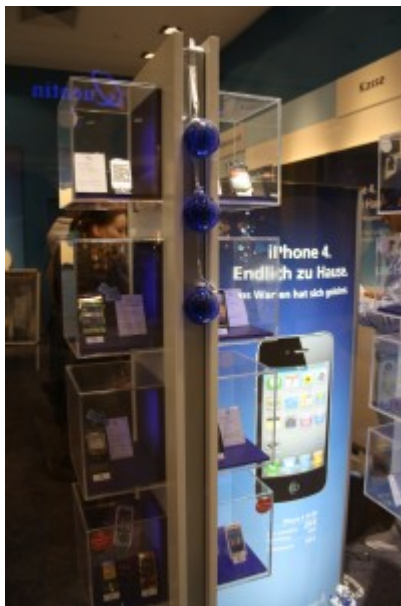


<http://www.wired.com/threatlevel/2010/12/breaking-gsm-with-a-15-phone-plus-smarts/>

## Breaking GSM With a \$15 Phone ... Plus Smarts

- By [John Borland](#)
- December 28, 2010
- 1:25 pm
- Categories: [Chaos Computer Club](#), [privacy](#)

BERLIN — Whatever assurances have been given about the security of GSM cellphone calls, forget about them now.



Use at your own risk.

Speaking at the [Chaos Computer Club \(CCC\) Congress](#) here Tuesday, a pair of researchers demonstrated a start-to-finish means of eavesdropping on encrypted GSM cellphone calls and text messages, using only four sub-\$15 telephones as network “sniffers,” a laptop computer and a variety of open source software.

While such capabilities have long been available to law enforcement with the resources to buy a powerful network-sniffing device for more than \$50,000 (remember *The Wire?*), the pieced-together hack takes advantage of security flaws and shortcuts in the GSM network operators’ technology and operations to put the power within the reach of almost any motivated tech-savvy programmer.

“GSM is insecure, the more so as more is known about GSM,” said [Security Research Labs](#) researcher Karsten Nohl. “It’s pretty much like computers on the net in the 1990s, when people didn’t understand security well.”

Several of the individual pieces of this GSM hack have been displayed before. The ability to decrypt GSM’s 64-bit A5/1 encryption was demonstrated last year at this same event, for instance. However, network operators then responded that the difficulty of finding a

specific phone, and of picking the correct encrypted radio signal out of the air, made the theoretical decryption danger minimal at best.

Naturally this sounded like a challenge.

Working the audience through each step of the process, Nohl and [OsmocomBB](#) project programmer Sylvain Munaut demonstrated how the way in which GSM networks exchange subscriber location data, in order to correctly route phone calls and SMSs, allows anyone to determine a subscriber's current location with a simple internet query, to the level of city or general rural area.

Once a phone is narrowed down to a specific city, a potential attacker can drive through the area, sending the target phone "silent" or "broken" SMS messages that do not show up on the phone. By sniffing to each bay station's traffic, listening for the delivery of the message and the response of the target phone at the correct time, the location of the target phone can be more precisely identified.

To create a network sniffer, the researchers replaced the firmware of a simple Motorola GSM phone with their own alternative, which allowed them to retain the raw data received from the cell network, and examine more of the cellphone network space than a single phone ordinarily monitors. Upgrading the USB connection allowed this information to be sent in real time to a computer.

By sniffing the network while sending a target phone an SMS, they were able to determine precisely which random network ID number belonged to the target. This gave them the ability to identify which of the myriad streams of information they wanted to record from the network.

All that was left was decrypting the information. Not a trivial problem, but made possible by the way operator networks exchange system information with their phones.

As part of this background communication, GSM networks send out strings of identifying information, as well as essentially empty "Are you there?" messages. Empty space in these messages is filled with buffer bytes. Although a new GSM standard was put in place several years ago to turn these buffers into random bytes, they in fact remain largely identical today, under a much older standard.

This allows the researchers to predict with a high degree of probability the plain-text content of these encrypted system messages. This, combined with a two-terabyte table of precomputed encryption keys (a so-called rainbow table), allows a cracking program to discover the secret key to the session's encryption in about 20 seconds.

This is particularly useful, the researchers said, because many if not most GSM operators reuse these session keys for several successive communications, allowing a key extracted from a test SMS to be used again to record the next telephone call.

"There is one key used for communication between the operators and the SIM card that is very well protected, because that protects their monetary interest," Nohl said. "The other key is less well protected, because it only protects your private data."

The researchers demonstrated this process, using their software to sniff the headers being used by a phone, extract and crack a session-encryption key, and then use this to decrypt and record a live GSM call between two phones in no more than a few minutes.

Much of this vulnerability could be addressed relatively easily, Nohl said. Operators could make sure that their network routing information was not so simply available through the internet. They could implement the randomization of padding bytes in the system information exchange, making the encryption harder to break. They could certainly avoid recycling encryption keys between successive calls and SMSs.

Nor is it enough to imagine that modern phones, using 3G networks, are shielded from these problems. Many operators reserve much of their 3G bandwidth for internet traffic, while shunting voice and SMS off to the older GSM network.

Nohl elicited a laugh from the audience of hackers when he called the reprogrammed network-sniffing phones "GSM debugging devices." But he was serious, he said.

"This is all a 20-year-old infrastructure, with lots of private data and not a lot of security," he said. "We want you to help phones go through the same kind of evolutionary steps that computers did in the 1990s."

Access on 26.07.2011