MIFARE Classic is a contactless smartcard technology owned by NXP Semiconductors. More than 1 billion cards and one million readers have been sold. Without a doubt this is the contactless smartcard technology with the highest market share. In fact, MIFARE Classic dominates the smartcard market for public transportation ticketing systems in cities around the world. Taipei’s MRT uses Easycards featuring MIFARE Classic as do the ticketing systems for metropolitan mass transportation systems in these countries: Argentina, Brazil, Australia, Canada, China, Denmark, Germany, India, Ireland, Korea, Sweden, Turkey, UK, and the U.S.

MIFARE Classic cards run on miniscule amount of energy that its wire loop collects from a quickly varying electromagnetic field. Aside from a small amount of control circuitry, it is basically a memory stick with flash memory divided into several sectors, each with four blocks. In the standard MIFARE Classic each block is 16 bytes. The MIFARE Classic uses NXP’s proprietary CRYPTO1 cryptosystem for access control. Before any sector is read, the card and reader carry out an authentication protocol to assure that they have the same keys.

NXP kept CRYPTO1 under wraps as a trade secret in an effort to keep MIFARE Classic safe, but this is doomed to fail nowadays, due to the free flow of information. Shanghai Fudan Electronics was reportedly able to build clone cards compatible with official MIFARE Classic readers as early as 2004. This can only mean that the secret has already leaked. More rumors circulated in 2006 that academics finally had reverse-engineered CRYPTO1, which at the end of the following year was confirmed at Chaos Communication Congress 2007 by Nohl and Pi’otz, two engineers hailing from Germany, who publicized their results at USENIX security Symposium 2008. Finally, in 2008 another team from Raboud Universiteit Nijmegen publicized their onset on MIFARE Classic. Actually NXP had sought to prevent this via legal means, but their case was thrown out of court on Freedom of Expression grounds.

MIFARE Classic has been a huge commercial success. It is cheap, convenient and sturdy, enabling it to penetrate many public transportation ticketing systems in less than a decade. However, as a cryptographic project it is sadly deficient, which means that it cannot assure the basic security. We will briefly summarize some of the design errors in its cryptosystems and protocols. MIFARE Classic cards communicate with readers in three different stages: anti-collision, certification, and storage operations (read/write). The anti-collision conforms to the ISO-14443 standard and marks the beginning of a session. A reader can then triggers the certification mechanism which establishes a session key for the encryption of all ensuing communications, including all reads and writes and authentication to other datasectors during this session.

As mentioned above, MIFARE Classic embraces a proprietary cryptosystem called CRYPTO1. This is a stream cipher, enabling you to generate from any key a pseudorandom stream of bits (“keystream”), which is XORed to the message bits to form the ciphertext bits. If a stream cipher is good enough, then one cannot distinguish the pseudorandom bitstream from a really random one and security is guaranteed by Shannon’s theorem on OTPs (One-Time Pads). However, for a stream cipher to be good enough, it requires that an attacker have many keystream bits along with enormous computational power. This is because attackers often know or could guess with high probability certain parts of the message, and
hence could obtain the corresponding keystream bits. This is called a "Known Plaintext Attack" and happens, for example, when a card transmits a known control character encrypted as a response of a protocol. Unfortunately, MIFARE Classic is not good enough, and we list below some reasons:

- CRYPTO1 uses a short — 48-bit — secret key, making it easy to be searched with modern computing power. NXP made other mistakes but this is clearly the worst one. If one could eavesdrop on an authentication session or have access to cheap and off-the-shelf commercial radio equipment, one can break CRYPTO1. Our group did so using only 16 nVidia graphics cards (from two generations ago, and they are standard—not specialty cards) in 14 hours. This attack also applies to MIFARE Classic Plus, used in 2nd generation MRT Easycards.

- The MIFARE Classic protocol uses parity check bits, which is fine — except when you first compute the parity bit and then transmit it along with the message byte. Clearly this leaks information. What is worse is that this parity check bit is encrypted with the same bit of keystream that is used for the first bit of the next byte, leading to leakage of extra information. A rough estimate is that this problem leaks about 1/8 of the bits in a key.

- In first-edition MIFARE Classic cards, the random number generator used for the nonce ("number used just once") has only 216 = 65536 outputs. This makes it ridiculously easy to go over all possibilities, and one can even make timely attack so as to repeat a nonce, making brute-force attacks much easier.

- When an authentication phase is not complete, theoretically a card should always give the same response, some equivalent to "I do not understand." However, MIFARE Classic fails to do so, and different responses to failure give an attacker even more ways to garner side channel information.

The only saving grace among all these problems is that none of them leaks the master signing key of the vendor (i.e., Taipei's Easycard company). However, an eavesdropped session let an attacker (through attacking CRYPTO1) read and modify all data on a MIFARE Classic card, making it the equivalent of an unprotected USB drive on a network as far as security is concerned. The MIFARE Classic Plus did patch the latter 3 holes, but compatibility means that the short key length has to be retained. Therefore as mentioned above, brute-force attacks still works fine against the 2nd generation Easycards.

In summary, making micropayments with Easycards does make life easier, but the security of MIFARE Classic as part of the supporting infrastructure should be carefully scrutinized. Of course MIFARE Classic makes up but one small—and terminal—piece of the puzzle, but lower security means that forgery and leakage of personal information raises the hidden cost of using this technology. In particular, catering to legacy cards means that to sustain the system the users would lose out in terms of privacy. The corporations dealing with MIFARE Classic cards such as Taipei's Easycard must be carefully monitored and held accountable, and not allowed to transfer the cost to the society as a whole. Only when such contactless smart cards are made secure can authenticating and micropayments based on such cards be popularized safely, resulting in the greater good.