What's RFID?

> Radio-frequency identification (RFID) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking.

What is NFC

> Near field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (2 in) of each other.

RFID Hardware

Reader/Writer

Touch-a-tag



C3L is in possession of several Touchatag readers which work fine on Linux (after some hacking)

If you want to get one for yourself, you should hurry up because the manufacturer closes it's store on the 31. December ’12. If you order from Benelux you should visit getdigital.de. They sell and deliver them very fast.

ACR122U



A good piece of hardware with a good linux support.

Proxmark



Works like a charm under linux!

NFC Tags



NTAG216

Those are the NFC tags we use to chip our Hackerspace passports.
Capacity: 888 Byte.
Standard: NFC Forum Type 2 Tag ISO 14 443 A

```
nfc-mfultralight r dump.mfd
nfc-mfultralight w dump.mfd
```

RFID Software

libnfc

```
sudo apt-get install libnfc-dev
```

RFIDIOt

A bunch of python scripts. Preinstalled on Kali linux.

mfoc

Mifare Classic Offline Cracker is a tool that can recover keys from Mifare Classic cards.

Website

mfcuk



Installation procedure was from 2012. Now the installation is straight forward!

MFCUK - MiFare Classic Universal toolKit. Toolkit containing samples and various tools based on and around libnfc and crapto1, with emphasis on Mifare Classic NXP/Philips RFID cards.

Special emphasis of the toolkit is on the following:

- mifare classic weakness demonstration/exploitation
- demonstrate use of libnfc (and ACR122 readers)
- demonstrate use of Crapto1 implementation to confirm internal workings and to verify theoretical/practical weaknesses/attacks

**Website **

mfoc & mfcuk installation guides

Ubuntu

Install the pcscd package.

```
sudo apt-get install pcscd
```

Install libccid

```
sudo apt-get install libccid
```

Install autoreconf

```
sudo apt-get install autoreconf
```

Install libnfc-1.3.9

```
autoreconf -vis
./configure
make
sudo make install
```

Download mfoc

```
autoreconf -vis
./configure
make
sudo make install
```

If you encounter problems after the execution, do this:

```
sudo ln -s /usr/local/lib/libncf.so* /usr/lib/
```

Now mfoc should be up and running.

Download and install libnfc-1.5.1

```
autoreconf -vis
./configure
make
sudo make install
```

Download mfcuk

```
svn checkout http://mfcuk.googlecode.com/svn/trunk/ mfcuk-read-only
```

Symlink shared object libs!

```
sudo ln -s /usr/local/lib/libncf.so* /usr/lib/
```

Install mfcuk

```
autoreconf -vis
automake --add-missing
autoconf
./configure
```

Now open the Makefiles in /mfcuk-read-only & /mfcuk-read-only/src and search for the line LIBS = .Replace it with:

```
LIBS = $(LIBNFC_LIBS)
```

Now...

```
make
sudo make install
```

Final step

```
cd /mfcuk-read-only/src
cp data /usr/local/bin
```

Now you should be ready for ownage!

From:
https://wiki.c3l.lu/ - **Chaos Computer Club Lëtzebuerg**

Permanent link:
https://wiki.c3l.lu/doku.php?id=projects:security:rfid

Last update: **2021/10/10 22:51**