

July 2008

Security of RFID Systems in spite of hacked Mifare-Classic RFID chips

Since the coding algorithm of Mifare-Classic RFID Chips has been hacked, millions of users of such RFID cards question the security of this technology for applications such as access control or payment systems.

FEIG ELECTRONIC, a worldwide leading manufacturer of RFID readers, has no concern regarding this issue. The following methods can be used to re-establish the security of the cards.

Ways to allow continuous use of hacked Mifare-Classic-Cards

One option is to make card cloning more complicated by connecting the card's serial number to the data stored and additionally encrypting this data with the host-system. This way, the data is not directly readable, even if the Mifare-Classic key is known.

Another option is to encrypt the stored data with a customized encryption key, where every card receives an individual code. This method prevents the delivery of the code for all cards for a specific application, once an individual card has been hacked.

Although both alternatives require additional programming, they can be easily implemented, even into the infrastructure of already existing systems. System Terminals can be used in order to convert cards that are already in circulation.

Monitoring transaction data by using a clearing-system is another method for fraud defense. For this purpose, a transaction counter can be easily installed on the card. Another way to increase the level of security is saving the specific time a transaction is made. In case a cloned card enters circulation, the clearing-system should recognize the irregular actions and freeze the card.

Change to transponder cards with higher security architecture

Despite the multiple opportunities to additionally increase the security level of Mifare-Classic Cards, switching over to other transponder cards with a higher grade security architecture is another alternative. Available are Mifare Plus cards, my-d proximity cards and cards with a processor chip.

It is recommended to use cards with a processor chip in addition to the higher grade security card mentioned above.

With its OBID[®] reader family *classic-pro*, FEIG ELECTRONIC supports all ISO14443 cards from many different manufacturers with recognized security infrastructure such as AES and 3DES. By using SAM modules, the highest security standards can be achieved.

Today, FEIG ELECTRONIC is working on a more user friendly implementation of the Mifare DESFire functions of the reader. Until now all security functions have to be processed at the host level. With this new firmware, the encryption takes place at the reader and frees the host from this process, making it more user-friendly.

To summarize the subject, hacked Mifare-Classic Cards are not a lasting threat to the safety of RFID technology that is used in the fields of access control and payment systems. Despite the fact that cards can now be cloned, one can either find multiple ways to continue running applications safely or switch to new card technologies.

Please contact FEIG ELECTRONIC to discuss your individual solution.

OBID[®] - RFID by FEIG ELECTRONIC

About FEIG ELECTRONIC GmbH

FEIG ELECTRONIC is a German, worldwide leading manufacturer of RFID reader systems.

OBID[®] readers are in use worldwide – they are developed, manufactured and distributed by FEIG ELECTRONIC worldwide.

OBID[®] readers are developed according to public RFID standards, in very closed collaboration with every leading manufacturer of transponder chips.

OBID[®] readers are available for all common frequencies as LF, HF and UHF.

www.feig.de