to crack.

Nohl has created an open-source program that will enable a peer-to-peer network of up to 80 computers to share the computing required to break the code. Since the files are distributed across the network, it will be virtually impossible to remove the code-breaking tool from the Internet. When the encryption code is cracked it will be compiled into a code book that could be used to decode any data sent to or from a GSM phone.

Computing time for the project is being speeded up by the use of components not usually found in a standard computer, such as the expensive Xilinx Virtex field-programmable gate arrays and Nvidia's compute unified device architecture (CUDA) graphics cards. According to Nohl, graphics cards are faster than CPUs for certain applications, such as computing the A5/1 code.

The goal of the exercise, according to Nohl, is to highlight the vulnerability inherent in GSM technology and to encourage mobile phone operators still using the system to upgrade their digital phone system to 3G, which has better encryption, or to use the more advanced A5/3 encryption technology instead of A5/1.

GSM phone networks in the U.S. include AT&T and T-Mobile. Commercial tools that decrypt GSM communications have been available for some time, but they cost from $100,000 to $250,000. When Nohl's project cracks the key and publishes the code book on the Internet, it will be possible for almost anyone to get the encryption key for any GSM call and eavesdrop on the call or read SMS messages.

via IEEE Spectrum

© 2009 PhysOrg.com

Citation: GSM system about to be compromised (2009, December 8) retrieved 19 April 2024 from https://phys.org/news/2009-12-gsm-compromised.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.