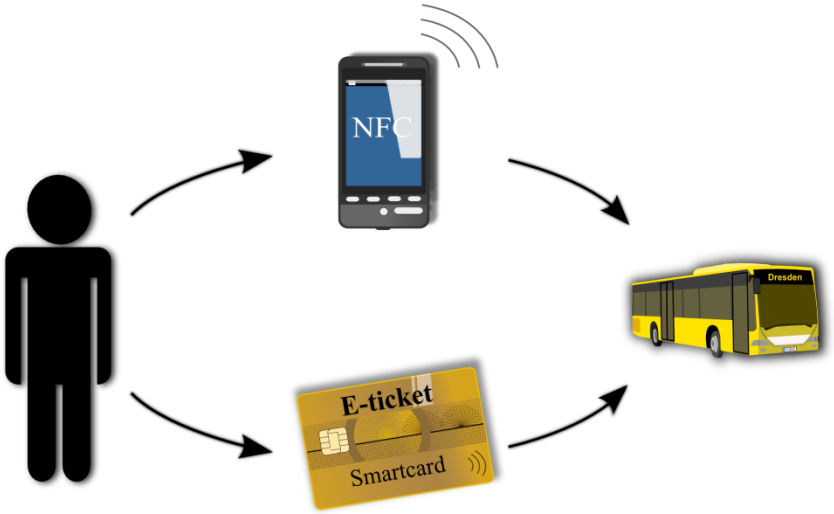
Datenschutzfreundliche eTicketing-Systeme basierend auf RFID/NFC



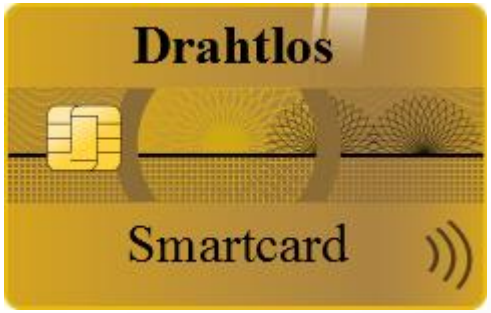
Ivan Gudymenko
Manuel Weißbach
Felipe Sousa

Einführung

NFC/RFID-Systeme, Datensicherheit und Datenschutz

Worum es geht

- Systeme basierend auf
  - NFC (Near Field Communication, oder Nahfeldkommunikation)
  - RFID (Radio Frequency Identification, proximity coupling – Nahfeld)
- Heutzutage hat es fast jeder (ggf. ohne es zu wissen)
- Häufig als „allgegenwärtige Systeme“ bezeichnet



Herausforderungen

- Trotz der zahlreichen Vorteile, eine **Reihe von Herausforderungen**
- ***IT-Sicherheit***
- ***Datenschutz (Privacy)***

} **JEDER IST BETROFFEN!**

In der Öffentlichkeit

heise Security

News Hintergrund Erste Hilfe

Security > Angriffsziel Smartphone

Angriffsziel Smartphone

21.10.2010

iPhone und Android-Smartphones sind zu mobilen Taschencomputern avanciert, deren Besitzer damit oft häufiger im Netz unterwegs sind, als mit dem heimischen PC. Somit wird das Smartphone für Kriminelle zur lukrativen Zielscheibe, um dem Nutzer Zugangsdaten zu Diensten, Kreditkartendaten und andere wertvolle Informationen zu stehlen.

Die Artikel "Mobile Bedrohungen - Spionageangriffe und Abzocke auf Android und iPhone" und "Ungesicherte Einsichten - Sicherheit von Apps für Android und iPhone" setzen sich mit der Sicherheit der Plattformen sowie der darauf laufenden Anwendungen auseinander. Sie zeigen, welche technischen und organisatorischen Maßnahmen die Hersteller ergriffen haben, um Angriffen Einhalt zu gebieten, wie erfolgreich diese sind und wie man sich und sein Gerät selbst schützen kann.

In der Öffentlichkeit (2)

heise Security

News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2014 > KW 24 > Vorinstallierte Spionagesoftware auf China-Smartphones

14.06.2014 06:00 « Vorige | Nächste »

Vorinstallierte Spionagesoftware auf China-Smartphones

vorlesen / MP3-Download

Auf einer billigen Kopie des Samsung Galaxy S4 ist ab Werk installierte Spionagesoftware entdeckt worden. Diese lässt sich so gut wie nicht entfernen, kann alle persönlichen Daten des Nutzers kopieren und Anrufe belauschen.

Sicherheitsforscher von G Data haben vorinstallierten Schadcode in der Firmware des Smartphones Star N9500 entdeckt. Der Trojaner erlaubt es, die Nutzer des Handys umfassend auszuspionieren: persönliche Daten können uneingeschränkt kopiert und Gespräche mitgehört werden. Auch das Mikrofon kann beliebig aus der Ferne eingeschaltet werden und verwandelt das Handy auf Kommando in eine Wanze. Das Star N9500 ist eine kostengünstige Kopie des Samsung Galaxy S4, die weltweit bei verschiedenen Online-Händlern für 130 bis 165 Euro vetrieben wird.

Dieses Handy hat's in sich: Vorinstallierte Malware, die der Benutzer nicht loswerden kann

Bild: Go4Android

Käufer werden ans Messer geliefert

Bei Untersuchungen nach Testkäufen des Gerätes

In der Öffentlichkeit (3)

heise Security

News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2012 > KW 30 > Android- und Nokia-Smartphones per NFC übernommen

26.07.2012 13:05

« Vorige | Nächste »

Android- und Nokia-Smartphones per NFC übernommen

vorlesen / MP3-Download

Der Sicherheitsspezialist Charlie Miller hat auf der Hackerkonferenz Blackhat in Las Vegas demonstriert, wie gefährlich der Nahfunkstandard NFC sein kann, der bereits in viele Smartphones integriert ist: Es gelang ihm, die Smartphones verschiedener Hersteller über NFC mit Schadcode zu infizieren – und zwar ohne Eingreifen des Handybesitzers.

In der Öffentlichkeit (4)

Technology Review
DAS MAGAZIN FÜR INNOVATION

JOBS KONGRESS NACHWUCHSPREIS FORUM

ENERGIE INFOTECH LEBEN PR

Technology Review > Infotech > Alles funkt

Alles funkt

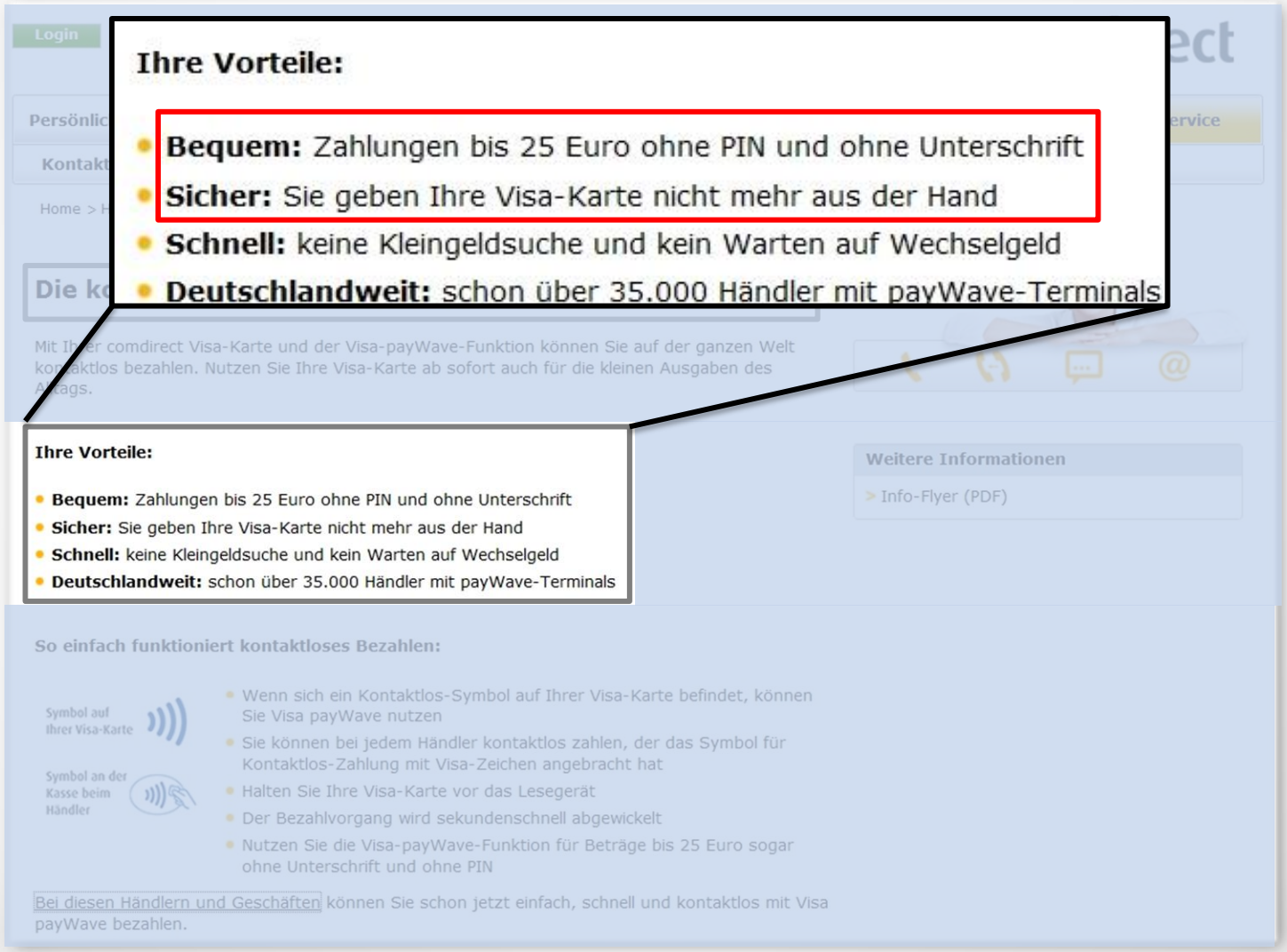
20.09.2013 – **Boris Hänßler**

Es war die Dauervision des neuen Jahrtausends. Nun ist es Realität: Das Internet der Dinge verbindet Geräte, Maschinen und Produkte über das Web. Bislang etabliert sich die Vernetzung vor allem hinter den Kulissen der Unternehmen – doch Verbraucher sollten sich schon mal damit vertraut machen.

…nicht jedem bekannt!

Visa PayWave)))

Visa PayWave)))



Kartennumer Auslesen

02.07.2014 15:44 « Vorige | Nächste »

Betrug mit Online-Zugtickets: Bahn um hunderttausende Euro geprellt

vorlesen / MP3-Download

Die Online-Tickets wurden mit gestohlenen Kreditkartendaten bezahlt: Vier Verdächtige aus Hamburg sitzen wegen eines groß angelegten Betrugs in U-Haft. Der Schaden für die Deutsche Bahn ist hoch.

Vier junge Männer aus Hamburg sollen die Deutsche Bahn durch den Betrug mit Online-Tickets um rund 700.000 Euro geprellt haben. Die 18 bis 26 Jahre alten Verdächtigen sitzen wegen Verdachts des banden- und gewerbsmäßigen Computerbetrugs in Untersuchungshaft, wie der Sprecher der Hamburger Staatsanwaltschaft, Carsten Rinio, am Mittwoch sagte.

Inhärente Trade-Offs

- Sicherheit vs. Funktionalität und Bequemlichkeit
- Sicherheit vs. Datenschutz
  - Ein Extrembeispiel: Der Überwachungsstaat

NFC/RFID Funktechnologien: Anwendungsbereiche

- Dutzende Systeme setzten darauf
  - Banking-Karten
  - Smart-Poster, usw
- Unter anderem ÖPNV (eTicketing)

Datenschutzfreundliche eTicketing-Systeme im ÖPNV

• • •

eTicketing-Systeme im ÖPVN, Datenschutzprobleme,

unsere Lösung

eTicketing-Systeme: ÖPNV

[Courtesy of Münstersche Zeitung]

Haupttypen

- Check-in/Check-out basiert
  - Ermöglichen monatliche Abbrechung
- Abo-basiert (wie etwa in Dresden)
  - Das eTicket mit sich führen und bereit für die mögliche Kontrolle sein

Was ist ein eTicket

- Eine digitale Version von der ÖPNV-Fahrberechtigung
- Gespeichert als eTicket auf dem Nutzermedium
- Nutzermedium:
  - Smartcard (auch Visa PayWave)
  - NFC-fähiges Smartphone

Reale eTicketing-Systeme

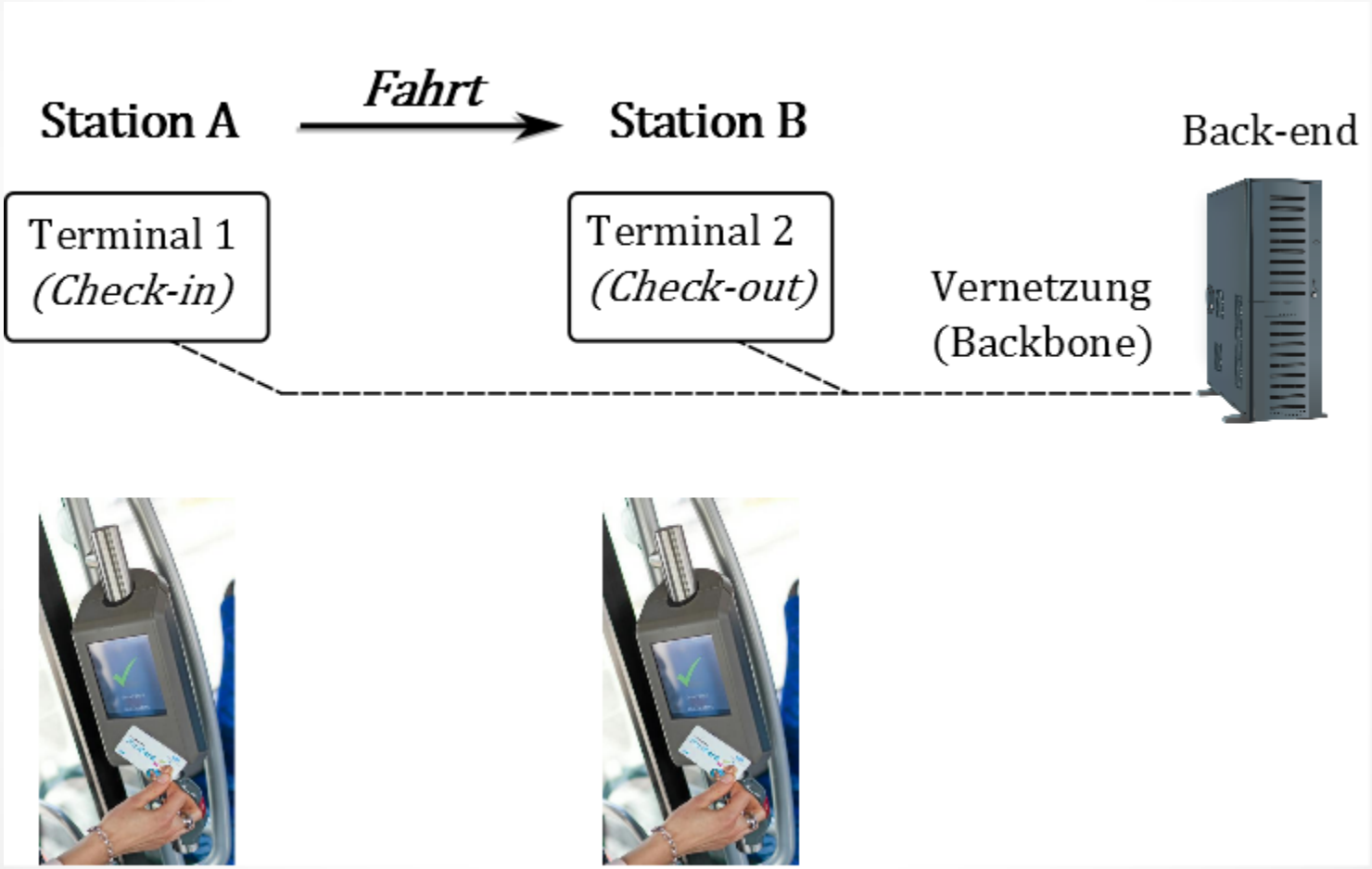
- OV-Chipkaart in den Niederlanden
- London Oyster Card
- EZ-Link in Singapore
- Octopus Card in Hong-Kong
- Bilhete Único, São Paulo, Rio de Janeiro

Bilhete Único, Rio

Bilhete Único, Rio

Bilhete Único, Rio

Systemarchitektur

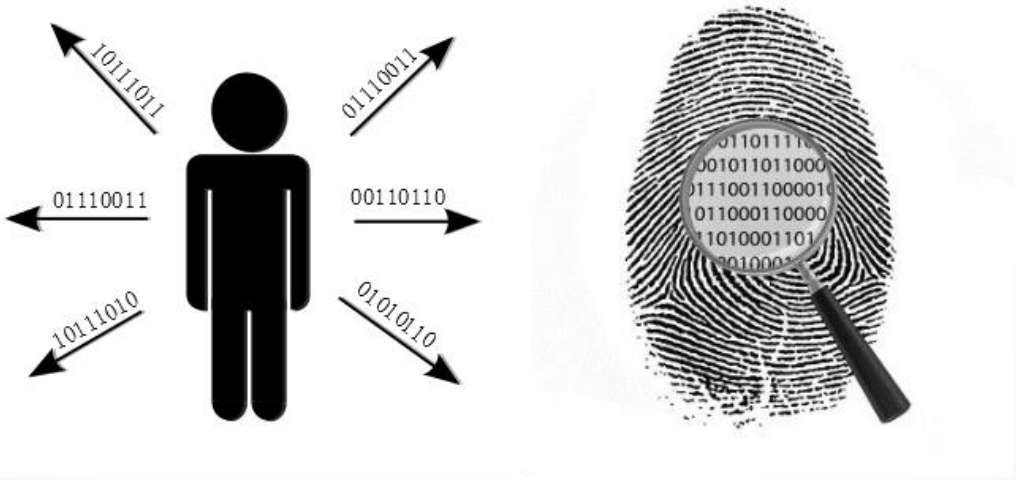


eTicketing-System: Anforderungen

- Datenschutz (Privacy)
  - Untraceability (keine Verfolgung)
  - Unlinkability (Unverkettbarkeit)
  - Pseudonymity/Anonymity (Pseudonymität/Anonymität)
- Sicherheit
  - Integrität (transactions integrity);
  - Verfügbarkeit (availability), usw.
- Funktionalität
  - Detaillierte Abrechnung
  - Effizienz (vor allem im Front-End)

Datenschutz im ÖPNV

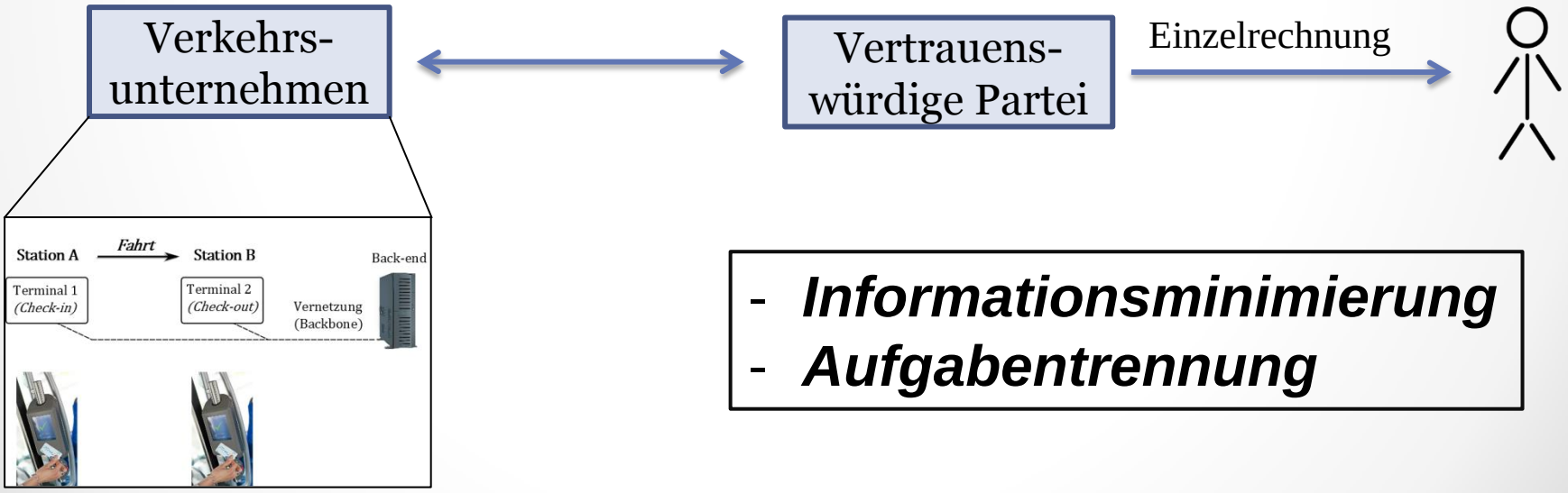
- Ubiquitäre Systeme – allgegenwärtige Datenspuren!
  - Vor allem im Frontend → das Beispiel mit der Visa Karte!
- Anonymität/Pseudonymität gegen die ÖPNV-Unternehmen und Drittparteien



Unsere Lösung

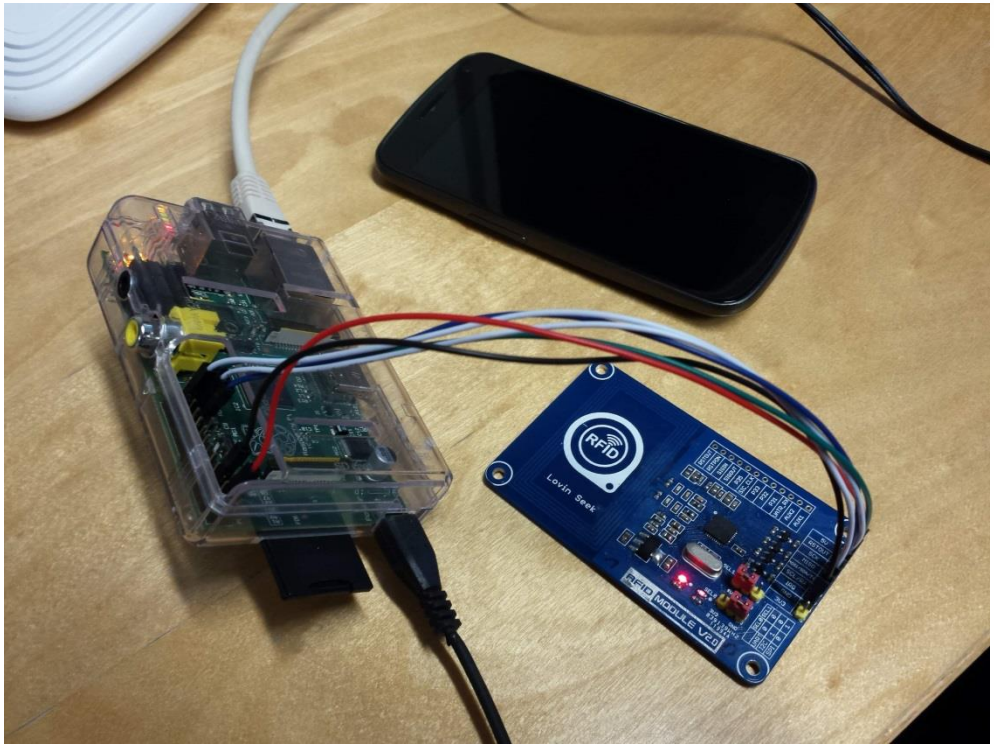
- Kennt die Fahrtenprofile
- Kennt die Nutzer nicht
  - (Pseudonymisierung)
- Die Terminals könnten zwischen den Nutzern nicht unterscheiden

- Kennt die Nutzer (kann identifizieren)
- Kennt die Fahrtenprofile nicht



- ***Informationsminimierung***
- ***Aufgabentrennung***

Implementierung: Demo



- Terminal:
  - PN532 Breakout Board via SPI auf
  - einem Raspberry Pi Model B 256MB RAM
- Nutzermedium:
  - NFC Smartphone:

    Samsung Galaxy Nexus GT-I9250

Zusammenfassung

- Datenschutz und Datensicherheit in Systemen basierend auf NFC/RFID:
  - Eine Reihe von Herausforderungen und viele offene Fragen
  - Keine einheitliche Lösung ist vorhanden (leider)
- Die ÖPNV-eTicketing-Systeme sind keine Ausnahme
  - Unsere datenschutzfreundliche Lösung wurde kurz vorgestellt

Glückwunsch! Sie haben es geschafft! ☺

• • •

Fragen? Anmerkungen? Vorschläge?

(Sie dürfen jetzt aufwachen)