The perfect clone: Researchers hack RFID smartcards

November 3 2011

Professional safecrackers use a stethoscope to find the correct combination by listening to the clicks of the lock. Researchers at the Ruhr-University Bochum have now demonstrated how to bypass the security mechanisms of a widely used contactless smartcard in a similar way. Employing so-called "Side-Channel Analysis" the researchers of the Chair for Embedded Security (Prof. Dr.-Ing. Christof Paar) can break the cryptography of millions of cards that are used all around the world.

RFID smartcards (Radio Frequency Identification) of the type DESFire MF3ICD40 are widely employed in payment and access control systems. The security of these cards is based on Triple-DES, a cipher that is unbreakable from a purely mathematic point of view. DESFire cards are for instance used by the public transport agencies in Melbourne, San Francisco and Prague. The DESFire MF3ICD40 is manufactured by NXP, the former semiconductor division of Philips Electronics.

A person is identified as a passenger, employee or customer when his RFID smartcard is placed in the proximity of a reader. To guarantee the necessary level of security, a secret key is stored on the integrated chip inside the card. But just like for the safe, the security mechanism produces the electronic equivalent of the clicks of a mechanic lock. "We measured the power consumption of the chip during the encryption and decryption with a small probe", says David Oswald. The fluctuations of the electro-magnetic field allow the researchers to conclude to the full 112-bit secret key of the smartcard.

Having extracted the keys, an attacker can create an unlimited number of undetectable clones of a given card. The required time and effort are quite low: "For our measurements, we needed a DESFire MF3ICD40 card, an RFID reader, the probe and an oscilloscope to measure the power consumption", says Oswald. This equipment only costs a few thousand euros. Having obtained knowledge on the characteristic properties of the smartcard, the attack takes three to seven hours. The manufacturer NXP confirmed the security hole in the meanwhile and recommends his customers to upgrade to a newer version of the card.

Already back in 2008, researchers around Prof. Dr.-Ing. Christof Paar used Side-Channel Analysis to break supposedly secure systems. Three years ago, garage and car doors "mysteriously" opened for the researchers of the Chair for Embedded Security. The employed KeeLoq RFID system – which customers and manufacturers trusted blindly before – turned out to be highly susceptible to Side-Channel Analysis.

More information: www.emsec.rub.de/

Provided by Ruhr-University Bochum