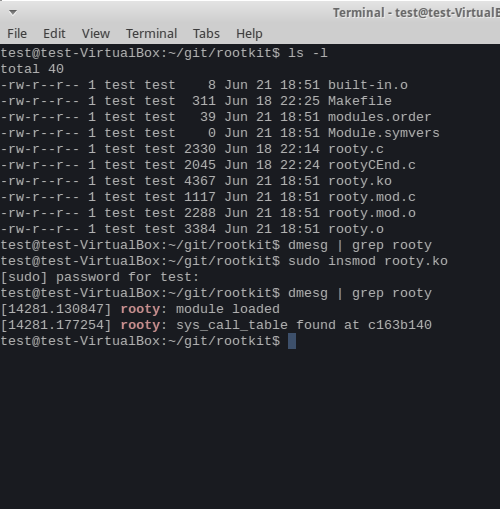
**ReaFID**

**Ein RFID Reaktionsspiel auf Basis eines Arduinos**



**Semesterarbeit Désirée Sacher, ZHAW**

6. /7. Semester 29. Juni 2014

**Danksagung**

**Inhaltsverzeichnis**

[1. Einleitung 4](#_Toc397541224)

[2. Umsetzung der Seminararbeit 5](#_Toc397541225)

[2.1. Aufgabenstellung 5](#_Toc397541226)

[2.2. Arbeitsplanung 5](#_Toc397541227)

[2.3. Seminarumsetzung 6](#_Toc397541228)

[3. Über Rootkits 7](#_Toc397541229)

[3.1. Zur Lektüre 7](#_Toc397541230)

[3.2. Definition Rootkit 7](#_Toc397541231)

[3.3. Anforderungen an ein Rootkit 7](#_Toc397541232)

[3.3.1. Anforderung A1 – Verstecken 7](#_Toc397541233)

[3.3.2. Anforderung A2 – Hintertüre 7](#_Toc397541234)

[3.3.3. Anforderung A3 – Installationsskript 7](#_Toc397541235)

[3.3.4. Anforderung A4 – Spurenvernichtung 7](#_Toc397541236)

[3.4. Lösungsansätze 7](#_Toc397541237)

[3.4.1. Anforderung A1 – Verstecken 7](#_Toc397541238)

[3.4.1.1. User Level Rootkits 7](#_Toc397541239)

[3.4.1.2. Kernel Level Rootkits 7](#_Toc397541240)

[3.4.2. Anforderung A2 – Hintertüre 7](#_Toc397541241)

[3.4.3. Anforderung A3 – Installationsskript 7](#_Toc397541242)

[3.4.4. Anforderung A4 – Spurenvernichtung 7](#_Toc397541243)

[3.5. Weitere Angriffsansätze 7](#_Toc397541244)

[3.5.1. Bootkit 7](#_Toc397541245)

[3.5.2. Virtualisierungs- und Emulations-Rootkit 7](#_Toc397541246)

[3.6. Schutzmassnahmen 7](#_Toc397541247)

[3.6.1. User Level Rootkit 7](#_Toc397541248)

[3.6.2. Kernel Level Rootkit 7](#_Toc397541249)

[3.6.3. Bootkit 8](#_Toc397541250)

[3.6.4. Virtualisierungs- und Emulations-Rootkit 8](#_Toc397541251)

[4. Praktische Erfahrung mit einem Rootkit 9](#_Toc397541252)

[4.1. Einleitung 9](#_Toc397541253)

[4.2. Erfahrungsbericht 9](#_Toc397541254)

[4.2.1. Ausgangslage 9](#_Toc397541255)

[4.2.2. Erstellen eines Treibermoduls 9](#_Toc397541256)

[4.2.3. Verstecken des Moduls 9](#_Toc397541257)

[4.2.4. Manipulation der SYS\_CALL\_TABLE 9](#_Toc397541258)

[4.3. Analyse 9](#_Toc397541259)

[4.4. Fazit 9](#_Toc397541260)

[4.5. Ausblick 9](#_Toc397541261)

[5. Diskussion des eignen Beitrags 10](#_Toc397541262)

[5.1. Eruieren von Herausforderungen für das Schreiben eines Rootkits 10](#_Toc397541263)

[5.2. Schreiben eines Rootkits in der UNIX-Umgebung 10](#_Toc397541264)

[6. Verzeichnisse 11](#_Toc397541265)

[6.1. Literaturverzeichnis 11](#_Toc397541266)

[6.2. Abbildungsverzeichnis 11](#_Toc397541267)

[6.3. Tabellenverzeichnis 12](#_Toc397541268)

[7. Anhang 13](#_Toc397541269)

[7.1. Glossar 13](#_Toc397541270)

# Verzeichnisse

## Abbildungsverzeichnis

## Tabellenverzeichnis

# Zusammenfassung

# Einleitung

Diese Arbeit soll als Möglichkeit dienen, sich mit der RFID Technologie auseinanderzusetzen. Da die RFID Technologie, speziell der in Europa verbreitete Mifare Standard, in den letzten Jahren häufig an Hackerkonferenzen thematisiert wurden, sind dessen Schwachstellen in der Impementation ausreichend bekannt.

Ursprünglich war geplant, die von InterCard hergestellten Studentenausweise der ZHAW genauer zu analyiseren, allerdings wurde diesem Vorhaben von den Sicherheitsbeauftragen der ZHAW einige Hürden in Form von NDAs in den Weg gestellt, welche eine sinnvolle Auseinandersetzung inklusive der Dokumentation der Befunde erschwert hätten.

Stattdessen wurde auf Basis von einem Arduino und einem RFID Shield ein Spiel entwickelt, welches die Technologie kreativ nutzt. Der ursprüngliche Fokus von „Hacken“ und „Reverse Engineeren“ der Technologie wurde verlegt auf das Entwerfen und Programmieren eines Spiels in einer bis jetzt dem Autor unbekannten Sprache. Da die RFID Technologie in beiden Projektzielen verwendet wird, kann trotzdem das Wissen über die Technologie angeeignet und entwickelt werden.

Ziel dieser Arbeit ist entsprechend ein Spiel auf Basis der RFID Technologie mit Hilfe eines Arduinos. Zur Programmierung des Spiels wurde Python verwendet. Die Spiellogik wurde selbst entwickelt.

# Umsetzung der Seminararbeit

## Aufgabenstellung

Die Aufgabenstellung wurde im EBS wie folgt definiert:

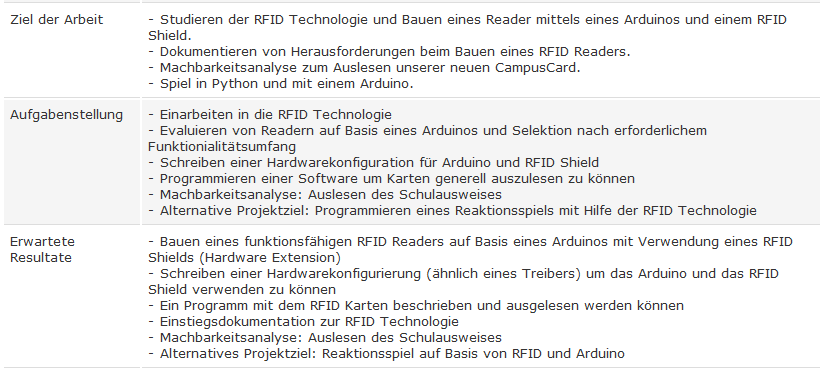


Abbildung 1: Aufgabenstellung

## Arbeitsplanung

In der ersten Phase wurden die Arbeiten in Stories aufgeteilt und der Aufwand wurde geschätzt. In dieser Phase konnte auch geklärt werden, dass das ursprüngliche Ziel (Auslesen eines Schulausweises) aus rechtlichen Gründen nicht sinnvoll als Semesterarbeit umsetzbar ist. Zum Design Review wurde entsprechend entschieden, dass stattdessen das Alternative Projektziel „Programmieren eines Reaktionsspiels mit Hilfe der RFID Technologie“ verfolgt wird. Aus diesem Grund fand zu diesem Zeitpunkt eine neue Arbeitsplanung über die restliche Zeit hinweg statt, welche hier in der Phase 2 festgehalten ist. Bis zu Projektende wurden 3 Sprints geplant und die Arbeitsschritte auf diese verteilt.

Die Aufwände wurden dabei jeweils in 2-Stundenblöcke (analog zur Pomodoro-Technik) unterteilt und über die zur Verfügung stehenden Wochen der Semesterarbeit verteilt. Der Fortschritt wurde in Jira festgehalten.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sprint** | **Jira Bezeichnung** | **Beschreibung** | **Aufwand in Stunden** |
| 1 | RFID-1 | Setup Projekt | 3 |
| 1 | RFID-2 | Learn Python (Code Academy) | 8 |
| 1 | RFID-3 | RFID einlesen Technologie | 8 |
| 2 | RFID-4 | Unterschiede der Arduino RFID Reader ausfindig machen | 6 |
| 2 | RFID-5 | Bestimmen genauer Typ Karte | 4 |
| 2 | RFID-6 | Erstellen des Auslesenscript & auslesen | 12 |

**Tabelle 1: Phase 1 des Projekts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sprint** | **Jira Bezeichnung** | **Beschreibung** | **Aufwand in Stunden** |
| 3 | RFID-7 | ReaFID-Funktion – konfigurieren von Karten | 8 |
| 3 | RFID-8 | ReaFID Funktion – lesen von Karten | 8 |
| 3 | RFID-9 | ReaFID Spiel Funktion - Zeitstoppen | 5 |
| 3 | RFID-12 | ReaFID Dokumentation | 10 |
| 3 | RFID-20 | ReaFID Project Management/Admine 1 | 1 |
| 4 | RFID-10 | ReaFID Spiel GUI – Spieloberfläche Hauptfenster | 15 |
| 4 | RFID-11 | ReaFID Spiel GUI – Abbrechen/Stoppen Spiel | 5 |
| 4 | RFID-13 | ReaFID Dokumentation 2 | 10 |
| 4 | RFID-21 | ReaFID Project Management/Admin 2 | 2 |
| 5 | RFID-14 | ReaFID Dokumentation 3 | 20 |
| 5 | RFID-22 | ReaFID Project Management/Admin 1 | 1 |
| Backlog | RFID-15 | ReaFID GUI – Topscorer Liste | 8 |
| Backlog | RFID-16 | ReaFID GUI – Spieloberfläche Kartekonfiguration | 12 |
| Backlog | RFID-17 | ReaFID GUI – Anzeige Auslesen Karte | 6 |
| Backlog | RFID-18 | ReaFID GUI – Menüpunkt Select Modus | 4 |
| Backlog | RFID-19 | ReaFID Spiel Advanced Mode erstellen | 20 |

**Tabelle 2: Phase 2 des Projekts**

## Seminarumsetzung

Für das Projekt galten folgende Termine:

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Termin** | **Beschreibung** |
| **1** | 24.03.14 | Kick Off |
| **2** | 29.04.14 | Präsentationstermin Security BSides London 2014 |
| **2** | 11.07.14 | Design Review |
| **3** | 12.09.14 | Abgabetermin |
| **4** | 05.11.14 | Präsentationstermin |
| **5** | 17.02.14 – 09.03.14 | Sprint 1 |
| **6** | 12.03.14 – 30.03.14 | Sprint 2 |
| **7** | 14.07.14 – 03.08.14 | Sprint 3 |
| **8** | 04.08.14 – 24.08.14 | Sprint 4 |
| **9** | 25.08.14 – 12.09.14 | Sprint 5 |

**Tabelle 3: Termine**

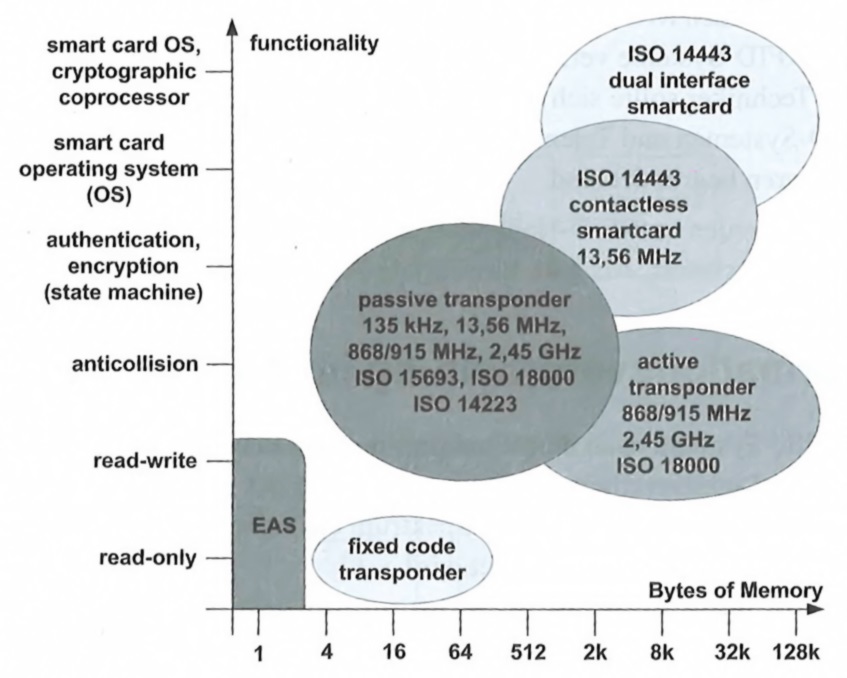
Zwischen Sprint 2 und 3 wurden nicht nur die rechtlichen Abklärungen getätigt, sondern auch ein 15 Minuten Vortrag für die BSides London („Rookie Track“) vorbereitet. Da diese Arbeiten nur die Erkenntnisse aus den technischen Abklärungen zu RFID und Arduino verwendeten und aufbereiteten, und nicht direkt für die Semesterarbeit waren, wurden diese nicht in Jira festgehalten und sind entsprechend nicht in der Projektplanung berücksicht. Die Informationen aus der Präsentation wurden allerdings in dieser Semesterarbeit miteinbezogen und beeinflussten entsprechend die Story „Dokumentation“ positiv.

# Über die eingesetzten Technologien

## RFID

### RFID Technologie und Einsatzgebiete

RFID steht für „radio-frequency identification“, was einer „Identifizierung mit Hilfe elektromagnetischer Wellen“ entspricht. Die Imlpementationen basieren dabei auf der „Low Frequency“ (9 kHz bis 135 kHz), „High Frequency“ (6,78 MHz, 13,56 MHz, 27.125 MHz, 40,680 MHz) oder dem „Ultra High Frequency“ (Europa: 865-869 MHz, USA/Asien: 950 MHz). Während frühere Implementationen (zum Beispiel für Zutrittssysteme von Gebäuden, Hotelzimmern, Verfolgen von Gegenständen) mit Low Frequency durchgeführt wurden, hat in den letzten Jahren der High Frequency einiges an Verbreitung gewonnen.



**Abbildung 2: Übersicht RFID Typen, aus dem RFID Handbuch - Finkenzeller, Abbildung 2.18**

In den meisten Systemen wird ein aktives Lesegerät und ein passiver Tag verwendet. Sobald der Tag in die Nähe des Lesegeräts gelangt, werden elektromagnetische Wellen erzeugt. Das Protokoll der Übertragung wird in diversen Standards festgelegt, welche inzwischen zum Teil ISO genormt sind. Hersteller verwenden allerdings aus „Sicherheitsgründen“, wobei es sich dabei mehr um „Security by Obscurity“ handelt, oft eigene Implementationsvarianten.

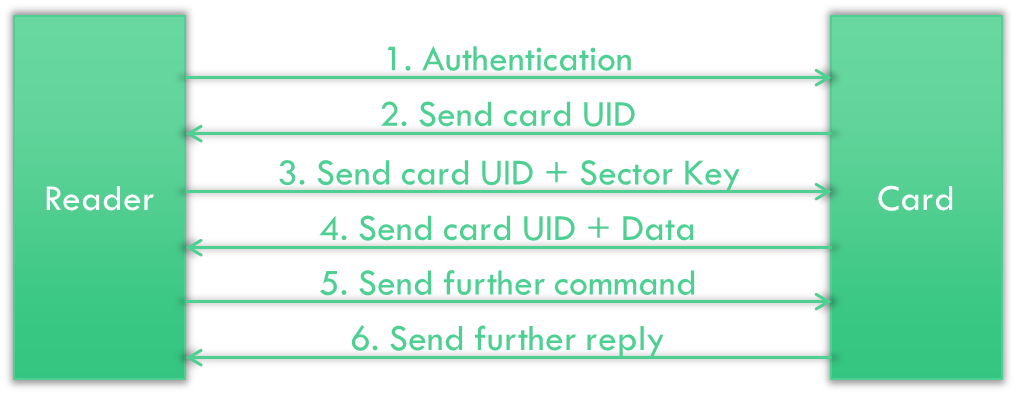
Durch eine zielgerichtete Recherche betreffend des Studentenausweises konnte einfach festgestellt werden, dass es sich bei dem bei uns verwendeten System um ein nach ISO 14443 auf der Frequenz 13,56 MHz festgelegten Standard handelt, wobei sich die ZHAW für die Implementation ohne Chip, also dem „Mifare Classik 1k“ Standard entschieden hatte.

Implementationen mit Chip sind einiges Leistungsfähiger als die ohne, so können zum Beispiel RFID Kreditkarten mit Chip für jede Transaktion einen neuen CVV Code generieren. Dies ist einer der Hauptgründe, warum das RFID Kreditkarten System mit „Chip und Pin“, so wie es in Europa verbreitet ist, einiges sicherer ist als das in den USA verbreitete ohne Chip.

### Mifare Standard

Die Tags welche im Mifare Standard verwendet werden, können in mehreren Formen erhalten werden. Für die Studentenausweise wird zum Beispiel die Form einer Karte verwendet. Die Norm für 1k Tags besagt, dass ein Tag 16 Sektoren hat, wobei jeder Sektor vier Blöcke enthält. Jeweils der letzte Block jedes Sektors enthält den „Access Key“, welcher für verschlüsselte Sektoren nötig ist. Pro Sektor kann es maximal zwei verschiedene Access Keys geben, wobei diese unterschiedliche Zugriffsberechtigungen besitzen können. Der erste Block (Block 0) enthält die UID der Karte und ist normalerweise schreibgeschützt. Karten mit veränderbaren UIDs sind relativ einfach über das Internet erhältlich. Falls ein Sektor verschlüsselt ist, wurde dafür die Crypto1 Verschlüsselung verwendet. Informationen zu dieser Verschlüsselung wurden schon vor Jahren am CCC präsentiert inklusive der Information, wie die verschlüsselten Inhalte tatsächlich ausgelesen werden können.

Die Authentisierung, welche per Sektor möglich ist, findet nach folgendem Schema statt:

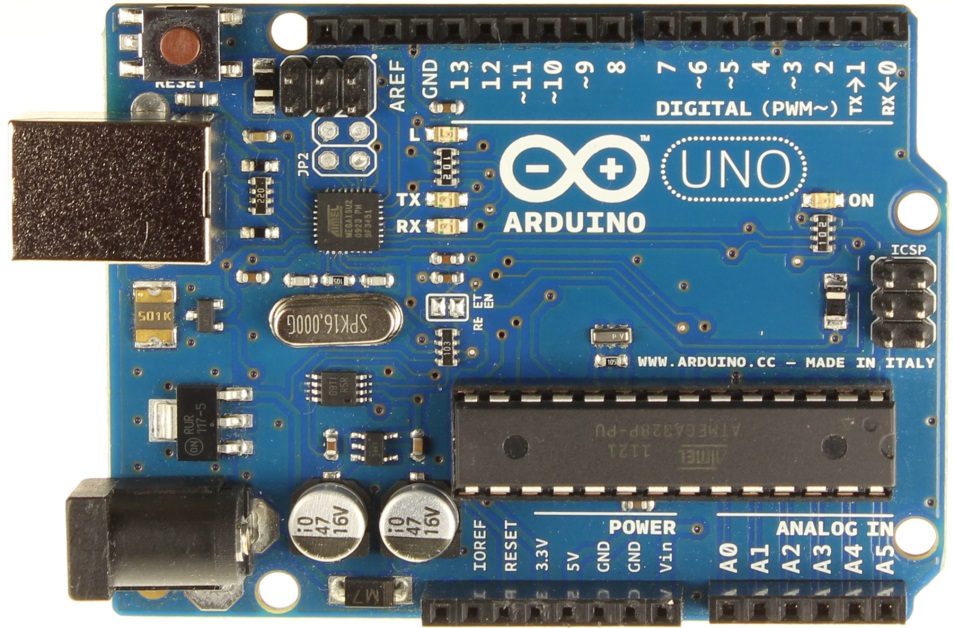


Bereits in den Protokoll Informationen wird der verwendete Sektor mitangegeben. Entsprechend ist dies eine Implementation welche auf dem Reader stattfindet.

Da es sich um eine drahtlose Kommunikation handelt, ist ein Angriff über Mithören der Übertragung und danach separate Abfrage möglich. Zudem können Karten geklont werden. Da die Verschlüsselung in Sicherheitskreisen als unsicher gilt, sind die darauf abge legten Informationen schlecht geschützt. Häufig wird aus diesem Grund bei Implementationen auf das abspeichern auf der Karte verzichtet und stattdessen jegliche Informationen auf dem „Backend System“ gespeichert. Bei der Prüfung der Karte wird lediglich die UID abgerufen und geprüft, ob diese im System konfiguriert ist. Jegliche Kontrollmechnaihanismen müssen entsprechend auf dem Backend System implementiert sein.

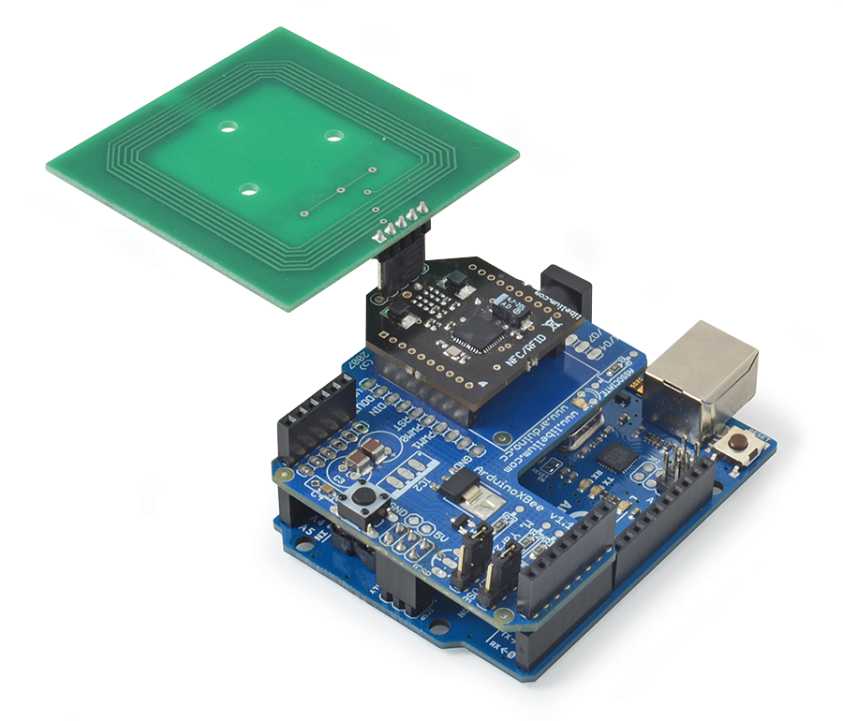
## Arduino

Ein Arduino ist eine Open Source Computerplattform, welche auf einem simplen Mikrokontroller (Atmel ATMEGA8) basiert und eine dazugehörige Entwicklungsumgebung mitbringt. Der Mikrokontroller kann Programme in Form einer daueraktiven Statemachine verarbeiten und wird deshalb oft für die Zusammenarbeit mit Sensoren jeglicher Art verwendet.



**Abbildung 3: Arduino UNO Version 3**

Um die Verknüpfung mit diesen Sensoren (welche generell als Input Systeme verstanden werden können) zu optimieren und Installationen weniger anfällig zu machen, wurden einige „Boards“ oder „Shields“ entwickelt, welche direkt auf das Arduino aufgesetzt werden können. Sie beanspruchen gewöhnlicherweise mehr Schnittstellen, machen die Installationen aber auch ein wenig robuster.



**Abbildung 4: Arduino UNO mit einem XBee RFID Shield**

Es gibt heute eine Vielzahl an Shields und Sensoren, welche über normale WLAN Interfaces, über RFID/NFC bis zu Feuchtigkeitsmesser gehen. Falls kein Shield vorhanden ist, können die Sensoren gewöhnlicherweise direkt oder mit Hilfe eines Breadboards angehängt und angesprochen werden. Starter Kits für Arduinos liefern nicht nur eine vielzahl solcher Sensoren mit sondern beinhalten auch detaillierte Anleitungen, wobei diese auch kostenlos Digital auffindbar sind.

Der Output findet normalerweise über Dioden, dem Computerbildschirm (über das serielle Interface) oder einem direkt angehängten Bildschirm statt.

## Python

Python ist eine relativ moderne Sprache (Erscheinungsjahr 1991) zu welcher Entwurfsphilosophie stark die Programmlesbarkeit und Einfachheit der Syntax gehört. In den letzten Jahren fand sie starke Verbreitung durch Online Lernprogramme wie von Codeacademy und den omnipräsenten Einsatz bei Google sowie anderen Open Source Projekten.

Die Sprache unterstützt mehrere Programmierparadigmen, unter anderem auch den Objekt orientierten und den strukturierten Ansatz. Durch diese Vielfältigkeit, kann ein zur Aufgabe passendes Paradigma ausgewählt werden, ohne das neue Syntax erlernt werden müssen.

Zusätzlich ist es hilfreich, dass für Python eine grosse Auswahl an Bibliotheken und Entwicklungsumgebungen existieren, so dass diese jeweils den Bedürfnissen angepasst werden können.

# ReaFID – Reaktionsspiel auf Basis von RFID und Arduino

## Einleitung

Um sich genügend mit der RFID Technologie, sowie Arduinos und Python auseinandersetzen zu können, wurde ein Spiel entwickelt, welches auf den gewählten Konzepten basiert. Die Spielidee wurde selber entwickelt, ist grundsätzlich aber für Kleinkinderspiele in ähnlicher Form Analog bekannt. Neu ist an der Idee, die Umsetzung über RFID durchzuführen. Zudem sind die Varation der Schwierigkeitsstufen in bekannten Implementationen nicht so auswählbar.

## Erfahrungsbericht

### Ausgangslage

Zu Beginn der Semesterarbeit hatte bereits ein initiales Kennenlernen betreffend Arduinos und RFID stattgefunden. Um allerdings die Technologien weiter kennen zu lernen, war ein Projekt nötig. Die Sprache Python wurde ausgewählt, da sie vielseitig einsetzbar ist und in Zukunft damit schnell Projektideen umgesetzt werden sollen.

Die Entwicklung wurde auf einer Arch Linux Installation durchgeführt, wobei als IDE Eclipse eingesetzt wurde. Zur Interpretation von Python wurde das Plugin PyDev verwendet. Das Arduino wurde über die dazu gelieferte IDE programmiert, die Arduino Ausgaben wurden über den Serial Port ausgelesen. Die Kommunikation zwischen RFID Reader und Python findet entsprechend auch über einen Seriellen Anschluss statt.

Zum Thema RFID und Arduino sind im Internet bereits einige Anleitungen und Codebeispiele zu finden. Auf der Basis der Anleitung von Cooking Hacks wurden die Hardwarekomponenten bestellt. Die Beispiel Skripte konnten für das auslesen von leeren RFID Karten verwendet werden. Um den Zugriff für das Spiel allerdings zu optimieren, wurden die Skripte minim angepasst.

Da es sich bei dem Projekt um ein Reaktionsspiel handelt, ist der Faktor Zeit eine wichtige Komponente. Für das Spiel wurde entsprechend das auslesen optimiert und der Handshake wird nach auslesen der Karten UID beendet. Ein verändern der RFID Karten oder der darauf geschrieben Daten findet für unser Spiel nicht statt. Dies ermöglicht es, die Spielkarten beliebig zu erweitern und zum Beispiel mit verschiedenen Studentenausweisen das Spiel durchzuführen. Andere Kategorien wurden in Bezug auf Studentenkarten als eine erste Idee in der Implementation berücksichtigt.

### Serielle Verbindung zum Arduino

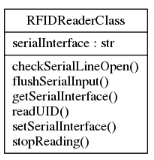
#### Implementation Arduino

Das Arduino erhält den Code über die Entwicklungsumgebung. Über eine IDE-interne „Hochladungsfunktion“ kann der erstellte Programcode auf das Arduino gespielt werden. Danach wird der programmierte Ablauf in einer ständigen Schlaufe ausgeführt. In unserer Schlaufe ist das das permanente Auslesen von UIDs der Karten, wobei diese entsprechend im Skript markiert werden damit sie anschliessend von Python ohne Probleme erkannt werden können.

Eine Herausforderung der Implementation war das übertragen von „Noise“, welches auch nach optimieren des Skripts nicht vollständig ausgeschlossen werden konnte.

#### Implementation Python

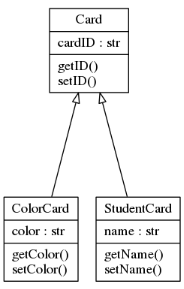
Auf Seite von Python wurde das Auslesen in der Python Klasse RFIDReaderClass realisiert. Dabei wird im Konstruktor der Zugriff auf das Serial Interface geöffnet und erst beim beenden des Spiels wieder entfernt. Um dabei keine parallelen Zugriffe zu erlauben, wurde diese Klasse als Singleton implementiert.



### Entwickeln der Spiellogik

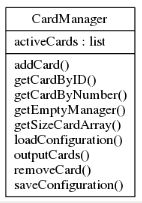
#### Managen der Karten

Bei der Implementation wurden zuerst jegliche Hilfsklassen implementiert. Über ein Factory Pattern wurde so das generieren von Objekten für die RFID Karten abgelegt.



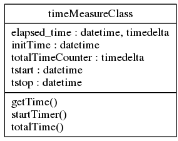
Der Sinn davon war, dass beim Erstellen ein anderer Typ von Karte erzeugt wird und danach jeweils mit Hilfe einer Typenprüfung die richtige Methode aufgerufen wird. So sollen einfach weitere Klassen für weitere Typen von Karten bei Bedarf hinzugefügt werden.

Die Karten selber werden dabei über den CardManager verwaltet. Nur diesem ist es möglich, Karten zu aktivieren, sie zu suchen, zu entfernen oder auszulesen, wie viele Karten überhaupt vorhanden sind.



#### Zeitmessfunktion

Das messen der Zeit wurde in der Klasse timeMeasureClass realisiert. Die separate Klasse ermöglicht eine einfache Kapselung der Funktion und wird nur bei Bedarf vom aktiven Spiel Modus aufgerufen.



### Entwickeln des GUI

#### Analyse

#### Eingesetzte Pattern

## Fazit

## Ausblick

# Diskussion des eignen Beitrags

## Studieren der RFID Technologie und Bauen eines Reader mittels eines Arduinos und einem RFID Shield

## Dokumentieren von Herausforderungen beim Bauen eines RFID Readers

## Machbarkeitsanalyse zum Auslesen unserer neuen Campus Card

## Spiel in Python und mit einem Arduino

# Literaturverzeichnis

|  |  |
| --- | --- |
| Nr. | Verweis |
| L1 | RFID Handbuch von Klaus Finkenzeller: ISBN 978-3-446-42992-5 |
| L2 | Link zu Vortrag an der BSides London: <http://www.youtube.com/watch?v=MGPGv2HnGtU> |
| L3 | Link zu den Slides des Vortrags an der BSides London: <http://www.slideshare.net/d3sre/bsideslondon-rookie-talk-rfid-hacking-an-introduction> |
| L4 |  |
| L5 |  |
| L6 |  |
| L7 |  |
| L8 | Bild Arduino R3 Front: <http://arduino.cc/en/uploads/Main/ArduinoUno_R3_Front.jpg> |
| L9 | Bild Arduino mit Xbee RFID Shield:http://www.cooking-hacks.com/documentation/tutorials/rfid-13-56-mhz-nfc-module-for-arduino |
| L10 |  |
| L11 |  |
| L12 |  |
| L13 |  |
| L14 |  |

Tabelle : Literaturverzeichnis

# Anhang

## Glossar

| ID | Begriff | Beschreibung |
| --- | --- | --- |
| G1 |  |  |
| G2 |  |  |
| G3 | Pomodoro Technik | Methode zum Zeitmanagement, welche Arbeiten in Blöcke unterteilt und Pausen miteinrechnet. Das System wurde für die vorliegende Arbeit angepasst und stattdessen mit zweimal 60-Minutenblöcken gearbeitet.  Siehe: <http://de.wikipedia.org/wiki/Pomodoro-Technik> |
| G4 | Scrum | Agiler Projektmanagementprozess basierend auf Iterationen mit festen Iterationsfenstern.  Siehe: <http://de.wikipedia.org/wiki/Scrum> |
| G5 | Kanban | Agiler Projektmanagementprozess, der ebenfalls wie Scrum mit Iterationen arbeitet, allerdings nicht feste Iterationsfenster nutzt, aber die Anzahl in Bearbeitung befindlicher Tasks limitiert.  Siehe: <http://de.wikipedia.org/wiki/Kanban> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Tabelle : Glossar