

- Press Statement -

Karsten Nohl – nohl@virginia.edu
Starbug – starbug@berlin.ccc.de
Henryk Plötz – henryk@ploetzli.ch

January 8, 2008

Lost Mifare obscurity raises concerns over security of OV-Chipkaart

During the 24C3 conference in December we discussed the cryptography used in Mifare Classic wireless smartcards, whose security we found to be insufficient for many of its applications. In light of a recent debate over the security of the Dutch OV-Chipkaart used in public transportation, we would like to clarify several aspects of our assessment.

We reverse-engineered the cryptographic components of the Mifare Classic RFID tags. This type of card is used in various micro-payment applications including the Oyster card and the OV-Chipkaart. We have neither published the details of our findings nor actively attacked any real-world system.

The security of the Mifare Classic cards relies on secret keys with a key length of a mere 48 bits. Knowing the details of the cipher would permit anyone to try all possible keys in a matter of days. Given basic knowledge of cryptographic trade-offs and sufficient storage, the secret keys of cards can be found in a matter of minutes. Regardless of the cryptographic strength of the cipher, the small key space therefore permits counterfeiting of any card that is read wirelessly.

Work by undergraduate students at the University of Amsterdam (published in July) has already demonstrated the possibility of free-riding by copying or recharging temporary passes. The same weaknesses will permit copying and potentially recharging the permanent passes once the details of the Mifare crypto are disclosed. While sound cryptography would have protected the data on the tags from being read by illegitimate reading devices, security weaknesses in other parts of the system design permit copies of tags to be used.

We falsely stated during our presentation that the same technology was used in car theft protection systems. While the cipher used in Hitag2-secured car keys is different, it is related to the cipher in the Mifare tags and does not provide any more security from a cryptographic standpoint. Other types of RFID tags by Philips including the Hitag2+ tags and the Mifare DESfire are not affected by our findings. The latter type of card in particular is likely to provide high levels of security as its cryptography relies on peer-reviewed, certified, and established primitives.