22 July 2013 Last updated at 08:58 ET

Millions of Sim cards are 'vulnerable to hack attack'

http://www.bbc.co.uk/news/technology-23402988

A flaw with mobile phones' Sim card technology is putting millions of people at risk of being spied on and robbed, according to a leading security expert.

Mr Nohl said one in eight Sim cards might be vulnerable

Karsten Nohl has said he has found a way to discover some Sims' digital keys by sending them a special text message.

He warned criminals could potentially use the technique to listen in on calls or steal cash.

Industry organisation - the GSMA - said it was looking into the findings.

"Karsten's early disclosure to the GSMA has given us an opportunity for preliminary analysis," said a spokeswoman for the association, which represents global network operators,

"We have been able to consider the implications and provide guidance to those network operators and Sim vendors that may be impacted.

"It would appear that a minority of Sims produced against older standards could be vulnerable."

Mr Nohl has posted preliminary details of the vulnerability on the website of his company, Berlin-based Security Research Labs.

Intercepted calls

Sim (subscriber identity module) cards effectively act as a security token, authenticating a user's identity with their network operator.

They also store a limited amount of data such as text messages, contacts' telephone numbers and details used for some applications - including a number of payment and banking services.

The message contained a bogus digital signature for the network.

He said most phones cut contact after recognising the signature as being a fake - but in about a quarter of cases, the handsets sent back an error message including an encrypted version of the Sim's authentication code.

The encryption is supposed to prevent the authentication code being discovered, but Mr Nohl said that in about half of these cases it was based on a 1970s coding system called Digital Encryption Standard (DES), which was once thought secure but could now be cracked "within two minutes on a standard computer".

Once the attacker had this information, Mr Nohl said, they could download malware to the Sim written in the Java programming language.

He said these could be used by the hacker to send texts from the device to premium rate numbers they had set up, to discover and listen in to the target's voicemail messages and to track their location.

In addition, he warned that combined with other techniques, it could act as a surveillance tool.

"Sim cards generate all the keys you use to encrypt your calls, your SMS and your internet traffic," Mr Nohl told the BBC.

"If someone can capture the encrypted data plus have access to your Sim card, they can decrypt it.

"Operators often argue that it's not possible to listen in on 3G or 4G calls - now with access to the Sim card, it very much is."

Mr Nohl said that his research suggested about an eighth of all Sim cards were vulnerable to the hack attack - representing between 500 million to 750 million devices.

Although Mr Nohl would not reveal at this time in which countries DES encryption remained most common, he did say that Africa-based users had particular cause for concern.

"Here in Europe we use a Sim card to make phone calls and texts, but many people in Africa also use them for mobile banking," he said.

"Someone can steal their entire bank account by copying their Sim card.

"That adds a certain urgency because you imagine fraudsters would be most interested in breaking into their Sim cards - especially when it can be done remotely."

Mr Nohl says that mobile banking customers in Africa rely on the security offered by their Sim cards

Black Hat

Mr Nohl said he expected network operators would not take long to act on his study, and should be able to provide an over-the-air download to protect subscribers against the vulnerability.

The GSMA said that it had not yet seen the full details of his research, but planned to study it to pinpoint any issues that could be fixed.

It added that "there is no evidence to suggest that today's more secure Sims, which are used to support a range of advanced services, will be affected".

The UN's telecoms agency - the International Telecommunications Union - said that it would now contact regulators and other government agencies worldwide to ensure they were aware of the threat.

Mr Nohl said he planned planned to reveal more information about the vulnerability at the Black Hat security conference in Las Vegas later this month.

However, he said he would not publish a survey showing which phone owners were most at risk until December to give operators an opportunity to address the problem.