hgi
Horst Görtz Institut
für IT-Sicherheit

Remote keyless entry system for cars and buildings is hacked
RUB security experts discover major vulnerability
Access from a distance of 300 feet without traces

Bochum, Germany, March 31, 2008

Researchers from Ruhr University Bochum, Germany, presented a complete break of remote keyless entry systems based on the KeeLoq RFID technology. The shown vulnerability applies to all known car and building access control systems that rely on the KeeLoq cipher. “The security hole allows illegitimate parties to access buildings and cars after remote eavesdropping from a distance of up to 100 meters” says Prof. Christof Paar. His Communication Security Group in the Electrical Engineering and Information Sciences Department has developed the break as part of their research in embedded security.

Two Intercepted Messages are Sufficient

Prof. Paar’s team applied the newest code breaking technologies for developing several attacks. With the most devastating attack, car keys (or building keys) can be cloned from a distance of several 100 meters. “Eavesdropping on as little as two messages enables illegitimate parties to duplicate your key and to open your garage or unlock your car”, says Prof. Paar. With another malicious attack, a garage door or a car door can be remotely manipulated so that legitimate keys do not work any more. As a consequence, access to the car or the building is not possible any more.

Newest Code Breaking Techniques

A KeeLoq system consists of an active Radio Frequency Identification (RFID) transponders (e.g., embedded in a car key) and a receiver (e.g., embedded in the car door). Both the receiver and transponder use KeeLoq as encryption method for securing the over-the-air communication. The attack by the Bochum team allows recovering the secret cryptographic keys embedded in both the receiver and the responder. The attack is based on measuring the electric power consumption of the receiver. Applying what is called side-channel analysis methods to the power traces, the researchers were able to extract the manufacturer key from the receivers. The attack – which combines side-channel cryptanalysis with specific properties of the KeeLoq algorithm – can be applied to all known variants in which KeeLoq is used in real world systems. The practicality of the attack has been confirmed by attacking actual systems which are using KeeLoq.

KeeLoq: widely used since the mid-1990s

KeeLoq has been used for access control since the mid-1990s. By some estimates, it is the most popular of such systems in Europe and the US. Besides the frequent use of KeeLoq for garage door openers and other building access applications, it is also known that several automotive manufacturers like Toyota/Lexus base their anti-theft protection on assumed secure devices featuring KeeLoq.

IT Security Research in Bochum

Prof. Paar’s group is part of the Horst Görtz Institute for IT Security (HGI), one of the largest university-based security research centres in Europe. Prof. Paar’s group is internationally renowned for their work in securing and analysing embedded security systems. Ruhr University Bochum has the most comprehensive offerings in IT security education (Bachelor, Master, distance learning) in Germany.

Further Information

Prof. Dr.-Ing. Christof Paar, Communication Security Group, Faculty of Electrical Engineering and Information Science, Ruhr University of Bochum, D-44780 Bochum, Germany
Email: keeloq@crypto.rub.de
Phone: +49 234 32 22994

Web links

More information about the KeeLoq attack:
www.crypto.rub.de/keeloq

Chair of Communication Security of Prof. Christof Paar:
http://www.crypto.ruhr-uni-bochum.de/en_news.html

Horst Görtz Institute for IT Security:
http://www.hgi.rub.de/index_en.html

Ruhr University of Bochum:
http://www.ruhr-uni-bochum.de/index_en.htm