Privacy in Mobile-ticketing

Rushil Dave
Aalto University School of Science and Technology
rdave@cc.hut.fi

Abstract

The electronic ticketing in public transportation has provided numerous benefits for both travelers and transport operators. The mobile ticketing in public transportation is a form of electronic ticketing which provides an easy way to use mobile phone as a travel card in which user can also purchase tickets anywhere, anytime via mobile internet. In this technique, travel card readers sense the data inside mobile phones using RFID or similar technology to validate the ticket. However, mobile-ticketing also introduces several privacy concerns such as the confidentiality of personal information and travel history of users. These privacy concerns can be addressed on the level of business modeling, government regulations as well as on technical basis. This paper introduces mobile-ticketing and related privacy concerns. The paper introduces several privacy requirements for mobile-ticketing. The paper also presents survey results of user expectations for privacy and related business modeling for mobile ticketing keeping privacy as a vital theme. In the end, the paper discusses several improvement proposals for mobile ticketing privacy.

KEYWORDS: privacy, mobile ticketing, user, business

1 Introduction

The public transportation services are a life line to the world population. The usage of such services eases many problems including traffic congestion and pollution. With increasing public transport services, easy use and access of such services are important. For example, the electronic ticketing has provided numerous advantages to both travelers and transport operators. [4] In most of the scenarios, public transportation ticketing systems must handle large user population with minimal restrictions on travel and electronic ticketing system helps achieving this. In many countries now, the contact-less smart cards are available, also known as travel cards, which can be loaded with ticket values or travel time period. Such travel cards shall be shown to card reader devices on transportation services to pay the ticket values or authenticate time period for the travel.

With introduction of various mobile technologies, the users now use mobile services apart from making calls and sending text messages. Mobile internet has provided the mobile users an access to World Wide Web. Mobile-ticketing is a service, in which users can use their mobile phones as a travel card and travel card readers in public transportation can sense data inside mobile phones while validating the tickets. [5] With this system, users can also purchase tickets anytime anywhere using mobile internet making public transportation feasible and ease to use.

The Near Filed Communication (NFC) [3] or RFID [12] technology is used in such service which integrates mobile tickets and mobile payments. By using this technology, travel card readers cannot distinguish the mobile phone from travel card. Mobile phone works as a travel card even when battery is depleted. Several high-end mobile ticketing applications also allow user to access locations, calendar, and journey planner while integrating them with ticketing and payment system. Users can also opt for receiving discount coupons and advertisements based on their locations or journey route.

Though mobile ticketing makes travel stress-free, certain user privacy and security concerns should be taken care of. The mobile phone contains user data and because of this, privacy mechanism [15] and confidentiality settings are essential while exposing mobile devices to the card readers. Also some mobile-ticketing applications provide users with location based services, journey planner and calendar integration making applications vulnerable to user privacy breaches. The payment solution and ticketing mechanism should be secured with powerful network security techniques while preventing user information leaks. Business modeling [8] of mobile services is important but most of the time, security and privacy issues are ignored while designing such models. In such service designs, trusted parties and security providers should be engaged throughout the process and service provision.

This paper has four sections emphasizing on mobile-ticketing privacy, related business analysis and privacy improvement suggestions. Section 2 describes the privacy concerns and requirements in details especially in mobile-ticketing application and service. Section 3 presents a survey for privacy expectations in mobile-ticketing. The survey results show the how and why user wants privacy in such mobile services and what measures they would like service providers to take for such services. Section 4 illustrates business analysis and modeling related to mobile-ticketing service while considering privacy as a significant part of business. Section 5 proposes several privacy improvement suggestions for mobile-ticketing service. In the end, conclusion describes the summary of the paper reviewing points made for privacy in mobile-ticketing service.

2 Privacy concerns in Mobile-ticketing

2.1 Working of Mobile-ticketing

Mobile-ticketing [5] is a mechanism works with intuitive touch-based interaction of mobile phones having Near Field Communication (NFC) technology. In many countries, the travel cards or paper tickets are used as a ticketing medium. Mobile ticketing brings the travel card or paper ticket into user's mobile device. In this way, users with mobile internet access can purchase tickets anytime, anywhere. Mobile devices can be used just like the ordinary card even when the battery of mobile device is depleted.

Near Field Communication (NFC) [3] technology is the basis of mobile ticketing. NFC is a short range technology aimed at mobile phones which works in radius of less than 10 centimeters. NFC is based on RFID and it has three modes of operations: i) card emulation, ii) read/write, iii) peer-to-peer.

Mobile ticketing application allows users to purchase mobile tickets with their mobile devices while replacing their travel cards. Mobile ticketing integrates mobile ticketing and payment systems therefore involving many security risks. Apart from basic ticketing functionality, high-end mobile ticketing solution also allows users to get several location-based, journey planner and event management services. The user could opt to receive advertisements relevant to his location and/or coupons used to receive discounts at retail locations near the planned route. [5] Other context aware information may also be utilized such as indoor location and traffic information. Such services involve very sensitive user data operations and to protect the privacy of user data should be the main importance.

The application runs on the cloud and stores relevant data on common cloud servers which can be accessed using network. Such cloud mechanism also involves user data privacy and there must be a mechanism to preserve it.

2.2 Potential privacy risks

As described in previous section, mobile-ticketing introduces several threats on user privacy. The authentication mechanism in mobile-ticketing may lose privacy if the information is leaked to the unauthorized third parties. Mobile-ticketing, in this case, should ensure that no user sensitive information should be revealed to the entities not trusted by the users. Also mobile phones contain user's personal data in digital format which can be copied while exposing mobile devices to the card reader. The corresponding security and privacy protocols to verify mobile-ticketing may also be subject to different attacks such man-in-the-middle, replay etc. The goal of mobile-ticketing system should be to prevent ineligible users from using transport system and thus most of the attacks or information leaks are intended to volatile this goal. Several privacy threats [15] and attacks [12] related to mobile-ticketing are described below:

1. *Location Threat:* Users carrying NFC device can be monitored and their locations can be revealed. Also the location of NFC device itself, regardless of who is carrying, can be disclosed with unauthorized access.

2. *Preference Threat:* The mobile device could be identified uniquely if proper access mechanism is not embedded in the device. Such information could disclose user's device preferences making them available to competing forces.

3. *Constellation Threat:* NFC is based on RFID technology forming a unique constellation around the user. Adversaries can track people without necessarily knowing their identities.

4. *Transaction Threat:* User's transaction information can be used to gather her location and time preferences. Also several financial data could be disclosed if transactions are not protected enough with proper network security protocols.

5. *Impersonation Attack:* Unauthorized entities in mobile-ticketing can provoke this attack by faking the user identity. Underlying protocols may fail to prevent man-in-the-middle as well as replay attacks on the system and such attacks may lead to the impersonation.

6. *Tracing Attack:* This attack can be done to acquire user sensitive information like user's location, behavior and preferences. When using authentication mechanism, token can be identified enabling attackers to trace user movements. If user uses payment method to purchase online tickets, the issuer can use link token to identify user's private information. Also eavesdropping of wireless communication may lead to a complete loss of user's privacy.

2.3 Privacy Requirements

Based upon privacy risk analysis in previous section, several requirements [15] [7] are gathered and illustrated as below for mobile-ticketing service:

1. *Confidentiality:* No unauthorized access to user-sensitive and personal data.

2. *Anonymity:* Unauthorized token (NFC Tag) identification should be impossible.

3. *Location Privacy:* Unauthorized tracing of user location and movements should not be allowed.

4. *Traceability:* Accessing current state of NFC token should not allow tracing previous as well as future protocol runs.

5. *Authentication:* No unauthorized users are allowed to use or access system. Only valid user tokens are accepted by verifier.

6. *Unforgeability:* Emulation and cloning of valid tokens or devices shall not be permitted.

7. *Accountability:* Provide users with accounted environment where contracts can be negotiated and users can choose between private and public data.

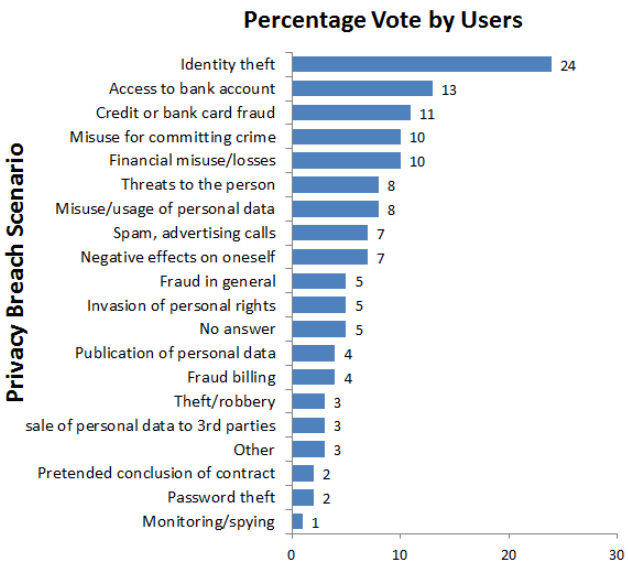

Figure 1: User Privacy Survey by Nokia Siemens Networks [13]

8. *Flexibility and Openness:* Provide users with flexible control to manage their personal information. Also, provide users with choice of selecting agents or software developed by third party privacy management companies.

9. *Ease of Use:* Provide users with user interface and functions to manage personal data easily.

10. *User Perception and Control:* Provide users with complete control over their private data. Allow them to decide what information should go to the engaged applications and systems.

3 User Expectations for Privacy - A Survey

3.1 Survey Scenario and Results

The survey [13] presented in this section was done by Nokia Siemens Networks in August and September 2009 with the views and behaviors of some 9,200 mobile phone and Internet users between the ages of 16 and 65. The sample was drawn from 14 countries, representing very different markets, such as Germany, China, the US and Argentina. The results presented in Figure 1 were gathered from the answer to the user privacy based question **"What are people most worried about?"**

3.2 Analysis of survey

Today's consumer demands more personalized services along with ease-of-use experience. Technologies are making such services increasingly available with access to more relevant content and security of user data. Users are at heart of such service provisioning making their wishes, behavior and personalized information very important to deal with.

The survey results show that most users are concerned regarding the privacy of their personal data in one or the other way. But this concern doesn't stop them to share personalized information when they think that the sharing is beneficiary. This discrepancy leads to the need of privacy mechanism implementation in the system architecture as well as in the business model especially in case of mobile and web services.

The users are worried about identity theft the most as identity theft may lead to several other privacy breach problems and abuses. Misuse of financial information in some or the other way is also marked as worrisome by significant portion of users. In mobile-ticketing scenario, several breaches are possible such as identity theft, misuse of financial information, fraud, sale of personal data, monitoring etc. and care should be taken to avoid such privacy breach while providing users with necessary control over their personal data.

4 Business Modeling for Mobile-ticketing Privacy

4.1 Privacy in Business

User control enhancements, business modeling and enforcement of government regulations are necessary to strengthen user perception of privacy. Privacy is required to be an important mechanism while building trusted electronic transactions and services. Businesses should embed privacy as one of the organizational block to the model as to address user privacy needs and enhance trust mechanism in the business.

The business model [14] defines architecture for the product, service and information flows, including a description of the various business actors and their roles; a description of the potential benefits for the various business actors; and a description of the sources of revenues. The focus, in this section, will be on the privacy function and their roles for the actors of the business model. Also the impact of privacy implementation on value proposition and revenue flows will be discussed. Figure 2 illustrates various actors of Mobile-ticketing service and the process flow among them.

The important actors for privacy implementation in Mobile-ticketing are Public Transport Operators, Financial Institutions, Trusted Service Manager, Mobile Network Operators, Handset Manufacturers and Users. The description of privacy implementation and related impact on their business functions is described below:

1. **Public Transport Operators** *Privacy Function:* Provide privacy and security enhancements for card reader; Act as a valid token (or ticket) verifier; Provide user authentication mechanism. *Impact on Value Proposition:* Enhanced security and privacy; Growth in user base; Minimal fraud. *Impact on Revenue:* Outflow on implementation of privacy and security mechanism; Inflow due to growth in user base and fraud minimization.

2. **Financial Institutions** *Privacy Function:* Provide network security for financial transaction; Provide privacy mechanism for personalized user data; Provide ease-of

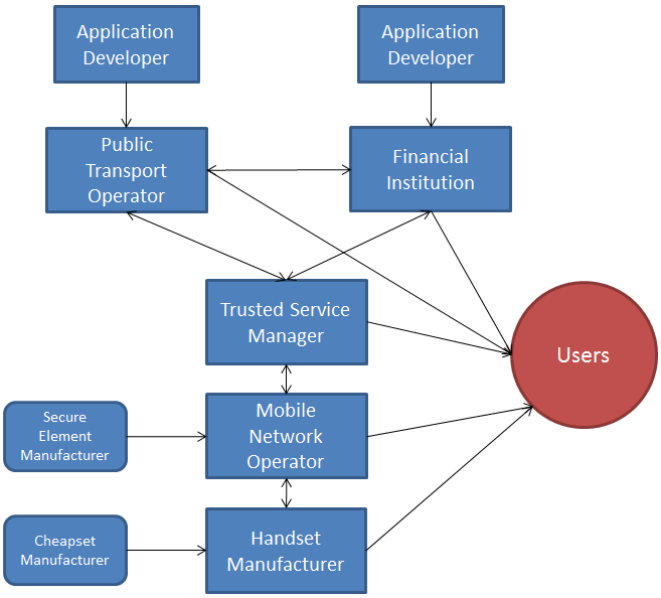

Figure 2: Business Actors and Process Flow in Mobile-ticketing [5]

use access and user control. *Impact on Value Proposition:* User base increment, User satisfaction; Charges from service operators. *Impact on Revenue:* Inflow due to user base and service charges.

3. **Trusted Service Manager** *Privacy Function:* Provide privacy enhancement tools and services; Provide users with user interface to manage personal information. *Impact on Value Proposition:* Business growth; Service charges from operator. *Impact on Revenue:* Outflow due to privacy platform implementation; Inflow due to service charges and business growth.

4. **Mobile Network Operators** *Privacy Function:* Provide communication network security over mobile internet; Provide security against location tracking and preference threats. *Impact on Value Proposition:* User satisfaction; User services introduction; Growth in new potential business areas. *Impact on Revenue:* Outflow due to security enhancements; Inflow from Mobile internet and network service charges.

5. **Handset Manufacturers** *Privacy Function:* Provide NFC device security against location, preference and constellation threats; Enhance Mobile handset security against information leaks. *Impact on Value Proposition:* Enhanced mobile device functionality; Potential business growth. *Impact on Revenue:* Outflow due to R and D cost for NFC and security enhancements; Inflow due to sale of NFC mobile devices.

6. **Users** *Privacy Function:* Provide feedback to service operator; Get aware of privacy risks; Manage privacy for personal information. *Impact on Value Proposition:* Enhanced mobile ticketing service; Ease-of-use calendar, location services. *Impact on Revenue:* Service charges outflow; Discount coupons.

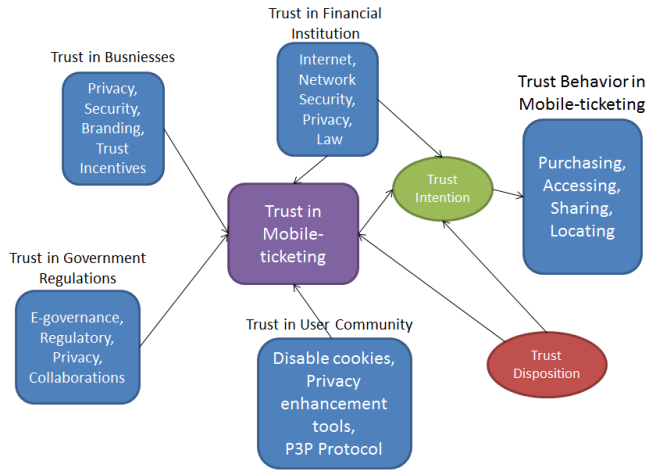

Figure 3: Trust Intentions by Players of Mobile-ticketing Business [8]

4.2 Privacy and Trust Model

The privacy and trust model described in this section is a common thread throughout all the business actors' interventions for privacy and trust. [8] In online and mobile services environment, the perception of trust and privacy often depends on individual perceptions of personal information. Figure 3 depicts the trust intentions by the actors of mobile-ticketing service. Business firms, providing this service, shall provide network security and privacy enhancements in the applications and service architecture itself. Government provides privacy by introducing regulations and collaborations among the institutions involved in provision of this service. Financial institutions shall enforce network security and privacy in online transactions taking place in mobile-ticketing. Users are also part of trust provisioning and they should take care of their personal information while disabling cookies and using several privacy enhancement tools. User community shall often provide feedback to the service providers as to improve privacy and trust in the service. All such trust intentions are needed in defining the behavior of mobile-ticketing service. Such trust intentions shall enhance the activities such as purchasing tickets, accessing user data, sharing user data and location based information gathering.

5 Privacy Improvement Proposals

5.1 Privacy for NFC device (tag)

NFC devices can be loaded with encrypted PIN or password. So when user registers their device with service operator, the PIN will be exchanged between user device and service operator. [12] Card reader then uniquely detects NFC device when shown to verify mobile ticket. Such mechanism is also possible with pseudonyms where NFC device can contain small collection of pseudonyms and rotates it at time intervals. Card reader must be in sync with NFC device to uniquely identify and verify the ticket. Third party may develop "NFC device guards" to protect NFC devices from privacy leaks and users can also have choice to select from

range of such solutions. Also sleep mode for NFC device enhances the privacy of device where NFC devices shall remain in sleep mode and only valid card readers can awake them up.

5.2 Government and Legislation

Governments and related organizations can help improving privacy in such services oriented for users. Policy making, Trust building, collaborations among participants, support for PKI infrastructure, Online trust education, e-governance etc. should be provided by government which helps building trust among users. Government shall also provide a mechanism to check the trust rating for service providers and other parties involved in the business. Legislation should provide data protection guidelines for NFC technology as well as important public services. Public services such as mobile-ticketing must abide to privacy and data protection laws [6] introduced by legislation.

5.3 Privacy in Business Model

Business shall provide data/information fragmentation within a sector or among various sectors to protect user data with highest priority. Such mechanism can be achieved by introducing pseudonimity, anonymizers, cookie breakers [8] and business divisions. Another option to enhance privacy in mobile-ticketing business model is the introduction of Infomediaries [2] which act as trusted privacy providers similar to trusted service managers mentioned earlier in this paper (See Figure 2). Such Infomediaries can be divided into two categories:

1. **Customer Oriented Infomediary:** These infomediaries act for users' benefit. They have their own databases and enlarged marketing skills. They collect product offering related information, build user profiles, match profiles with service provider specifications as well as offer an interface between service providers and super infomediary. They also connect to other customer oriented infomediaries if they cannot find user's profile in their own database.

2. **Super Infomediary:** These infomediaries are trusted by both service providers and users. These infomediaries can be formed by public-private partnership model where governments and legislative bodies also participate to strengthen their functions. Super infomediaries administer and control model procedures. They set up PKI infrastructure for customer oriented infomediaries. They protect privacy, anonymity and authenticity in the model. They collect and protect users' personal information and preferences.

Introduction of infomediaries can help anonymity-aware and privacy-concerned users to protect their private information while using mobile-ticketing like services. Such model allows users not to disclose their preferences and personal data to the service providers and at the same time allows service providers to sell their service offering without violating users' privacy.

5.4 User-tailored Privacy

Users shall be provided the personalized tutoring with virtual e-learning environment to share awareness of personal data protection. [10] Another approach to share privacy knowledge among users is to implement privacy awareness system [11] which assists users to know about privacy and gives ability to users to respect other users' personal information. This system provides tools to collect and process user data along with the interfacing system which connects such collection and processing tools to help users to keep their promises. Such system allows users to stick to their statements and actions making them accountable to the information they have provided.

A recommendation system shall be designed in a user-friendly non-intrusive manner [9] while including possibility of discontinuing. A tailored web and mobile portal shall be provided to users to manage their personal information. In this approach, service designers should allow users to have different views and options while dealing with sensitive information. Users should be provided with different sections categorized according to information sensitivity. Users shall also be provided with warnings if certain data is used by or sent to third-party.

P3P [1] is a well-known standard defined by W3C consortium which enables users to define their own privacy settings with user interface generally in a matrix or choice box form. P3P generates machine readable format of user privacy settings to protect user's personal data. Mobile-ticket system can implement such interface and provide it to users while they register for the service. In this way, users can easily define their privacy settings related to the mobile-ticketing service. It should also be possible for users to integrate such settings from trusted third party P3P interface providers making settings more generic and easy to use.

6 Conclusion

Mobile and web services market is growing rapidly and services are helping users to make their lives easy. Many of such services use and store personal information of users which makes user data privacy a very important concern. Privacy, thus, is becoming an integrated part of any such services providing protections against user data leaks. Mobile ticketing service is no difference here where users' preferences, locations, behavior and mobile device data have potential privacy threats. In this paper, several threats and attacks are explained for mobile-ticketing which may apply to the services falling in line with mobile-ticketing. Privacy requirements are also discussed in this paper which leads to better service architecture for mobile services. A survey mentioned in this paper indicates that around 95 percent users are concerned about privacy in one or the other way making personal data protection a viable need. Business model, illustrated in this paper, shows privacy function and its impact on value as well as revenues for various business actors involved in mobile-ticketing business. Finally, several privacy improvement proposals are discussed which can be used to gain better privacy and data protection in mobile-ticketing service scenario. All in all, this paper shows how and why privacy is an important

aspect in mobile services while taking technical and business impacts into consideration for mobile-ticketing service.

References

[1] L. F. Cranor. P3p: Making privacy policies more useful. *IEEE Security and Privacy*, 1:50–55, 2003.

[2] D. Gritzalis, K. Moulinos, and K. Kostis. A privacy-enhancing e-business model based on infomediaries. In *Information Assurance in Computer Networks*, pages 72–83. Springer Berlin / Heidelberg, 2001.

[3] E. Haselsteiner and K. Breitfuß. Security in near field communication (nfc). *In Workshop on RFID Security*, 2006.

[4] T. Heydt-Benjamin, H. Chae, K. Fu, and B. Defend. Privacy for public transportation. In G. Danezis and P. Golle, editors, *Privacy Enhancing Technologies*, volume 4258, pages 1–19. Springer Berlin / Heidelberg, 2006.

[5] A. Juntunen, S. Luukkainen, and V. Tuunainen. Deploying nfc technology for mobile ticketing services - identification of critical business model issues. In *Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on*, pages 82–90, June 2010.

[6] E. C. Justice. Data protection. Internet Article.

[7] D. Jutla and P. Bodorik. Architecture for user-controlled e-privacy. In *Proceedings of the 2003 ACM symposium on Applied computing*, SAC '03, pages 609–616, New York, NY, USA, 2003. ACM.

[8] D. Jutla and P. Bodorik. A client-side business model for electronic privacy. *16th Bled eCommerce Conference and Transformation*, pages 463–479, 2003.

[9] D. Jutla, P. Bodorik, and J. Dhaliwal. Supporting the e-readiness of small and medium sized enterprises: Approaches & metrics. *Internet Research Journal: Electronic Networking Applications and Policy*, 12(2):139–164, 2002.

[10] A. Kobsa. Tailoring privacy to users' needs. In M. Bauer, P. Gmytrasiewicz, and J. Vassileva, editors, *User Modeling 2001*, pages 301–313. Springer Berlin / Heidelberg, 2001.

[11] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In G. Borriello and L. Holmquist, editors, *UbiComp 2002: Ubiquitous Computing*, pages 315–320. Springer Berlin / Heidelberg, 2002.

[12] H. Lee and J. Kim. Privacy threats and issues in mobile rfid. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, volume 5, pages 20–22. IEEE, Apr. 2006.

[13] N. S. Networks. Privacy survey 2009. Technical report, Nokia Siemens Networks, 2009.

[14] T. Paul. Business models for electronic markets. *CommerceNet*, sep 1998.

[15] A. Sadeghi, I. Visconti, and C. Wachsmann. User privacy in transport systems based on rfid e-tickets. In *1st International Workshop on Privacy in Location-Based Applications*, 2008.