Developing Privacy-respecting E-ticketing Systems

Ivan Gudymenko
Outline

- E-ticketing Systems Under Concern:
  - E-ticketing: A General Application Scenario
  - Fare Collection Approaches
  - Underlying Technology and Standards
  - Main Use Cases

- Security Issues Affecting Privacy

- Specific Privacy Threats

- Dissertation Goals and Their Achievement

- Privacy Preservation

- Challenges

What to protect

Dis. Focus

Klausurtagung II/2012
What Should Be Protected
E-ticketing Systems Under Concern

- Part of UbiComp
- Focus on E-ticketing in Public Transport
- E-ticketing Systems [1]:
  - Account-based
    - Card-based
  - E-ticket:
    - Online-based
    - “Smart ticket”
E-ticketing Systems Under Concern (2)

1. Online ticket
2. Smart ticket

- Public transport
  - Sport events
  - Concerts
- Event ticketing
  - Fitness & leisure
  - Fitness studious
  - Ski pass
E-ticketing: A General Application Scenario

E-ticket Distribution

Trip Begin
- Check-in
  - E-ticket
  - On-board Reader (Terminal)

Event Processing Unit (e.g. GPS-based)

Trip End
- Check-out
  - E-ticket

Back-end System
- Event Storage
- Distance Calculation
- Billing
- Customer Accounts Management
- Statistics

Klausurtagung II/2012
Fare Collection Approaches

1. Electronic Paper Ticket (EPT)

2. Check-in/Check-out based (CICO)
   a) Pure CICO
   b) Seamless CICO
      i. Walk in/Walk out (WIWO)
      ii. Be in/Be out (BIBO)
## Underlying Technology and Standards

<table>
<thead>
<tr>
<th>Architecture</th>
<th>ISO EN 24014-1 <em>(conceptual framework)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Interfaces</td>
<td>EN 15320 <em>(logical level, abstract interface, security)</em></td>
</tr>
<tr>
<td></td>
<td>EN 1545 <em>(data elements)</em></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 7816-4 <em>(commands, security)</em></td>
</tr>
<tr>
<td>Communication Interface</td>
<td>ISO 14443 <em>(parts 1-3 required)</em></td>
</tr>
</tbody>
</table>

**RFID-based E-Ticketing Stack**

- **E-ticket**
- **Smartcard**

**The NFC Forum Architecture**

**The NFC Forum Specifications**
Main Use Cases (Front-end)

- Java Cards
- NFC Smart Phones
Main Use Cases: Java Cards

• “Secure by design and tamper-resistant” [2]

• Java Card Platform
  ▪ Response-based communication (C/R-APDUs)
  ▪ Two component JCVM (off-card, on-card)
  ▪ Memory: ROM, RAM, EEPROM
  ▪ Constrained resources
    • reused exception objects
    • optional Garbage Collection, etc.
Main Use Cases: NFC Smart Phones

- An extremely promising concept
- P2P and Card Emulation modes for e-ticketing
- Trusted execution environment provided by the SE (e.g. a SIM card)
- SE ↔ NFC front-end: via SWP or S²P
- No need for phone battery (card emulation, SWP)
- Secure updates through OTA possible (flexibility)
Further Focus: User Privacy
Security Issues Affecting Privacy

Real System

E-ticket Distribution

Trip Begin

Event Processing Unit (e.g. GPS-based)

On-board Reader (Terminal)

Trip End

Back-end System

- Travel Records Storage
- Distance Calculation
- Billing
- Customer Accounts Management
- Statistics

1) Eavesdropping

2) Compromising the Reader

3) Compromising the Back-end Database

Check-in

E-ticket

Check-out

E-ticket

(user_ID, terminal_ID, in(time, cooridn), out(time, cooridn))
## Specific Privacy Threats

<table>
<thead>
<tr>
<th>Threats</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Unintended customer identification:</strong></td>
<td></td>
</tr>
<tr>
<td>a) Exposure of the customer ID:</td>
<td></td>
</tr>
<tr>
<td>i. Personal ID exposure (direct)</td>
<td>Privacy-respecting authentication; ID encryption/randomization; access-control functions [6]</td>
</tr>
<tr>
<td>ii. Indirect identification</td>
<td>ID encryption</td>
</tr>
<tr>
<td>b) Unencrypted ID during anti-collision</td>
<td>Randomized bit encoding [7]; bit collision masking [8, 9] (protocol dependent)</td>
</tr>
<tr>
<td>c) PHY-layer identification</td>
<td>Shielding; switchable antennas [10]</td>
</tr>
<tr>
<td><strong>2. Information linkage</strong></td>
<td>Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing</td>
</tr>
<tr>
<td><strong>3. Illegal customer profiling</strong></td>
<td>Privacy-respecting data storage (back-end); the same as in threat 1</td>
</tr>
</tbody>
</table>
Main Goal of the Dissertation

- Targeting the user privacy from the outset
- In a holistic way across the system components
- A cross-layer approach is desirable
Goal Achievement

- Clearly define the system architecture
  - Online/Off-line e-ticket authentication, *etc.*
- Assign trust levels to the system components
  - Honest, semi-honest, malicious
- State-of-the-art (against the defined architecture)
- Concept development
- Validation

Klausurtagung II/2012
Concept Validation

- Theoretical Evaluation
- Experiments (labor set up, equipment)
- Student assignments
  - Lightweight crypto (Hauptseminar Techn. Datensch., finished)
  - Kryptografische Methoden auf einer Javacard (Praktikum, finished)
  - Abgesicherte Kommunikation von Android-basierten Smartphones mit Hilfe der NFC-Schittstelle (KP, planned for WS 2012)
  - Nicht-triviale Kryptoverfahren auf einer Java-Karte (KP, planned for WS 2012)
  - Joint E-ticket Application for JCP and NFC (Master Thesis, WS ’12)
  - ...
Privacy Preservation

• Privacy/performance trade-off
  ▪ Full privacy preservation
    • Blind Bill Computation (e.g. our paper [3])
    • “Optimistic payment” [4]
  ▪ Partial privacy preservation
    • One of the system components is fully trusted (typically, the back-end)
    • Based on the protocol of [5], for example
    • Secure Computations in the back-end
Full Privacy Preservation: Blind Bill Computation [3]

- Flexibility for a customer
- Requires bill processing in the back-end
- Based on partial homomorph. encr. (Paillier)
- Special bit encoding scheme
- Allows logical operations on ciphertexts: \( \Lambda, == \)
- Additionally, Negation Service required: \( \neg \)
  - Full functional basis in the end (\( \Lambda, \neg \))
Full Privacy Preservation (2)

- Two parts:
  - E-ticket authentication on Entry/Exit
    - ZKP of ID possession due to Schnorr
    - Database look up
    - Additional k-anonymous ID for search speed up
  - Bill Computation in the back-end
    - Travel Records creation
    - Travel Records Processing
      - Using the homomorph. properties and encryption scheme
Challenges (Blind Bill Comp.)

- Efficiency
  - Back-end
  - Front-end (proprietary encryption)
  - Processing cost can be prohibitive...
- Necessity to have a TTP for key mgmmt.
General Challenges

• Non-trivial Crypto on Java Card:
  ▪ Running arithmetic ops at the app. layer is a significant performance limiting factor
  ▪ The necessity to tunnel computations the cryptographic co-processor

• Securing the NFC communication interface

• Back-end efficiency
  ▪ During the look up for blind bill computation
  ▪ General look up
Plan For The Near Future

- Focus on the specified systems
- Define and stick to a certain system architecture (mobile/fixed terminals, etc.)
- Devise a privacy-preserving concept
- A paper for a doctoral symposium
  - Concept discussion
Thank You Very Much For Your Attention!

Questions? Comments? Suggestions?
References


