source: H-Online

At the 28th Chaos Communication Congress (28C3) in Berlin, security researchers have demonstrated a new technique for attacking GSM mobile phones. Karsten Nohl from Security Research Labs and his colleague Luca Melette have demonstrated a technique for using a mobile phone emulator based on open source software to make calls and send texts to expensive premium rate phone numbers. Nohl says that the attack carries a high risk of abuse and is already being actively used by criminals. In contrast to other known attacks, most of which are aimed at listening in on phone conversations, this attack poses a threat to anyone with a GSM mobile phone.

The new threat is based on prior work by the team of cryptographic experts. At last year's congress, Nohl and his team demonstrated a method of rapidly decrypting and listening in on GSM phone calls using an upgraded low cost mobile phone, a laptop and the open source application Osmocom . The technique exploited a known vulnerability in the widely used A5/1 encryption algorithm. To use the technique, an attacker needed to know the Temporary Mobile Subscriber Identity (TMSI) and secret key.

The researchers explained and then demonstrated how, using the above technique and easily procurable tools, attackers are able to emulate a mobile phone to make phone calls and send text messages. They noted that some users have already received bills totalling thousands of euros for calls and texts to Caribbean premium rate services. In many cases, an attacker can, by simulating a GSM mobile, also query that subscriber's mailbox providing they know the

subscriber's location and the key has not been changed.

Nohl called for mobile network operators, network equipment suppliers and device manufacturers to finally implement available techniques for improving GSM encryption mechanisms. These should, he believes, use better random numbers, switch frequencies, and stop recycling of previously used session keys. The researchers are also calling on users to collate information, using an interactive online map , on the extent to which network operators have eliminated known vulnerabilities in the GSM standard, some of which have been in the public domain for years. Their initial findings show that best in class in the UK is Vodafone, in Germany is T-Mobile, and in France SFR. None of the mobile phone operators have implemented all available security features, however.

In the medium term, Nohl is counting on a switch to the A5/3 encryption standard which significantly reduces the attack surface. Once mobile phone operators switch to this standard, he believes that the mobile phone itself is likely to remain the weakest link for some time to come. Almost all modern mobiles are able to use A5/3. According to Nohl, the failure by a single vendor – despite its claims to the contrary – to implement the updated algorithm is currently preventing mobile operators from carrying out trials.

Nohl also encouraged the hackers at the congress to protect themselves. Following a trip earlier this year to the Mecca of the "cyber-industrial complex", the Intelligent Support Systems (ISS) trade fair which is held at various sites in Asia and the Middle East, Nohl reports that the bestselling items in the espionage community at present are devices for monitoring mobile phones, such as IMSI catchers. These operate as base stations and entice nearby mobiles to connect by emitting a very strong signal, making it easy to locate phones and listen in on calls.

Nohl has responded by establishing an online platform at opensource.srlabs.de , hosting a wiki
on which users can collate factors indicating that an IMSI catcher is in use. There is also an Osmocom-based application called
Catcher Catcher
, which uses these factors to indicate the likelihood that a mobile phone is being monitored by an IMSI catcher. Catcher Catcher also enables users to determine whether security services have sent a silent SMS to their mobile. Over the last year, Germany's customs service, internal security services and criminal investigation service have all made enthusiastic use of these techniques to locate suspects.