**OV-chipkaart**
*OV-chipkaart, inside out*

---

**Doe het zelf**

# Lees dit aandachtig door!

**IK LEG NIET UIT HOE JE GRATIS REIST OF HOE JE EEN KAART MANIPULEERT, IK LEG ALLEEN UIT HOE JE DE SLEUTELS VAN DE MIFARE CLASSIC 1K EN 4K BEVEILIGING VERKRIJGT EN DE INHOUD VAN DE KAART NAAR EEN BESTAND OPSLAAT!!!**

**Alles geschreven een weergegeven op deze website is uitsluitend bedoeld om van te leren, ga niet reizen met een gemanipuleerde of gekopieerde ov-chipkaart, de kaart word geblokkeerd, of nog erger, je word gepakt.... het is legaal om je kaart te analyseren, het is illegaal om je kaart te kopiëren of te manipuleren.**

**IK BEN NIET VERANTWOORDELIJK VOOR DE GEVOLGEN VAN DEZE INSTRUCTIE EN/OF WEBSITE!**

**Genoeg rode tekst, laten we beginnen**

# Hardware en software

## Hardware

Het begint allemaal met een RFID lezer, ondersteunt in libnfc (zie hun compatibiliteits matrix), Ik gebruik zelf de ACS ACR122U, deze lezer werkt goed samen met libnfc, je kunt ook een “Touchatag” lezer gerbuiken, beide kunnen lezen van en schrijven naar MIFARE kaarten en kosten rond de € 30.


Deze instructie is gebaseerd op de ACR 122U, heb je een andere libnfc ondersteunde lezer, wees creatief.

Is je lezer niet ondersteunt in libnfc?, Sorry, de later gebruikte software is allemaal gebaseerd op libnfc.....

## Drivers

Ten tweede hebben we ~~l33t klik en ga Windows skiddie software~~ Linux nodig.
Ik heb Ubuntu 10.10 gebruikt voor dit project, het werkt goed, als je de basis van Linux niet kent, draai dan nu om!

De driver installatie van de ACR122U is erg makkelijk, met *apt-get install pcscd* heb je de basis, libnfc doet de rest voor je.

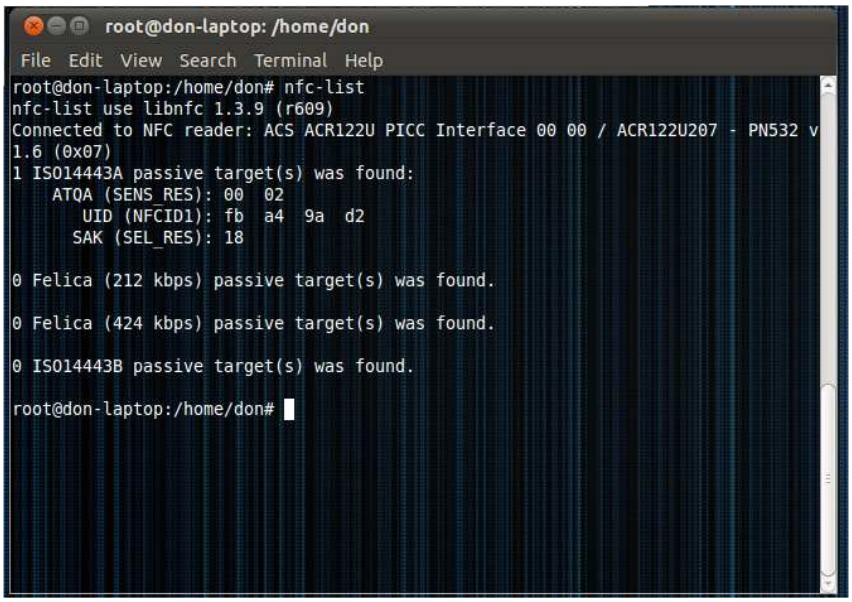
## Libnfc

Nu is het tijd om libnfc te installeren (ik heb versie 1.3.9 gebruikt), download de broncode hier.

Om libnfc te installeren voer de volgende commando's uit (i hoop dat je al weet hoe je programma's van broncode compileert in Linux):

1. *tar xvzf libnfc-1.3.9.tar.gz*
2. *cd libnfc-1.3.9*
3. *./configure* (als je foutmeldingen tegenkomt (meestal ontbrekende pakketten) los deze dan op)
4. *make*
5. *make install*
6. sluit de lezer aan
7. wacht op een rood licht (als het lampje uit blijft gaat er iets mis)
8. leg een kaart op de lezer (licht zal nu groen worden, als het goed is)

9. voer *nfc-list* uit
10. Als je de identificatiecode van de kaart ziet gaat het goed, dat ziet er ongeveer zo uit:




## MFOC

Nu we libnfc en de lezer aan de gang hebben, hebben we een programma nodig om de sleutels te ontfutselen, voor deze complexe taak gebruiken we een programma genaamd MFOC. MFOC is een opensource programma om sleutels uit MIFARE classic kaarten te ontfutselen, het is niet erg stabiel, maar met veel tijd en moeite (ongeveer een uur) kun je alle 80 A en B sleutels vinden.

Download de MFOC broncode hier.

Om MFOC te installeren, voer de volgende commando's uit:

1. *tar xvzf mfoc-0.09.tar.gz*
2. *cd mfoc-0.09*
3. *./configure* (als je foutmeldingen tegenkomt (meestal ontbrekende pakketten) los deze dan op)
4. *make*
5. *make install*

Nu heb je alle tools om aan de slag te gaan, gebruik deze tools op een wijze manier!

# Het echte werk

Het is belangrijk om iedere gevonden sleutel om te slaan in een bestandje, MFOC slaat de sleutels niet voor je op!

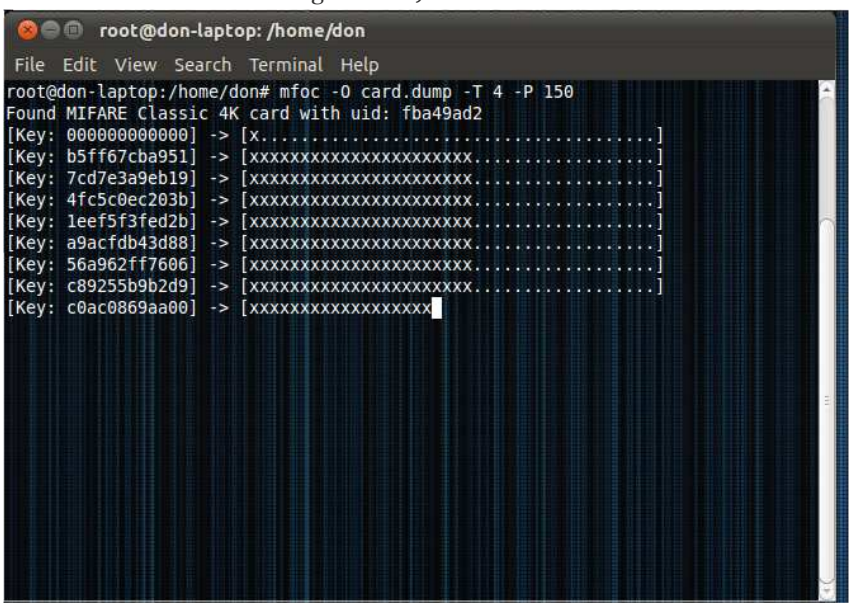
MFOC kan aangeroepen worden met diverse parameters, het is aanbevolen om het aantal pogingen te verhogen (-P option) en de afstand te verlagen (-T option), de afstand verlagen zorgt voor aanzienlijk minden crashes.

Start MFOC met het volgende commando:
*mfoc -O mifarecard.dump -P 150 -T 4*

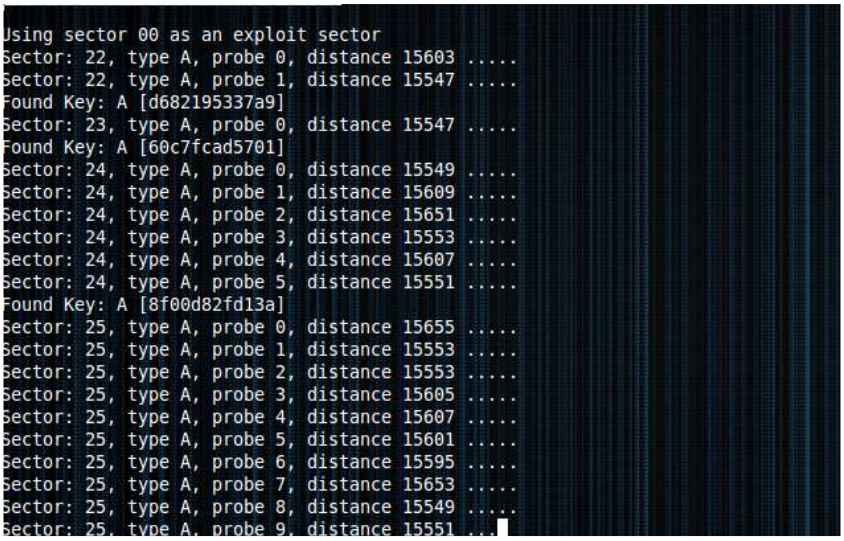
MFOC begint met het testen van standaard sleutels, en zal daarna sector-voor-sector alle sleutels zoeken. Aan het eind worden de gegevens van de kaart opgeslagen in het bestand aangegeven met de -O optie.

[advanced talk]*To greatly improve the performance you can change the source code and remove all the bad keys, hard coding the found keys will improve the performance and will greatly reduce the time needed to retrieve the keys (for example: you've found 20 of the 40 keys, the program crashed, just hard code the 20 keys into mfoc, start the program, and it will start at the 21st key, instead of the 1st key), the keys are stored in the mfoc.c file.*[/advanced talk]

Dit proces ziet er ongeveer zo uit (in jouw scherm zie je misschien 1 [X.....], dit is een aangepaste versie van MFOC met wat sleutels erin gebakken):




Na deze initiële start zal MFOC verder naar sleutels graven, dit ziet er als volgt uit:




Nu heb je alle sleutels ontfutseld van een ~~miljarden~~ triljoenen project  met 30 euro aan apparatuur, dat noemen ze beveiliging.....

Nu kun je de dump gaan analyseren met een hex editor.... het makkelijkste om te vinden is je geboortedatum, zoek maar is naar jj jj mm dd (in hex uiteraard).

### 2 Responses to *Doe het zelf*

**Omutsu** *says:*

October 11, 2010 at 4:44 pm

Huh, wonder why it's illegal to copy a card and travel with it... Unrelated OV-Chipcard fun: get one of those GPS jammers from an outfit like dealextreme.com, hop on the bus or tram and travel at "instaptarief" (EUR0.78). Fucking never fails! And, of course, you're doing your fellow travellers a favor too.

Now I'll just wait for the reader to arrive and play with it on my Linnuks machine. Then see how long it takes until my Mifare card is blacklisted

Reply

**Omutsu** *says:*
October 19, 2010 at 7:22 pm

Got my reader from Touchatag but not much luck. Wasted four hours compiling binaries on my Ubuntu 10.04 64 bit box and still I get "SCardEstablishContect: RPC Transport Error."

I'm gonna watch some TV now...

Reply