The MIFARE Classic Story

Keith E. Mayes
Information Security Group – Smart Card Centre
Royal Holloway, University of London
Egham, U.K.
keith.mayes@rhul.ac.uk

Carlos Cid
Information Security Group
Royal Holloway, University of London
Egham, U.K.
carlos.cid@rhul.ac.uk

Abstract

The MIFARE Classic product from NXP Semiconductors has been much maligned over recent years and whilst some of the criticism is well justified by virtue of the inherent security problems, it is by no means the weakest card/RFID in use today. In this article we give a brief overview of the MIFARE Classic card, its use, design and security. We start by looking at the range of card and RFID products and placing the MIFARE Classic in its intended position. The process of risk assessment is then discussed as a means of choosing "appropriate" products and solutions. We then discuss the history of the MIFARE Classic, its design, security features and associate attacks. The long-lasting effects of the attacks and publicity are considered with respect to not only the MIFARE Classic, but for similar products risk reviews.

1 Introduction

A best-practice system design considers requirements first, and technology and general implementation at a later stage. Part of the requirements definition should include security risk assessment as this has influence on security measures within the system and the choice of technologies and products. Unfortunately this is not always so clear-cut in smart card and RFID systems: what one is functionally able to do may be severely constrained by available resources, and perhaps only one technical approach is feasible from a business case perspective. Whether a range of technology choices is available or not, it is still very important to carry out a thorough risk assessment as it provides the means to estimate the likelihood and impact of potential problems and the opportunity to compensate by other available means, for instance improved back-office detection or human processes.

The MIFARE Classic was introduced in 1994 by Philips (now NXP Semiconductors [11]), and is one of the most widely deployed contactless smart cards. Over the years various system owners came to the conclusion that the MIFARE Classic was an appropriate product to use, i.e. a fair compromise between functionality, speed, security and cost. Any short comings were usually addressed by back-end system security measures that were deemed adequate against the likely threats. Whether this conclusion was always correct is a matter for debate, although in the light of recent attacks and publicity it would be hard to argue against the fact that the solution offers less security than system designers expected.

Before considering the events and attacks that eroded confidence in the MIFARE Classic, it is worthwhile considering where it was intended to fit within the range of contactless smart cards and RFID devices.

2 RFID and Smart Card Security Spectrum

There has always been some confusion when defining what a smart card is and what an RFID is. In fact the terminology comes from different industry sectors that have products with overlapping characteristics. An RFID in its simplest sense is something that communicates and identifies itself by radio means. It does not imply any security nor does it mean some small-size tag that we have come to associate with the name. For example radar and Identification Friend or Foe (IFF) systems are cited as early forms of RFID systems and a mobile phone could be regarded as a very sophisticated long-range RFID. RFIDs can be active, i.e. have power sources and transmitters, or more commonly passive using a reader electromagnetic field for power and communication over a short range.

Smart cards as the name suggests are cards that can be used in a "smart fashion". Normally we think of a plastic card containing an IC; however there are still those who refer to magnetic-stripe cards as smart cards. The plastic card with the IC can be generically referred to as a chip card and it comes in the contact and contactless varieties. The contact card is inserted into a reader which makes physical contact with the gold coloured pads on the card, e.g. such as a chip and PIN POS reader. Contactless cards are brought into proximity of a reader and are powered and communicate via the electromagnetic field.

The contactless chip-card and the RFID are clearly members of the same family. An RFID chip embedded into a plastic card would probably be described as a contactless chip card, whereas departing from the card form-factor means that one would usually call it an RFID. The most sophisticated chip-cards have attack resistant microcontrollers and would generally be regarded as smart cards, whereas the classification of other chip-cards as "smart" is more subjective. RFID and smart cards have a wide range of uses in the modern world. They can be used as tokens for authentication, inventory control, electronic purses, anti-theft devices, e-passports, etc. It is clear that the security requirements also vary with their different applications. Cryptographic protection may not always be required (e.g. with simple passive RFID tags which simply broadcast their ID and are used for inventory control), while in

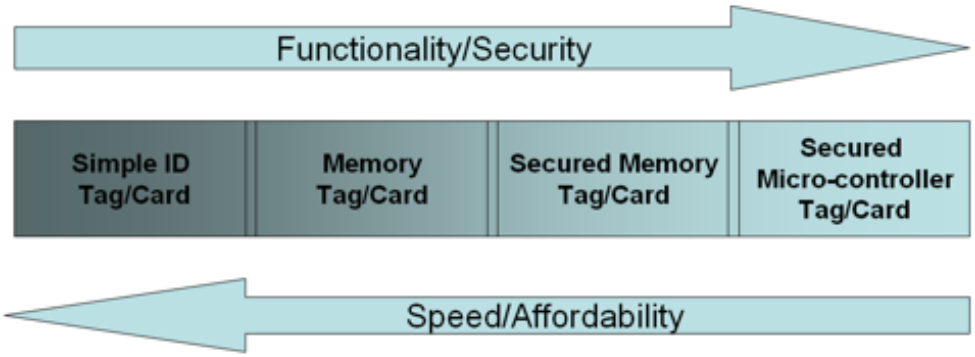

Figure 1: The range of generic Smart Cards and RFIDs

some cases more robust security mechanisms are needed, e.g. when there are privacy concerns or unclonability requirements.

The range of card/tag types is illustrated in Figure 1 along with the general trends that affect the product choice.

Simple ID/Tag. This is the simplest and least secure member of the family. The one security property is that the ID can be made read only and unique across legitimate devices. As there is no protocol other than responding with the ID, it is easy to eavesdrop the transmission and replicate it via an emulator device or, if available, a similar ID/Tag that permits control of the ID field.

Memory ID/Tag. Such cards usually have a unique ID (like the ID/Tag) plus an open memory with read/write access. As there is no security protocol, it is possible to read the data contents and/or use the information in an emulator or clone platform. However if the issuer adds integrity protection to the data (e.g. via use of MAC algorithm) then at least an attacker should be prevented from modifying the existing data or generating new data, providing reader devices have the functionality and keys to verify the MAC.

Secured Memory ID/Tag. These cards implement cryptographic protocols to control access to memory contents. Typically the ID/Tag and reader will mutually authenticate before allowing access to memory, usually with data transfers encrypted under session keys. Some cards divide the memory up into smaller partitions that have different keys, so multi-application support is possible with different keys assigned to various application providers.

Secured Microcontroller ID/Tag. This is the high-end of the range. With a microcontroller you can not only store data, but also load custom functionality. Various mature standards exist for security management including Global Platform [6] and there is maximum flexibility on the card functionality and general capabilities. The

most advanced products include cryptographic co-processors for common symmetric and asymmetric cryptographic functionality such as encryption, verification and signing.

The MIFARE Classic was selected in numerous real-world systems as a Secured Memory ID/Tag. The design claims the functionality required for this class and the product is fast enough for demanding applications yet relatively low cost. However, as it should become evident from our discussion in later sections, the product should now be regarded as a simple un-secured memory card. This does not automatically mean that it is unusable, although any risk reviews and decisions based on the product's intended capabilities are now in question and should be revisited.

3 MIFARE Classic Security Features

MIFARE Classic communication is based on the ISO 14443 standard [8] (although much is compliant with [8], part of the communication protocol implemented by NXP differs from the standard). The memory in the card is divided in data blocks, which in turn are grouped in sectors. Each sector contains two secret 48-bit keys, shared with legitimate readers. A reader will need to authenticate using one of the keys to access data and perform operations in a particular sector.

The MIFARE Classic uses a 3-pass mutual authentication protocol based on the ISO 9798-2 standard [7], with however some proprietary components. After identification based on its UID, card and reader authenticate to each other; freshness is based on 32-bit nonces. Nonces in the card are generated using a PRNG. Following authentication, communication between reader and card is encrypted. Both authentication and encryption are based on the CRYPTO1 algorithm, a proprietary LFSR-based stream cipher designed by NXP.

The MIFARE Classic is a fairly old design from 1994 that soon became a successful product. If we are looking for any other successful smart card system of the day as a design benchmark, we know that at the time GSM and SIM cards had been used commercially for a couple of years. A reviewer tasked with considering and comparing the security of the MIFARE Classic and the GSM SIM could have produced Table 1 below.

	MIFARE Classic	**GSM SIM**
Authentication key length	48 bits (multiple keys)	128 bits
Random number/Nonce length	undisclosed	128 bits
Authentication Algorithm	undisclosed/proprietary	undisclosed/proprietary
Encryption key length	undisclosed	64 bits maximum
Encryption Algorithm	undisclosed/proprietary	A5/1

Table 1: MIFARE Classic and GSM SIM comparison

At the time, the reviewer would have little information to go on in the MIFARE Classic case except for the key size, which can be compared with GSM. At the time,

mobile phone calls were still very expensive and there were major concerns over privacy and call eavesdropping. The industry was still smarting from the attacks on the analogue phone system and so security had a high profile, and a robust and attack-resistant design was attempted. The result is a large difference in the authentication key sizes and a brute force attack against GSM would require on average 2^{80} times more attempts than one against the MIFARE Classic. It could be argued that GSM was perhaps being over protective; however we note that the DES block cipher, at the time already an 18-year-old design, had a key-size of 56 bits and so it would require on average 2^8 times more attempts to brute force DES than the MIFARE Classic. The point is that it may not be that straightforward to conclude that the MIFARE Classic key size was simply a "bad" design choice, but rather that the product was never intended for high security and/or high value protection systems.

Moving our review to the end of the decade, we should also recall the Electronic Frontier Foundation-sponsored effort to build a dedicated DES key cracker in the late 1990s. It culminated with the recovery in 1999 of a DES secret key in little over 22 hours. Thus a review of the MIFARE Classic around 2000 would likely have said that the product is vulnerable to brute force attack if the algorithm becomes public and a dedicated key cracker is implemented. Such a review should probably also stress that the security of systems based on the MIFARE Classic seemed to be relying (at least partially) on the secrecy of the cryptographic algorithm itself. A well-known principle in cryptography states that a cryptosystem should not rely on the secrecy of the algorithm for its security. This is known as Kerckhoffs' principle, named after the 19th century Dutch cryptographer Auguste Kerckhoffs. This reliance is known amongst the security community as "security by obscurity" and is widely derided as a flawed design principle for security systems. There a number of reasons for this. First, it is widely accepted that sooner or later the algorithm will be leaked (e.g. by "trusted" employees, sub-contractors or lost documents) or simply recovered, by reverse-engineering of the card. Indeed, by the mid-2000s there were already rumours in the industry of unauthorised MIFARE Classic type products being sourced in Asia. The date on one of the datasheets goes back to 2004 and so there is a strong suspicion that the product design was reverse engineered or otherwise disclosed for commercial gain, although the design was not put into the public domain at the time.

3.1 Weaknesses and Attacks against the MIFARE Classic

Despite being kept secret by NXP, the design, implementation and security algorithms of the MIFARE Classic were eventually publicly disclosed following the work from two groups of security researchers: first, German researchers reverse engineered the cryptographic algorithm by reconstructing the circuit in the chips and eavesdropping the communication between reader and card. Their findings were presented at the CCC conference in 2007 [9]. Independently, researchers from Radboud University in the Netherlands recovered the logical description of the cipher and communication protocol [4, 5]. The work of the two groups disclosed several weaknesses in the security of the MIFARE Classic, and gave rise to several devastating attacks.

One of the first weaknesses observed was the poor use/design of the PRNG. De-

spite the protocol making use of 32-bit nonces, the PRNG used to generate the nonces was LFSR-based with a 16-bit state, based on time of operation (thus the same nonces will be generated within relatively short, predictable intervals). Furthermore, the generating LFSR is reset to a known, constant state once the card starts operation. This means that it is relatively easy to predict and control the values of the nonces being generated by the card [4, 9, 10].

It was already well known that the CRYPTO1 algorithm made use of 48-bit keys. Due to this relatively short length, knowledge of the details of the cipher would make possible the design of dedicated hardware to brute-force the algorithm for recovering of the key. Unfortunately, the short key length is not the only problem for CRYPTO1 as it also suffers from other weaknesses. The findings from the academic research following its disclosure showed that CRYPTO1 also presented structural weaknesses, which lead to attack optimisations that are far more efficient that exhaustive key search [1, 5]

This analysis made possible a wide range of devastating attacks against the MIFARE Classic: by exploiting the weaknesses in the PRNG one can mount replay attacks in straightforward way, disclose or modify the content of memory sectors, and in some situation close cards [9, 4]. Exploiting the cryptographic flaws in the CRYPTO1 however allows one to mount key recovery attacks within a few seconds, to completely defeat the security provided by the card in several scenarios. For example, an attacker capable of eavesdropping a genuine exchange between a reader and a card can recover secret keys, and clone and trace the card with little effort [5]. Several of these attacks were demonstrated in practice.

3.2 Repercussion

The work described above received much attention of the media and security community. Smart cards, RFID tags and their security became front page news, much to the confusion and concern of the general public. Furthermore, the reverse engineering effort by the two teams did spark an ethical debate at least behind closed doors. One argument was that this was similar to breaking into NXP and stealing confidential documents. Another argument was that if research aims to find out new things then the best that the reverse engineering could do was to find out what was known to the NXP designers back in 1994. Yet another view was that the research may have revealed reverse engineering techniques, the knowledge of which could be used to design more tamper resistant devices in future. Whichever viewpoint is preferred, it is generally agreed that it is very hard to keep a design secret.

One of the major reasons that the attacks against the MIFARE Classic attracted so much attention was that a new transport ticketing scheme (*OV-Chipkaart*) was being rolled out in the Netherlands and would be making use of the MIFARE Classic [12]. This made the reverse engineering work and resulting attacks a top national and political issue. Researchers were also posting videos of exploits onto the internet and being interviewed by the press, which all served to fuel interest in the story and generate further public and political concern.

As a result of the continued pressure the Dutch Ministry of Transport, Public

Works and Water Management requested to Trans Link Systems (TLS) to carry out a technical and security assessment of the system and the researchers claims. In turn, TLS commissioned the widely respected Dutch independent research centre TNO[1] to carry out this work and produce a report [13], which critics claimed played down the serious and urgency of the situation. Such was the need for assurance that the Ministry of Transport decided to use an independent expert third party to carry out a counter expertise review of the TNO study. The selected independent expert third party was the Information Security Group Smart Card Centre (SCC) at Royal Holloway, University of London. The report from the review is in the public domain [14], and the main findings were:

- The reported security weaknesses were well founded on fact and attacks could be carried out without very specialist or hard to obtain equipment.

- That the system should work swiftly towards a state of migration readiness to move to an improved security solution.

The wide range of attacks (most of which were only demonstrated in practice after release of the reports) supported the findings in item 1. They showed how one could either interact with a legitimate reader only, eavesdrop communication between a card and reader, or interact with card only, to mount several types of attacks; these could be used to replay/relay information, modify encrypted data, recover key information to clone and/or trace cards.

Regarding the second point it is important to realise that the system is in a fragile state. Whilst this could exist indefinitely without adverse effect there is a risk that a significant event could dramatically undermine the system security measures. For example a cornerstone of the residual security of the MIFARE Classic is the unique and unchangeable ID number which should prevent the cloning of a legitimate card. Emulators of course do not have this restriction and although some "enthusiasts" will be willing to travel around with detectable emulator equipment they are thought to be few in number. This situation could change dramatically if open clone card platforms became easily available; recall that there are "unauthorised" MIFARE products on sale, although to the best knowledge of the authors, none so far with reprogrammable IDs.

Another area of concern is the use of NFC mobile phones. Whilst there is a lot of interest in the use of such phones to emulate cards for legitimate reasons there is also interest from researchers/enthusiasts to use the phone as an attack platform. The goal is that the NFC phone replays the emulator equipment that attacks require today, either emulating cards using captured credentials or interrogating legitimate cards to gather the credentials in the first place. There is potential for a software only exploit (using normal NFC phone hardware) which would widen the scope of attack to all such phone owners, simply by downloading a phone application. This is not just speculation as existing work has reprogrammed such phones to emulate both the card and the terminal in a SDA protocol transaction [2] and as a peer-to-peer relay

[1] `http://www.tno.nl`

exploit [3]. It would appear that the general purpose NFC phone relay is not too far off which would be a threat to any contactless system, not just MIFARE Classic as the attack does not need to identify keys and algorithms. Moreover, if stream cipher algorithms are deployed using non-cryptographic data integrity mechanisms (such as CRCs) instead of MACs, then NFC phone-based active attacks can also look feasible, where card data contents may be modified using an NFC phone relay and some bit-flipping relay software.

4 Conclusions

The MIFARE Classic and its security have received much attention recently. This article could be seen as describing perhaps the long-predicted demise of the MIFARE Classic. The card is a fairly old design from 1994 that soon became a successful product; although we could conclude from our discussion that the MIFARE Classic security features (in particular its short key size) were the result of a "bad" design choice, one could argue however that the product was perhaps rather never intended for high security and/or high value protection. This demonstrate the requirement of a thorough risk analysis of any system that makes use of smart cards and RFID tags, to assess whether the security provided is sufficient for the intended use (and whether there are other existent weaknesses in the system regardless of the underlying card technology and algorithms). This can be harder than one would think, particularly when considering systems aimed for long term deployments (and taking into account possible unforeseen future uses which may go beyond its original intended use). Our discussion also provides support to the idea of modular card and reader security solutions as attractive design feature, to help future-proof the system. Finally, the MIFARE Classic story provides further strong evidence that use of proprietary cryptography and "security by obscurity" are design principles that should be avoided at any cost in public systems. The cost of reverse engineering (in financial terms as well as in expertise) is ever getting lower, while the incentives for researchers to work on attacks against such systems is high enough, so we can foresee the story being repeated whenever this advice is ignored.

References

[1] N.T. Courtois, K. Nohl and S. O'Neil. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166. `http://eprint.iacr.org/2008/166`

[2] L. Francis, G. Hancke, K. Mayes and K. Markantonakis. Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. *Proceedings of The First International Workshop on RFID Security and Cryptography, (RISC 2009), in conjunction with The 4th International Conference for Internet Technology and Secure Transactions, (ICITST 2009).* pp. 1-8. London (2009)

[3] L. Francis, G. Hancke, K. Mayes and K. Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. *Proceedings of the 6th Workshop on RFID Security (RFIDSec 2010)*. Istanbul (2010)

[4] G.K. Gans, J.H. Hoepman and F.D. Garcia. A practical attack on the MIFARE Classic. *Proceedings of the 8th Smart Card Research and Advanced Application Workshop (CARDIS 2008)*. LNCS 5189, pp. 267–282. Springer, Heidelberg (2008)

[5] F.D. Garcia, G.K. Gans, R. Muijrers, P. Rossum, R. Verdult, R.W. Schreur and B. Jacobs. Dismantling MIFARE Classic. *Proceedings of ESORICS 2008*, LNCS 5283, Springer, 2008, pages 97–114.

[6] Global Platform. `http://www.globalplatform.org`

[7] ISO/IEC 9798-2 *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*. 1999.

[8] ISO/IEC 14443 *Identification cards – Contactless integrated circuit cards – Proximity cards.* 2008.

[9] K. Nohl, Starbug and H. Plötz. Mifare, little security, despite obscurity. Presentation on the 24th Congress of the Chaos Computer Club (CCC), December 2007.

[10] K. Nohl, D. Evans, Starbug and H. Plötz. Reverse-engineering a cryptographic RFID tag. USENIX Security 2008.

[11] NXP Semiconductors. `http://www.nxp.com`

[12] OV-Chipkaart System. `http://www.ov-chipkaart.nl/`

[13] TNO. Security analysis of the Dutch OV-Chipkaart. *Technical Report TNO report 34643*, TNO Information and Communication Technology, 2008.

[14] TNO. Counter Expertise Review of the TNO Security Analysis of the Dutch OV-Chipkaart. Technical report, Royal Holloway University of London, Information Security Group - Smart Card Centre, 2008.