

**Projectverslag**

Aan: Maarten Luyts & Tim Dams

Van: Michael Marivoet & Ward

Datum: 15/01/2016

Pagina’s:

**RFID cloner**

Information Security

## Uitleg Project

Wij hebben gekozen voor het project RFID Stealer. We vonden dit beiden een boeiend project aangezien we de voorbije jaren weinig hebben gewerkt met de beveiliging en de toegankelijkheid van bepaalde gevoelige data.

Dit project leek ons op het eerste zicht een interessant project omdat we op die manier konden laten zien hoe gemakkelijk het is om gevoelige data te pakken te krijgen zonder dat de gebruiker hiervan op de hoogte kan zijn.

Het werken met een Raspberry PI is in dat opzicht eveneens een openbaring voor ons. Ervoor werkten we vooral met Arduino’s en VirtualBox om een programma te kunnen schrijven waarmee we informatie konden halen van derden.

Wat we zouden bekomen na het project leek me ook in dat opzicht een boeiend gegeven. Het verkrijgen van toegang tot een bepaalde module (sorteerstraat, klaslokaal, …) leek ons opwindend.

## Belangrijke scripts

We zijn op verschillende manieren begonnen aan het project. Terwijl de ene persoon bezig was met de werking van een Raspberry PI uit te dokteren, was de andere bezig met het schrijven van een programma met Arduino om op die manier de gegevens die op een NFC kaart te verkrijgen en te kopiëren.

Nadat we besloten om zelf onze componenten aan te kopen, moesten we een aantal weken wachten op deze componenten. We konden wel al tutorials opzoeken die het mogelijk maakten om onze opdracht tot een goed einde te brengen.

De zaken die we zelf hebben aangekocht zijn RFID readers, lege kopieerkaarten en sleutelhangers die eigenlijk hetzelfde doen als de RFID readers. We hebben ook nog een aantal zaken gebruikt die we konden krijgen van de leerkracht. Dit waren Long-Range USB adapter, Raspberry PI en de nodige kabels om alles met elkaar te kunnen verbinden.

In het begin zochten we vooral naar een gemakkelijke manier om data te bekomen van een NFC kaart. Toen zochten we vooral naar manieren om dit te doen via de Raspberry PI, nadien wouden we ook eens kijken of er nog een andere manier was om dit te doen met een Arduino.

Dit bleek zo te zijn, er zijn al gemakkelijkere programma’s geschreven voor Arduino die eigenlijk hetzelfde werk opknappen als een Raspberry PI. We besloten dan ook om te stoppen met zoeken naar code die we konden gebruiken voor de Raspberry PI en ons te focussen op de code die gebruik maakt van een Arduino. Op die manier heeft ons dat veel tijd en vooral veel opzoekwerk uitgespaard.

Het programma dat voor Arduino geschreven is, is gevonden via een tutorial die allereerst een programma uitlegt waarmee je de info die op een NFC kaart staat, kan bekomen in de Seriële monitor.

Het tweede programma beschrijft een manier om enerzijds informatie te lezen en op te slaan in het geheugen van de Arduino en anderzijds om die gegevens ook te schrijven naar een nieuwe en lege NFC kaart.

Op die manier kopiëren we eigenlijk de data die op de NFC kaart staat.

Het probleem met dit programma is dat er zowel voldoende statisch geheugen als dynamische geheugen moet zijn om de data die staat op een NFC kaart te kunnen opslaan in het dynamische geheugen van de Arduino. We konden dit oplossen door een Arduino te nemen die een groter geheugen heeft dan diegene die normaal gezien op school beschikbaar zijn.

## Werkwijze

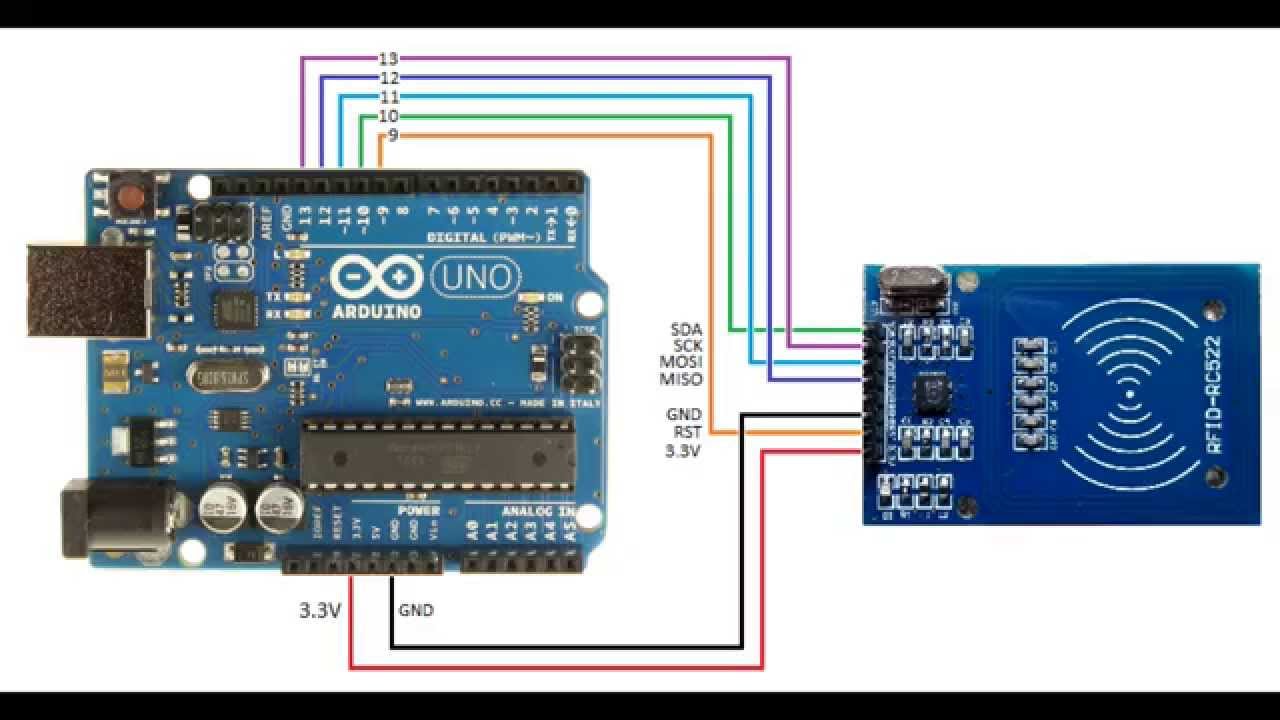
### Verbinden van de RFID reader met de Arduino

Het verbinden van een RFID reader met een Arduino verschilt van Arduino tot Arduino.

Het verschilt in die mate doordat de MOSI, MISO en SCK verschilt van bordje tot bordje.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Signaal | RFID Reader Pin | Arduino  Uno Pin | Arduino Mega Pin | Arduino Nano v3 Pin | Arduino Leonardo /Micro Pin | Arduino Pro Micro Pin |
| RST/ Reset | RST | 9 | 5 | D9 | RESET / ICSP-5 | RST |
| SPI SS | SDA (SS) | 10 | 53 | D10 | 10 | 10 |
| SPI MOSI | MOSI | 11 / ICSP-4 | 51 | D11 | ICSP-4 | 16 |
| SPI MISO | MISO | 12 / ICSP-1 | 50 | D12 | ICSP-1 | 14 |
| SPI SCK | SCK | 13 / ICSP-3 | 52 | D13 | ICSP-3 | 15 |

Bij een Arduino Uno geeft dit dan deze verbinding met de RFID reader.



Wat er echter niet verandert bij een verschillend Arduino bordje zijn de plaats waar de voeding(3,3 V), de grond en Slave Select (SS) worden aangesloten met de RFID reader.

### Schrijven van code

We schrijven de code en gebruiken de libraries en tutorials die beschreven staan in het volgende punt.

### Verifiëren van de code

We passen de code aan als er tijdens het compileren fouten zijn gevonden door de compiler. Indien nodig zoeken we op het internet naar veel gemaakte fouten om ons op die manier te helpen.

### Uploaden van de code

We laden onze code op het bordje en testen het programma uit. Indien er iets fout loopt, dan passen we de code aan of zoeken we de fout op het internet op.

De meest gemaakte fout in deze context is het onjuist kiezen van het soort van bordje en COM poort. Een van ons had het probleem dat er geen COM poort kon geselecteerd worden. Dit werd verholpen door een ander bordje te kiezen.

Een andere fout was dat het dynamische geheugen van de poort te klein was om de lokale variabelen te kunnen opslaan. Hier werkt oftewel het veranderen van chip maar wel hetzelfde bordje blijven behouden oftewel het veranderen van bordje

Als alles goed is verlopen, testen we of het programma ook effectief werkt. We hebben ons programma bij voorbeeld getest met de lege NFC kaart en de sleutelhanger die we hebben gekregen bij de RFID reader.

## Gebruikte libraries en bronnen

We hebben voornamelijk de SPI library gebruikt om de communicatie tussen de RFID reader / writer met de Arduino te vergemakkelijken.

Daarnaast hebben we ook nog de MRFC22 library gebruikt om de RFID reader / writer aan te kunnen spreken en functies die oftewel in de library staat of een zelf geschreven functie uit te voeren.

## Verloop

Door Michael Marivoet.

### Onderzoek

Allereerst zijn we begonnen met te zoeken naar informatie, tutorials, scripties, etc. die over het lezen, schrijven, kopiëren, etc. van RFID tags gaan. We hebben veel geleerd over de MIFARE classic RFID tag dankzij de scriptie van Wee Hon Tan.

## Bronnen

### [Practical Attacks on the MIFARE classic by Wee Hon Tan](http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.pdf)

### [MakeCourse: using MF522 RFID reader with Arduino](http://makecourse.weebly.com/week10segment1.html)

### [RFID/Arduino: copy a card with known keys](https://ebc81.wordpress.com/2014/11/16/rfid-arduino-copy-a-card-with-known-keys/)

### [Arduino RFID library for MFRC522 – Miguel Balboa](https://github.com/miguelbalboa/rfid)

## Link naar GitHub Repository

[GitHub Repo](https://github.com/MichaelMar93/InfoSec_RFIDcloner.git)