



Mifare (In)security Update January 2008

By Dr David Everett, CEO, Smart Card Group



David Everett

Mifare: Little Security, Despite Obscurity was the title of the paper given at the 24th Congress of the Chaos Communication Congress that took place in Berlin on the 28th December 2007. Given by Karsten Nohl (University of Virginia) and Henryk Plötz but also involving Starbug from the Chaos Computer Club the presentation gave a first hand account of reverse engineering the Crypto-1 algorithm employed in the Mifare RFID chips. These chips are widely used particularly in the mass transit area such as the London transport Oyster card and the ITSO cards deployed across Scotland and as also proposed for the new Dutch National public transport smart card scheme (OV chipcard).

There have been lots of discussions over the security of the Mifare card particularly because of the extended business applications such as an ePurse being proposed for this platform. Expressions such as low security are thrown around in a way that could confuse or even misrepresent the platform. In any scheme it is the overall security that matters not the individual components. It is also fundamental to ensure that the components are used in the right way, in most high visibility failures it has been a protocol or procedure failure that has resulted in the end disaster. However memory cards such as Mifare do have restricted security functionality and when the cryptographic security relies on keeping the algorithm secret that is an additional risk that has now exploded. It should be noted that the researchers have not published their findings in detail (and may never do so) but they have publicly demonstrated not only that it is possible with limited equipment to reverse engineer the random number generator and the algorithm but also to point out many weaknesses in the actual Crypto-1 implementation.

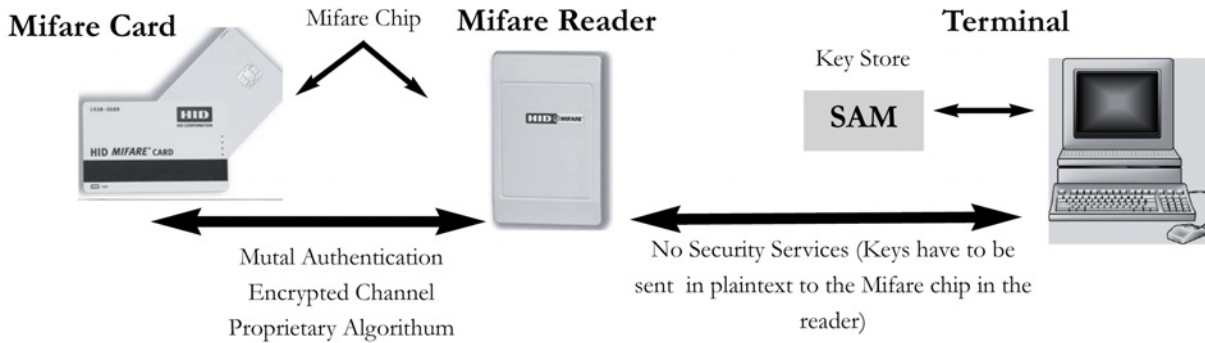
The Mifare chip technology is based on a simple contactless memory device with discrete logic to provide some security functionality across the air gap with the reader (i.e. at the radio frequency level). This technology is proprietary to Philips Semiconductors and requires their IPR to be available in both the Smart Card chip and the Mifare reader. In practice this means that both the smart card and the reader need to have a Philips (or a Mifare licensed chip, e.g. Infineon) chip embedded within them. The original Mifare 1K memory was introduced in 1994 and there are now 6 chips in the Mifare range from NXP (previously Philips Semiconductors);

- Mifare Classic (1 Kbytes of EEPROM non-volatile memory),
- Mifare 4K (4 Kbytes of EEPROM),
- Mifare DESFire (4 Kbytes of EEPROM),
- Mifare Ultralite (64 bytes of EEPROM),
- Mifare ProX (1 Kbytes or 4 Kbytes Mifare emulation in a micro controller chip. Total chip EEPROM including Mifare emulation memory is 16 Kbytes)
- Smart MX (a more advanced Mifare ProX replacement series with up to 72 Kbytes of EEPROM).

The Mifare ProX and the Smart MX are micro controller based chips and provide the Mifare functionality as an emulation in the chip. These chips are used for example by the IBM JCOP30 and JCOP40 Java Cards respectively. The discussion that follows relates to the Classic 1k Mifare but the arguments would hold for most other memory cards.

Mifare Card Operation: The Mifare 1K card has its 1 Kbyte memory arranged as 16 sectors, each with 4 blocks of 16 bytes. The last block in each sector stores two keys, A and B, which are used to access (depending on the access conditions also set in this block) the other data blocks. The Mifare reader interacts with the card as follows; 1) Select card (ISO 14443 allows multiple cards in its field), 2) Log-in to a sector (by providing key A or key B) and 3) Read, Write, Increment, or Decrement a block (must conform to the access conditions). The Increment and Decrement operations allow the block to be treated as an electronic purse.





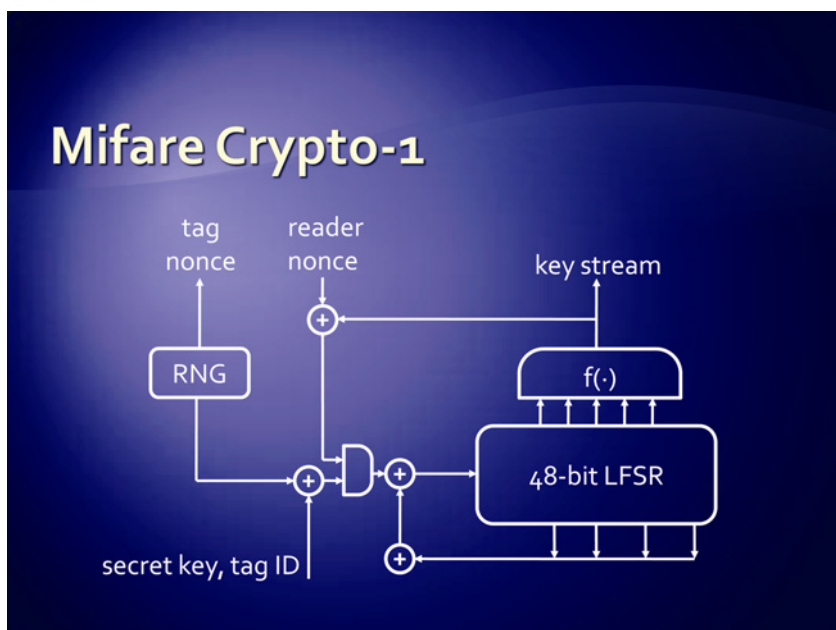
It is important to note that the cryptographic interchange takes place between the reader and the card and more precisely between the Mifare chip in the reader and the Mifare chip in the card. The terminal has to present the appropriate key to the reader and normally this key would be derived from a Master key stored in a Secure Access Module (SAM) at the terminal. The card ID and parameters, which are unique to each card, can act as the derivation factor. This means that each card is using a different key set to protect a particular sector. Breaking an individual card will not reveal the Master keys. The Login process referred to above implements a mutual authentication process (a challenge/response mechanism) which then sets up an encrypted channel between the card and the reader using Philips proprietary Crypto-1 algorithm. These security services operate at the RF (Radio Frequency) level and cannot provide any cryptographic audit trail. In essence this means that you must trust the terminal but more particularly you have no evidence if it misbehaves.

Mifare Vulnerabilities: The threats to the Mifare scheme are in three areas;

- 1) Attacker breaks the cryptographic algorithm,
- 2) Attacker implements a key exhaustion attack
- 3) Attacker obtains the cryptographic keys.

The scheme opens up an additional vulnerability in that Mifare cannot provide secure messaging. In other words because the Mifare chip doesn't have a CPU it can't cryptographically protect transactions for confidentiality, data integrity, or authentication on any form of end to end basis. This also means that message replays and deletions cannot be detected which is fundamental to most security schemes.

Strength of the Cryptographic Algorithm: The Mifare Crypto-1 algorithm is proprietary and has not been published. However the work undertaken by Karsten Nohl (University of Virginia), Starbug and Henryk Plötz in so far as they have released their results is very informative giving the block diagram below reproduced from their presentation,





In addition to this drawing they have also released further information about the RNG which is a 16 bit LFSR with characteristic polynomial,

$$X^{16} + X^{14} + X^{13} + X^{11} + 1$$

The RNG is seeded by the time delay between power on and the reception of message data from the contactless card reader. As they point out this is rather easy to control but they also noticed by intercepting messages between the card and reader that there were already repeats of the random number used as part of the authentication protocol and which is also input to the main 48 bit LFSR. This main LFSR has 16 feedback taps defined by its characteristic polynomial and apparently 20 taps are used for the key stream output function. <We can also comment that the LFSR is most likely designed for a maximum length sequence (e.g. High order X48, has an even number of taps, etc) which reduces the possibilities.>

In subsequent discussion the authors have also commented that the exclusive OR input with the secret key and tag ID is not quite as simple as shown in the slide.

When a cryptographic algorithm is widely available one suspects it is only a matter of time before it gets into the public domain either due to a malevolent employee or by a reverse engineering attack on the chip. This has happened in many other cases such as in the GSM world and the DVD protection algorithm. Public attacks on the Internet swiftly followed. It is believed that counterfeit Mifare chips are already available from China, the companies concerned would need to have reverse engineered the chip in order to produce such copies.

Key Exhaustion Attack: The design of cryptographic algorithms is normally based on the assumption that knowledge of the algorithm is assumed. In other words the algorithm itself is adequately strong and that the security depends on obtaining the secret cryptographic keys. Assuming there is no flaw in the algorithm or its implementation then the security of the scheme falls down to key exhaustion. Key exhaustion would require an emulation of the algorithm where all the keys in the key space are tested one by one using matching plain text and cipher text. Alternatively the keys in the key space can be tested one by one against a valid implementation of the algorithm (e.g. an authentic card). The first condition requires the algorithm to be known as per the above comments and for the key space to be practically realisable.

The Mifare algorithm uses a 48 bit key, this gives a total key space of 2^{48} or approximately 3 with fourteen noughts. With today's processing power this would not be deemed adequate by experts in the field. The single DES algorithm with its 56 bit key has long since been dismissed (it has been practically exhausted in 10 hours) in favour of triple DES with an effective key length of 112 bits (in practice it can be attacked with slightly less effort but still insurmountable). Today anything much less than a 96 bit key would not be deemed secure against such an exhaustion attack. An alternative approach would be to take a valid card and literally try each key in turn from the key space. This would require a card select followed by a login process. Just assuming this could be done in say 10 mS then an attack would take, $2^{48} \times 10 \text{ mS} = 89194$ years. This attack is clearly not viable.

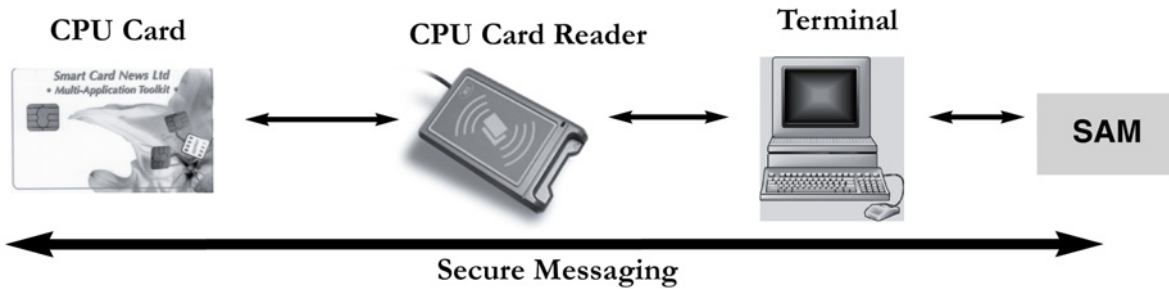
Key Vulnerability: The vulnerability of the keys arise from these considerations; 1) An exposure in key management (including the terminal and reader) and 2) An exposure to an attack on the card. As mentioned previously because the keys have to be transmitted to the reader there is an assumption that the terminal can be trusted. This may be reasonable in some closed schemes such as a mass transit application but in the more general case this would not be an acceptable assumption. Apart from the obvious invasive attacks on the chip, we have in recent years, seen very successful attacks on Smart Cards by intercepting the power consumed by the chip whilst undertaking cryptographic operations. Called Differential Power Analysis (DPA) by their inventor Paul Kocher these techniques were originally applied against the RSA secret keys but later used against symmetric algorithms such as DES. Such forms of attacks may well be applicable to the Philips Mifare algorithm.

Secure Messaging: In a transaction-based scheme it is standard practice to protect the messages with some Cryptographic Check Value (CCV) or digital signature. This ensures the authenticity of the source of the message and that the message has been unchanged in transit from source to destination. This requires that the Smart Card is able to both create and check such CCVs or digital signatures. Without such security services being applied it is not easy to resolve disputes and the scheme is vulnerable to a wide range of





attacks. The Mifare card because it hasn't got a CPU is not capable of creating or checking such cryptographic messages. Consider the operation of a CPU Card as shown.



Both the card and SAM can encipher messages or create and check cryptographic checksums as necessary and appropriate

In this case the transactions operate between the SAM (Secure Access Module) and the card. Cryptographic protection operates between these end points. Consider for example the case where you want to increment the value of a purse stored on the card. The card is set up so that the command to increment the purse has a CCV attached, the chip checks this CCV before it effects the value load process. This cryptographic CCV is created by the Secure Access Module (SAM) attached to the terminal. Nowhere in this scenario are the cryptographic keys available in plain text. Even if the terminal is attacked with some Trojan software, the transaction records can be subsequently checked for authenticity. It is not possible for the Trojan operation to fool this process. In addition sequencing controls can be incorporated in the messages which are checked by the CPU to stop replays.

User Authentication: The Mifare card has no facility for checking user PINs or passwords. This means that you cannot adequately bind a user to the card which is necessary in any form of Identity management scenario.

Summary: Memory cards with discrete security logic such as Mifare can offer adequate security for some closed business scenarios. In the more open transaction model the increased security functionality offered by a CPU chip with cryptographic capability is highly desirable. In the light of the latest public attack on the Crypto-1 algorithm system integrators would be advised to upgrade to a more resilient algorithm. The NXP DESFire memory RFID product for example uses Triple DES but we see little advantage in a memory only device given the small overhead of a CPU micro-controller.



LEGIC embeds badge and purse into NFC mobile phones

Mobile telephony is already something we can't imagine being without. New NFC (Near Field Communication) technology will revolutionise our daily transactions further still and make many deeds even easier. Buying a bus ticket, paying at a machine or kiosk, opening a door or accessing information services: in the future, the mobile telephone will be able to do all.

NFC pilot project with and at Swisscom

LEGIC, Swisscom and Selecta are pursuing new paths with this NFC pilot project. In the Swisscom's modern buildings in Bern, Switzerland, Swisscom staff use their mobile phones to get chilled drinks and snacks from Selecta vending machines. The ability to connect a mobile phone to contactless applications, such as to make cashless payments using electronic purses, is opening up endless possibilities thanks to LEGIC's new card-in-card solutions. For a long time these two worlds, with their different technologies, were not compatible. Buying drinks using an electronic purse was only possible with the contactless staff badge, while the mobile phone was used for standard communication purposes.

