Privacy-Preserving Electronic Toll Pricing

Abschlusspräsentation PAWI Projekt

Horw, 13. Februar 2012

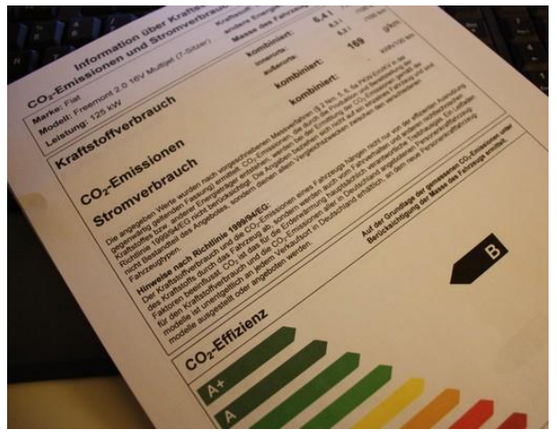
Christoph Moser, Thomas Galliker

Agenda

- **Einführung Strassenfinanzierung**
- **Privacy-Preserving Electronic Toll Pricing**
- **Umsetzung des PrETP Prototypen**
- **Demonstration**
- **Diskussion & Fazit**
- **Fragen & Antworten**

Einführung Strassenfinanzierung
Situation Schweiz

- **Aktuelle Strassenbenutzungsgebühr**



- **Ziele durch den Einsatz eines Road-Pricing Systems**
  - Verkehrsproblem in den Städten und Agglomerationen entschärfen
  - Finanzierung der Strasseninfrastruktur sicherstellen

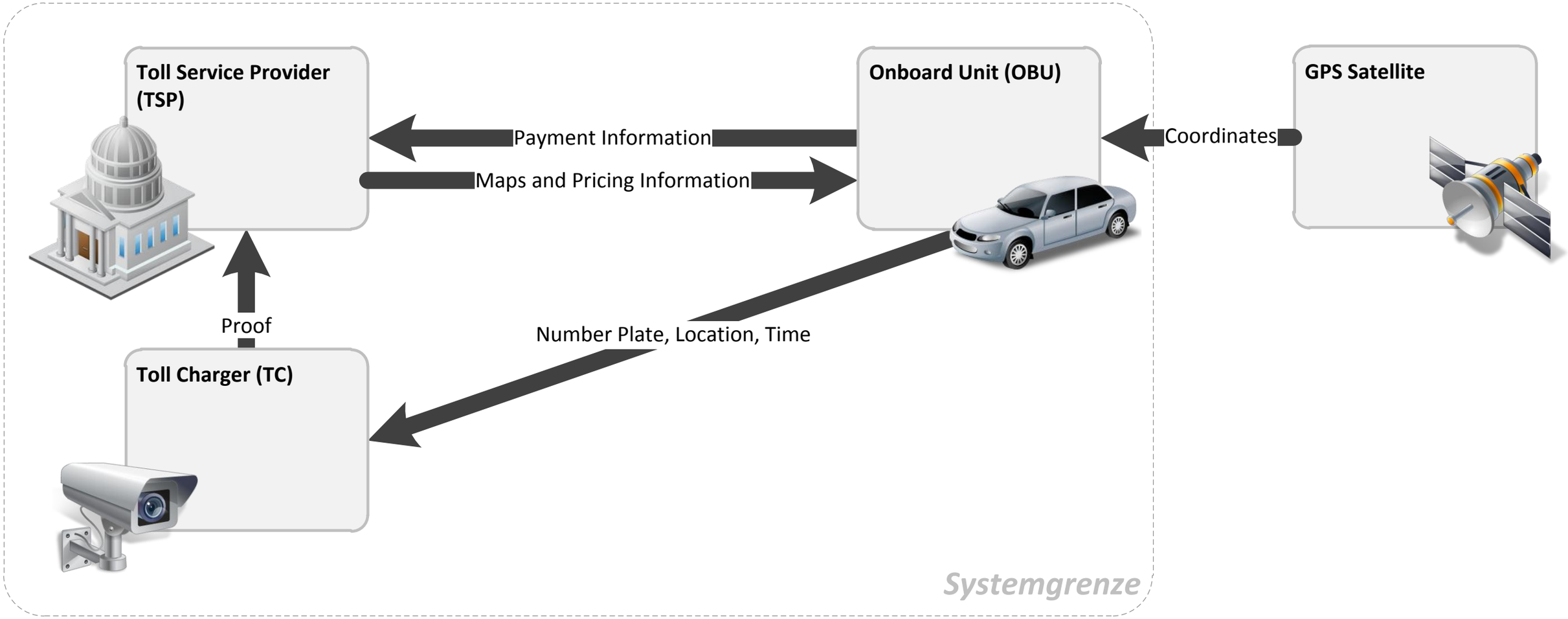
Einführung Strassenfinanzierung
Pläne der Europäischen Union

- **Aktuelle Situation**
  - Schwerverkehr

  - Mautstationen

- Die EU hat im Oktober 2009 entschieden ein **einheitliches Road Pricing System** einzuführen

Privacy-Preserving Electronic Toll Pricing
Systemübersicht



Privacy-Preserving Electronic Toll Pricing
Allgemeine Funktionsweise

- TSP definiert **Rahmenbedingungen** für Betrieb
  - Tarifzonen und Preis Profile
  - Parameter für Kryptofunktionen
- OBUs zeichnen **Wegpfade** auf und verrechnen diese segmentweise mit den gegebenen Preis Profilen
- TSP erhält von TCs **Positions-/Zeitnachweise** für Fahrzeuge
- Während einer Abrechnungsphase liefert OBU **verschlüsselte** Positions-/Zeit- und Preisinformationen an TSP
- TSP prüft mit Positions-/Zeitnachweisen die **Korrektheit der Abrechnungsinformationen**

Privacy-Preserving Electronic Toll Pricing
Interessensschutz

- **Interessen des Staats**
  - Mobilitätsproblem
  - Strassenfinanzierung
  - Gewährleistung der Rechtssicherheit

- **Interessen der Anwender**
  - Mobilitätsproblem
  - Ökonomisches Fortbewegen
  - Schutz der Privatsphäre

- **Interessen der Industrie**
  - Neue Absatzmärkte

Privacy-Preserving Electronic Toll Pricing
Arten von Missbrauch

- Fahren mit **deaktivierter OBU**
  - Fehlende Commitments für Lokation/Zeit auf TSP
  - Challenge-Proofs können nicht bestätigt werden

- GPS **Wegpfade** manipuliert
  - Vergleich von Proofs mit Location/Time Commitments

Privacy-Preserving Electronic Toll Pricing
Arten von Missbrauch

- **Falsche Preise** für Segmente verrechnet
  - Preise für Tarifzonen werden von TSP signiert
  - Challenge-Proofs liefern die signifikante Position/Zeit sowie das Commitment-Opening und den Preis zurück
- Falsche Berechnung der **Gesamtsumme**
  - Homomorphe Commitments: Produkt der einzelnen Commitments muss mit dem Commitment der Summe übereinstimmen

Umsetzung des PrETP Prototypen
Optimistic Payment

TSP

1.0 **Initialisierung des Security Managers**

2.0 **Group Parameters für OBU generieren**

3.0 **Optimistic Payment Anfrage lancieren**

OBU

1.0 **Neuer Wegpunkt festhalten**

2.0 **Neuer Payment Record erzeugen**

3.0 **Optimistic Payment Prozess ausführen**

Umsetzung des PrETP Prototypen
Proof-Challenge

- Beweise werden laufend erfasst

- Nach erfolgten Optimistic Payment Prozess werden die erfassten Beweise geprüft

Umsetzung des PrETP Prototypen
Design-Entscheide

- **GPS Lokalisierung**
  - Aufzeichnungsintervall ist abhängig von der Fahrtgeschwindigkeit
  - Anlegen von GPS Wegpunkten und Payment Records verursacht hohen Rechenaufwand
- **Preisberechnungsfunktion**
  - Distanz zwischen zwei Punkten berechnen
  - Kartenzugehörigkeit des Punktes bestimmen
  - Zonentarif für Map abfragen

Demonstration

Generelle Vorgehensweise:

Wegpunkte aufzeichnen → Challenge erfassen → Optimistic Payment Prozess starten → Proof-Challenge starten

Fall 1: Abrechnung mit korrekten Daten

– Erwartetes Resultat: Alle Verifikationen korrekt.

Fall 2: Payment Record mit ungültigem Preis

– Erwartetes Resultat: TSP erkennt, dass OBU einen nicht-TSP-signierten Preis verwendet hat.

Demonstration

Fall 3: Abrechnung mit falschem Totalpreis

– Erwartetes Resultat: Commitments der Payment Records stimmt nicht mit Commitment der Totalsumme überein.

Fall 4: Abrechnung mit manipulierten GPS Daten

– Erwartetes Resultat: OBU kann keinen passenden Wegpunkt finden und liefert daher keine Antwort an TSP

Diskussion & Fazit

- **Schwierigkeit** einer praktischen Umsetzung
  - Nachweisbarkeit von Manipulationen
  - Umgang mit Funkschatten
  - Positionierung der Toll Charger
  - Zeitsynchronisation (TC←→OBU)

- **Vorteile**
  - Datenschutz gewährleistet
  - Finanzierung der Strasseninfrastruktur gesichert
  - Dynamisches Preismodell erlaubt Verkehrsproblem zu entschärfen

Danke für Ihre Aufmerksamkeit.

Haben Sie Fragen?