Technion team cracks GSM cellular phone encryption

By Hadar Horesh

Researchers at the Technion claim to have found an effective way to crack the encoding system for cellular telephone conversations conducted over GSM (Global System for Mobile) networks.

The team of researchers in Haifa, including Professor Eli Biham and doctoral students Elad Barkan and Natan Keller, presented their findings at the Crypto 2003 conference held two weeks ago at the University of California, Santa Barbara. The research has aroused great interest among cellular companies and equipment manufacturers, but none of the companies are ready to comment on this potential threat to the security of cellular networks.

GSM is one of the two standards widely used for cellular service. This digital technology was originally developed for Europe, but now accounts for over 70 percent of the world market. There are now some 540 cellular companies providing GSM services to approximately 870 million subscribers throughout the world.

In order to solve the encoding problem identified by the Technion researchers, cellular companies would, among other measures, need to replace all of the cellular phones used by their subscribers.

GSM systems are considered relatively secure. The only case of widespread eavesdropping on cellular telephone conversations in Israel involved tapping into the phone conversations of senior news reporters at Yedioth Ahronoth and Maariv. This eavesdropping was conducted with a system developed by ECI Telecom for use by intelligence agencies. The system was only capable of intercepting conversations on Pelephone's analog network, and is not effective in tapping into the digital networks now deployed to service subscribers of Pelephone, Cellcom and Partner.

Cellular conversations are conducted via digital signals. The voice message is translated by the phone into a series of digital signals that

Top Articles

Eight ways to be a leader
Over 1,500 Israelis came to hear Robin S. Sharma, author of "The Monk Who Sold His Ferrari," remind them of things they already knew but had forgotten.
By Shiri Lev-Ari

Soncino Casino R.I.P.
We have pretty bad news today for the Mifal Hapayis national lottery and the Finance Ministry; 60 illegal casinos on Soncino Street, Tel Aviv are desolate, almost closed.
By Nehemia Strasler

More Headlines

17:08 Police won't seek preemptive pardon over 2000 riots

16:05 Sources close to Abbas deny he plans to quit Thursday

13:33 Police question PM's son Gilad Sharon on 'Greek island' affair

16:13 Police arrest brother of Jewish terror suspect Sela Tor

16:50 Hit-and-run driver convicted of negligent manslaughter

18:20 Katsav holds radio chat with listeners in his native Iran

17:02 Soccer player Halfon to be tried for cocaine smuggling

carry the data and pass through an encoding process. These digital signals go through a decoding process on the receiving end of the conversation before being transformed back into a voice message. During the cellular conversation, there is also a filtering process of signals passing between the cellular phone and the nearby antenna. During this process, signals that are damaged for one reason or another are filtered out.

The Technion team explained at the conference that their system of cracking the GSM encoding mechanism would enable hackers to "hunt" codes used by cellular phones by collecting the digital signals sent to and from the cellular antennas. They could then eavesdrop on conversations by entering the cellular network "disguised" as one of the cell phones whose codes were cracked.

Four years ago, a number of articles were published by Israel researchers - including Prof. Biham - warning of the possibility of cracking the GSM code. An even earlier study on this potential problem was conducted by Professor Adi Shamir of the Weizmann Institute of Science, a world expert in cryptography whose encryption system is widely used in the field of satellite television.

The cellular companies responded to these earlier publications by explaining that it would be very difficult to implement these theoretical scenarios. To crack the codes, a hacker would need to tap into a conversation at the precise moment it began and there is really no chance of doing this, the cellular firms said.

But now, claims Prof. Biham, hackers could use the results of the latest research to immediately decipher the codes of telephones used in cellular conversations. According to Biham, this is possible due to a mistake by the designers of the GSM standard, who gave greater priority to improving the quality of the conversation than to perfecting the encoding system.

"We selected the GSM standard because someone else already demonstrated that the rival standard, CDMA [Code Division Multiple Access], could be cracked," Biham said yesterday. "The GSM code was considered stronger until now, but we've found a way to crack it. I don't work for a commercial company that stands to make profit from the discovery. I'm only attempting to check the strength of the codes," he added.

Until now, no practical methods of cracking the GSM code have been published in the media. The veteran private investigator Meir Pelovsky said yesterday that cellular conversations are considered relatively secure and that there are no devices available in the civilian market

that can tap these conversations.

This does not mean that it is impossible to listen in on cellular conversations. Each of the cellular providers are equipped with systems that enable locating and tapping into each conversation in its network. The license these companies received required them to allow authorized agencies to listen to any conversation after presenting an appropriate court order.

But not everyone wishing to listen in on cellular conversations is authorized or interested in asking for a court warrant. Intelligence agencies operating in foreign countries, private investigators and criminal elements would all be happy to get their hands on a device that enables them to eavesdrop on cellular conversations. The findings of the Technion team, which has already applied for a patent, is likely to enable a relatively inexpensive device to be built that will increase the risk of eavesdropping on the cellular conversations of GSM users.

(It is generally assumed that the U.S. National Security Agency (NSA) - which has received larger budgets in the wake of the September 11 terrorist attacks - has cracked the GSM code and is capable of tapping into any telephone in the world.)

Even if the cellular companies choose not to fix the breach discovered in the GSM security system, this problem will disappear when the cellular operators move to the third generation of cellular technology. According to Biham, the problem does not exist in this next-generation standard. But it will be several years before the third-generation technology is fully deployed. Partner plans to begin trial use of the new technology next year, with commercial operation starting only at the end of the year or in 2005.

Top

emoH | News | Business | Editorial & Op-Ed | Features | Sports | Books | nootraC | Site rules |