Card Details

- NXP MIFARE Classic® 1k
- ISO/IEC 14443 - 3(NFC-A)
- Total memory: 1kb
- Blank, white, printable with a Card Printer
- Write endurance (typical cycles): 200,000
- Data Retention: up to 10 years
- 4-byte UID
- CRYPTO1 cryptography supported

The MIFARE Classic 1K card can be configured as either read-only or read/write. A read-only MIFARE Classic 1K card contains information that cannot be changed or updated. This type of card is commonly used for applications such as ticketing or identification, where the information stored on the card is fixed and does not need to be updated. It contains 1 kilobyte of memory and is organized into 16 sectors, each containing 4 blocks of data. Each block can store up to 16 bytes of data, and can be either read-only or read/write.

Mifare Classic 1K contains variety of data

- User information: This can include details about the cardholder, such as their name, address, and contact information.
- Access control information: This can include data about the areas or facilities that the cardholder is authorized to access, such as a door or turnstile.
- Payment information: This can include details about the cardholder's account balance or transaction history for a payment system.
- Ticketing information: This can include details about the cardholder's ticket or travel information, such as the destination or fare amount.
- Security keys: MIFARE Classic 1K cards use a proprietary encryption algorithm to secure the data stored on the card. The card can contain various security keys that are used to authenticate the card and protect the data from unauthorized access

Protocol used is CRYPTO1

CRYPTO1 is a proprietary encryption algorithm used in the MIFARE Classic 1K smart card. It is a stream cipher that operates on 48-bit keys and is used to protect the communication between the card and the reader.

The CRYPTO1 algorithm works by generating a pseudorandom bitstream that is XORed with the plaintext data to produce the ciphertext. The key used to generate the pseudorandom bitstream is derived from the key that is stored on the card and the unique serial number of the card. This makes it difficult for an attacker to intercept and decode the communication between the card and the reader, as they would need to know the key and serial number in order to decrypt the data.[16]

However, the CRYPTO1 algorithm has been found to have weaknesses that make it vulnerable to certain types of attacks. In particular, it has been shown that the key can be easily recovered through a process known as a "nested attack," which involves performing a series of authentication attempts and analyzing the responses from the card.[15] As a result, the security of the MIFARE Classic 1K card has been called into question, and it is generally not recommended for use in high-security applications.

There are several smart card technologies that are considered more secure than MIFARE Classic 1K, such as MIFARE Plus, DESFire, HID iCLASS SE, and FeliCa. These cards use stronger encryption algorithms, support mutual authentication, and offer additional security features to protect against attacks. The choice of card will depend on the specific application and security requirements of the system.

Vulnerabilities in MIFARE classic 1k

The MIFARE Classic 1K card has several known security vulnerabilities, which can be exploited by attackers to access or manipulate the data on the card. Here are some examples of these vulnerabilities and how they can be exploited:

- Weak encryption: The MIFARE Classic 1K card uses a proprietary encryption algorithm called Crypto-1, which has been shown to be vulnerable to certain types of attacks. For example, an attacker could use a specialized RFID reader to

intercept the communication between the card and the reader and recover the encryption keys used to protect the data on the card.

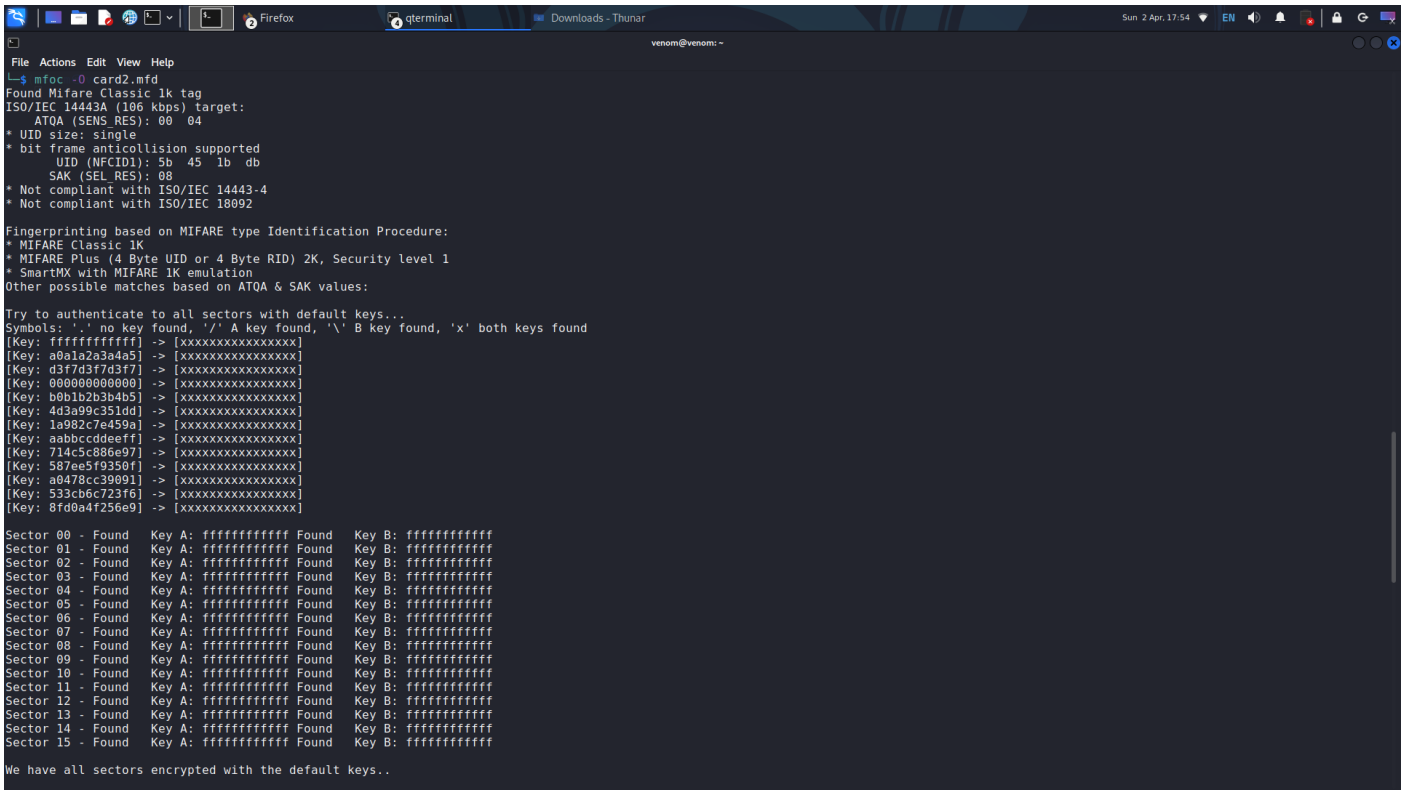
- Card cloning: Because the MIFARE Classic 1K card has weak encryption, it is possible for an attacker to create a cloned card that contains the same data as the original card. This can be done using a specialized RFID reader/writer that can copy the data from the original card onto a blank card which needs to be a T5577 card.
- Data manipulation: An attacker who has access to a cloned or genuine MIFARE Classic 1K card can also manipulate the data stored on the card. For example, an attacker could change the access control information on the card to gain unauthorized access to a building or facility.
- Brute-force attacks: The MIFARE Classic 1K card has a limited number of keys that can be used to access the data on the card. An attacker could use a brute-force attack to try all possible combinations of keys until the correct one is found.

Nested attack using MFOC

Nested attack is a technique used by MFOC for key cracking of MIFARE classic cards. Using MFOC for a nested attack involves trying out a set of default keys that are hard-coded on the card for authentication. Should there be no luck with the default keys, MFOC moves on to the next phase where it can perform a dictionary attack.

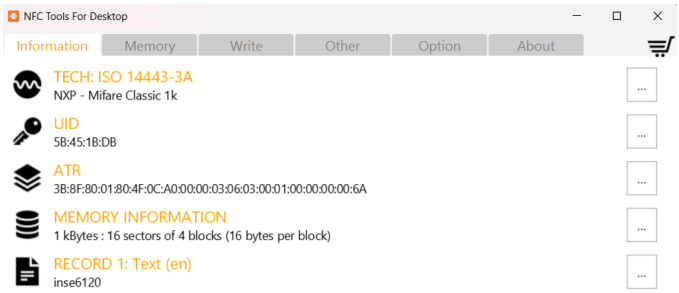
MFOC utilizes a nested approach in a dictionary attack by testing multiple keys (usually drawn from a pre-computed key space or a custom dictionary file) until the correct key is found. Rather than attempting all keys simultaneously, MFOC conducts authentication attempts, with each subsequent attempt using the result of the prior attempt as input. This approach reduces the number of authentication efforts necessary to crack the keys, accelerating and streamlining the attack process.

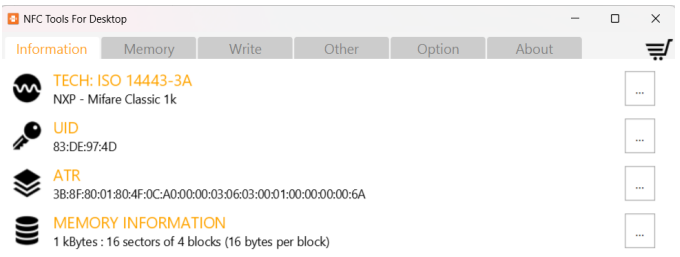
To increase the likelihood of success and hasten the attack, MFOC utilizes incremental keys search and partial matching, in addition to other techniques. Once the correct key is found, MFOC can read or write data to the card, allowing unauthorized access to the information on the card.

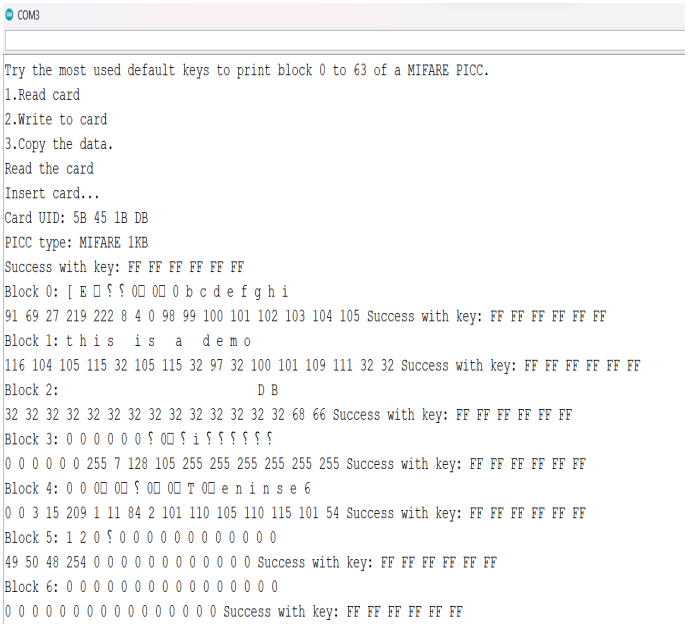


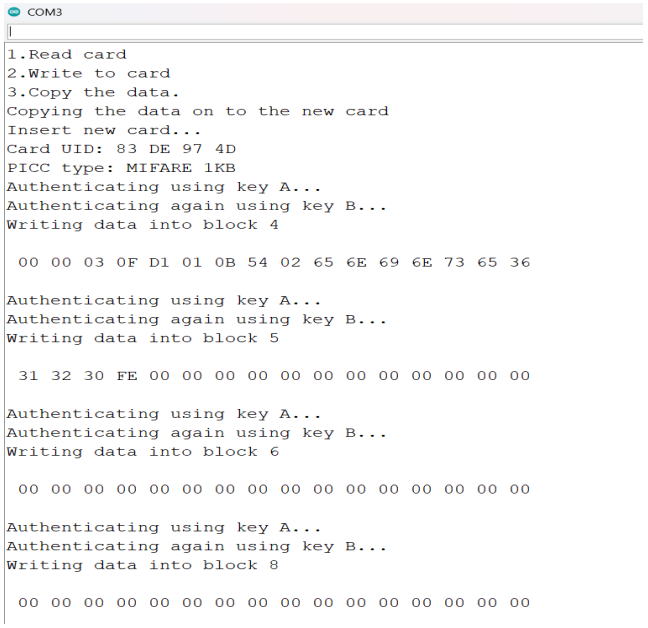
RFID card data duplication using RC522 and Arduino uno R3

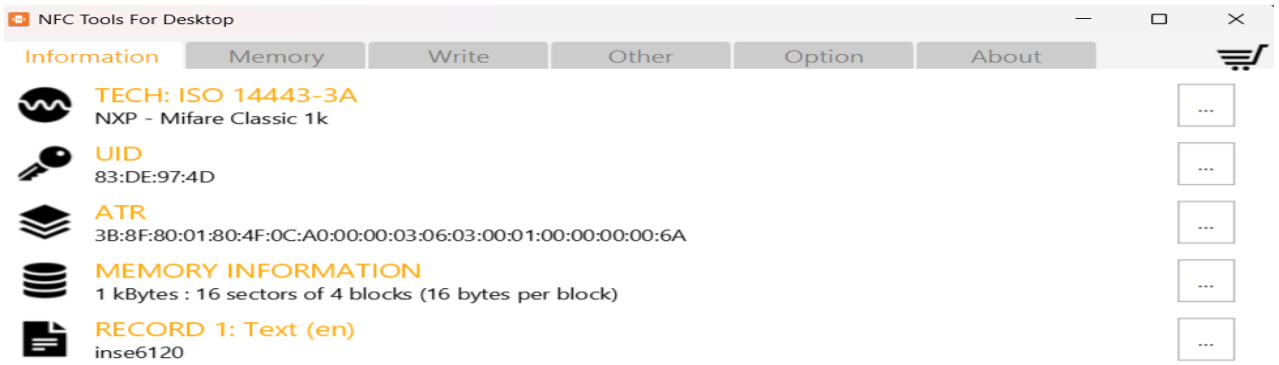
We have used Arduino Uno R3 and RC522 modules to read and clone data from one card to another. The RC522 module is a common RFID reader module that is designed to work with Arduino microcontrollers. It communicates with the microcontroller via SPI (Serial Peripheral Interface) and is capable of reading data from Mifare Classic RFID cards.











References:

1. Azhari, F. (2014), "Quick detection of NFC vulnerability: Implementation weakness exploitation", Information Management & Computer Security, Vol. 22 No. 2, pp. 134-140. https://doi.org/10.1108/IMCS-09-2013-0067
2. “MF1S50YYX_V1 MIFARE Classic EV1 1K -Mainstream contactless smart card IC for fast and easy solution development,” 2018. Available: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf
3. F. D. Garcia, P. van Rossum, R. Verdult and R. W. Schreur, "Wirelessly Pickpocketing a Mifare Classic Card," 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2009, pp. 3-15, doi: 10.1109/SP.2009.6.
4. Golić, J.D. (2013). Cryptanalytic Attacks on MIFARE Classic Protocol. In: Dawson, E. (eds) Topics in Cryptology – CT-RSA 2013. CT-RSA 2013. Lecture Notes in Computer Science, vol 7779. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36095-4_16

Vanshika

[1]A. Alrawais, “Security Issues in Near Field Communications (NFC),” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020, doi: https://doi.org/10.14569/ijacsa.2020.0111176.

[2]T. Kim, Tae Hyun Kim, and S. Hong, “Breaking Korea Tansit Card with Side-Channel Analysis Attack-Unauthorized recharging -,” *https://www.blackhat.com/docs/asia-17/materials/asia-17-Kim-Breaking-Korea-Transit-Card-With-Side-Channel-Attack-Unauthorized-Recharging-wp.pdf*, 2017. https://www.semanticscholar.org/paper/Breaking-Korea-Tansit-Card-with-Side-Channel-Kim-Kim/a3537e75e46a82bcfe222edd0a3ec9b0f0758ab0 (accessed Apr. 03, 2023).

[3]Y. C. Lee, “Smart-card-loss-attack and Improvement of Hsiang et al.’s Authentication Scheme,” *Journal of Applied Research and Technology*, vol. 11, no. 4, pp. 597–603, Aug. 2013, doi: https://doi.org/10.1016/s1665-6423(13)71567-0.

[4]Z. Zorz, “Vulnerabilities in smart card drivers open systems to attackers,” *Help Net Security*, Aug. 13, 2018. https://www.helpnetsecurity.com/2018/08/13/vulnerabilities-smart-card-drivers/#:~:text=Most%20of%20the%20vulnerabilities%20he (accessed Apr. 03, 2023).

[5]J. Markoff, “Vulnerability Is Discovered In Security for Smart Cards,” *The New York Times*, May 13, 2002. Accessed: Apr. 03, 2023. [Online]. Available: https://www.nytimes.com/2002/05/13/business/vulnerability-is-discovered-in-security-for-smart-cards.html

[6]“NFC Tutorial | Tutorial on NFC Protocol | How NFC works,” *www.rfwireless-world.com*. https://www.rfwireless-world.com/Tutorials/NFC-Near-Field-Communication-tutorial.html

[7]L. Sportiello, “‘Internet of Smart Cards’: A pocket attacks scenario,” *International Journal of Critical Infrastructure Protection*, vol. 26, p. 100302, Sep. 2019, doi: https://doi.org/10.1016/j.ijcip.2019.05.005.

[8]
“Smart cards: security risks | Computer Weekly,” *ComputerWeekly.com*. https://www.computerweekly.com/ehandbook/Smart-cards-security-risks (accessed Apr. 03, 2023).

[9]“What is NFC?,” *STMicroelectronics*, 2023. https://www.st.com/content/st_com/en/support/learning/essentials-and-insights/connectivity/nfc.html#:~:text=What%20is%20NFC%3F- (accessed Apr. 03, 2023).

[10]“A method for resynchronizing a random clock on smart cards ... Didier Moyart -Régis Bevan Oberthur Card Systems.” Accessed: Apr. 03, 2023. [Online]. Available: https://www.nmda.or.jp/nmda/ic-card/proceedings/30-1440-DMoyart.pdf

[11]H. Handschuh and H. M. Heys, “A Timing Attack on RC5,” *Selected Areas in Cryptography*, pp. 306–318, 1999, doi: https://doi.org/10.1007/3-540-48892-8_24.

[12]“Low Cost Attacks on Tamper Resistant Devices,” *www.break-ic.com*. https://www.break-ic.com/topics/attack-microcontroller.asp (accessed Apr. 03, 2023).