Card Cloning

The Short Version

We are using two types of card technology on this set up; Low Frequency and High Frequency (LF and HF).

LF is an older tech with a longer range and often no real encryption (not always the case).

HF is newer, supports fancy tech and encryption.

The Long Version - LF

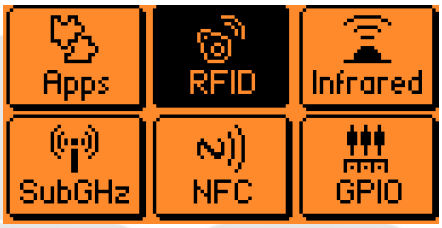
The **LF standard** in use is the **EM4100** (very old!) and the readers were **very cheap**. When energized, the **chip just splurts** a card **number to the reader** which **checks with the controlle**r, opening the door if valid. You will be able to clone M'lud or The Punisher.

You can clone this with the Flipper or a cheap device off Amazon.

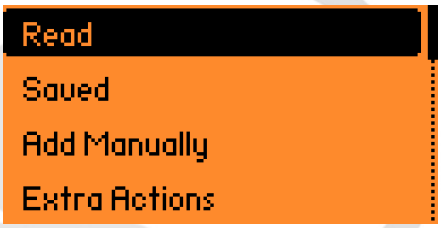
Go to: RFID → read card → more → emulate and present the Flipper to the reader.

If you'd like to try cloning to a new card, ask Phil for a blank card.

1



2

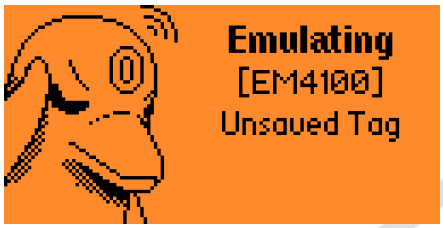


3

4

5

6



Enquiries@StyxSecurity.org

We don't knock.

The Long Version – HF Card Cloning

These are **high frequency** cards which use the **Mifare Classic** chip. The MFC **encryption has been broken** several different ways. The card will **require a decryption key** from the reader to **release data** stored in **locked memory** blocks.

UID

Unique identifier is essentially the card's **serial number**. It's **not protected** information. A lot of systems come **out of the box** just using the **UID to validate credentials** for the sake of compatibility. This **is supposed to be sorted** after installation. It's often the case this **default setting is left** because, well, it's easier and the customer won't know.

UID is stored in block 0 on the card and is supposed to be unmodifiable from the factory. Of course, there are lots of cards with modifiable block 0 (aka "Magic Mifare" or "UID Changeable").

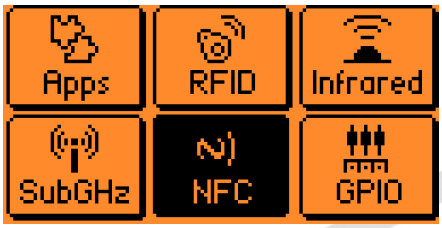
Keys

There are **16 sectors** available, each with **two keys, A and B**. So in total a card **can have 32 keys**. This rarely happens in practice and is only the case when a Miscreant Crèche demands a hardened card and a Proxmark is combined with alcohol.

Another giant issue with MFC was the **keys being left as default** or other known values. **Dictionary attacks** are therefore the first port of call and the Flipper can do this. **You'll be able to clone the default keys Mifare Classic card with the Flipper. The others won't work.**

Go to: NFC → Read → More → Emulate and present to reader.

1



2

3

4

Enquiries@StyxSecurity.org

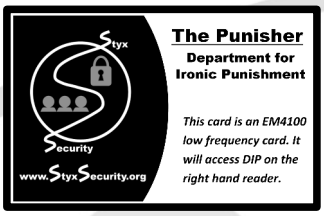
We don't knock.

What Are These Cards?

The Cards

You'll have noticed there are several different types of RFID card here. This is a breakdown of each one.

M'lud and The Punisher



These are **low frequency**, no security **EM4100** cards representative of **early 1990s** technology.

Mifare Classic Cards

Mifare Classic is from roughly the **late 1990s** and is a **high frequency** standard. It supports **encryption** and demands a key to open any particular sector and release the data. The **encryption is broken** but the **cards are still in** use and there are ways of mitigating the risk. In the right environment, they have their place but new kit should really be moving on.

Default Keys (RED) – This card is a Magic card and uses ult keys. It is a replica of a card I found in use in the field. The organisation changed this system shortly afterwards.

Hardened Custom Keys (GREEN) – This card is also a Magic card and uses custom keys so will not be cracked by the Flipper's dictionary attack, because they are not in its dictionary. You will find that doesn't really matter as I've also set the Honeywell reader up as found at the same site with the default keys card.

Genuine NXP (BLUE) – This is a genuine NXP card, which matters as it means other attacks (darkside, etc) will work on it. I gave it lots and lots of keys but a Proxmark will autopwn it.

Seos Cards

Seos is a **proprietary system** from HID and is relatively state of the art. There are different levels of Seos and there are 32bit / 48bit standard keys and a 48 bit iCE (iClass Elite) key. You are welcome to try and crack them, it's unlikely you will (if you do, HID would like to know). If you interrogate these with the Proxmark, it has a note that Iceman would like a copy of the output. I checked and HID aren't bothered, but I'd appreciate it if you didn't.

Flipper Zero

What is it?

An **electronic multitool** which is also a pet dolphin.

The Flipper zero is **aimed at teens and hacker types** and is an introduction into many electronic principles and basic security. It has **reduced the barrier to entry** for many electronic attacks but most of what it can do is mischief.

If the Flipper Zero can bypass your security, criminals have had the tools for around a a decade.

The Flipper makes demonstrating electronic attacks very easy and removes the need for highly specialist tools.

Negatively, the Flipper does increase the range of attacks available to the “curious teen” but it also massively **increases awareness** and helps **hold manufacturers accountable**.

Enquiries@StyxSecurity.org

We don’t knock.