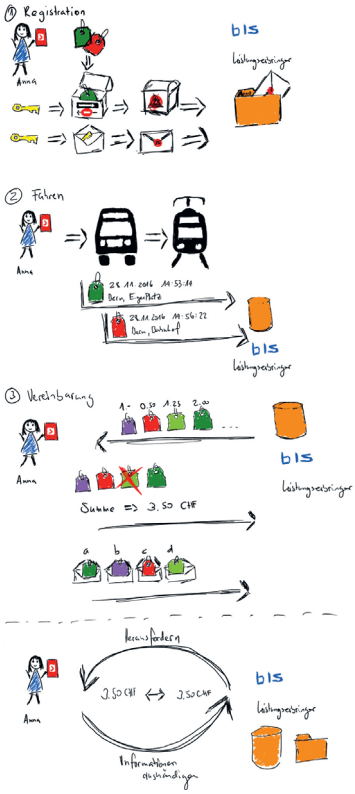
Schutz des Bewegungsprofils in der Mobility Pricing-Anwendung Lezzgo

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Dr. Eric Dubuis
Experte: Xavier Monnat (Post CH AG)

Aufgrund des stetigen Wachstums des Verkehrs kommt es besonders während den üblichen Verkehrszeiten zu Engpässen. Die Durchführung diverser Pilotprojekte soll mit Hilfe von Mobility Pricing eine gleichmässigere Auslastung sowohl auf der Schiene wie auch auf der Strasse erreichen.

Ausgangslage

Basis solcher Pilotprojekte sind Smartphone-Applikationen, welche es erlauben die öffentlichen Verkehrsmittel zu benutzen, ohne vor Fahrtantritt eine Fahrkarte oder ein Abonnement zu kaufen. Eine dieser Applikationen ist Lezzgo der BLS. In dieser checkt der Benutzer vor dem Einsteigen in das Verkehrsmittel ein und startet somit die Aufzeichnung. Nach der Fahrt signalisiert er durch das Auschecken dessen Beendigung. Auf Basis der aufgezeichneten Daten berechnet der Leistungserbringer die effektiven Kosten und stellt diese dem Kunden in Rechnung.
Die Erfassung der Fahrwege und -zeiten sowie die Möglichkeit, diese Daten dem Kunden zuordnen zu können, erlauben es dem Leistungserbringer Bewegungsprofile zu erstellen und diese zu seinen Gunsten auszunutzen. Es stellt sich also die Frage, wie die Daten geschützt werden können, um die Generierung solcher Bewegungsprofile zu verhindern.



Darstellung der drei Phasen des VPriv-Protokolls.

Lösungsansatz

Das sogenannte VPriv-Protokoll von Raluca Ada Popa, Hari Balakrishnan und Andrew Blumberg verspricht die Wahrung des Datenschutzes soweit, dass der Leistungserbringer nie weiss, welche Aufzeichnungen zu welchem Kunden gehören. Initial wird dabei in der Phase vor Fahrtantritt ein definierter Datenbestand generiert und durch kryptografische Mechanismen verändert zum Leistungserbringer übertragen. Während der Fahrphase wird regelmässig, zusammen mit Zeitstempel und Standortaufzeichnungen (zum Beispiel GPS-Koordinaten), ein zufälliger Schlüssel aus dem Datenbestand des Kunden an den Leistungserbringer übertragen.
Die Kostenberechnung erfolgt auf dem Smartphone des Kunden und wird dem Leistungserbringer für die Rechnungsstellung mitgeteilt. Die Richtigkeit der Berechnung ermittelt der Leistungserbringer durch die Herausforderung des Smartphone des Kunden anhand eines Rundenprotokolls. Es werden seitens Kunden nur Daten bekannt gegeben, damit die Berechnung bestätigt werden kann, der Leistungserbringer aber nicht die Zugehörigkeit der Daten zum Kunden definieren kann.

Prototyp

Im Rahmen dieser Bachelor-Thesis wurde eine Client-Server-Applikation in Java umgesetzt, welche das VPriv-Protokoll implementiert und als Simulation Fragen bezüglich technische Implementierung, Machbarkeit, Datenmenge und Datenschutz beantwortet. Eine Unterbrechung der Simulation nach jeder Phase bietet weiter die Möglichkeit, den Datenbestand auf der Seite des Leistungserbringers zu analysieren, um die fehlende Zuordnung der Daten zum Endbenutzer zu beweisen.

Fabian Hutzli