On Protection of the User's Privacy in Ubiquitous E-ticketing Systems Based on RFID and NFC Technologies

Ivan Gudymenko
Faculty of Computer Science, TU Dresden, Germany
ivan.gudymenko@mailbox.tu-dresden.de

Keywords: Customer Privacy, E-ticketing, NFC, RFID

Abstract: The issues of customer privacy in e-ticketing systems for public transport based on RFID/NFC technologies are addressed in this paper. More specifically, having described the target system, the specific privacy threats are identified and respectively classified. This is performed by analyzing the system under concern against the specifically defined privacy properties (pseudonymity, confidentiality, unlinkability). The process of the respective countermeasures development together with the recommendations for their integration into the real e-ticketing system for public transportation are further discussed.

1 INTRODUCTION

Different areas of public life are being increasingly affected by a plethora of technologies which can be collectively referred to as Ubiquitous Computing (UbiComp). The latter has already gone far beyond the initial UbiComp paradigm which is believed to have been coined by Marc Weiser in his seminal paper (Weiser, 1991).

One of the areas being tangibly affected by UbiComp is the so-called Electronic Ticketing (E-ticketing) where a conventional ticket is represented by an electronic medium[1] holding a digital proof of possession of rights to claim a certain service, e.g. a travel permission. E-ticketing can be used in various application areas: public transport, event ticketing (sport events, concerts), fitness and leisure (ski pass, fitness studious tickets), etc.

The current paper focuses on public transport systems which can substantially benefit from incorporating the e-ticketing concept. In this case, it enables to automate the process of fare collection (Automated Fare Collection, AFC) and paves the way to the so-called seamless travel, when a customer can use a single e-ticket between different transport companies possibly across countries in a seamless manner (Integrated Ticketing). E-ticketing has already been in use in several developed countries around the world. For example, Dutch OV-Chipkaart (Trans Link Systems, 2012), London Oyster Card (Transport for London, 2012), EZ-Link in Singapore (Land Transport Authority, 2012), Hong-Kong Octopus Card (Octopus Cards Limited, 2012), etc.

Despite introducing various benefits both for customers and public transport companies, e-ticketing systems raise serious concerns over the invasion of customer privacy. This problem is in focus of the current paper which explores possible privacy threats endemic to such systems and subsequently analyzes the countermeasures.

The rest of the paper is organized as follows. Section 2 describes the e-ticketing system under concern. Privacy violation scenarios and privacy threats together with the generic countermeasures are analyzed and discussed in Section 3. We briefly review the related work in Section 4 and conclude the paper as well as outline future work in Section 5

2 E-TICKETING SYSTEMS UNDER CONCERN

Before addressing privacy issues in the e-ticketing system under concern, its concise description is performed in this section creating the necessary basis for further threat analysis and discussion.

2.1 General System Description

The public transport system under concern consists of three parts: *(1)* back-end, *(2)* front-end, and *(3)* a bridging element (i.e. terminals). The back-end

[1] For example, a Radio Frequency Identification (RFID) chip.

of such a distributed ubiquitous system incorporates powerful internetworked processing centers controlling the system functionality and performing billing, customer accounts management, etc. (see Back-end System in Figure 1). E-tickets interacting with the terminals compose its front-end (see E-ticket, Figure 1). In order to interconnect front-end and back-end, a bridging element is needed essentially acting as a bridge between the two other system components and being represented by terminals (with incorporated readers for e-tickets) in the public transport system (depicted as On-board Reader in Figure 1).

Most of the current e-ticketing systems for public transportation adhere to the so-called Check-in/check-out (CICO) principle for fare collection and ticket validation (see Check-in and Check-out in Figure 1). It allows for establishment of flexible billing schemes in the back-end and facilitates the creation of various loyalty programs for customers.

It is preferable that the interface between an e-ticket and a terminal is contactless, since it implies faster validation times (shorter queues) and the absence of moving parts which can be worn out (the service is intended for daily use). It, therefore, provides a higher degree of durability for the front-end part of an e-ticketing system. There is set of different contactless technologies which can be used as enablers of such an e-ticketing system. The most suitable, however, are two lightweight technologies, which are based on a similar principle: Radio Frequency Identification (RFID) and Near Field Communication (NFC). The former has already been extensively used in smart cards area, namely RFID cards based on ISO 14443 standard (ISO, 2011). NFC is not so well-established but is also an extremely promising technology that is rapidly gaining importance in the area of lightweight contactless communication, especially in the smart phone industry.

2.2 A High-level Description of a System Architecture

The e-ticketing system for public transport described above functions as follows. Firstly, a customer obtains an e-ticket in one of the ticket distribution offices (see step 1 in Figure 1). Depending on the preferred e-ticket carrier medium, this can be either a certified application downloaded to an NFC-enabled smart phone and respectively configured or a smart card issued by a public transport company with a pre-installed e-ticketing application[1]. A trip begins when a customer enters a vehicle and performs check-in by putting the electronic medium with an installed e-ticketing application into the vicinity of an on-board reader, or a terminal (step 2a, Figure 1). On successful e-ticket authentication, the reader forwards the user ID (u_ID) and its own ID ($terminal\_ID$) to the Event Processing Unit (see Figure 1). The latter registers the check-in event by adding the time and location (e.g. geographical coordinates) and temporarily storing the resultant record. When the trip ends, the same procedure is repeated (see step 2b, Figure 1). Event Processing Unit then sends the combined record (resulted from the check-in/check-out events) to the back-end over the backbone network in time intervals according to the specification of a concrete e-ticketing system[2] (see step 3, Figure 1). If a trip consists of several transits, the aforementioned procedures are repeatedly carried out. In the back-end, the combined travel records are stored (Events Storage, see Figure 1) and respectively processed for billing purposes (Distance Calculation, Billing). Customer accounts management and travel statistics analysis are performed in this part of the system as well.

The system architecture described above is generic enough to be used as an abstraction for different real world public transport systems based on e-ticketing. At the same time, it enables to perform a privacy analysis of e-ticketing systems for public transportation, which is done in the next section.

3 PRIVACY ANALYSIS

Having described the target system, the issues of customer privacy are addressed in this section. Firstly, the generic privacy threats endemic to e-ticketing systems are discussed. The possible countermeasures are considered in Section 3.2. A further elaboration on this issue is presented in Section 3.3.

3.1 Generic Privacy Threats in E-ticketing Systems

Since the notion of privacy is fairly ambiguous and not easily considerable from a technical perspective,

[1] In a real public transport system, a support for the conventional paper tickets may be required (for example, for compatibility reasons). In this paper, however, the focus is specifically made on e-tickets.

[2] In this case, the system can be organized differently in terms of the time periods when the combined travel records are transmitted to the back-end. Two extreme cases can be distinguished: the online system (immediate transfer of travel records, always connected to the back-end, e.g. via a GSM wireless channel) and the offline one (when travel records are only transferred at certain stationary points, e.g. at the route final stations).

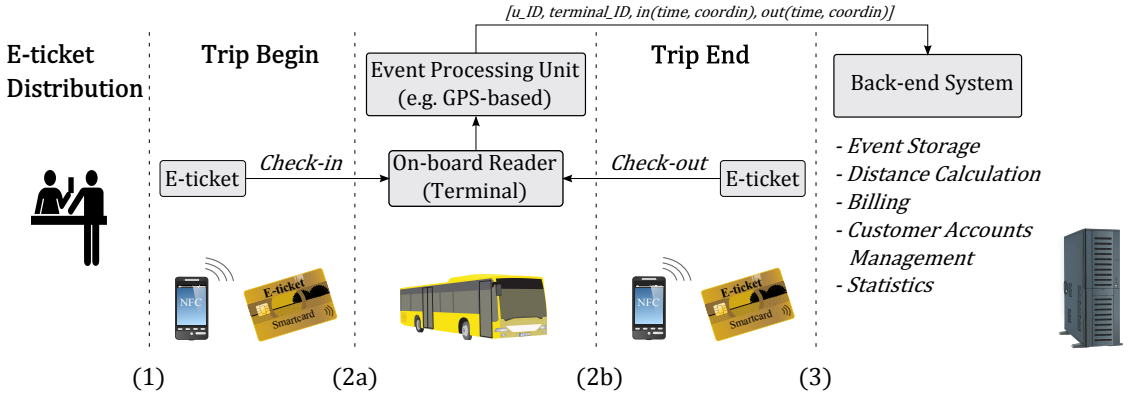

Figure 1: E-ticketing System Under Concern.

the following privacy properties similar to the classic CIA triad in information security (confidentiality, integrity, availability) are going to be defined below: *(1)* Pseudonymity, *(2)* Confidentiality, and *(3)* Unlinkability. The introduction of these notions enables to consider privacy from a technical point of view and therefore facilitates the subsequent process of technical countermeasures development.

Definition 1: *Pseudonymity* enables the communicating entities to perform the necessary information exchange without disclosing their Personally Identifiable Information (PII) during the communication session. In case the exchanged information is persistently stored, its pseudonymized form should prevent malicious parties from illegal identification of the respective entities. It is, however, possible to perform *subsequent identification*[1] by a special entity with respective authorization to ensure accountability (e.g. for billing purposes).

Definition 2: *Confidentiality* of information exchanged between communicating entities, which can also be persistently stored, ensures that the content of such a conversation is disclosed only to the legitimate parties possessing the respective authorization (e.g. the ones being authorized to use the respective message decryption key).

Definition 3: *Unlinkability* prevents a malicious party from performing linkage of different pieces of information which pertain to a certain entity (its information traces) and are distributed in time and/or space and therefore from illegally obtaining the entity's PII.

Analyzing the e-ticketing systems described in Section 2 against pseudonymity, confidentiality, and unlinkability, the following privacy threats can be identified, see Table 1.

[1]In contrast to the *anonymity* case when the subsequent identification should not be possible.

Table 1: The classification of privacy threats in e-ticketing systems for public transportation.

1. Unintended customer identification:
   (a) Exposure of the customer ID:
      i. Personal ID exposure (direct identification),
      ii. Indirect identification through the relevant object's ID[2] (de Chantérac and Graindorge, 2009).
   (b) Exposure of a non-encrypted identifier during the anti-collision session[3] (Bartels et al., 2009);
   (c) Physical layer identification (RFID fingerprinting[4]).
2. Information linkage;
3. Illegal customer profiling.

The first class of the aforementioned privacy threats (*Unintented Customer Identification*) considers the front-end of a target e-ticketing system. More specifically, the privacy issues may arise during the customer's check-in/check-out (see Figure 1). Moreover, the so-called "passer-by" attack (illegally initiating a short communication with an e-ticketing medium) is also possible. Consider the case of an exposure of a non-encrypted identifier during the anti-collision session (threat 1b, Table 1) or RFID fingerprinting (threat 1c). The vulnerabilities implied by this class of privacy threats can be exploited to mount the following attacks which can be used to infringe on

[2]For example, electronic medium ID (e.g. unique card number), application ID (the unique identifier of the installed e-ticketing application), etc.

[3]For example, during the check-in/check-out events.

[4]For instance, using the deviations in the backscatter frequency of an RFID chip as a distinguishing factor, see (Zanetti et al., 2011).

the customer's privacy:

- Intervening with the Radio Frequency interface between the e-ticket medium and the terminal:
  - Communication eavesdropping;
  - Relay attacks;
- Unintended interaction with the e-ticket medium (also outside the specifically designed locations for check-in/check-out) in order to compromise the privacy of its owner (Threats 1b, 1c).
- Spoofing the e-ticket medium into interacting with a malicious reader presenting itself as a legitimate terminal.
- Compromising the legitimate terminal (e.g. to mount replay attacks).

The second class of privacy threats (*Information Linkage*) addresses the cases when different pieces of information[1] directly and indirectly pertaining to a customer are combined with the purpose of obtaining an *identifiable* piece of information. This kind of (illegal) information processing can pave the way for subsequent violations of the customer's privacy and should, therefore, be considered during the development of a privacy-respecting e-ticketing system for public transportation.

The last threat class listed in Table 1 (*Illegal Customer Profiling*) addresses the issue of (illegal) creation of customers' profiles which is not foreseen by the system specification (e.g. for the loyalty programs) and therefore endangers the customer privacy and violates the privacy regulation. An example would be selling of the collected private user data to the third parties for marketing purposes, etc.

3.2 Countermeasures Discussion

Having provided a holistic classification of privacy threats in the previous section, a set of possible countermeasures is discussed below.

We suggest that the classic privacy-preserving mechanisms are used as an initial point of countermeasures development, namely:

- Anonymization (resp. Pseudonymization) techniques;
- Zero-Knowledge proofs (e.g. during the e-ticket authentication or bill computation);
- Encryption of the privacy-relevant information;
- Data Minimization.

[1]It can be, for example, information traces "left" by a customer as a result of the vulnerabilities implied by the first class of privacy threats listed in Table 1.

It is still an open research question how the aforementioned generic countermeasures can be *efficiently* applied to an e-ticketing system (without hindering its performance) across the system components (back-end, front-end) in a cross-layered fashion. Most of the privacy-preserving frameworks developed by the academia and implemented in real e-ticketing systems so far are rather tailor made targeting a specific privacy issue arising in a certain part of a system (e.g. customer anonymity in the front-end against a semi-honest terminal). A holistic approach which would consider the user privacy from the outset treating the e-ticketing system as a whole is, however, still missing.

In order to address this issue, a preliminary analysis of possible countermeasures against the privacy threats listed in Table 1 can be performed. An example is shown in Table 2. The resultant set of generic countermeasures forms the necessary basis for the further countermeasures elaboration required for the creation of a privacy-respecting solution.

3.3 Further Elaboration

Having obtained a set of generic countermeasures against the privacy threats classified in Table 1 (a holistic overview), a further elaboration is performed, namely:

1. Prioritization of the privacy threats listed in Table 1 with their respective countermeasures (determine which issues are of particular importance in a particular system).
2. Analysis (estimation) of the efficiency of countermeasures implementation:
   (a) A holistic system consideration (back-end, front-end);
   (b) Trade-off analysis (taking into account threat priority, item 1) and resolution of possible conflicts.
   (c) Registration of privacy threats against which the respective countermeasures can not be efficiently implemented in a system[2]
3. Creation of an elaborated set of countermeasures.

Prior to the countermeasures elaboration, it may be beneficial to formally assign trust levels to the system components. In order to ensure that the direct functionality requirements of a system are satisfied, we suggest that the back-end is considered to be *honest*. That is, the back-end can extract and process the private information containing in the combined travel

[2]This can be further used for privacy risk analysis and estimation of the system privacy friendliness, e.g. for certification purposes.

Table 2: Generic privacy threats and possible countermeasures.

Threats	Countermeasures
1. Unintended customer identification:	
a) *Exposure of the customer ID:*	
i. Personal ID exposure (direct)	Privacy-respecting authentication; ID encryption/randomization; access-control functions (Juels and Pappu, 2002)
ii. Indirect identification	ID encryption
b) *Unencrypted ID during anti-collision*	Randomized bit encoding (Lim et al., 2008b); bit collision masking (Choi and Roh, 2006; Lim et al., 2008a) (protocol dependent)
c) *PHY-layer identification*	Shielding; switchable antennas (Gudymenko, 2011)
2. Information linkage	Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing
3. Illegal customer profiling	Privacy-respecting data storage (back-end); the same as in threat 1

records (see Section 2.2) for billing purposes and loyalty programs. A bridging element (terminals), to the contrary, should not be fully trusted, since it is broadly distributed within the network for public transport and not always can be reliably secured against attacks (and manipulations). Therefore, a bridging element is assigned a *semi-honest* trust level and treated accordingly. The e-ticket itself together with its carrier mediums (smart cards, NFC smart phones), which form the front-end of a system, is in the possession of customers, out of the constant control of the public transport company, and hence is particularly vulnerable to a wide range of attacks. In order to adequately address this issue and secure the assets of a provider of a public transport service, the front-end should be treated as a *semi-honest* component.

Based on the assigned trust levels, a trade-off between the protection of the customer privacy (important for customers) and system security (in the direct interest of a public transport company) can be further considered. We believe that it can be effectively performed using the concept of a multilateral security (Pfitzmann, 1999; Rannenberg, 2000) which addresses the issues of *negotiation* of each party's protection goals in a multi-party environment.

4 RELATED WORK

There are several works explicitly addressing privacy issues in public transport systems. For example, the authors of (Sadeghi et al., 2008) developed a cryptography-based solution for a privacy-preserving authentication (during e-ticket validation) introducing the so-called trusted anonymizers. The latter can be used in an add-on fashion by a customer and is decoupled from the direct functionality of a system. That is, the e-ticket can still be validated in a non-privacy-preserving way if the respective customer's anonymizer is for some reason unavailable.

In (Hoepman et al., 2010), it was demonstrated how a protocol for proving anonymous credentials developed in (Batina et al., 2010) can be applied to the e-ticketing domain. The solution considers Java Cards as a carrier medium for an e-ticket and can be used for a privacy-preserving validation of an e-ticket.

Both of the aforementioned approaches, however, are targeted at a specific problem (privacy-preserving e-ticket validation) and do not holistically address the customer privacy in the public transport environment. A decent step towards this was made by the authors of (Heydt-Benjamin et al., 2006) who recognized the importance of privacy issues in e-ticketing systems and proposed a formal framework to protect the customer privacy using e-cash, anonymous credentials, and proxy re-encryption. It is unclear, though, if it can be used in the system described in Section 2.1 which is based on the check-in/check-out principle and regular billing (involving the transfer of combined travel records to the back-end and their subsequent processing).

5 CONCLUSION AND FUTURE WORK

The main focus of this paper is the protection of the customer privacy in ubiquitous e-ticketing systems for public transportation based on RFID/NFC technologies. In order to adequately address this issue, an ab-

straction of a target e-ticketing system was created. It was subsequently used to holistically consider the customer privacy across the system components and to identify the generic privacy threats. The resultant privacy threats classification, therefore, forms a sound basis for countermeasures development to protect the customer privacy in real systems. We provide the discussion of possible countermeasures together with the way of countermeasures refinement (elaboration) and their integration into a final privacy-preserving solution.

Having specified the framework for developing privacy-respecting e-ticketing systems for public transportation, we are going to actively use it in future for the development of our privacy-respecting solution for such systems. It is still unclear, however, if all of the identified privacy threats can be effectively considered within a real system and what the possible trade-offs are, which is left for the future work.

ACKNOWLEDGEMENTS

This work has been funded by the Free State of Saxony and the European Social Fund (ESF). The author would like to express his gratitude to the colleagues of Chair of Privacy and Data Security, TU Dresden, for fruitful discussions and their support.

REFERENCES

Bartels, C. et al. (2009). TR 03126 - Technische Richtlinie für den sicheren RFID-Einsatz. TR 03126-1: Einsatzgebiet "eTicketing im öffentlichen Personenverkehr". BSI, Deutschland.

Batina, L., , et al. (2010). Developing Efficient Blinded Attribute Certificates on Smart Cards via Pairings. In Gollmann, D. et al., editors, *Smart Card Research and Advanced Application*, volume 6035 of *Lecture Notes in Computer Science*, pages 209–222. Springer Berlin Heidelberg.

Choi, W. and Roh, B.-h. (2006). Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms. In Gavrilova, M. et al., editors, *Computational Science and Its Applications - ICCSA 2006*, volume 3983 of *Lecture Notes in Computer Science*, pages 279–287. Springer Berlin / Heidelberg.

de Chantérac, G. and Graindorge, J.-L. (2009). Focus Paper on Privacy in Transport IFM Applications. IFM Project, `http://www.ifm-project.eu/fileadmin/WP2/Draft_Deliverable_2.2.pdf`. Draft Deliverable 2.2.

Gudymenko, I. (2011). Protection of the Users Privacy in Ubiquitous RFID Systems. Master's thesis, Technische Universitt Dresden, Faculty of Computer Science.

Heydt-Benjamin, T. et al. (2006). Privacy for Public Transportation. In Danezis, G. and Golle, P., editors, *Privacy Enhancing Technologies*, volume 4258 of *Lecture Notes in Computer Science*, pages 1–19. Springer Berlin Heidelberg.

Hoepman, J.-H. et al. (2010). Privacy and Security Issues in e-Ticketing – Optimisation of Smart Card-based Attribute-proving. In Cortier, V. et al., editors, *Workshop on Foundations of Security and Privacy, FCS-PrivMod 2010*.

ISO (2008-2011). ISO 14443 Standards family. Identification cards – Contactless integrated circuit cards – Proximity cards.

Juels, A. and Pappu, R. (2002). Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In *Financial Cryptography 03*, pages 103–121. Springer-Verlag.

Land Transport Authority (2012). EZ-Link. `http://www.ezlink.com.sg/index.php`. Accessed on 30.10.2012.

Lim, T.-L. et al. (2008a). A Cross-layer Framework for Privacy Enhancement in RFID systems. *Pervasive and Mobile Computing*, 4(6):889 – 905.

Lim, T.-L. et al. (2008b). Randomized Bit Encoding for Stronger Backward Channel Protection in RFID Systems. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PERCOM '08, pages 40–49, Washington, DC, USA. IEEE Computer Society.

Octopus Cards Limited (2012). Octopus. `http://www.octopus.com.hk/home/en/index.html`. Accessed on 30.10.2012.

Pfitzmann, A. (1999). *Multilateral Security in Communications*, chapter Technologies for Multilateral Security, pages 85–91. Addison-Wesley-Longman.

Rannenberg, K. (2000). Multilateral Security – A Concept And Examples for Balanced Security. In *Proceedings of the 2000 workshop on New Security Paradigms*, NSPW '00, pages 151–162, New York, NY, USA. ACM.

Sadeghi, A.-R. et al. (2008). User Privacy in Transport Systems Based on RFID E-Tickets. In Bettini, C. et al., editors, *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PiLBA), Malaga, Spain*.

Trans Link Systems (2012). OV-Chipkaart. `http://www.ov-chipkaart.nl/`. Accessed on 30.10.2012.

Transport for London (2012). Oyster Online. `https://oyster.tfl.gov.uk/oyster/entry.do`. Accessed on 30.10.2012.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American Special Issue on Communications, Computers, and Networks*.

Zanetti et al. (2011). On the Practicality of UHF RFID Fingerprinting: How Real is the RFID Tracking Problem? In Fischer-Hübner, S. and Hopper, N., editors, *Privacy Enhancing Technologies*, volume 6794 of *Lecture Notes in Computer Science*, pages 97–116. Springer Berlin / Heidelberg.