

Security Evaluation of the MIFARE Plus Architecture

Horst Görtz Institute for IT Security
Ruhr University Bochum, Germany
www.hgi.rub.de

1 System Description

The MIFARE Plus architecture is designed to be used in security related applications. The main functions that can be realized with MIFARE Plus products are (1) authentication and (2) secure storage of data in non-volatile memory. MIFARE Plus supports the privacy of the user and can ensure the confidentiality and authenticity of the transferred information. All communications are securely protected against several attacks. This report evaluates the security and privacy provided by the MIFARE Plus architecture in compact form.

With respect to security, the MIFARE Plus architecture applies two main cryptographic schemes. One is the AES encryption and decryption algorithm, the other one is a CMAC that is also based on AES. In both cases the MIFARE Plus architecture uses the 128-bit version of AES which is considered as an extremely secure modern encryption algorithm. It is widely used in many commercial standards as well as some government applications with very high security requirements. There are no realistic attacks against AES known and it can be considered a very secure module of the MIFARE Plus architecture.

Furthermore, MIFARE Plus offers several innovative security features, such as a proximity check and a privacy enhanced authentication.

2 Security and Privacy Assessment

There are several security and privacy related issues which have been considered in the design of the MIFARE Plus architecture. The most important ones are listed below:

- The MIFARE Plus architecture introduces the use of a random identifier (RID) instead of the unique identifier (UID) to provide enhanced privacy for privacy-critical applications. Privacy-critical information is only exchanged in encrypted form, ensuring confidentiality of that information.

- The proximity check which is offered by the MIFARE Plus architecture ensures that a card is physically close to the reader device and can thereby impede relay attacks. Furthermore, it makes side channel attacks more difficult and performs a first mutual authentication.
- MIFARE Plus architecture also employs a special truncation scheme for the result of AES-based CMAC which shows a higher resistance to DPA attacks without influence on the cryptographic strength compared to CMAC with standard truncation method. The AES-CMAC with special truncation is employed in proximity check and for the integrity protection of secure messaging. Hence, the proximity check and the integrity protection of secure messaging feature an increased level of security against DPA adversaries.
- Mutual authentication between card and reader is bi-directional and secured by the aforementioned AES module. This ensures that both sides (card and reader) share a common secret and are known as legitimate to each other.
- As mentioned before, the confidentiality of the communication between the card and the reader can be provided by the AES encryption scheme. Moreover, the integrity of the transferred information can be ensured by attaching a MAC generated by the AES-based CMAC module over the plain or encrypted messages.
- MIFARE Plus supports a key diversification scheme, which is strongly recommended by the MIFARE Plus architecture, to prevent that different cards use the same keys. This ensures that even if one card gets compromised, the rest of the system remains secure.
- The protection of data sessions uses session keys, which are generated from two random values negotiated between card and reader during authentication. Using session keys reduces the amount of times where pre-shared keys have to be used and bounds any potential vulnerability (which has not been detected) to the current session.
- MIFARE Plus also ensures session freshness by including a transaction identifier and a read and write counter in the protocol. It strengthens the security of the card and its robustness against several attacks.

3 Summary

Despite extensive and careful analysis, we have not identified any security weakness with practical relevance. We consider the MIFARE Plus architecture to be secure if all security mechanisms are activated as recommended in the MIFARE Plus documentations. The CC evaluation of the card further supports our belief that NXP succeeded in designing a very secure contactless authentication and storage system.

The MIFARE Plus architecture is well documented. Security and privacy aspects have been explored in the documentation. Residual vulnerabilities are well evaluated. Several countermeasures are included in the architecture, and additional ones can be employed in the back end implementation. In general, the architecture allows for several performance-security tradeoffs. We recommend to do security analysis for the target application when ignoring any security feature which is provided and recommended by MIFARE Plus architecture.