PrETP: Privacy-preserving Electronic Toll Pricing

Josep Balasch, Alfredo Rial, Carmela Troncoso, Christophe Geuens*, Bart Preneel, Ingrid Verbauwhede

KULeuven ESAT/SCD/COSIC
*KULeuven ICRI

19th Usenix Security Symposium
11 August 2010
Outline

• Electronic Toll Pricing
• Public Road Pricing in European Union
• Privacy Issues
• PrETP: Privacy-preserving Electronic Toll Pricing
• Performance Analysis
• Conclusions
Electronic Toll Pricing (I)

- Apply direct charges to drivers for the use of roads
- Motivation: improve transportation network
  - Example: fuel taxes (up to 60% in some European states)

Still, mobility issues in peak hours
Electronic Toll Pricing (II)

- System to address congestion pricing
  - Different fees depending on vehicle’s **location** and **time**

<table>
<thead>
<tr>
<th>System Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gantry-based</td>
<td>City of Stockholm</td>
</tr>
<tr>
<td>Gate-based</td>
<td>Highways (USA)</td>
</tr>
<tr>
<td>Satellite-based</td>
<td>Insurance Companies</td>
</tr>
</tbody>
</table>

- European Union has chosen a satellite-based system to deploy public road pricing
Public road pricing requirements

**Functional requirements**
Fee depends on vehicle’s location and time of the day
Location data gathered by in-vehicle On-Board Unit (OBU)

**User requirements**
Pay only for corresponding road usage
Check correctness of the bill (verifiability)

**Provider requirements**
Enforce correct usage of the system (misuse detection)

**Domain assumptions**
Random spot-checks (e.g., via license plate readers)
Straightforward Tolling Model

GPS Satellites

Provider’s Database

Service Provider

Driver

OBU

GSM

GPS

Fee Calculation

Bill

Location Data

Location records

Payment

Toll Charger

PrETP: Privacy-preserving Electronic Toll Pricing
Straightforward Enforcement Model

Location data of drivers is disclosed to external entity!
Importance of Privacy

• Privacy Issues:
  o Fine grained GPS data allows for inferences:
    • Medical issues (visit to Cancer specialized clinic)
    • Political affiliation (visit to headquarters of political party)
  o Insurance companies experience:
    • “Surveillance fears force Norwich to scrap PAYD car policies”, The Independent (UK), 17 June 2008 [1]

• Consequences:
  o “Will the ‘antisocial’ Big Brother solve traffic jams?”, De Standaard (BE), 17 November 2009[2]

PrETP: Privacy-preserving ETP

- **Goal:** Design a privacy-friendly system for ETP

- Follow Privacy-by-Design guidelines:
  - Introduce privacy as a **requirement** of the system

**Privacy requirements**
Location data of individuals not disclosed to external entities

- Functionality of the system not altered
- Avoid impractical or expensive solutions
Privacy-preserving Tolling Model

- Keep personal data in user’s domain [TDKP07]

○ Data minimization
  - Only final fee is sent to Service Provider
  - Only driver has access to his own location records
Introduction of new threats

POLICY

<table>
<thead>
<tr>
<th>HOUR</th>
<th>TYPE ROAD</th>
<th>PRICE mile</th>
</tr>
</thead>
<tbody>
<tr>
<td>00u – 08u</td>
<td>1</td>
<td>$0.3</td>
</tr>
<tr>
<td>20u – 00u</td>
<td>3</td>
<td>$0.1</td>
</tr>
</tbody>
</table>

ATTACKER

- Change policy prices
- Change subfees
- Send incorrect final fee

GPS

GSM

Changepolicy prices

Changesubfees

Send incorrect final fee

PrETP: Privacy-preserving Electronic Toll Pricing
Privacy-preserving Enforcement Model

- Location records no longer available to Service Provider
  - Goal: Enforce while keeping privacy requirements

```
(1) V-728-ACF + loc + time
(2) V-728-ACF + loc + time
(3) commit phase
(4) V-728-ACF + loc + time
(5) open phase
(6) response

Toll Charger

Service Provider

License Plate Reader

OBU
```
Commit Phase

- Slice trajectory in segments (e.g., 1 mile)

Each segment has assigned a certain price per mile \((p_i)\)

The price is specified by the policy, example:

\[ p_i = f \text{ (road type, time day)} \]
Commitments to location data and price (I)

1 mile segments

OBU

HIDING PROPERTY

BINDING PROPERTY

Service Provider
Commitments to location data and price (II)

OBU

Look for correct segment in the location records

Service Provider

Location request

Look for the price assigned to the segment

Price request
Homomorphic Commitments to Price

Service Provider

fee = ∑ pay

fee = ∑ p_k

fee = ∑ k

OBU

11 August 2010 16
One last issue...

- Attacker can send a commitment to a “negative price”
  - High impact threat (difficult to detect)

- **Solution**: Zero-knowledge Proofs of Knowledge
  - Prove that an statement is true, without revealing anything other than the veracity of the statement
  - Example: TPMs using Direct Anonymous Attestation

- Electronic Toll Pricing scenario:
  - OBU proves to the Service Provider that the prices used in the homomorphic commitments are in accordance to the policy
Proof of possession of a signature

<table>
<thead>
<tr>
<th>OBU</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>![OBU Image]</td>
<td>![Service Provider Image]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>00u00 – 07u00</th>
<th>22u00 – 00u00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highway</td>
<td></td>
</tr>
<tr>
<td>p₁</td>
<td>p₂</td>
</tr>
<tr>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>p₃</td>
<td>p₄</td>
</tr>
<tr>
<td>Residential</td>
<td></td>
</tr>
<tr>
<td>pₙ₋₁</td>
<td>pₙ</td>
</tr>
</tbody>
</table>

“STATEMENT”
Price pₖ used in the commitment is signed by the Toll Service Provider

NON-INTERACTIVE VERIFICATION
Reduces communication overhead
Instantiation of the protocol

<table>
<thead>
<tr>
<th>OBU</th>
<th>TSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>// Main loop</td>
</tr>
<tr>
<td>2</td>
<td>For all $1 \leq k \leq N$ tuples do:</td>
</tr>
<tr>
<td>3</td>
<td>$p_k = f(\text{lock}_k, \text{time}_k)$</td>
</tr>
<tr>
<td>4</td>
<td>// Hash computation</td>
</tr>
<tr>
<td>5</td>
<td>$h_k = H(\text{lock}_k, \text{time}_k)$</td>
</tr>
<tr>
<td>6</td>
<td>// Commitment computation</td>
</tr>
<tr>
<td>7</td>
<td>$\text{open}_{p_k} \leftarrow {0, 1}^{l_n}$</td>
</tr>
<tr>
<td>8</td>
<td>$c_{p_k} = g_0^{p_k} g_1^{\text{open}_{p_k}} \pmod{n}$</td>
</tr>
<tr>
<td>9</td>
<td>// Proof computation</td>
</tr>
<tr>
<td>10</td>
<td>$\text{open}_w, w \leftarrow {0, 1}^{l_n}$</td>
</tr>
<tr>
<td>11</td>
<td>$A = A_0^w \pmod{n}$</td>
</tr>
<tr>
<td>12</td>
<td>$c_w = g_0^{w} g_1^{\text{open}_w} \pmod{n}$</td>
</tr>
<tr>
<td>13</td>
<td>$r_\alpha \leftarrow {0, 1}^{l_n}$</td>
</tr>
<tr>
<td>14</td>
<td>$t_{c_{p_k}} = g_0^{r_\alpha} g_1^{\text{open}_{p_k}}$</td>
</tr>
<tr>
<td>15</td>
<td>$t_Z = \mathcal{A}^r \mathcal{P}_k \mathcal{S}_w (g_0^{-1})^{r_w}$</td>
</tr>
<tr>
<td>16</td>
<td>$t_c = g_0^{r_w} g_1^{\text{open}_w}$</td>
</tr>
<tr>
<td>17</td>
<td>$t = c_{\nu}^w (g_0^{-1})^{r_w} (g_1^{-1})^{r_{\text{open}_w}}$</td>
</tr>
<tr>
<td>18</td>
<td>$s_\alpha = r_\alpha - ch \cdot \alpha$</td>
</tr>
<tr>
<td>19</td>
<td>$\pi_k = (A, c_w, ch, s_\alpha)$</td>
</tr>
<tr>
<td>20</td>
<td>End for</td>
</tr>
<tr>
<td>21</td>
<td>// Fee reporting</td>
</tr>
<tr>
<td>22</td>
<td>$\text{fee} = \sum_{k=1}^N p_k$</td>
</tr>
<tr>
<td>23</td>
<td>$\text{open}<em>{\text{fee}} = \sum</em>{k=1}^N \text{open}_{p_k}$</td>
</tr>
<tr>
<td>24</td>
<td>$m = [\text{tag}, \text{fee}, \text{open}<em>{\text{fee}}, (h_k, c</em>{p_k}, \pi_k)]_{k=1}^N$</td>
</tr>
<tr>
<td>25</td>
<td>$s_m = \text{OBU} \text{sign} (\text{msg}_{\text{OBU}}, m)$</td>
</tr>
</tbody>
</table>

**BOTTLENECK**

RIPEMD-160
Damgård-Fujisaki integer commitment scheme
Proof of possession of CL-RSA signature

August 2010

PrETP: Privacy-preserving Electronic Toll Pricing
Performance Analysis (I)

- Proof-of-concept OBU embedded platform
  - SD Card for external static storage
  - GSM/GPS module
  - 32-bit ARM7 microcontroller
  - Implementation in software (incl. crypto library)
- TSP implementation on commodity computer
Performance Analysis (II)

• Tolling Operations: 25 % time
  o Processing of GPS strings requires 900 seconds/hour in average

• Enforcement Operations:
  OBU timings and average speed tolerance

<table>
<thead>
<tr>
<th>Operation</th>
<th>Security</th>
<th>Medium (1024 bit)</th>
<th>High (1536 bit)</th>
<th>Very High (2048 bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process one segment</td>
<td></td>
<td>7.88 s</td>
<td>22.13 s</td>
<td>47.79 s</td>
</tr>
<tr>
<td>Max. Speed</td>
<td></td>
<td>350 mph</td>
<td>124 mph</td>
<td>57 mph</td>
</tr>
</tbody>
</table>

• Tuning parameters of the system
  o Security level; Segment size; GPS strings
Performance Analysis (III)

• TSP verifications:

<table>
<thead>
<tr>
<th>Security Commit</th>
<th>Medium (1024 bit)</th>
<th>High (1536 bit)</th>
<th>Very High (2048 bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>One segment</td>
<td>0.0105</td>
<td>0.0295</td>
<td>0.0587</td>
</tr>
<tr>
<td>One month</td>
<td>15.750</td>
<td>44.250</td>
<td>88.050</td>
</tr>
</tbody>
</table>

TSP capacity tolerance assuming vehicle drives an average of 1500 miles/month

<table>
<thead>
<tr>
<th>Security Commit</th>
<th>Medium (1024 bit)</th>
<th>High (1536 bit)</th>
<th>Very High (2048 bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5 miles</td>
<td>82 000</td>
<td>29 000</td>
<td>14 000</td>
</tr>
<tr>
<td>1 miles</td>
<td>164 000</td>
<td>58 000</td>
<td>29 000</td>
</tr>
<tr>
<td>2 miles</td>
<td>329 000</td>
<td>117 000</td>
<td>58 000</td>
</tr>
</tbody>
</table>
Conclusions

• Privacy-preserving Electronic Toll Pricing is possible

• PrETP offers strong security and privacy guarantees
  o Minimum location data disclosed to the provider
  o Fraud attempts detected with high probability

• Proof-of-concept using OBU embedded platform in software
  o Low cost hardware support could easily improve by factor 10
Thanks for your attention

• Questions?

• References