# Road Pricing Architectures

Bart Jacobs

Institute for Computing and Information Sciences, Radboud University Nijmegen
www.cs.ru.nl/B.Jacobs

*SURFcert & SURFibo*, The Hague, 4/2/2010





## Outline







## Variations in road pricing

- Zone-based
  - for instance in London & Stockholm
  - based on Automatic Number Plate Recognition (ANPR)
- Point-to-point
  - on motorways in France, Italy, . . .
  - via (electronic) gates
  - since 2005 in Germany for trucks (*LKW-Maut*, via DSRC)
- Pay-as-you-drive
  - First in NL, later possibly elsewhere (Be, EU, . . . )
  - Satellite-based (GPS, Galileo)





## Pay-as-you-drive road pricing

- Replaces “flat road tax” by “distance related pricing”
- Pricing may depend on:
  - type of road
  - type of car (esp. emission characteristics)
  - time of day (esp. rush hour, via *spitstarief*)
  - location
- Aims, apart from fairness,
  - congestion steering/reduction
  - environmental impact reduction
- More refined steering & control possible than with fuel price.





## Issues in road pricing

- Reliability
- Cost-effectivity (aim in NL: overhead < 10%)
- Ease of use / transparancy
- Fraud resistance (e.g. GPS can be manipulated/shielded, power supply can be interrupted, . . . )
- Ease of enforcement
- Ease of dispute resolution
- Security (protection against attacks, manipulation, . . . )
- Privacy
- User acceptance, requiring trust!

There will be many hostile users





## Road pricing: technical set-up

- Cars get a special box, called **OBE**, for “on-board equipment”, or in Dutch: *registratievoorziening*.
- . . . which can at least:
  - determine its own position, via GPS or Galileo
  - communicate with backoffice, via GSM, GPRS, Wifi, . . .
  - calculate & store data
- Tariff map needed for fee calculation on basis of “trajectory parts”

## Big Question

- Where to store trajectory information?
  - in the back-office of the authorities / service providers
    (who use it for billing and/or marketing/profiling)
  - in the vehicle, i.e. in the OBE
    (so OBE contains map-data for aggregation)
- This is an architectural decision about information flow
- But also about division of power in society
  (balance citizen – state)

Architecture is politics
(M. Kapor, EFF)





## Centralised ↔ decentralised architectures

- Centralised
  - Data outside user control: privacy depends heavily on organisational measures
  - Easier abuse (e.g. by insiders) or loss (accidentally, or via hacking)
  - Convenience for user
  - Easier maintance & policy enforcement
  - Informational control leads to societal control (profiling/datamining)
- Decentralised
  - Privacy-friendly, in-context storage of data
  - More responsibility/activity on user side required
  - Fraud resistance possibly more difficult





## Own involvement

- Coauthor of scientific publication:

  *W. de Jonge and B. Jacobs, Privacy-friendly Electronic Traffic Pricing via Commits. Proceedings of the workshop Formal Aspects in Security and Trust (FAST), LNCS 5491, p.143-161, 2009.*
  `http://www.tipsystems.nl/files/ETPprivacy.pdf`

- and of more accessible version:

  *B. Jacobs and W. de Jonge, Safety in Numbers - Road Pricing beyond 'Thin' and 'Fat', In: Thinking Highways (Europe/RoW edition), Vol.4(3), Sep/Oct 2009, p.84-87.*
  `www.tipsystems.nl/files/RoadPricingBeyondThinAndFat`

- Occasional role in the media.





## Overview

- Law *Kilometerprijs* sent to parliament, with focus on:
  - fee issues (3 cent/km in 2012 and 6.7 cent/km in 2018)
  - punishment: if your OBE does not work, up to $\frac{1}{2}$ year in prison; if you manipulate/sabotage, up to 4 years.
- Much controversy, also about privacy
  (esp. *Telegraaf* newspaper: *Stasibox*, *Staat Gluurt Mee* headlines)
- Very little architectural/technical information available so far





## Organisational set-up: 5 tasks

1. Trajectory registration & aggregation
2. Transfer of aggregated trajectory information
3. Fee calculation
4. Billing
5. Enforcement (notably fraud detection).

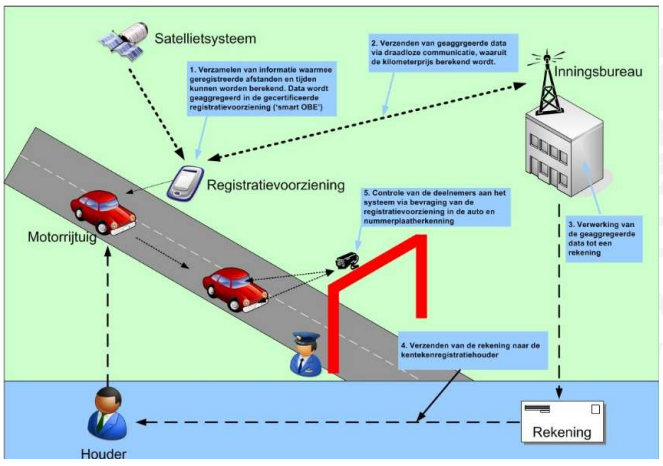
Tasks 1–4 can be done commercially, by service providers

- Transport Ministry has its own implementation track (*garantiespoor*), for the time being.
- Uniform enforcement is problematic with multiple systems

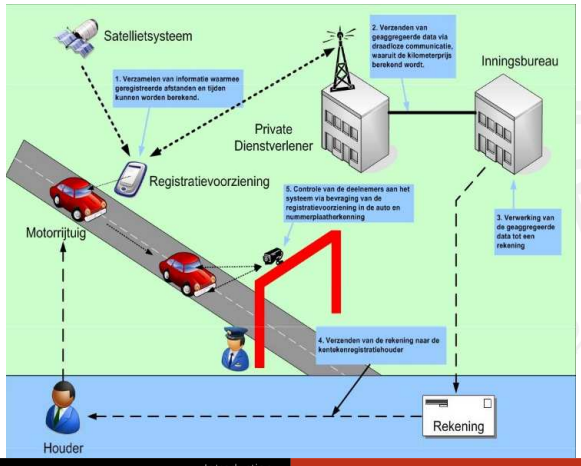




## *Garantiespoor* picture (source: ministry)



## Picture, with commercial service provider








## Privacy requirements articulated so far

- Car owner has access to own location data, via OBE.
- Authorities possess only:
  - aggregated data used for billing
  - enforcement data (photos, communication messages)

  These data are stored for at most 5 years.
- Commercial service providers may store & use location data, but only after explicit permission of client.
- Minister: law enforcement / intelligence services will have access to location data. But what does “access” mean?
  - Enforcement data is available, but is limited
  - Access to historical data possible via seizure of OBE.
  - Real-time access possible via commercial providers that store location data: “road tap”.
  - Real-time access via obligatory backdoor? Not clear!





## Overview: three OBE names

1. Thin (*dun*)
   - OBE sends all location data to central server
   - Probably preference of commercial parties
2. Fat (*dik*)
   - OBE aggregates itself
   - Forseen in minstery’s track (*garantiespoor*)
3. Well-rounded (*volslank*)
   - OBE sends only hashes to central server
   - Proposed by Wiebren de Jonge & BJ
     (details available in online paper)

In the end you can vote!
Watch carefully to determine your preference.





## 1. Thin OBE: essentials

- OBE activities restricted to:
  - calculation of trajectories
  - passing on these trajectories to the back-office, say every minute
- OBE does not aggregate, for privacy protection
- Easy enforcement via passive spot checks: take photo and compare it (later) to location data sent to back-office





## 1. Thin OBE: pros and cons

+ Simple and transparant architecture, with simple and cheap OBEs
+ Failure of physical OBE protection not catastrophic
+ Central storage enables (real-time) location-based services
– Much communication (cost) involved
– Privacy only procedurally protected, depending on policy of service provider
– Central database introduces risks:
  - data compromise may embarass people
    (look for politicians who visited prostitute areas)
  - data protection relevant for personal security
    (e.g. whereabouts of people under threat)
  - single point of failure / bottleneck
  - road tap possibility





## 2. Fat OBE: essentials

- OBE aggregates itself, and passes only aggregated data on to the back-office
  (For instance: NL is divided into red, green, blue . . . roads, each with their own tariff; the OBE communicates, say every month, how many kilometres have been driven on which colour, in which time segment.)
- OBE must thus contain map-data & timing for aggregation
  (which must be securely updated, occasionally)
- OBE must contain trusted element (smart card), for secure storage, communication & updates
- Spot checks are non-passive and complicated:
  - Two-way communication, while driving by
  - requesting most recent trajectory data
  - noticable, and likely to generate warning to other drivers

## 2. Fat OBE: pros and cons

+ Privacy technically protected, via decentralised storage and aggregation
– Complicated and expensive OBE
– OBE must be fully trusted: succesful (physical) attack on OBE is catastrophic
– Complicated, non-passive spot checks





## Intermezzo on hash functions

- Hash function $h$ takes arbitrary message $m$ as input, and produces a fixed length output $h(m)$, so that:
  - $h(m)$ is like a secure fingerprint of $m$
  - $m$ cannot be reconstructed from $h(m)$
  - different $m, m'$ give different $h(m), h(m')$, in practice
  - given $x = h(m)$, it is easy to check if $m$ is the "pre-image" of $x$, namely just compute $h(m)$ and check if $h(m) = x$.
- Some example (128 bit md5) hashes:

| message | hash value |
|---|---|
| 'my route to Amsterdam' | 95355cb89417d2675f69131b07ee55c5 |
| 'my route to amsterdam' | b8ecc8b9826471398fdba6c41bc6486c |





## 3. Well-rounded OBE: essentials

- OBE regularly sends hashes of its trajectory parts to the back-office
- These hashes reveal nothing, but commit the OBE/car
- Spot check can be passive, via photo: OBE must later show that spot check location was in pre-image of a hash in the back-office
- Fee calculation can be done by anyone: OBE, PC of car owner, (several) service providers, etc.
- Fee verification can also be done "locally"
  (see paper for details)





## 3. Well-rounded OBE: pros and cons

+ Privacy technically protected
+ Flexible approach,
  - allowing many different realisations, with/without commercial service providers
  - allows (inter)nationally uniform system (including spot checks) with different options chosen by clients
+ Breakdown of physical OBE protection is not catastrophic
+/– Spot checks easy & (necessarily) passive, but verification requires careful timing (after all hash commits) and explicit revealing action
+/– Requires open standard for trajectory parts
(proprietary in many current GPS systems)
– Difficult to explain to general audience





## Two questions for you (answers added afterwards, for 132 voters)

1. Which of the three presented systems would you trust most and want to use yourself?
   - 7% (a) thin OBE, sending location data to central server;
   - 29% (b) fat OBE, aggregating itself;
   - 64% (c) well-rounded OBE, sending hashes to central server.
2. Suppose you are transport minister (or member of parliament). Which overall approach would you choose?
   - 2% (a) Current proposal, allowing multiple (commerical) systems and fat OBE as back-up scenario;
   - 18% (b) Allowing multiple (commerical) systems and well-rounded OBE as back-up scenario;
   - 15% (c) Single national system, namely fat OBE, allowing (commercial) variations;
   - 65% (d) Single national system, namely well-rounded OBE, allowing (commercial) variations.





## Finally . . .

**Thanks for your attention!**

**Any questions / comments?**

Slides will appear at www.cs.ru.nl/~bart/TALKS