Categories

Tips (33)

Tag Clone (9)

MTools (4)

Logs (1)

Testing Report (1)

Proxmark3 (6)

iCopy-X (5)

PN532 (2)

Videos (4)

Tags

ACR122U ChameleonTiny Clone ICode iCopy-X ISO15693 macOS Mi Band NFC mtools PCR532 PM3 PN532 Proxmark3 RFID Tools tips

Archives

May 2023

March 2023

February 2023

January 2023

December 2022

November 2022

October 2022

August 2022

TIPS

What's the Difference between 3 Generations of Mifare Magic Card

There are 3 generations of UID Changeable Mifare Classic 1K/4K cards on the market. To those who are new to RFID magic cards, here's the complete summary of those cards in 2023.

Gen1

PROTOCOL	UID LENGTH	SIZE	MECHANISM	ANDROID NFC	PN532 / ACR122U	PROXMARK3 / ICOPY-X
Mifare S50	4 Byte	1kb 16 sectors 64 blocks	Backdoor Command	Not Support UID Changing	Support UID changing	Support UID changing

The gen1 magic card is also named UID Card, which has the backdoor command to unlock the card and change the UID under the Mifare Classic 1K S50 protocol. It has 16 sectors, each sector has 4 blocks. With the ability of the backdoor command, anyone can use the external reader to write any data to every block, from block 0 to block 63. You can read any blocks or change the keys of the trailing block easily and no need for authentication. Even if you write an invalid BCC of UID or wrong ATQA value, it can be done, but never be read by any readers after that.

Advantages of Gen1

- Super fast to change the UID

- Recoverable after invalid data written

- Cost-effective for Mifare S50 cloning

Disadvantages of Gen1a

- Backdoor detective – Some access systems may not allow this magic card to pass because of it can be identified with its built-in controller.

Branches of Gen1

Alias	Backdoor	Features
UID Card	Detectable	Never dead
FUID Card	Undetectable	Onetime UID written
UFUID Card	Detectable After locked – undetectable	Lock UID permanently

Gen2

Protocol	UID Length	Size	Mechanism	Android NFC	PN532 / ACR122U	Proxmark3 / iCopy-X
Mifare S50	4 Byte	1kb 16 sectors 64 blocks	Keys authentication	Support UID Changing	Support UID changing	Support UID changing

The 2nd generation of the Chinese Magic Card is also named **CUID Card**. The mechanism to change the UID is to authenticate sector 0 with keys and change the whole block data of block 0, which much include the bytes of UID, BCC, ATQA, SAK, and Manufacturer Information.

If you have got the dump file of Mifare Classic 1K, you can easily write it to the CUID card with Mfiare Classic Tool built-in function or MTools App to change the UID can whole data. This can also be done with a PN532-based or Proxmark3-based Reader, it needs authentication like the common Mifare Classic Cards.

Advantages of Gen2 Magic Card

- Easy to change UID on the Android Phone

- Cover most access systems, no backdoor.

Disadvantages of Gen2 Magic Card

- Cause dead sector if written with invalid access control byte.

- Unfixable if written with invalid block 0.

Gen3

Protocol	UID Length	Size	Mechanism	Android NFC	PN532 / ACR122U	Proxmark3 / iCopy-X
Mifare S50	4 Byte / 7 Byte	1kb 16 sectors 64 blocks	Backdoor Command	Not Support UID Changing	Support UID changing	Support UID changing
Mifare S70	4 Byte / 7 Byte	4kb 40 sectors Sectors 0-31: 4 blocks per sector Sectors 32-39: 16 blocks per sector	Backdoor Command	Not Support UID Changing	Support UID changing	Support UID changing

The 3rd generation of Magic cards brings 4 Bytes and 7 Bytes UIDs on both S50 and S70 protocols. It is another type of backdoor command than the gen1 type. To change the UID of the gen3 magic card, before 2023, you have to use a Proxmark3-based reader, such as Proxmark3 X or iCopy-XS reader. And now you can also use the PN532 BLE reader with MTools Lite app with the built-in terminal functions for free.

To add Bluetooth support to the PN532 module, you can choose All-in-one PN532 or PCR532 reader in the MTools Tec store. Or DIY the PN532 module with the BLE module.

Advantages of Gen3 Magic Card

- More protocols support

- New Mechanism to change the UID

- UID can be locked permanently

Disadvantages of Gen3 Magic Card

- Locked UID cannot be unlocked

Other types of Magic Cards

UFUID Card

It can be considered as the gen1 magic card with a lock. If the lock is unlocked, it can respond to the gen1 backdoor command, just like the gen1 magic card. If it's locked, it's just a common Mifare classic 1k card. And it cannot be unlocked again.

External Readers for Magic Cards

- PN532

- All-in-one PN532 – Official PN532 BLE Reader

- PCR532 – A small PN532-based reader with USB-C and Bluetooth

- ACR122U – An 16-year-old RFID reader till 2023. Only has USB connections.

- Proxmark3 X – A Bluetooth version of Proxmark3 and independence ID copy mode.

- iCopy-XS – The most powerful handheld RFID reader with a screen.

Programs for External Readers

	Android	iOS	Windows	Linux
PN532	RFID Tools MTools MTools Lite	MTools Lite	Mifare One Tool	libnfc
ACR122U	RFID Tools MTools	–	PCSC Mifare Program	libnfc
Proxmark3 iCopy-X	RFID Tools MTools	–	PM3 GUI	proxmark3

This entry was posted in Tips. Bookmark the permalink.

< New Features added to MTools Lite App

ONE THOUGHT ON "WHAT'S THE DIFFERENCE BETWEEN 3 GENERATIONS OF MIFARE MAGIC CARD"

Jasper F. says:

I had no idea there were so many differences between the different generations of Mifare Magic cards. Thank you for providing all this useful information!

JUNE 3, 2023 AT 12:00 AM   REPLY

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

☐ I am human

hCaptcha
Privacy - Terms

POST COMMENT

Information

> About Us

> Contact Us

> Shipping

> Returns

> FAQ

Account

🔍 Track My Order

👤 My Orders

✔ My License Key

⚲ Log Out

Newsletter

Subscribe the new launches.

Your Email

Subscribe

Privacy   Terms