

ANNALIZA SAVAGE SCIENCE APR 13, 1998 9:59 AM

Cell-Phone Security Far From Airtight

The Smartcard Developer Association claims to have cracked the algorithm used to secure the subscriber information in about 80 million digital cell phones worldwide.



SAVE THIS STORY

A GROUP OF California-based computer experts claims to have compromised the cryptographic security behind the world's most popular digital cell-phone system, making it possible to clone any phone using the GSM standard.

The Smartcard Developer Association says it cracked the algorithm used as the basis for the The Global System for Mobile Communications (GSM) -- a digital cellular phone system that is used in about 80 million cell phones, primarily in Europe and Asia. Many US networks are starting to implement GSM standards, too, and this attack was launched against a card issued by Pacific Bell. If the group's claims are true, it could lead to a recall or reissue of the smart cards used in GSM-based phones.

"GSM is likely to face fraud problems of the same magnitude as analog systems have had," said Marc Briceno, a member of the SDA who said that analog systems have lost billions of dollars because of cellular phone cloning.

phone and contains information that is used to identify subscribers and their account information to the GSM network. The SIM card must be inserted into a GSM Mobile handset to obtain access to the network, and one of the primary benefits of the technology is that cell phones have access to GSM networks worldwide.

However, to clone a SIM card, a would-be cracker would have to have physical possession of one. Unlike the cloning used in analog systems, the crack does not yet include being able to listen in on peoples phone calls or obtain a SIM ID via the airwaves, although the SDA has stated that an "over-the-air attack should not be ruled out."

The SIM uses encryption to keep the identity of the phone secret, and the encryption algorithm used on most of the GSM network is called COMP128. The SDA was able to obtain the secret ciphers used by the GSM network. After verifying authenticity, the group turned them over to UC Berkeley researchers David Wagner and Ian Goldberg, who were able to crack the COMP128 algorithm within a day. In 1995, Wagner and Goldberg succeeded in another high-profile hack when they compromised the crypto code used in Netscape's Navigator browser, which was supposed to secure credit-card transactions.

"Within hours they discovered a fatal flaw," said Briceno. "The attack that we have done is based on sending a large number of challenges to the authorization module in the phone. The key can be deduced and recovered in about 10 hours."

A group of hackers gathered with security and crypto experts Friday evening at a San Francisco hacker club called New Hack City, for a demonstration of the hack, but it never came off. Eric Hughes, a member of the SDA and founder of the Cypherpunks cryptography group, discussed the technical aspects of the hack, but had to give up the planned demonstration after threats of legal action from Pac Bell and other telephone company executives. It is illegal in the United States to possess cellular phone cloning equipment, although legitimate businesses are exempted. The telephone companies dispute SDA's claims to legitimacy.

"There is no way that we would have been able to break the cryptography so quickly if the design had been subjected to public scrutiny," said Wagner.

The GSM standard was developed and designed by the European Telecommunications Standard Institute, an organization that has about 500 members from 33 countries, representing administrations, network operators, manufacturers, service providers, and users.

"There's going to be an orgy of finger pointing," said Hughes, referring to all the engineers and other people associated with the design of the GSM network.

The SDA say that they were able to crack the GSM network algorithm due to weak encryption in the original design. When the system was being designed, several European government agencies were successful in their demands to weaken encryption standards for government surveillance purposes.

The SDA also claimed that the GSM security cipher that keeps eavesdroppers from listening to a conversation called A5 was also made deliberately weaker. The A5 cipher uses a 64-bit key, but only 54 of the bits are actually in use -- 10 of the bits have been replaced with zeroes. The SDA's Briceño blames government interference.

"The only party who has an interest in weakening voice privacy is the National Security Agency," he said.

The SDA said that a proper demo will be taking place soon from somewhere outside the United States. The group has also released the source code for COMP128 and A5 for further testing.

Sign up for the Daily Newsletter

Get our biggest stories, handpicked for you each day



READ MORE

Why One VC Thinks Quantum Is a Bigger Unlock Than AGI

Venture capitalist Alexa von Tobel is ready to bet on quantum computing—starting with hardware.

ZOE SCHIFFER



DHS Has Been Collecting US Citizens' DNA for Years

Newly released data shows Customs and Border Protection funneled the DNA of nearly 2,000 US citizens—some as young as 14—into an FBI crime database, raising alarms about oversight and legality.

DELL CAMERON

Worried About Phone Searches? 1Password's Travel Mode Can Clean Up Your Data

Travel Mode not only hides your most sensitive data—it acts as if that data never existed in the first place.

JACOB ROACH



Critics say looksmaxxing—the trend of men boosting their physical attractiveness—often uses eugenic beauty standards. Some Black influencers are struggling to fit in, while others are fighting back.

JASON PARHAM

How Signal's Meredith Whittaker Remembers SignalGate: 'No Fucking Way'

The Signal Foundation president recalls where she was when she heard Trump cabinet officials had added a journalist to a highly sensitive group chat.

KATIE DRUMMOND



She Fought the Far Right Online for Years. Now She Wants to Do It in Congress

Kat Abughazaleh, 26, made her name swatting down right-wing talking points on social media. Now she's hoping internet fame can propel her to Congress.

KATE KNIBBS



For years, influencer Nick Fuentes was too extreme even for MAGA. Now he's working his way into the mainstream—and has a plan for his secret followers to seize the levers of power.

DAVID GILBERT

Chewy Promo Codes: \$20 Off in September 2025

Explore Chewy coupon codes for great discounts, like a \$20 gift card with a purchase of \$49 or more.

MOLLY HIGGINS



Save \$36 on a Cool, Compact Hall Effect Keyboard

The Keychron Q1 HE brings our favorite new type of keyboard switch to the mainstream.

BRAD BOURQUE

WIRED Roundup: The Right Embraces Cancel Culture



MANISHA KRISHNAN

\$3,800 Flights and Aborted Takeoffs: How Trump's H-1B Announcement Panicked Tech Workers

President Trump's sudden policy shift sent tech firms scrambling to get immigrant workers back to the US and avoid \$100,000 fees.

ZEYI YANG

 **PRIVACY INFORMATION**