ANFRAGE

der Abgeordneten Eder, Parnigoni
und GenossInnen
an den Bundesminister für Verkehr, Innovation und Technologie
betreffend die Abhörsicherheit österreichischer Mobiltelefone

Ein kürzlich erschienener Artikel in der angesehenen Zeitschrift „NewScientist" vom 13. September 2003 wurde die aktuelle Abhörsicherheit von GSM-Mobiltelefon als niedrig beurteilt (siehe auch Beilage).

Entsprechend Aussagen von Experten aus Israel und den USA bestehen demnach im Vercodungssystem von GSM-Telefonnetzen fundamentale Sicherheitslücken. Das GSM-System entscheidet dabei entsprechend der Empfangsstärke welches Codirungsniveau gewählt wird. Vor allem der einfachere Code ist mit relativ einfacher, kostengünstiger und im Handel erhältlicher Computertechnologie knackbar.

Eine verringerte Abhörsicherheit von GSM-Telefonen wäre ein schwerer Anschlag auf das geschäftliche und das privat Leben jedes Einzelnen. Die KonsumentInnen müssten rasch über die mangelnde Sicherheit ihres GSM-Telefons informiert werden.

Die unterzeichneten Abgeordneten stellen in tiefer Sorge um die Abhörsicherheit österreichischer Mobiltelefone an den Bundesminister für Verkehr, Innovation und Technologie nachstehende

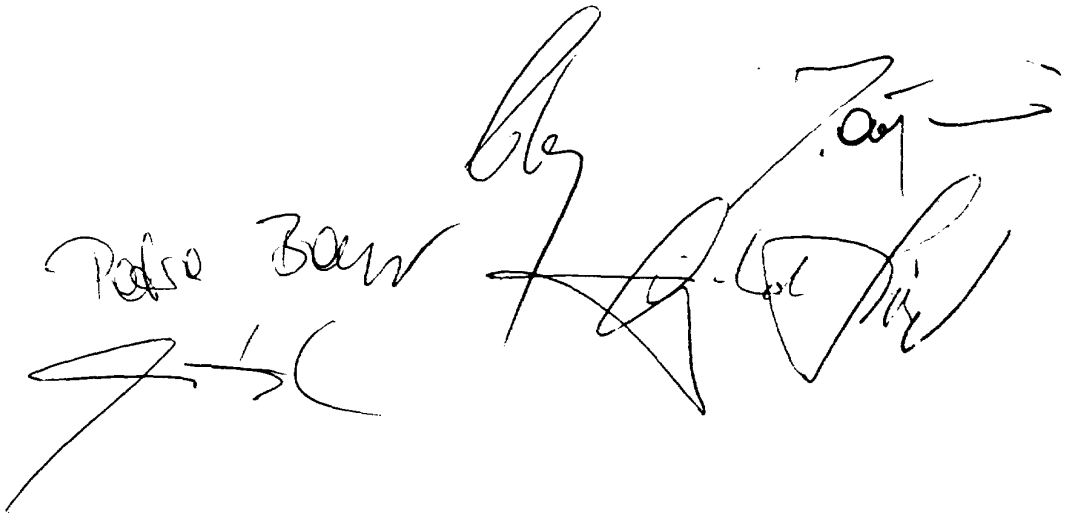
Anfrage:

1. Wie beurteilen Sie angesichts der offensichtlich weitgehenden bekannten Vercodungsmuster die aktuelle Abhörsicherheit österreichischer Mobiltelefone?

2. Welche technologische Möglichkeiten sehen Sie, die Abhörsicherheit von Mobiltelefonen entsprechend dem heutigen Stand der Technik zu verbessern?

3. Welche Zeiträume sind dafür erforderlich?

4. Sind Sie bereit, den österreichischen Mobiltelefonbetreibern entsprechende Auflagen zur Erhöhung der Abhörsicherheit von Mobiltelefone zu erteilen?



Flawed code leaves phones wide open to eavesdroppers

JUDY SIGEL-ITZKOVITCH, JERUSALEM

SERIOUS flaws have emerged in the encryption system that protects the privacy of most of the world's mobile phones. The weak points mean calls can be cracked using relatively cheap computing and listening equipment, allowing almost anybody to listen in.

The flaws, discovered by a team of Israeli cryptologists, affect the GSM (global system for mobile communications) set-up, which was designed in the late 1980s and is now used by 850 million people around the world. The system has two levels of encryption – a strong version known as A5/1 and a weaker one known as A5/2. When a call begins, the phone's base station chooses the level of encryption according to factors such as the quality of reception.

How the GSM encryption ciphers operate was a closely guarded secret until 1999, when Marc Briceno of the University of California at Berkeley worked them out. "Since then many attempts have been made to crack them," says Eli Biham, a cryptologist at the Technion-Israel Institute of Technology in Haifa.

However, the code encrypting a call can only be cracked if the eavesdropper knows at least some of the call content. "Since there is no way to know call content, these attempts never reached a practical stage," says Biham. But he and his students Elad Barkan and Nathan Keller have now discovered two flaws that make eavesdropping possible.

"At first I didn't believe it but we checked our finding again and again and it was true. This is a basic mistake in GSM design"

First, the team found that the GSM system adds an error-correcting code to the call content before encrypting it. This code is always structured in the same way, so knowing its sequence is like having part of the call content in advance. This makes the weaker A5/2 code straightforward to crack. It is a basic mistake in the GSM design, says Biham. "At first, I didn't believe it. But we checked it again and again, and it was true."

A second flaw is that the system can be tricked into using the same encryption key twice, first for a call made with the strong level of encryption and then with a weakly encrypted call. To decode a strongly encrypted call, the eavesdropper first records it in encrypted form and singles out the initial "challenge" between the base station and the phone. This is the first part of a call in which the unique key to encrypt the rest of the conversation is agreed upon. At this stage the key is strongly encrypted and can't be read.

But the eavesdropper then pretends to be a base station trying to make an incoming call to the target phone. At the beginning of the call, the eavesdropper retransmits the original encrypted challenge instructing the phone to use the same key again, but this time it commands the phone to switch to the weaker A5/2 level of encryption. The eavesdropper then cracks the weaker code, revealing the key that was used to encrypt both calls. The eavesdropper can use this to decipher the first call.

All this can be done with relatively cheap computing and listening equipment, says Biham, who announced the discovery at the recent annual Crypto Conference in Santa Barbara, California. He says the technique works for all GSM calls including the so-called "2.5 generation" GPRS service and for a new generation of GSM encryption known as A5/3, which has yet to be released.

"If you are the target of serious investigation you can get a higher level of confidence using a 3G handset"

The GSM Association, a trade organisation representing the mobile phone industry, has attempted to play down the work. It says setting up a bogus base station is illegal in most countries and so is unlikely to catch on. But Biham counters that the error-correcting flaw in GSM is so severe that there is a way to decipher the strong A5/1 code, even without the key obtained from a bogus base station challenge. He is keeping details of this technique under wraps, but admits that the amount of computing power necessary is beyond what would be available to most people.

Ross Anderson, a computer security expert at the University of Cambridge, says that the new generation of 3G networks use a different form of encryption and are safe for the time being. "If you are the target of serious investigation you can get a higher level of confidence using a 3G handset," he says. ●