RFID Workshop Challenge Bundle

by Vanhoecke Vinnie

Date: 2024-08-10

1. Table of content

1. Table of content 2
2. Introduction 3
3. Challenges 4
   3.1. Workshop RFID Cards 4

Challenge #0: Identify 5
Challenge #1: HID Clone 7
Challenge #2: Basic Flag 8
Challenge #3: Username 10
Challenge #4: Access Bits 12
Challenge #5: Key Recovery 13
Challenge #6: Nested Attack 14
Challenge #7: Hardnested Attack 16
Challenge #8: Darkside Attack 17
Challenge #9: Vault 18
Challenge #10: Employee Card 19
Challenge #11: Vending Machine 20
Challenge #12: Hotel Rooms 21
Challenge #13: Speedrun challenge 22

2. Introduction

Welcome to the Challenge bundle of the Playing with RFID workshop. This document describes the challenges that need to be performed during the workshop. Please refer to the Solution bundle in case you want to peek into walkthroughs on how to solve each challenge but use it wisely, avoid just copying commands from the solutions bundle since it can be counterproductive. In case something is not clear you can always ask the workshop instructor.

3. Challenges

3.1. Workshop RFID Cards

You have received three RFID cards:

- Card A: Spencer (Mifare Classic 1K)
- Card B: Harper (Mifare Classic 1K)
- Card C: Banker card (T5577)

Below more information about the data on the card

Card A: Spencer (Mifare Classic 1K)

Each sector on the Mifare card will represent a challenge. Keep in mind that sector numbering start at 0.

- Sector 0
  Challenge 9: Vault
- Sector 1
  Challenge 2: Basic Flag
- Sector 2
  Challenge 3: Username
- Sector 3
  Challenge 4: Access Bits
- Sector 4
  Challenge 5: Key Recovery
- Sector 5
  Challenge 6: Nested
- Sector 6
  Challenge 8: Hardnested attack
- Sector 7
  Challenge 7: Darkside attack
- Sector 8
  Challenge 10: Employee Card
- Sector 10
  Challenge 12: Vending Machine
- Sector 11
  Challenge 13: Hotel Rooms

Card B: Harper (Mifare Classic 1K)

Card C: Banker card (T5577)

Currently, the card will only be used for Challenge number, where an HID card needs to be cloned, using a Card C which is a T7755 card that can be configured with any particular ID.

Challenge #0: Identify

Difficulty:	Easy
Goal:	Identifying the protocols and frequencies used by the challenge RFID cards and testing if your tools are setup correctly and working.
Requirements:	Proxmark and Flipper can identify all cards, with ACR122U you can only identify high frequency cards.
Workshop Cards	All workshop cards can be used for this challenge

Description

When assessing and testing RFID systems, the first thing you do is identify what RFID protocol the card operates on. Usually this requires a low and high frequency antenna to identify all types of RFID protocols.

Proxmark

Make sure you have the Proxmark client running, and you flashed the same version as the client you are using. Run the Proxmark CLI on your laptop by executing the **./pm3** file in your local Proxmark source code folder.

For high frequency cards you can use the command called **hf search**:

```
[usb] pm3 --> hf search
```

For low frequency cards you can use the command called **lf search**:

```
[usb] pm3 --> lf search
```

Flipper Zero

Flipper Zero can both read LF and HF cards.
Use the NFC module on your flipper to detect high frequency cards:

Use the 125 kHz RFID Module for low frequency cards:

ACR122U

The ACR122U is an NFC compliant device and has a high frequency antenna ($13{,}56_{Mhz}$) this makes it possible to identify all kinds of RFID protocols included in the NFC bundle with the ACR122U. In order to use the CRID tool to identify cards with the ACR122U, you can issue the following command:

```
crid --identify
```

Keep in mind that not all cards can be identified with this reader, the card that can't be identified will only be used for one challenge. so it does not impact your experience much. The instructor also has some simple LF readers for that challenge.

Bonus:
Test any other cards in your wallet or you brought to the workshop to detect its protocol.

References

Proxmark Command Cheat Sheet	https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/cheatsheet.md

Challenge #1: HID Clone

Difficulty:	Easy
Goal:	Understand how HID RFID Cards can be cloned
Requirements:	Proxmark, Flipper Zero or other LF RFID device
Workshop Cards	Card C

Description

Can you gain access to the bank by cloning the Badge of the bank employee? The badge you will need to clone will be available at the OctoBox within the workshop.

Proxmark

When running the Proxmark CLI you can initiate the lf hid reader command to get the data stored on the card. Run this command on the card you would want to clone.

To create a copy on Card C, you can use the command called lf hid clone, where the -r parameter, review the help menu to understand which parameter you would not to provide to clone the data of the card on Card C in the correct format.

Flipper Zero

In the previous exercise we made use of the 125 kHz RFID Module for low frequency cards, use the more options after you scanned the card to clone the card to your Card C.

ACR122U

Unfortunately, this challenge is not possible on the ACR122U since it's only operating on NFC compliant RFID protocols.

Tips

Proxmark	Make use of the lf hid commands
Flipper Zero	Make use of the 125 kHz RFID module.
ACR122u	Not possible with this device.

Challenge #2: Basic Flag

Difficulty:	Easy
Goal:	Learn how to read data from a Mifare Classic Card
Requirements:	Any HF RFID reader and required drivers/software client Both Mifare Classic Cards
Challenge Points	25 points

Card A or B	Sector 1

Description

Now that we've determined which card uses which protocol, this challenge will introduce how to read data from a Mifare Classic Card. During this challenge you can use any of the Mifare Classic Cards.

The goal is to read the flag present in sector 1 on both Mifare Classic Cards, this sector will contain some binary data representing ASCII Text that represent the flag. Once you obtained the flag, you can enter the flag in the scoreboard. For this challenge the access keys will be provided for sector 1 will be provided:

Access Key A: FFFFFFFFFFFF
Access Key B: 111111111111

Proxmark

Reading Mifare Classic card with the Proxmark can be done using the hf mf commands, in particular the **hf mf rdsc** can be used to read one of the sixteen sectors of a Mifare Classic card. To explore all Mifare commands implemented in the Proxmark, please use **hf mf** command to list all subcommands for Mifare Classic.

The command **hf mf rdbl** can be used to read one block from the Mifare Classic Card. Please make use of the help menu to understand how the Proxmark requires you to specify any arguments to the command, such as which block and keys.

Important to note that normally you need specify either Key A or Key B to read data from to a Mifare Classic card. But for this challenge, you can omit the keys from your command and let Proxmark use the default FF FF FF FF FF FF key.

Flipper Zero

Flipper Zero has an option within the NFC module to read a card, this command can take some time since it's also trying to brute force and find any other keys on the card. (Explained later in the workshop). You could cancel the read action since the data for this Sector will be retrieved at the start since its using the default key and its mostly spending time on the other sectors where no default keys are configured.

ACR122U

Use the --read_sector or --read_block command within the CRID tool to initiate a read on the Mifare Classic Card. The help menu can show how to provide the options for the read operation, take note of the keys and data format flags.

References

Proxmark3	Use the Proxmark3 CLI to find which hf mf command you need to use.
ACR122U (CRID)	use the crid tool with read_sector

Data Conversion	Use CyberChef (https://cyberchef.org/) to convert from Hex to ASCII.

Challenge #3: Username

Difficulty:	Easy
Goal:	Learn how to write data to a Mifare Classic Card
Requirements:	Any HF RFID reader/writer and required drivers/software client Both Mifare Classic Cards
Challenge Points	75 points

Card A or B	Sector 2	Block 8

Description

This challenge will introduce you to writing data to a Mifare Classic Card and will be the first challenge you will be able to perform on the OctoBox.

The goal is to write your username in the first block of sector 2 (Block 8) on both Mifare Classic Cards. This means that the username can only be 16 bytes or 16 characters long, if your username is shorter than 16 characters, please append null bytes (Hex: 00). An example for the username Spencer (Please use a different name):

Convert the username from text to hexadecimal using CyberChef or any other tool of your liking:

https://cyberchef.org/#recipe=To_Hex('None',0)&input=U3BlbmNlcg

This would give you the following result in hexadecimal. if not familiar with hexadecimal, each character is converted here to two characters (0-9,a,b,c,d,e,f)

```
5370656e636572
```

Since you would need to specify the full block during the commands for writing you would need to append leading zeros until the full data contains 32 characters in hexadecimal. 14 characters are giving for the username Spencer in hex here, thus we would need to append 18 leading zeros (32 minus 14 equals 18) resulting in the following data for that block:

```
5370656e63657200000000000000000000
```

For this challenge the access keys will be provided:

Access Key A: FFFFFFFFFFFF
Access Key B: FFFFFFFFFFFF

Use your RFID device to write a username to your card and scan it at OctoBox to register for the scoreboard.

! Keep the username within that sector on both cards to make sure you get points in the scoreboard for the next challenges.

Proxmark

Similar on how the read commands work from the previous challenge, you might have noticed that the hf mf commands also contain the **hf mf wrbl** command, which will be the command you can use here. Any flags you need to specify with this command are for you to explore, but keep in mind to target sector 2 and block 8 particularly.

Flipper Zero

Small disclaimer, the blocks for the Flipper Zero start counting from 0 instead of 1 so for all exercises, please lower the block number within the challenge description by one.

Flipper Zero can read and modify card data in a few different ways, you can install the Mifare Classic Editor to change data, or create a dump of the Mifare Classic file when using the read function in NFC module,

store the export and then edit the data within the mobile application of the Flipper or either by downloading the dump of the Card through the qFlipper application and modifying the data in a text editor. The solutions will mainly use the latter one, but the concepts remain the same.

If you notice missing data in the later challenges, thus blocks of data that are marked as "??" you will need to run the read operation again and make sure it finishes completely which can take some time.

ACR122U

The crid tool has the --write_block function available to write data to Mifare Classic Card. Use the help menu to identify the required options and flags to make the write function succeed. Make sure the data you are providing is in total 32 characters long in hexadecimal.

References

Proxmark3	Use the Proxmark3 cli to find which hf mf command you need to use.
ACR122U (CRID)	use the crid tool with write_block and read_block features
Convert Data	https://cyberchef.org/#recipe=To_Hex('None',0)

Challenge #4: Access Bits

Difficulty:	Easy
Goal:	Understand what access bits and how to adept to it.
Requirements:	Any HF RFID reader/writer and required drivers/software client One of the Mifare Classic Cards
Challenge Points	75 points

Card A or B	Sector 3	Block 12

Description

During this challenge we will investigate access bits. Access bits can be used to specify what actions can be taken with the keys present within that sector. The different permissions:

- read
- write
- increment
- decrement/transfer/restore

Each sector has its own access bits and are always located at 7-10th bytes in the last block of the sector.

The goal of this challenge is to write some data in the first block of sector 3 (Block 12) on one of the Mifare Classic Cards and test it against the OctoBox. You will notice that the commands will need to change slightly since the access bits will be configured in some way. In order to understand how the access bit are configured for Sector 3. Take the 7-10 bytes from the last block within the sector:

787788

Use the following tool https://slebe.dev/mifarecalc/ to understand what these bytes mean and what needs to change to the commands to your write command work.

Proxmark also has the command hf mf acl -d XXXXXX that can help you figure out the access bits.

The data that can be written is the following:

String: flag{icanwrite!}
Hexstring: 666C61677B6963616E7772697465217D

The access keys are provided again for this challenge:

Access Key A: FFFFFFFFFFFF
Access Key B: A1A2A3A4A5A6

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox.

Tips

Mifare Access Bit Calculator	https://slebe.dev/mifarecalc/
Proxmark Access Bit Command	hf mf acl -d XXXXXX

Challenge #5: Key Recovery

Difficulty:	Medium
Goal:	Learn about brute force attacks for Mifare Classic cards
Requirements:	Any HF RFID reader/writer and required drivers/software client One of the Mifare Classic Challenge Cards
Challenge Points	100 points

Card A or B	Sector 4	Block 18

Description

Within this challenge you will need to obtain full access to sector 4 and write a flag to a specific block, that resides in sector 4. There is no need for fancy exploits for this one but just an old trick of the book, brute forcing the key is the goals here. Specifically, an “online” brute force attack.

Access Key A: FFFFFFFFFFFF
Access Key B: ????????????

The flag can be written on the third block of sector 4 (Block 18) on one of the Mifare Classic Cards and needs to look as follow:

String: flag{Brut333333}
Hexstring: 666C61677B4272757433333333333337D

Once you have done the write successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox

Proxmark

Take a look at the **mf hf chk** command implemented in the Proxmark, within the Proxmark repo you can find wordlists for Mifare in the folder **client/dictionaries** , mfc_keys_bmp_sorted.dic for example.

Flipper Zero

Flipper Zero does the brute force when initiating the read command, but the default list will not contain the correct key. In order to add new wordlists, copy the mf_classic_dict_user.nfc file onto the SD Card -> nfc -> assets folder. You can find the wordlist on the Flipper Zero GitHub repository:
https://github.com/UberGuidoZ/Flipper/blob/main/NFC/mf_classic_dict/mf_classic_dict_user.nfc

ACR122U

The crid tool has the ---brute_force_keys function available where you can specify a list of keys it will try. The list you could use is also available in the Crid repository:

https://github.com/VinnieV/crid/blob/main/mifare_access_keys_top100.dic

References

Mifare Keys	https://github.com/VinnieV/crid/blob/main/mifare_access_keys_top100.dic
Flipper Zero	https://github.com/UberGuidoZ/Flipper/blob/main/NFC/mf_classic_dict/ReadMe.md

Challenge #6: Nested Attack

Difficulty:	Medium
Goal:	Exploit a vulnerability to recover keys that are still unknown.
Requirements:	Any HF RFID reader/writer and required drivers/software client Only Mifare Card A will work here.
Challenge Points	125 points

Card A	Sector 5	Block 22

Description

Within this challenge you will need to obtain full access to sector 5 and write a flag to block 22, that resides in sector 5. For this use one of the first discovered Mifare vulnerabilities to recover the missing key, the nested attack.

Keep in mind that in order to execute a nested attack you need to know at least one valid key for any sector, that will need to be provided within the commands to initiate this attack, depending on the tool used.

Access Key A: FFFFFFFFFFFF
Access Key B: ????????????

The flag can be written on the third block of sector 5 (Block 22) on Mifare Classic Card A and needs to look as follow:

String: flag{H5ck3r}
Hexstring: 666c61677b4835636b33727d00000000

Once you have done the write successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox.

Proxmark

The Proxmark implements the nested attack within the **hf mf nested** command and look at the help menu how you would specify the following:

- The known key
- What block the key can be used for
- Which type of key it is (A or B)
- Which block you want to target
- Which type of key you want to obtain from target block

Once you have the full command ready you should be able to recover the key.

Flipper Zero

Flipper Zero has an application you can install called Mfkey32. It will be available under NFC within the apps modules once you installed the application. Running the tool might be confusing, but first you will need to save a dump of the current card into a file using the reader command in NFC module.

Once you have the card saved, you will need to open the saved card and use the Detect reader command. This will allow you to tap the reader a couple of times to capture nonces which are random cryptographic tokens generated during authentication, once enough nonces are collected the Mfkey32 can perform cryptographic operations and brute forcing to obtain the keys.

ACR122U

The crid tool does provide a --nested_attack flag, however it might be better to use the mfoc application directly, since crid is just a wrapper around that tool for this challenge. Using the mfoc is pretty straightforward, you don't need to specify any argument except, and output file and it will enumerate keys for you automatically and use them to crack all other keys on the card.

References	
Mifare Classic Offline Cracker	https://github.com/nfc-tools/mfoc
LibNFC	http://www.libnfc.org/api/

Challenge #7: Hardnested Attack

Difficulty:	Medium
Goal:	Perform hardnested attack
Requirements:	Any HF RFID reader/writer and required drivers/software client Only Mifare Card B will work here.
Challenge Points	150 points

Card B	Sector 6	Block 26

Description

Within this challenge you will need to obtain full access to sector 6 and write a flag to block 26, that resides in sector 6. Unfortunately, you most likely received the key for this sector already in the previous exercise, unless I was able to provide cards with hardened randomization that requires the hardnested attack.

Access Key A: FFFFFFFFFFFF

Access Key B: ????????????

The flag can be written on the third block of sector 6 (Block 26) on Mifare Classic Card B and needs to look as follow:

String: flag{h4rdn3st3d}
Hexstring: 666c61677b683472646e33737433647d

Once you have done the write successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox

Proxmark

The Proxmark implements the hardnested attack in the hf mf staticnested command. The options are similar to how the nested attack works.

Flipper Zero

Flipper Zero does not support hardnested attack in the original firmware. There is a project that implements the attack: https://github.com/AloneLiberty/FlipperNested

However, for this current version of the workshop I was not able to fully work this out yet (sorry).
Feel free to explore these guidelines:

https://github.com/AloneLiberty/FlipperNested/wiki/Usage-guide

ACR122U

In order to perform the hardnested attack using the ACR122U you will need to use the miLazyCracker tool.

References

miLazyCracker	https://github.com/nfc-tools/miLazyCracker
Paper about hardnested attacks	https://www.cs.ru.nl/~rverdult/Ciphertext-only_Cryptanalysis_on_Hardened_Mifare_Classic_Cards-CCS_2015.pdf
Crypto1 Hardnested attack C implementation	https://github.com/aczid/crypto1_bs

Challenge #8: Darkside Attack

Difficulty:	Medium
Goal:	Try to gain access to all the data
Requirements:	Any HF RFID reader/writer and required drivers/software client Any Mifare Card will work here.
Challenge Points	150 points

Card B	Sector 7	Block 30

Description

Within this challenge you will need to obtain full access to sector 7 and write a flag to a specific block, that resides in sector 7. For this use one of the first discovered Mifare vulnerabilities to recover the missing key.

Access Key A: FFFFFFFFFFFF
Access Key B: ????????????

The flag can be written on the third block of sector 7 (Block 30) on one of the Mifare Classic Cards and needs to look as follow:

String: flag{D4rKS1d3d!}
Hexstring: 666c61677b4434724b5331643364217d

Once you have done the write successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox

Proxmark

The Proxmark implements the darkside attack in the hf mf darkside command. Please take a look at the help menu on how to use the hf mf darkside attack. You will need to pass two parameters to make sure you obtain the correct key.

Flipper Zero

Flipper Zero does not support darkside attack in the original firmware.

ACR122U

The darkside attack specifically can be executed using the mfcuk tool.

References

mfcuk	https://github.com/nfc-tools/mfcuk

Challenge #9: Vault

Difficulty:	Medium
Goal:	Modifying the UID of the card
Requirements:	Any HF RFID reader/writer and required drivers/software client Any Mifare Card with the magic hat logo present
Challenge Points	150 points

Card A or B	Sector 0	Block 0

Description

The UID is the first 4 or 7 bytes within the first block of the card. This block is supposed to be read-only and a way to ensure authenticity. However, you can buy special Mifare cards called Magic Mifare Cards that have a modified chipset that allow modifying the UID. There are different versions of these, indicated with Gen1,2,… . It usually works by sending a custom ADPU command to enable writing the UID, most of the times this will be implemented in an easy command within your tool.

The goal of this challenge is modifying the UID of your card so it has the following UID:

UID: DEADBEEF

Once you have modified the UID of your card successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox

Proxmark

The hf mf csetuid command in the Proxmark CLI can be used to change the UID of the card.

Flipper Zero

Currently did not find a way to change the UID of the card using the Flipper Zero, but emulation is possible. So within the NFC module you can manually add a card with 4 byte UID.

ACR122U

Currently this is not implemented within the crid tool but there is a tool within the lib-nfc suite that allow you to write 4-byte UID's to magic cards. The tool can be executed using the **nfc-mfsetuid** command.

Challenge #10: Employee Card

Difficulty: Medium
Goal: Cloning of an employee card.
Requirements: Any HF RFID reader/writer and required drivers/software client
Challenge Points 150 points

Card A and B	Sector 8	Block 34

Description

Let's simulate an example of a real-life scenario where you would want to clone a specific employee card to gain access to the entrance of your target during a red team exercise.

1. First make sure you can read sector 8 fully.
2. Then analyse the data on sector 8 for both cards and identify how the system determines which employee scanned their badge.
3. Create an RFID card for the employee with employee number:

12307

If you did not have the keys yet for Sector 8:

Access Key A: FFFFFFFFFFFF
Access Key B: BE13377331EB

Only Block 34 needs to be written, block 33 can stay there as reference for the original value. But you can always reset the card if you want to have all data restored.

Once you have gained access of your card successfully, test it against the OctoBox.

If you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox

Challenge #11: Vending Machine

Difficulty:	Hard
Goal:	Learn how RFID implementation often use some data validation.
Requirements:	Any HF RFID reader/writer and required drivers/software client
Challenge Points	250 points

Card A and B	Sector 10

Description

OctoBox has a wonderful vending machine and the two workshop cards both have some credits assigned. Can you hack your way in to gain access to unlimited credits?

The goal is to scan a card with 1000 or more credits assigned. The vending machine makes use of sector 10.

In case you did not have the keys yet for Sector 10:

Access Key A: FFFFFFFFFFFF
Access Key B: AF720E83D0F1

You might need to **scan the card on the vending machine** to understand how much credits are currently present, which can be useful piece of information to understand the data on the card.

Once you have more than 1000 credits you can buy the flag in the vending machine and if you kept your username on the card in sector 2 it should allocate some points on the scoreboard.

Challenge #12: Hotel Rooms

Difficulty:	Hard
Goal:	Assuming a scenario where you would want to figure out how your hotel room access is working. Obtain access to room number 420 to obtain some points.
Requirements:	Any HF RFID reader/writer and required drivers/software client
Challenge Points	350 points

Card A and B	Sector 11

Description

Imagine you have access to your hotel room in room number 419 using Card A (Spencer) and coincidently you also found an expired badge Card B (Harper) close to your hotel room door. Can you understand how the door verifies that you have access to the room and obtain access to room number 420?

In case you did not have the keys yet for Sector 11:

Access Key A: 02872FB92433
Access Key B: 14318D91BFE5

With the access keys known you would read the data from both cards and attempt to understand what the data represents. Cross-referencing any known information in different data formats and modifying the data slightly while observing any behaviour changes.

Important information:

Assume the current date is: **10 August 2024**
And we booked a reservation between: **8 and 11 August 2024**

You gain the points if you can open hotel room 420 and if you kept your username on the card in sector 2 it should allocate some points for the scoreboard when you scan the card in the OctoBox.

Challenge #13: Speedrun challenge

Difficulty:	Hard
Goal:	Try to clone a badge as fast as possible
Requirements:	Any HF RFID reader/writer and required drivers/software client

Description

For this challenge you will need to clone a configured badge as fast as possible in any way you want, but with one rule:

Its not allowed to write or change the challenge card.

Make sure you are using a wiped challenge card provided by the instructor.

1. Place the challenge card on the reader and wait until the game screen highlights Ready and the play button becomes enabled.
2. Press the play button, where the card will be configured and as soon as the timer starts you can take the card and clone/emulate the card as fast as possible.
3. Place your cloned card on the reader when finished and observe your time.

Goodluck!