IBBT NextGenITS Project
Next Generation Intelligent Transport Systems

Josep Balasch
KULeuven ESAT/SCD/COSIC – IBBT, Belgium

BCRYPT Symposium on Embedded Security
24 June 2010

Acknowledgements: Carmela Troncoso
IBBT NextGenITS Project

• Implement and demonstrate a number of ITS services (ITS: Intelligent Transport Systems)

• Subprojects:
  o SP1. Traffic Information
  o SP2. E-Call (Emergency Call)
  o SP3. ISA (Intelligent Speed Adaptation)
  o SP4. Road Tolling [focus of this talk]
  o SP5. Cooperative Systems (V2V, V2I)
  o SP6. Multi-Application Platform
Sub-Project 4: Road Tolling

- Academic & Industry Partners involved:
Road Tolling

• Idea: Differentiated payment for mobility
  o Drivers should pay according to their road usage
    – Long trips, high density roads, rush hours ➔ higher fee
    – Sporadic use, second vehicle, young drivers ➔ smaller fee

• Motivation
  o Address mobility problem
  o Mentality and behavioral change
  o Fairness: heavy users have to pay more

• aka: Road Charging, Road Pricing, Electronic Toll Pricing,...
Road Tolling in European Union

• Introduced at European Level:
  o Directive 2004/52/EC (interoperability)
  o Commission Decision Oct. 2009 (technical elements)

• European Electronic Toll Service (EETS)
  o Architecture and actors involved
  o In-vehicle installation of On-Board Unit (OBU)
  o Interfaces and capabilities:
    • GNSS: Global Navigation Satellite System (GPS)
    • DSRC: Dedicated Short-Range Communications
    • GPRS/GSM network

• Within three years for vehicles above 3.5 tons, all other vehicles within five years
EETS straightforward implementation

- Most common architecture in Pay As You Drive (PAYD) insurance solutions
Stakeholders in EETS

• Government
  o **Interest**: Mobility problem
  o **Role**: Establish policies, law enforcement

• Industry (chip manufacturers, GSM providers, ...)
  o **Interest**: New business opportunities
  o **Role**: Provide infrastructure

• Users
  o **Interest**: Mobility problem, economics
  o **Role**: Using the system, but
    o Privacy at risk
Privacy at risk

• Issues for customers:
  o Fine grained GPS data allows for inferences:
    • Medical issues (visit to Cancer specialized clinic)
    • Political affiliation (visit to headquarters of political party)
    • Industry espionage (visits to other companies)
  o Pay As You Drive (PAYD) experience:
    • “Surveillance fears force Norwich to scrap PAYD car policies”, The Independent (UK), 17 June 2008 [1]
  o User acceptance of mandatory system:
    • “Will the ‘antisocial’ Big Brother solve traffic jams?”, De Standaard (BE), 17 November 2009 [2]

Privacy for Road Tolling

• What data is necessary for the provision of the service?
  o Final fee that users pays to provider/government

• Privacy-by-Design guidelines:
  o Introduce privacy as a requirement of the system
  o Data minimization; personal data in user’s domain
  o Overall goal of the system should not be altered

• Legal Issues:
  o Actors must not be able to cheat
  o Actors must be held liable in case of system’s misuse
Privacy-Friendly Electronic Toll Pricing

• No personal data leaves the domain of the user

○ Data minimization
  • Only final fee is sent to Toll Service Provider
  • Only driver has access to his own location data
    – Shared key between Toll Service Provider and driver
Data Flow and Operations

GPS DATA

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

ENCRIPT GPS

ENCRYPTED GPS DATA

ï{ÔiÚu¡lieG-ÚdÂYÅbA??z¿JC?e~d?G’Ý½µOÑbiw©?»QAPG±ô?h´Ç§àvi~HE} ...

MAP-MATCHING

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>

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

PREMIUM DATA

1.12 €

PREMIUM

ENCRYPT PREMIUM

ENCRYPTED PREMIUM

PREMIUM CALCULATION

ENCRYPT PREMIUM

ENCRYPTED PREMIUM

NextGenITS project
Law-Enforcement

• Technical means do not suffice
  o OBU in control of potentially malicious users
  o Attacker model: internal & external tampering

• Instead technology can help:
  o Detect vehicles with inactive OBUs
  o Detect vehicles using false location data
  o Detect vehicles using incorrect road prices
  o Detect vehicles reporting false final fees

• Combination of law + technology
Random spot-check model

- Remote attestation mechanism
  - Ad-hoc solution for privacy-preserving road tolling

* Diagram showing the interaction between Toll Charger, License Plate Reader, Toll Service Provider, and OBU (On-Board Unit) with steps labeled 1 to 6:
  1. (1) commit phase
  2. (2) \text{V-728-ACF} + loc + time
  3. (3) \text{V-728-ACF} + loc + time
  4. (4) \text{V-728-ACF} + loc + time
  5. (5) open phase
  6. (6) response
Commit Phase

• Slice trajectory in segments (e.g., 1 Km)

- Each segment has assigned a certain price per Km ($p_i$)
- The price is specified by the policy, example:
  \[ p_i = f (\text{road type, time day}) \]
- A payment tuple is created for each segment

Commitment to location data
Homomorphic commitment to price
Proof that price belongs to policy
Commitment to Location Data

1 Km segments

OBU

HIDING PROPERTY

Toll Service Provider

 Were you at ... ?

BINDING PROPERTY

NextGenITS project

24 June 2010
Homomorphic Commitments to Price

OBU

Toll Service Provider

\[ \text{fee} = \sum_{k=1}^{N} p_k \]

\[ \text{fee} = \sum_{k=1}^{N} \text{fee}_k \]

\[ \text{fee} + \text{fee} = \text{fee} \]

\[ \text{fee} \times \text{fee} = \text{fee} \]

NextGenITS project

24 June 2010

16
One last issue...

• Attacker can send a commitment to a “negative price”
  o Not detected unless vehicle is spotted in that segment, and commitments need to be opened.

• **Solution**: Zero-knowledge Proofs
  o Prove that an statement is true, without revealing anything other than the veracity of the statement

• **Road Tolling scenario**:  
  o OBU proves to the Service Provider that the prices used in the commitment are in accordance to its policy
Proof of possession of signature

OBU

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

“STATEMENT”
Price pₜ 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>$p_k = \text{f}(\text{lock}_k, \text{time}_k)$</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>$\text{open}_{p_k} \leftarrow {0, 1}^{\ell_n}$</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>$\text{open}_w, w \leftarrow {0, 1}^{\ell_n}$</td>
</tr>
<tr>
<td>11</td>
<td>$A = A_{g_0^{w}} \pmod{n}$</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>$r_{\alpha} \leftarrow {0, 1}^{\ell_o}$</td>
</tr>
<tr>
<td>14</td>
<td>$t_{c_{p_k}} = g_0^{r_{p_k}} g_1^{\text{open}_{p_k}}$</td>
</tr>
<tr>
<td>15</td>
<td>$t_Z = A^{r_{p_k}} R_{p_k} S_{r_{p_k}} (g_0^{-1})^{r_w \cdot e}$</td>
</tr>
<tr>
<td>16</td>
<td>$t_{c_w} = g_0^{r_{w}} g_1^{r_{\text{open}_{w}}}$</td>
</tr>
<tr>
<td>17</td>
<td>$t = c_{p_k}^{r_{p_k}} (g_0^{-1})^{r_w \cdot e}$</td>
</tr>
<tr>
<td>18</td>
<td>$c_h = H(\beta</td>
</tr>
<tr>
<td>19</td>
<td>$s_{\alpha} = \pi_{\alpha} - c_h \cdot \alpha$</td>
</tr>
<tr>
<td>20</td>
<td>$\pi_k = (A, c_w, ch, s_{\alpha})$</td>
</tr>
<tr>
<td>21</td>
<td>End for</td>
</tr>
<tr>
<td>22</td>
<td>// Fee reporting</td>
</tr>
<tr>
<td>23</td>
<td>fee = $\sum_{k=1}^{N} p_k$</td>
</tr>
<tr>
<td>24</td>
<td>open fee = $\sum_{k=1}^{N} \text{open}_{p_k}$</td>
</tr>
<tr>
<td>25</td>
<td>$m = [\text{tag}, \text{fee}, \text{open fee}, (h_k, c_{p_k}, \pi_k)]_{k=1}^{N}$</td>
</tr>
<tr>
<td>26</td>
<td>$s_m = \text{OBU sign}(m)$</td>
</tr>
</tbody>
</table>

$\alpha \in \{p_k, \text{open}_{p_k}, e, v, w, \text{open}_w, w \cdot e, \text{open}_{w \cdot e}\}$

$\beta = (\alpha || g_0 || g_1 || A || R || S || g_0^{-1} || g_1^{-1} || c_{p_k} || h || t_{c_w} || t_{c_{p_k}} || t_{c_w})$

### NextGenITS project

24 June 2010

---

RIPEMD-160

Damgård-Fujisaki integer commitment scheme

Proof of possession of CL-RSA signature

BOTTLENECK
• Build OBU embedded platform

- Off-the-shelf hardware components
- Free licensed software tools
Performance Analysis (II)

• OBU implementation details
  o Cryptographic library in software
    • Montgomery for modular arithmetic
    • Multiexponentiation algorithms \((a^{bc^d} \mod n)\)
    • Salsa20 stream cipher as random number generator
    • AES in CCM mode for authenticated encryption
    • PKCS #1 for Public Key Cryptography
  o Map-matching
    • Digital road maps not optimized for this purpose
    • Byte-oriented access library to SD Card external memory

• TSP implementation details
  o Commodity computer (IntelCore2Duo)
  o GMP library for cryptographic operations
Performance Analysis (III)

- Test scenario: 1-hour journey in urban area
- Full digital road map of Belgium in SD Card
- Evaluation for different security levels

OBU timings and average speed tolerance for a 1-hour journey

<table>
<thead>
<tr>
<th>Security Operation</th>
<th>Medium (1024 bit)</th>
<th>High (1536 bit)</th>
<th>Very High (2048 bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map-Matching</td>
<td>839.11 s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One segment</td>
<td>7.88 s</td>
<td>22.13 s</td>
<td>47.79 s</td>
</tr>
<tr>
<td>Max. Speed</td>
<td>350 km/h</td>
<td>124 km/h</td>
<td>57 km/h</td>
</tr>
</tbody>
</table>

TSP capacity tolerance assuming an average of 1500 km/month/vehicle

<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 Km</td>
<td>82 000</td>
<td>29 000</td>
<td>14 000</td>
</tr>
<tr>
<td>1 Km</td>
<td>164 000</td>
<td>58 000</td>
<td>29 000</td>
</tr>
<tr>
<td>2 Km</td>
<td>329 000</td>
<td>117 000</td>
<td>58 000</td>
</tr>
</tbody>
</table>

- Feasible, yet there is room for improvements:
  o Efficient map-matching, coprocessor, ...
Conclusions

• Design of privacy-friendly Road Tolling is possible

• Strong security and privacy guarantees
  o No location data disclosed to the provider
  o No actor can commit fraud without being detected

• Law compliant
  o Data minimization; personal data in user’s domain

• System is feasible, even for worst-case scenario
  o Proof-of-concept using OBU embedded platform
• Questions?

• References