

10.08.2011. The New York Times

Hacker to Demonstrate 'Weak' Mobile Internet Security

BERLIN — A German computer engineer said Tuesday that he had deciphered the code used to encrypt most of the world's mobile Internet traffic and that he planned to publish a guide to prompt global operators to improve their safeguards.

Karsten Nohl, who published the algorithms used by mobile operators to encrypt voice conversations on digital phone networks in 2009, said during an interview he planned to demonstrate how he had intercepted and read the data during a presentation Wednesday.

Mr. Nohl said he and a colleague, Luca Melette, intercepted and decrypted wireless data using an inexpensive, modified, 7-year-old Motorola cellphone and several free software applications. The two intercepted and decrypted data traffic in a five-kilometer, or 3.1-mile, radius, Mr. Nohl said.

The interceptor phone was used to test networks in Germany, Italy and other European countries that Mr. Nohl declined to identify. In Germany, Mr. Nohl said he was able to decrypt and read data transmissions on all four mobile networks — T-Mobile, O2 Germany, Vodafone and E-Plus. He described the level of encryption provided by operators as "weak."

In Italy, Mr. Nohl said his interceptions revealed that two operators, TIM, the mobile unit of the market leader, Telecom Italia, and Wind did not encrypt their mobile data transmissions at all. A third, Vodafone Italia, provided weak encryption, he said.

A spokeswoman for the GSM Association, the industry group based in London that represents global telephone operators, said the group would await details of Mr. Nohl's research before commenting. A spokesman for O2, which is owned by Telefónica of Spain, said the operator followed Mr. Nohl's research closely and would take account his findings in its own operations.

Vodafone said in a statement that "We regularly review security measures and carry out risk assessments to prevent the kind of exploit described. We implement appropriate measures across our networks to protect our customers' privacy."

Mr. Nohl said he developed his interception technology on an internal broadband network he set up at his research firm, Security Research Labs, in Berlin. His tests focused on mobile data networks that ran on the General Packet Radio Service, or GPRS, technology, which is used widely across the globe.

GPRS networks were introduced in 2000 as successors to GSM digital networks and were the first mobile networks to deliver significant data besides short text messages. GPRS networks are still widely used as backups for newer, faster 3G wireless networks, and consumers are often diverted to GPRS grids when they reach the limits of their monthly data plans.

Rogers Communications, a Canadian operator, estimates that 90 percent of mobile data traffic still runs on GPRS networks.

Mr. Nohl said he was surprised to find that the two Italian operators, TIM and Wind, did not encrypt their data traffic at all. In a statement, TIM would not confirm Mr. Nohl's claims.

"TIM confirms that it uses state-of-the-art radio mobile technologies from primary international vendors to guarantee the protection of its mobile communications," it said.

Mr. Nohl, who said he works for mobile operators who hire him to detect vulnerabilities in their systems, said many operators continue to run unencrypted data networks because it allows them to more easily filter out competing, unwanted services like Skype, an Internet-based service that allows consumers to make voice and video calls without using the operators' voice networks.

"One reason operators keep giving me for switching off encryption is, operators want to be able to monitor traffic, to detect and suppress Skype, or to filter viruses, in a decentralized fashion," Mr. Nohl said. "With encryption switched on, the operator cannot 'look into' the traffic anymore while in transit to the central GPRS system."

Mr. Nohl said he intended to release his instructions at a conference of the Chaos Computer Club, a computer hackers' group, which is being held near Berlin in Finowfurt, Germany. They will describe how to convert a Motorola C-123 cellphone, which is designed to run open-source software, into an interception device. But he said he would not release the keys to unlock the encryption used by operators to secure GPRS networks.

Mr. Nohl said his research was intended to prod mobile operators to improve the security of the wireless Internet, which he said was rudimentary compared with the safeguards protecting data sent over conventional, fixed-line computer networks. He said he destroyed the data he had intercepted from networks in Europe, and did not condone eavesdropping, a crime in Europe.

"We are releasing the software needed to reprogram cheap Motorola phones to become GPRS interceptors," Mr. Nohl said. "This exposes operators with no encryption, like those in Italy, to immediate risk."

Mr. Nohl said the release of the information would give mobile operators "a few months" to improve security before other hackers recreated his results and attempted to breach security of the mobile broadband networks.

http://www.nytimes.com/2011/08/10/technology/hacker-to-demonstrate-weak-mobile-internet-security.html?_r=2