Pri-PAYD: Privacy Friendly Pay-as-you-drive Insurance

Carmela Troncoso
George Danezis
Eleni Kosta
Bart Preneel

COSIC/ESAT
ICRI/Faculty Law

KU Leuven
Belgium

What is PAYD?

- Pay-As-You-Drive
- New car insurance policy
- Customer pay per kilometer driven
  - Risk factor
    - Type of road
    - Hour of day
    - Safe driving
    - …

Advantages

- Fair fees
- Customer can “choose” his premium
  - Second vehicles
  - Young drivers
- Social benefit: less use of cars, responsible driving, less accidents,…
- Environmental benefit

But…

- Implementations privacy invasive, huge databases of sensitive data. Danger of accidental leaks or…
  - “TrafficMaster sells clients' location info to UK gov”
    (http://www.theregister.co.uk/2007/09/25/trafficmaster_vehicle_tracking_government_sales/)
    (http://www.trafficmaster.co.uk/our_partners/strategic_partners.php)
  - “Big Brother is keeping tabs on satnav motorists”
    (http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=483682&in_page_id=1770)
- Legal implications:
  - Different subscriber/user (employee/employer, rental cars)
  - European Data Protection Directive
  - Minimization of data
  - …

“State of the art” (I)

- Three main types of policies depending on their privacy-invasive degree (Summarized in a table in the paper)
- **First Group** (Not privacy invasive):
  - data from odometer, recorded once/twice a year.
  - check speed limit

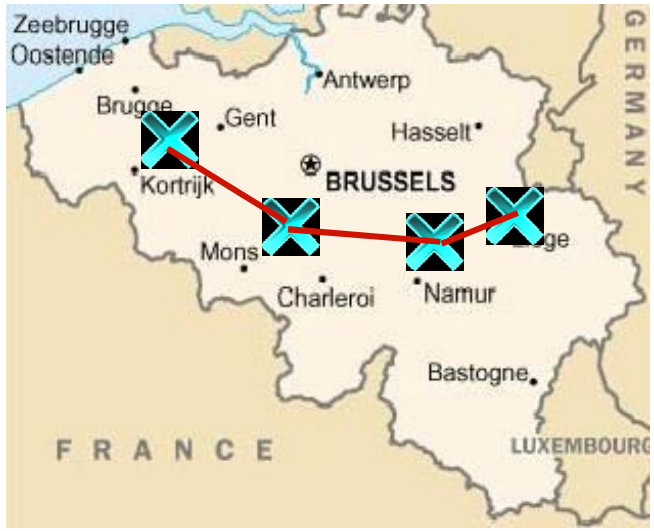

Corona Direct


Polis Direct


WGV

“State of the art” (II)

- **Second Group** (medium privacy invasive):
  - data from geographically distributed points (gas stations, credit card payments,…)
  - change data for discounts
  - more information



Aryeh Nedbank Aioi AVIVA Progressive Casualty

Pay&Go (3rd Party) DVB Winterthur

“State of the art” (III)

- **Third Group** (very invasive):
  - continuous collection of data
  - use GPS for location
  - use GSM for transmission (continuously or not)
  - more information
  - third parties

STOK (3rd party)

Hollard (Mobile Data)

Progressive Insurance

Norwich Union

Uniqa Group

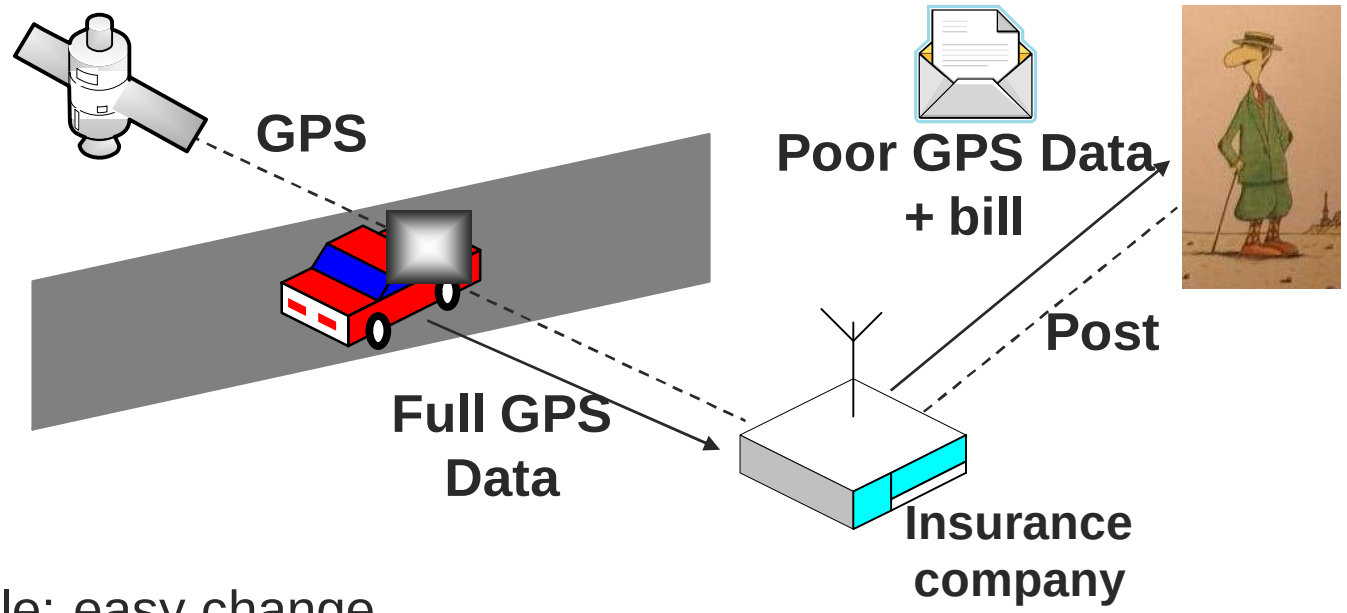
Sara

MAPFRE

iPAYD (3rd party)

“Current Model”

- Black box + GPS + (third party) + transmit

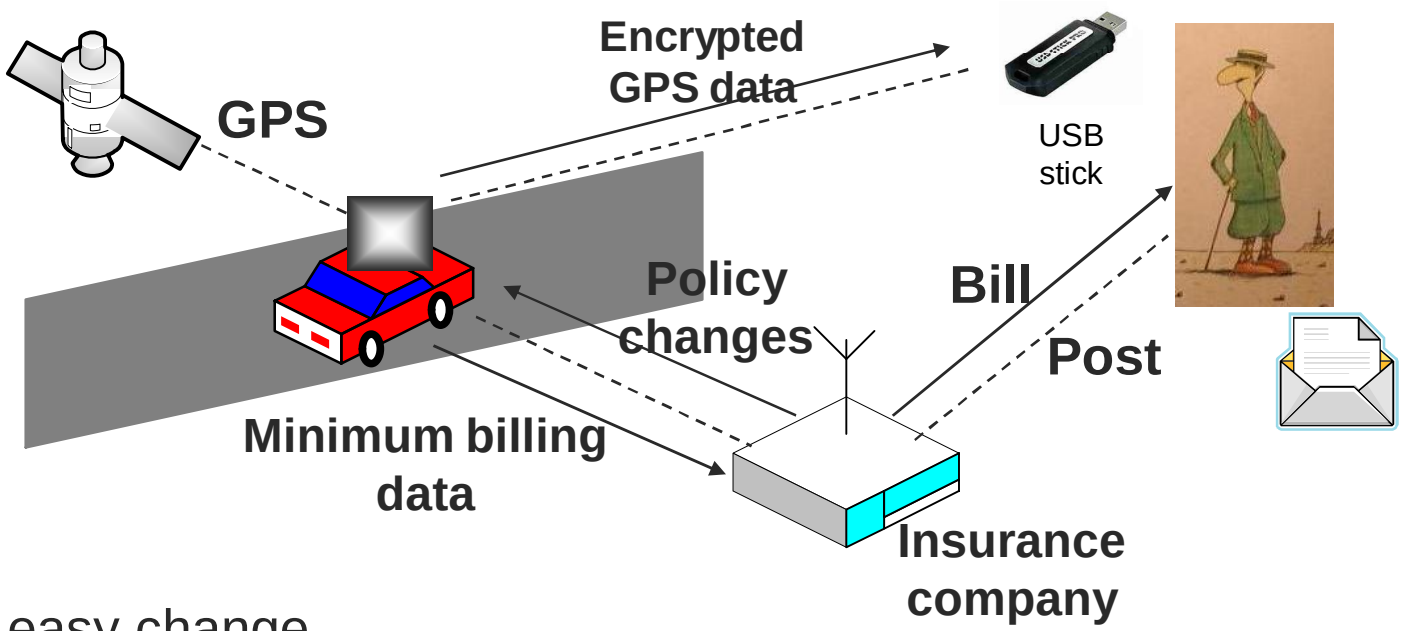


- Flexible: easy change
- Easy computation
- Business advantage: data mining and new services

- Privacy invasive: tracking
- Third parties (legal implications)

PriPAYD

- GPS + Black box (computation) + transmit billing

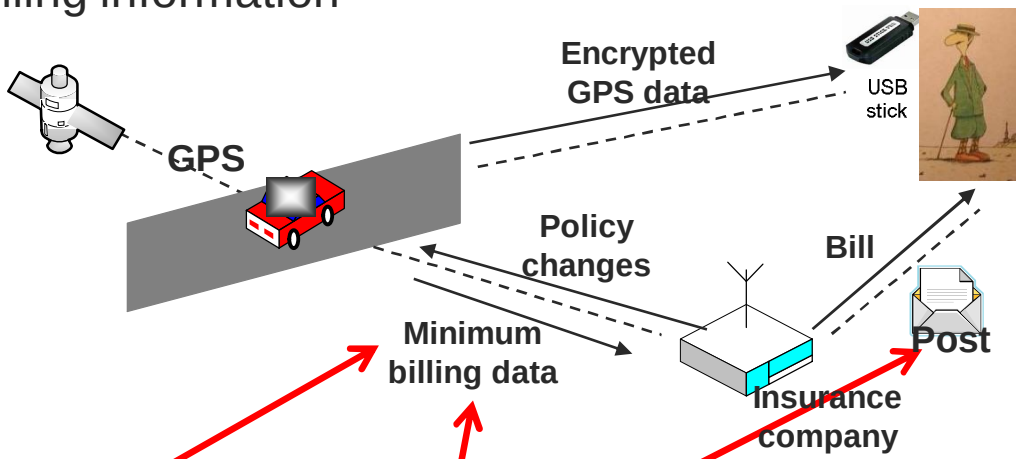


- Flexible: easy change
- Easy computation
- Low cost

- Privacy friendly
- Third parties do not carry personal data

The security of PriPAYD

- Two-level Bell-LaPadula
  - high: complete position (and others) records
  - low: billing information



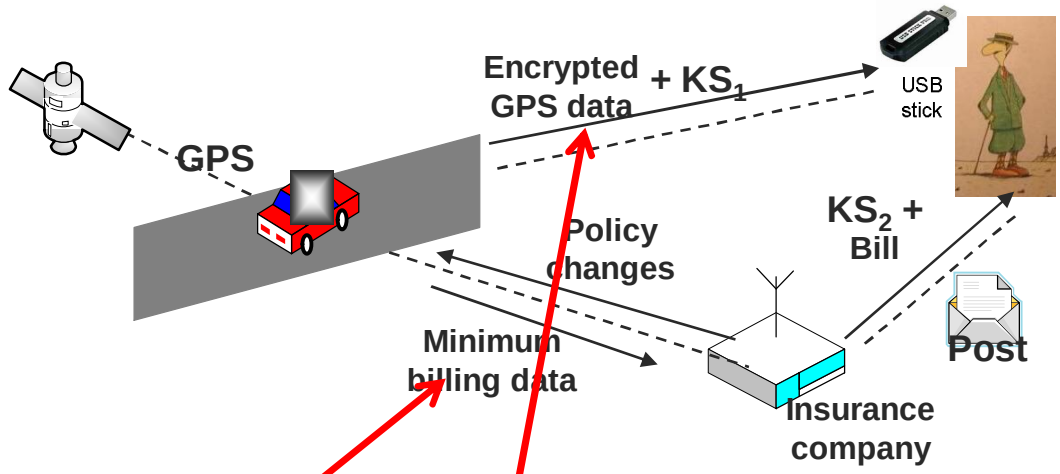
- **Authenticity**: data comes from black box

  Signature scheme (box should be tamper resistant)
- **Confidentiality**: only insurer and customer read billing data

  Public Key Encryption

  $Enc_{InsKey}\ (D=(Data,\ ID_{policy},\ ID_{code}),\ Sig_{BoxKey}(D))$

The security of PriPAYD



- **Privacy**:
  - only billing data transferred, avoid *covert channels*
    Signature schemes free or limited
  - logs only accessible to customer
    Symmetric key between box and customer:
    KS_1 and data from black box through USB stick
    KS_2 relied through insurer
    Possible change but loose contest ability

Discussion: legal considerations (I)

- **Proportionality/data minimization**: not all the GPS data is necessary for billing. No need for exact position/time.
  - *CNIL* in France.
- **Data processing:** (insurance and 3rd parties) only allowed to use the data for the provision of the service
- **Further processing**: companies for compatible purposes only
  - Anonymization?
- **Ownership of box/content**:
  - Eliminate the data inside the box (certification).
- **Use of GSM network**: GSM operator gets the data.
  - Location Based Service

Discussion: legal considerations (II)

- **Deletion of data**: after no longer necessary for providing the service.
  - But… mobile operator falls under Data Retention Directive (6 months – 2 years)
  - And the Insurance company?
- **Surveillance**: policy holder differs from driver (rental cars, company cars,…)

Discussion: cost

- **More computation in the black box**:
  - commercial GPS,
  - tamper resistance in ‘Current Model’
- **Cheaper communications**:
  - aggregate billing data (even SMS)
  - easy updates
- **Minimum trust architecture**:
  - no PKI (relationship user/insurer)
- **Same development cost**:
  - off-the-shelf
  - more engineering
  - But… back-office simpler (no personal data)

Discussion: privacy

- **Past information easy to delete**:
  - Destroy USB
  - Loose contesting ability…
- **GSM positioning**:
  - GSM shutdown except when transmitting
  - Only send from ‘home’ location

Discussion: certification

- Better not trust needed for maintain privacy (but for compute the bill)… still how to trust the box?
- Certification is expensive and no criteria exist
  - The user could check transmitted data (recording)
    - Malicious black box?
  - Device controlled by user to separate communication and computing
- How to ensure that the box does not record without certification?
  - Need physical access

Conclusions

- PAYD has many advantages but current implementations are very privacy invasive
- PriPAYD offers the same characteristics with strong privacy guarantees
  - No location data is provided to third parties
  - Known multi-level security
  - Relies on secure hardware only for accounting
  - Not more expensive than nowadays

Questions?!

Carmela.Troncoso@esat.kuleuven.be

(if you have legal aspects questions
Eleni.Kosta@law.kuleuven.be)