Simulation eines Road-Pricing Systems

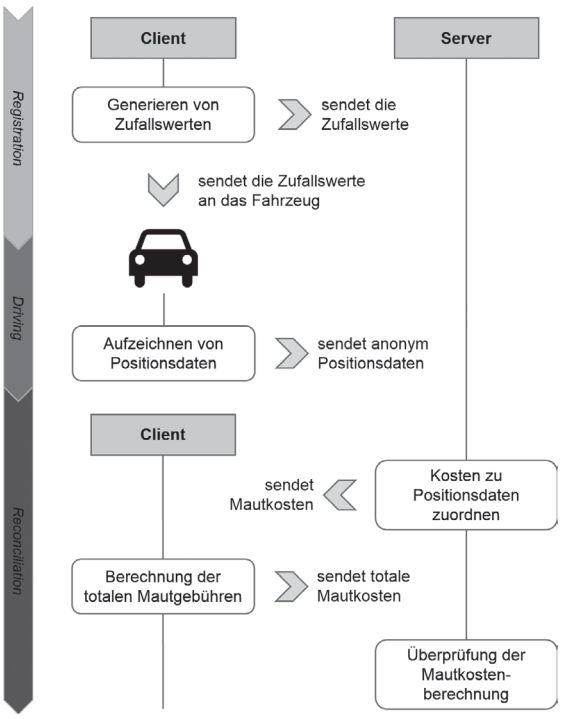
Fachgebiet: IT Security
Betreuer: Prof. Dr. Eric Dubuis
Experte: Stefan Berner (Diso Solution AG)

In der Schweiz wird aufgrund des zunehmenden Verkehrs über die Einführung eines Road-Pricing Systems politisch diskutiert. Ein solches Gebührensystem hat insbesondere zum Ziel, die Verkehrsteilnehmer verursachergerecht an den Kosten zu beteiligen und den aufkommenden Verkehr zu verringern. Ein Road-Pricing System nach dem VPriv Verfahren schützt die Privatsphäre des Fahrzeuglenkers mit Hilfe der Kryptographie. Im Rahmen der Bachelorarbeit wurde eine Verkehrssimulation mit integriertem Mautsystem programmiert.

Ausgangslage

Unter dem Begriff **Road-Pricing** versteht man das Erheben von Gebühren für die Benützung von Strassen. In bereits vorhandenen Mautsystemen werden die Fahrzeuge erfasst und die Daten zentral ausgewertet. Die standortbezogene Privatsphäre ist bei den eingesetzten Systemen nicht gewährleistet.

Ein Road-Pricing System erfasst die zurückgelegte Strecke eines Fahrzeuges und berechnet die entsprechenden Mautgebühren. Einerseits muss der Staat die Gebühren korrekt berechnen können, andererseits darf er keine Kenntnisse haben über Zeitpunkt und zurückgelegten Weg eines Fahrzeuges. Mit Hilfe moderner Kryptographie lässt sich diese Diskrepanz lösen. Die standortbezogene Privatsphäre ist gewährleistet.



VPriv Protokollablauf

VPriv Verfahren

Das **VPriv Verfahren** bietet eine mögliche Lösung diese Anforderungen zu erfüllen. VPriv wurde am Massachusetts Institute of Technology MIT entwickelt und in der Fachliteratur veröffentlicht.

Der VPriv Protokollablauf beinhaltet drei Phasen. Während der **registration phase** wird das Fahrzeug beim Server registriert. Die nötigen Daten für den Betrieb des Systems werden generiert. In der **driving phase** zeichnet das Fahrzeug Positionsdaten auf. Diese Daten werden anonym dem Server übermittelt. Den Protokollabschluss bildet die **reconciliation phase.** Am Ende der Rechnungsperiode überprüft der Server mit dem Rundenprotokoll die Korrektheit, der durch den Fahrzeughalter übermittelten Daten.

Ergebnis der Bachelor Thesis

Im Rahmen der Bachelor Thesis wurde das VPriv Verfahren studiert und mittels einer Verkehrssimulation mit integriertem Road-Pricing System umgesetzt. Die programmierte Simulationsanwendung dient zur detaillierten Demonstration von VPriv. Der Schutz der Privatsphäre des Autofahrers wird aufgezeigt, indem die auf dem Server vorhandenen Daten denjenigen des Clients gegenübergestellt werden.

Fazit

Das VPriv Verfahren ist eine mögliche Alternative zu den heute im Einsatz befindlichen Road-Pricing Systemen, hat jedoch den Nachteil, dass der gewonnene Schutz der standortbezogenen Privatsphäre ein Reduktion der Benutzerfreundlichkeit zur Folge hat.

Daniel Brönnimann

Michael Gautschi