U.S. News & WORLD REPORT

Guide to Breaking Cell Phone Security Revealed

Posted: December 30, 2009

Associated Press

MATT MOORE,
AP Business Writer

FRANKFURT—A German security expert has raised the ire of the cell phone industry after he and a group of researchers posted online a how-to guide for cracking the encryption that keeps the calls of GSM-standard cell phone users secret.

Karsten Nohl, 28, told The Associated Press this week that he, working with others online and around the world, created a codebook showing how to get past the GSM encryption used to keep conversations on more than 3 billion mobile phones safe from prying ears.

Nohl said the purpose was to push companies to improve security. The collaborative effort put the information online through file-sharing sites.

"The message is to have better security, not we want to break you," he said of the move. "The goal is better security. If we created more demand for more security, if any of the network operators could use this as a marketing feature ... that would be the best possible outcome."

GSM, the leading cell phone technology around the world, is used by several wireless carriers in the U.S., with the largest being AT&T Inc. and T-Mobile USA. Verizon Wireless and Sprint Nextel Corp. use a different standard.

The GSM Association, a trade group that represents nearly 800 wireless operators, said it was mystified by Nohl's rationale.

Claire Cranton, a spokeswoman for the London-based group, said that "this activity is highly illegal in the UK and would be a serious RIPA offense as it probably is in most countries." RIPA, or the Regulation of Investigatory Powers Act, is a British law governing the interception of user logs and e-mails of suspected criminals by security and intelligence agencies.

It has already been possible to intercept GSM calls, but the equipment is generally only available to law enforcement. Regular wiretapping of cellular calls is also possible, since they travel unencrypted over standard wiring after being picked up by a cell tower.

Even with Nohl's exploit, expensive and sophisticated radio equipment placed close to the target is required to pull the calls off the air.

Sujeet Shenoi, a professor of computer science at the University of Tulsa in Oklahoma, said that while the code-breaking guide raises privacy issues, his main concern is that organized crime will take advantage of it to make money, perhaps by eavesdropping on transactions between consumers and merchants.

"It's a shot across the bow" of the wireless industry, he said.

Nohls' effort undermines the 21-year-old algorithm used to ensure the privacy of phone calls made on GSM (global system for mobile communication) cell phone networks.

That algorithm, dubbed the A5/1 and made up of 64-bit binary code, was adopted in 1988. Since then 128-bit codes have been implemented to ensure caller privacy on newer, third-generation networks. The GSM Association has developed the A5/3 algorithm, which it says is gradually being phased in to replace A5/1.

"The GSMA heads up a security working group which looks at all issues re: security and this isn't something that we take lightly at all," Cranton wrote in an e-mail to the AP. "We have a new security algorithm that is being phased (in), as the protection and privacy of customer communications is at the forefront of operators' concerns."

Nohl, who holds a doctorate in computer engineering from the University of Virginia, said that going from a 64-bit code to 128-bit code "makes it some quintillion times more difficult" to crack.

He said the codebook was compiled and posted online not for malicious intent but as a call to the cell phone industry to improve the level of security for those who use GSM phones that are found worldwide and offered through numerous network providers.

"Being security researchers one thing we can do, and what we choose to do in this case, is to show how it can be done," he told the AP on Tuesday by telephone.

"We have created a tool, a codebook, that's used to decrypt GSM packs, or the GSM encryptions," he added, noting that with the codes phone calls could be recorded using a high-end PC, a radio and some software.

"In GSM this flaw was pointed out 15 years ago and 15 years seems long enough for the cypher to be replaced with something else. No one uses a phone that is 15 years old," Nohl said. "If they had taken steps they could have replaced everything three time times over."

Nohl made the announcement Sunday at the Chaos Communication Congress in Berlin, a four-day event that ends Wednesday.

While there has been criticism, there is also some faint praise and admiration for the effort.

"We're familiar with his work. It's proper stuff," said Simon Bransfield-Garth, chief executive of London-based Cellcrypt, which sells software to keep mobile phones secure.

"People have been trying to crack GSM for a long time," Bransfield-Garth told AP. "I think the science behind it is pretty sound," he added. "Whether putting it in the public domain was wise, is an entirely different debate."

___

Associated Press Technology Writer Peter Svensson in New York contributed to this story.

___

On the Net:

A5/1 Cracking Project: http://reflextor.com/trac/a51

GSMA: http://www.gsmworld.com

Cellcrypt: http://www.cellcrypt.com

Follow U.S. News Science on Twitter.