Scientists break satellite telephony security standards

February 8 2012

Satellite telephony was thought to be secure against eavesdropping. German researchers at the Horst Gortz Institute for IT-Security (HGI) at the Ruhr University Bochum (RUB) have cracked the encryption algorithms of the European Telecommunications Standards Institute (ETSI), which is used globally for satellite telephones, and revealed significant weaknesses. In less than an hour, and with simple equipment, they found the crypto key which is needed to intercept telephone conversations. Using open-source software and building on their previous research results, they were able to exploit the security weaknesses.

In some regions of the world standard cell phone communication is still not available. In war zones, developing countries and on the high seas, satellite phones are used instead. Here, the telephone is connected via radio directly to a satellite. This passes the incoming call to a station on the ground. From there, the call is fed into the public telephone network. So far this method, with the ETSI's encryption algorithms A5-GMR-1 and A5-GMR-2, was considered secure.

For their project, the interdisciplinary group of researchers from the areas of Embedded Security and System Security used commercially available equipment, and randomly selected two widely used satellite phones. A simple firmware update was then loaded from the provider's website for each phone and the encryption mechanism reconstructed. Based on the analysis, the encryption of the GMR-1 standard demonstrated similarities to the one used in GSM, the most common

mobile phone system. "Since the GSM cipher had already been cracked, we were able to adopt the method and use it for our attack", explained Benedikt Driessen, of the Chair for Embedded Security at the RUB. To verify the results in practice, the research group recorded their own satellite telephone conversations and developed a new attack based on the analysis. "We were surprised by the total lack of protection measures, which would have complicated our work drastically", said Carsten Willems of the Chair for System Security at the RUB.

Encryption algorithms are implemented to protect the privacy of the user. "Our results show that the use of satellite phones harbours dangers and the current encryption algorithms are not sufficient", emphasized Ralf Hund of the Chair for System Security at the RUB. There is, as yet, no alternative to the current standards. Since users cannot rely on their security against interception, similar to the security of standard cell phones, they will have to wait for the development of new technologies and standards, or make use of other means of communication for confidential calls.

More information: Details of the HGI results are available online at: gmr.crypto.rub.de

Provided by Ruhr-University Bochum