

November 10th, 2008

Dear MIFARE Classic user,

This letter serves to further inform you on the recent situation concerning the security deficiencies of our MIFARE Classic product.

By letters dated from February 2nd, March 13th, May 5th, July 11th and 29th 2008 we have informed you already on this subject.

NXP Semiconductors is aware of the fact that several research groups have developed attacks to break keys of MIFARE Classic-enabled cards. Amongst others there are the group around Karsten Nohl and Henryk Ploetz, who initially presented the reverse engineering of MIFARE Classic chips in December 2007 at the 24th Chaos Computer Congress in Berlin, the IT security specialists from the Radboud University of Nijmegen as well as Nicolas T. Courtois from the University College London.

We have clearly explained to all research groups the potential risks that a publication of their findings would entail. In order to allow our customers a reasonable time for appropriate system security updates in their MIFARE Classic infrastructures, we tried to delay a publication planned by the Radboud University of Nijmegen with an injunction. However the court in Arnhem decided per July 18th to allow the publication in the interest of freedom of speech.

On October 6th 2008 the Radboud University Nijmegen has presented a report during a conference, with information on how the protocol and algorithm were reverse engineered and the description of some practical attacks which can be carried out with limited means. On the same day Henryk Ploetz has published a document on the internet containing detailed information on attacks.

Subsequently additional code information has been revealed to the public anonymously on various websites, which significantly facilitates attacks on cards and infrastructures. NXP is trying to prevent these publications but due to the nature of internet it is to be expected that such an effort does not meet much success.

Therefore, as we did before, we feel it is appropriate to inform you once more about the potential consequences and necessary measures to be taken to minimize the impact of possible attacks for your system infrastructure.

We are investigating protection scenarios for systems using MIFARE Classic, as in some systems insufficient mechanisms to detect fraudulent cards may have been implemented. Mindful of the above, we urgently ask you to contact your system integrator for an assessment of your systems. Extensive additional protection mechanisms are recommended, both on how the data on the card is used as well as deploying additional security layers separate from the card.

Naturally, your risk assessment depends on the assets to be protected and whether the end-to-end system still meets your requirements, which only you and your system integrator can determine.

End to end measures should also be applied for access management infrastructures, often by complementing systems with additional measures e.g. camera surveillance, security personnel, etc. when valuable assets need to be protected. We recommend that your assessment of the impact of the recent and expected developments takes into account the particular way how the system is implemented and used, its relation to other protection in place, and specifically whether there is a need to prevent unauthorized single time access or access during a limited period of time. Depending on the specific situation in existing MIFARE Classic access management infrastructures, in many cases the usage of more sophisticated card ICs may be recommendable.

DESFire EV1 and MIFARE Plus (samples available in Q4 2008) are our recommended solution for new access management implementations where a strong level of security is required.

MIFARE Classic provides a benchmark in cost competitiveness, while the recently announced MIFARE Plus enables an optimal future-proof migration path when necessary. Both, MIFARE Plus and our new high-end product MIFARE DESFire EV1 offer strong AES encryption and are targeted to receive the internationally recognized Common Criteria certification.

NXP's expertise is the design and manufacturing of chips; although we do not design end to end security systems, we would be happy to continuously support your system integrator so that the best solutions are reached.

If you would have any questions, please contact us at mifare@nxp.com. If, in addition, you would like to be kept informed about the developments in this matter, please send an email to mifare@nxp.com as well. Additionally, we will be giving updates on the MIFARE website under http://mifare.net/security/mifare_classic.asp.

Sincerely yours
The NXP MIFARE team