An Embedded Platform for Privacy-Friendly Road Charging Applications

Josep Balasch, Ingrid Verbauwhede, and Bart Preneel

Katholieke Universiteit Leuven, ESAT-COSIC
Outline

- Road Charging
- PriPAYD architecture
- Our embedded solution
- Performance
- Conclusions
Road Charging

- Nowadays drivers pay flat fees for driving
- Satellite-based road charging
  - Drivers pay according to their road use
  - On-Board Unit (OBU) collects GPS location data
  - Typical policy: where, when, and how much
- Main applications so far:
  - Pay-As-You-Drive (PAYD): insurance companies
  - Public Road Pricing: european governments
- Straightforward architecture
  - OBU sends location data to Service Provider
  - Privacy issues: fine-grained location data disclosed
PriPAYD Architecture

- PriPAYD architecture [TDKP07]

- Only final fee transmitted to Service Provider
- Only driver has access to location data
  - Shared key between OBU and Service Provider
- Authenticity of reported fee and location data
- Confidentiality of communications
Our Embedded Solution (I)

- Focus on normal mode of operation
- Data flow and main operations

### GPS DATA

```
$GPGGA,092204.999,4250.5589,S,14718.5084,E,1,04,24.4,19.7,M,,,0000*1F ...
```

### MAPPED DATA

<table>
<thead>
<tr>
<th>HOUR</th>
<th>TYPE ROAD</th>
<th>DISTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:40:11</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>18:41:39</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

### MAP-MATCHING

### ENCRYPT GPS

### ENCRYPTED GPS DATA

```
ï{ÔlÚuį□G-ÜdÅYĂbA??z¿}C?e~d?G´Ý½µÕÑbiw©?»QÀPG±ô?h´Ç§äi-HE|ή...`
```

### POLICY

<table>
<thead>
<tr>
<th>HOUR</th>
<th>TYPE ROAD</th>
<th>PRICE Km</th>
</tr>
</thead>
<tbody>
<tr>
<td>00u – 08u</td>
<td>1</td>
<td>0,01€</td>
</tr>
<tr>
<td>20u – 00u</td>
<td>3</td>
<td>0,01€</td>
</tr>
</tbody>
</table>

### PREMIUM CALCULATION

| 1.12 € |

### PREMIUM DATA

### ENCRYPT PREMIUM

```
ënÝpd¤G±ü ...`
```
Our Embedded Solution (II)

- **OBU elements**
  - TELIT GM862-GPS
  - NXP LPC2388 (ARM7)
  - SD CARD
  - OpenStreetMap

- **Minimize cost:**
  - Off-the-shelf hardware components
  - Free licensed software tools
Our Embedded Solution (III)

- Battery management
  - Real-time operations vs Off-line operations

- Implementation details
  - Software level (incl. crypto library)
    - Coprocessors would increase production costs
  - Byte-oriented access to SD Card memory
    - Considerable communication overhead
  - Free licensed digital road maps
    - Not optimized for map-matching purpose

- Cryptographic Primitives
  - Authenticated Encryption ← AES-CCM
  - Public Key Encryption ← RSA-OAEP
  - Public Key Signature ← RSA-PSS
Performance

- Test Scenario
  - Compressed road map of Belgium in SD Card
  - Cryptographic RSA keys 2048 bits
  - Constraint: process data upon GPS reception

- Timing results
  - One hour journey (one GPS string / second)

<table>
<thead>
<tr>
<th></th>
<th>OPERATION</th>
<th>TIME @ 72 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REAL-TIME</strong></td>
<td>Map-Matching</td>
<td>0.328 seconds</td>
</tr>
<tr>
<td><strong>OFF-LINE</strong></td>
<td>Premium Calculation</td>
<td>0.096 seconds</td>
</tr>
<tr>
<td></td>
<td>GPS Encryption</td>
<td>10.691 seconds</td>
</tr>
<tr>
<td></td>
<td>Encrypt Premium</td>
<td>6.445 seconds</td>
</tr>
</tbody>
</table>
Conclusions

- Importance of privacy in road charging systems
- Embedded platform for PriPAYD model
  - Low production costs
  - Less GSM communication upon deployment
- Performance analysis for worst-case scenario
  - Minimum off-line overheads
  - Results not optimal, but rather upper bound
- Privacy-preserving solutions are not theoretical, but ready to be commercially deployed
References


Questions?

For more information: josep.balasch@esat.kuleuven.be
Support Slides

- Privacy issues: customers
  - User Acceptance
    - “Surveillance fears force Norwich to scrap PAYD car policies”
      The Independent (UK), 17 June 2008 (1)
    - “Will the ‘antisocial Big Brother” solve traffic jams?”
      De Standaard (BE), 17 November 2009 (2)

- Privacy issues: industry
  - Data Protection
    - “8 Million Reasons for Real Surveillance Oversight”
      Security and Privacy Analysis by Christopher Soghoian (US), 1 December 2009 (3)
  - Data Leakage
    - “Greek mobile wiretap scandal unpicked”
      The register (UK), 11 July 2007 (4)

- Prove that privacy-preserving solutions for road charging are feasible

Josep Balasch
K.U.Leuven (COSIC)

(1) http://www.independent.co.uk/news/business/news/848562.html
(3) http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html
(4) http://www.theregister.co.uk/2007/07/11/greek_mobile_wiretap_latest/