Using Proxmark3 to Clone a turnstile pass

Created By	Ⓓ Daniil A (Kiky Tokamuro)
Last Edited	@Sep 8, 2019
Tags	hacking proxmark3

My treasured package with “Proxmark3 Easy” came. In short, Proxmark3 is a powerful RFID tool designed to track, listen and emulate everything from low-frequency (125 kHz) to high-frequency (13.56 MHz) tags.

Before you continue reading, I hasten to warn you: ***This article is written for information only, and in no case does not encourage fraud RFID tags, as this contradicts the Criminal Code of the Russian Federation. The author is not***

responsible for any illegal actions committed by people using the information in this article.

This article assumes that you have already installed the necessary firmware on your Proxmark3 and can run the utility to work with it. If not, read this.

Let's start researching RFID tags.

In my educational institution, there are turnstiles at the entrance, and in order to pass you need to attach your pass. And since I often forgot the pass, I decided to copy it to the T5577 key that came with the Proxmark3. Similar keychains can be found on AliExpress.

First you need to find out what type of label is used in the pass, for this we apply it to the reader and run the proxmark3 utility:

> ./proxmark3 /dev/ttyACM0

How to start the utility, enter:

> proxmark3> lf search

> Checking for known tags:
> EM410x pattern found:
> EM TAG ID : 1234567890
> ...

In this case, my pass turned out to be a label like EM410x with ID 1234567890 (needed for copying). EM410x is an EM Microelectronic-Marin RFID tag format. This tag belongs to the class of passive RFID tags, since it does not have a built-in power supply. It operates in the frequency range of 125 kHz.

Next, remember the tag ID, and attach a keychain to the reader, onto which we will clone the pass. And enter the command:

> proxmark3> lf em 410xwrite 1234567890 1

After that you can see:

> Writing T55×7 tag with UID 0×1234567890 (clock rate: 64)
> #db# Started writing T55×7 tag ...
> #db# Clock rate: 64

This tells us that the label was copied successfully. You can safely go to College and check, I will say in advance that everything worked perfectly ;)

Links to research topic RFID tags:

- https://store.ryscc.com/blogs/news/92577601-making-a-physical-em4100-clone
- https://habr.com/post/325776/
- https://www.securitylab.ru/analytics/458814.php