

Technion scientists crack GSM cellphone encryption

By JUDY SIEGEL

Cryptology experts at the Technion in Haifa have cracked the code used by 850 million cellphones, finding faults that could be used by thieves to steal calls and even to impersonate phone owners in the middle of a call.

If the cellphone companies in 197 countries want to correct the code errors that expose them to trickery and abuse, they will have to call in each customer to make a change in the cellphone's programming.

The researchers — Prof. Eli Biham of the computer sciences faculty, doctoral student Elad Barkan, and master's degree graduate Nathan Keller — discovered a basic flaw in the encryption system of the GSM (global system for mobile communications) network, which is used by 71 percent of all cellphones. In Israel, GSM is the system used by Partner (Orange) and half of Cellcom's customers, but not by Pelephone, which uses CDMA.

Biham, who worked as a doctoral student with the Weizmann Institute's Prof. Adi Shamir — a leading expert in cryptography and data security and co-inventor of the widely deployed RSA scheme for encrypting satellite TV user codes — said he and his colleagues revealed their discovery two weeks ago at the Crypto Conference in Santa Barbara, California. The 450 participants, many of whom are leaders in encryption research, "were shocked and astounded" by their revelation that most cellphones are susceptible to misuse.

"They were very interested in our work and congratulatory," Biham said. "Elad found that the GSM network does not work in proper order: First, it inflates the information passing through it in order to correct for interference and noise and only then encrypts it. At first, I didn't believe it. We checked it, and it was true."

As a result of their discovery, during the past year the three Technion researchers developed a method that made it possible for them to crack the GSM encryption system at the initial ringing stage, even before a call begins. Later on, they could listen in on the call. With the aid



71% of cellphones used are GSM

of a special device that can also broadcast, they found it was possible to steal calls and even to take on the identity of one of the phone owners in the middle of a call.

Recently, a new encryption system was chosen as a response to previous attacks on encryption systems, but the Technion researchers managed to overcome this improvement, too. Their patent-pending technique works for all GSM networks.

Biham explained that encryption ciphers were kept absolutely secret until 1999, when an Italian researcher, Marc Briceno, succeeded in reverse-engineering their algorithms. "Since then many attempts have been made to crack them, but these attempts required hearing the call's content during its initial minutes in order to decrypt its continuation, and afterward, to

decrypt additional calls. Since there was no way to know call content, these attempts never reached a practical stage. Our research shows the existence of the possibility to crack the codes without knowing anything about call content," he added.

Biham sent a free copy of the research to the GSM Association in Dublin so its member companies could correct the problem if they wished. "They now have enough information to do so."

While they don't know if they will make any money from their personal patent, they will offer it only to legal users, such as law enforcement agencies that need to listen in on suspected criminals' cellphone conversations.

The GSM program was created some two decades ago and is now in its second generation. A third generation is being developed, Biham said, "and since we told them about the fault, they will be able to produce it without errors, but I don't know how long it will take before the new system is released."

Biham was not aware of any clever thief who has already used the fault to cheat phone users, but "any failure like this could eventually be discovered and used for illegal purposes. That's why we made the information known to GSM."

The GSM Association, a global trade association that represents the interests of more than 585 cellphone companies and 132 phone equipment manufacturers, says that GSM differs from first generation wireless systems in that it uses digital technology and time division multiple access transmission methods. Voice is digitally encoded via a unique encoder, which emulates the characteristics of human speech.

The association says this transmission method allows "a very efficient data rate/information content ratio" and is the "safest" in protection of privacy, "designed with stringent levels of inbuilt security. With constantly enhanced transmission protocols and algorithms added to the flexible and future proof platform, GSM remains the most secure public wireless standard in the world."

Until the Technion scientists broke it.