

Israeli Scientists Crack GSM Mobile Call Security

Wed September 3, 2003 11:35 AM ET

By Albert Robinson

TEL AVIV (Reuters) - An Israeli scientist said on Wednesday his team had found a way to break into mobile phone calls on ubiquitous GSM networks, potentially allowing eavesdroppers to listen in on conversations and even take on a caller's identity.

The GSM Association, representing companies which depend on the world's largest mobile system, which is used by more than 860 million consumers in 197 countries, confirmed the security hole but said it would be expensive and complicated to exploit.

Professor Eli Biham of the Technion Institute in Haifa said he was shocked when doctoral student Elad Barkan told him he had found a fundamental error in the GSM (Global System for Mobile communications) code.

"We can listen in to a call while it is still at the ringing stage and within a fraction of a second know everything about the user," Biham said. "Then we can listen in to the call."

"Using a special device it's possible to steal calls and impersonate callers in the middle of a call as it's happening," he said. GSM code writers made a mistake in giving high priority to call quality, correcting for noise and interference, and only then encrypting, Biham said.

Snooping on mobile calls was fairly simple with analog networks, but since the advent of digital technology like GSM in the early 1990s this has become much harder. Currently law enforcers and other government agencies can break into calls, only by using special equipment that starts at \$250,000, said security expert Motti Golan, owner of Spy-Shop in Tel Aviv.

The new approach found by the Israeli scientists was different and could pose a threat, he said. "In the hands of terrorists this would be a disaster, but I don't see how they could get access to it," said Golan, a former police detective.

The researchers said they would help the GSM Association to fix the hole. The method will be patented and usage will be restricted to law enforcement agencies, Biham said.

HARD TO EXPLOIT

The GSM Association said the security holes in the GSM system stemmed from its development in the late 1980s when computing power was still limited, but that this particular gap could only be exploited with complex and expensive technology and that it would take a long time to target individual callers.

"This (technique) goes further than previous academic papers, (but) it is nothing new or surprising to the GSM community. The GSM Association believes that the practical implications of the paper are limited," it said in a statement.

GSM, or Global System for Mobile Communications, accounts for 72 percent of the world's digital mobile phone market and 70 percent of the global wireless market, the GSM association said.

The GSM Association said an upgrade had been made available in July 2002 to patch the vulnerability in the A5/2 encryption algorithm.

The researchers claimed they also managed to overcome the new encryption system that was put in place as a response to previous attacks, Biham said.

They have sent a copy of their research to the GSM Association to help them correct the problem, and the method is being patented and will be used only by law enforcement agencies, he said.

Biham and the GSM Association said the problem would not affect third-generation (3G) phones since engineers had replaced the encryption, security mechanisms and protocols with 3G.

The GSM Association also said any attack would have to be an active one, requiring the attacker to transmit distinctive data over the air to masquerade as a GSM base station. An attacker would also have to physically stand between the caller and the base station to intercept the call.

Transmitting on an operator's radio frequencies is illegal in most countries.