Considering Context in Mobile Ticketing

Peter Fröhlich
ftw.
Donau-City Strasse 1
1220 Vienna, Austria
+43/1/505 28 30-85
froehlich@ftw.at

Oliver Jorns
ftw.
Donau-City Strasse 1
1220 Vienna, Austria
+43/1/505 28 30-64
jorns@ftw.at

Raimund Schatz
ftw.
Donau-City Strasse 1
1220 Vienna, Austria
+43/1/505 28 30-64
schatz@ftw.at

ABSTRACT
This paper discusses the role of context in a mobile ticketing system for public transport. Although context-awareness in this domain promises benefits such as simplified and smarter user-system interaction, the context of telecommunication services raises issues of security and privacy. We present a system architecture utilizing a privacy enhancing protocol that allows secure exchange of sensitive user-related data. This enables context-aware 3rd party applications for mobile ticketing which make use of dedicated telecom services while at the same time preserving user privacy.

Categories and Subject Descriptors
D.2.11 **[Software Engineering]**: Software Architectures - *Domain-specific architectures* , H.1.2 **[Information Systems and Principles]**: User/Machine Systems – *Human factors.*

General Terms
Design, Security, Human Factors.

Keywords
Mobile Context, Mobile Ticketing, Public Transport, Privacy and Security, Context Awareness.

1. INTRODUCTION
Understanding and using context is one of the main challenges in mobile human-computer interaction [12]. While mobile contexts in general impose strong constraints on human information processing and available interaction bandwidth [14], context detection and exploitation at the same time offers the advantage of tailoring services to the individual user's current situation and needs.

Various application scenarios and research prototypes for context-aware mobile services have been discussed, such as navigation aids, interactive advertising, tour guides, presence awareness systems, personalized news services, support of legal problem solving etc. (see [4, 11]). Ticketing processes increasingly constitute the basis of many transactions in mobile services. The most obvious application area of mobile ticketing is public transportation, but also other services and business models in the area of m-banking, retail and events have similar underlying processes [9]. We believe that in terms of social and economic relevance, mobile ticketing are promising candidates for mass-deployment of mobile context-aware services. The reason is that in this domain, context-awareness has the potential to simplify user-system interaction by automatizing certain steps and providing added benefits such as contextualized wayfinding.

Research into mobile context-aware systems and services started with a focus on technical development of context sensing technologies. In recent years, however, a strong trend towards the exploration of the human aspects of mobile context can be observed [5, 14]. Unfortunately, only a few research projects have managed to integrate both a strong user-oriented perspective with close-to-market technical maturity [3]. Often the proposed solutions of these projects are rather conceptual (i.e. not implemented due to technical infeasibilities) or hardly deployable on the market by now (e.g. because of privacy concerns or low commercial viability of the used context sensing technologies used).

One important issue to consider is which context factors are most relevant and useful for an envisaged application or service. Although it is true that "there is more to context than location" [12], even this most obvious mobile context parameter has only recently begun to be usefully exploited for mobile telecommunications services [3]. The role of context factors beyond physical location, most obviously time, but also system events and user preferences need to be explored more thoroughly with regard to the specific application and task domain. Especially the role of context in the domain of mobile ticketing is not yet satisfactorily explored.

Another basic requirement for the success of such systems deployed in the real world is to take care of human acceptance barriers. In particular when applications involve commercial transactions (such as in ticketing), users need to trust their applications. Therefore they do not want the appearance of the interface or application behaviour to change in uncontrolled or erratic ways [6]. In addition, users' tolerance for interruptions is also limited and context-dependent in itself [10]. This factor constrains possibilities for keeping users in the loop with semi-automatic context management. Therefore, the user's (inter)action costs have to be as low as possible (and of course definitely lower than the gain by the respective service). This means that data from the user (e.g. context factors such as personal preferences) needs to be captured in unobtrusive ways in order to ensure broad adoption. On the other hand, such automatic capture of data (such as location information and interaction history) will only be accepted if the user trusts not only the application itself, but also his service provider's data handling reliability and competence [2]. Therefore, secure network communications in general as well

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
MobileHCI'05, September 19–22, 2005, Salzburg, Austria.
Copyright 2005 ACM 1-58113-000-0/00/0004…$5.00.

as privacy-preserving transaction- and context-management mechanisms are essential prerequisites for services in this domain.

In this paper we present our approach to integrate context into a mobile ticketing system for public transport. In section 2 we discuss our ideas for including context in mobile ticketing processes. Section 3 presents our architectural approach, focusing on security and privacy issues. Section 4 summarizes our conclusions and provides an outlook on future work.

2. Context in Mobile Ticketing

2.1 Project Goals

Our approach to the abovementioned challenges is

- to take a user-centered perspective to service development in general and context factors in specific
- to develop technical solutions which integrate ticketing processes, context management and privacy handling
- to focus on context gathering techniques that are applicable to state-of-the-art mobile phones and telecommunications services
- to consider important user acceptance factors of context-aware services such as effortless interaction, usefulness and trust.

2.2 Mobile Ticketing Scenario

In the following, some of our basic ideas for context in ticketing processes are illustrated by means of usage situations and the underlying technical processes in the public transportation domain.

2.2.1 Episode 1: Automatic ticket offer

User situation: Fred is in a hurry, because he wants to visit a friend at the other end of the city. As he approaches the metro station he realizes that he still needs to buy a metro ticket. He grabs his mobile and sees that the mobile is already offering him to book a ticket.

Technical background: *Fred's mobile receives a link request from the station's ticketing application which broadcasts its service via bluetooth or WiFi within the vicinity of the station. As Fred has subscribed to the mobile ticketing service and his client application has already hooked in before with the same station's ticket application, his mobile application automatically accepts and displays the incoming ticket order request.*

2.2.2 Episode 2: Effortless interaction

User situation: Fred is not the only person who still has to buy a ticket today. The crowd in front of the ticket machine induces him to better buy the ticket comfortably via his mobile phone. He simply issues the voice command "One single ticket".

Technical background: *As soon as Fred's mobile application is wirelessly connected to the receiver embedded in the ticket machine, the context 'Metro station U1 entered' is established in the system. This explicit context allows ticket order using a short voice command, because it removes recognition and interpretation ambiguities.*

2.2.3 Episode 3: Reliability and verifiability

User situation: Immediately after booking his ticket, Fred receives a visual representation of it on his mobile. This way he can be sure to have no problems when being checked by a train conductor.

Technical background: *Additionally, depending on the respective ticket type, the ticket application further sends some codes such as e.g. background color and patterns or pictograms with watermarks to the mobile application. These codes change on a daily basis and allow the application to visualize the ticket. This, on the one hand gives Fred the affirmation that the ticket order is accomplished. On the other hand, this method represents a simple but secure method which allows fast visual verification of tickets.*

Figure 1. Fred buying a mobile ticket (Episodes 1-3).

2.2.4 Episode 4: The supportive ticket

User situation: Today, Fred's planned route is not viable because of construction work. Fortunately, the mobile ticketing service notifies him and provides him with map-enhanced directions providing an alternative route.

At the end of the trip, Fred is informed by the service that his time-limited ticket is about to expire and that he may extend the ticket life time. Fred is already in a meeting so he does not respond to the request, and the system automatically finalizes the ticket process.

Technical background: *The context manager embedded in the system interprets all incoming context information according to Fred's personal profile. Based on specific heuristics and ontologies, it decides from case to case whether the user should be notified or not and how this should be done. In the abovementioned way-finding example, the context manager checks user location, infers likely routes and destinations from usage history, interprets wider transportation system state (e.g. construction works, breakdowns), accesses route calculations, checks the personal profile and preferences to reason about the probability of help required.*

2.2.5 Episode 5: Ensured privacy

User situation: Fred does not hesitate a second to use untrusted 3rd party services. His trust may partly be grounded by the fact that he only subscribes to one major, well-renowned telco/service provider who ensures secure and anonymous connections to services from 3rd party providers he subscribes to.

Technical background: *Secure network connections and protection of personal information are preconditions for users' trust in mobile services. In this regard, the ticket system uses a privacy enhancing protocol which allows exchange of sensitive context and transaction-related data .*

3. Mobile Ticketing Service Architecture

In this section, we discuss the system architecture, which reflects some of the requirements as previously discussed. In addition we focus our solution for ensuring security and privacy.

3.1 System Architecture

The central part of the Ticketing Service Architecture is the Ticketing Application which comprises several information sources from telco services such as the Location Service which delivers location information or the Traffic Service which makes

available information about the current traffic condition (see Figure 2). Further, the system may also generate and send messages that are conveyed to users by a Messaging Service. The term message has in this context to be understood in the broader sense and may include e-mail, SIP, SMS, MMS as transport medium to deliver any kind of information that may be of interest for the user. In this context, messages range from notifications dedicated to user to inform about the necessity to change trains due to breakdowns to system messages which e.g. induce the mobile to update its location data at the Location Service.

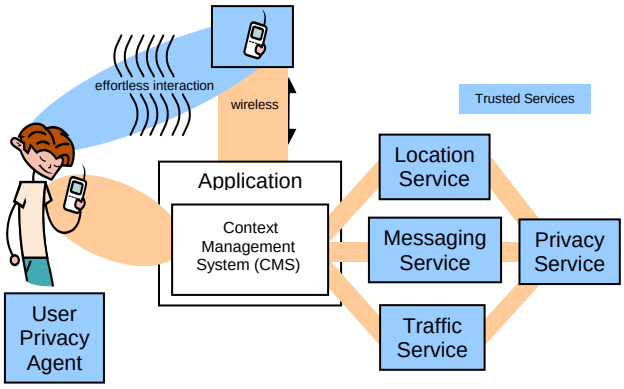

Figure 2. Ticketing Service Architecture

The heart of the ticketing application is the Context Management System (CMS). Its major task is to create, provide and subsequently process all kinds of transportation tickets.

This requires, that the CMS is extendable in terms of additional information services, which includes to the greatest possible extent, the ability to adapt application interfaces without the need of manual configuration. Another challenge is to achieve the CMS's ability to process almost any kind of ticket that factors in some predefined guidelines. This not only requires careful design of the tickets but also flexible and adaptive models of the mapped user context.

The user's mobile application implements a dedicated module which is called Privacy Agent. It is connected through the Privacy Service and allows secure and privy use of tickets. The next section discusses further important requirements that are closely related to the already mentioned general ticket requirements but rather concerns privacy enhancing mechanisms and protocols needed to prevent fraud.

3.2 Security and Privacy Solution

A highly important aspect in context-aware telecommunication services that is still not properly solved is the building block that deals with security and privacy. We believe, that the realization of the vision of context-aware systems cannot forge ahead without savvy security and privacy solutions at hand. It is clear, that "perfect" practicable privacy and security is hard to achieve, if at all. The more importantly is to understand, that any proposed privacy solution can only balance as many partly exclusive factors that influence the context-aware system.

To cope with this best possible, we apply the privacy enhancing protocol we introduced in [8]. It allows us to realize secure communication channels between each entity and further achieve a very high level of user's privacy without the need of high computation costs. The protocol is mainly based upon transaction pseudonyms which are generated by the user's Privacy Agent. This agent is part of the mobile ticket application and connected through the Privacy Service. For each request, the Privacy Agent generates a unique transaction pseudonym which can only be translated back to the respective user's identity or persistent pseudonym by the Privacy Service (see Figure 3). Although the ticket application processes tickets on behalf of each user, the identity of each user stays privy.

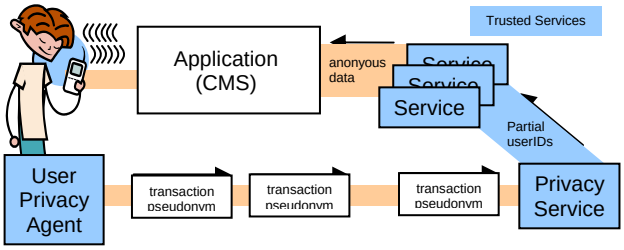

Figure 3. Transaction Pseudonyms translated back only to User Identities

3.2.1 Total Anonymity versus Pseudonymity

Depending on the respective application at hand, it sometimes seems to be the best be able to provide total user anonymity. If, for example, we look at the real world ticket scenario we can see that physical transport tickets are used anonymously. From this point of view it seems that also virtual tickets should be at least anonymous. Since anonymous real world tickets are widely accepted, at first glance it seems to make sense to provide total anonymity for digital tickets too. However, total user anonymity is too "privy" and imposes disadvantages in the sense that it restricts digital tickets to the same functional boundaries or even more rigid ones as they hold for paper tickets. For example, some sort of real world transport tickets are transferable whereas total anonymous digital tickets are not. Even if digital tickets are powerful through inclusion of additional services, user acceptance will suffer dramatically if basic functionality such as transferability is limited or even infeasible in favor of total anonymity.

3.2.2 Non-persistent and persistent Pseudonyms

According to varying requirements, the privacy enhancing protocol allows not only secure exchange of data. Furthermore, the protocol enables applications to subsequently process tickets of either total anonymous or pseudonymous users. Therefore, the protocol can be applied in two different ways. On the one hand the protocol uses only non-persistent pseudonyms. Non-persistent pseudonyms change for every single service request and allow secure and privy transmission of sensitive user data. Further, non-persistent pseudonyms enable applications to process tickets by preserving total user anonymity. On the other hand the protocol may also implement a combination of non-persistent and persistent pseudonyms (see Figure 4). Persistent pseudonyms allow applications to recognize particular users without the need of revelation of any identity data of the user. Therewith, given persistent pseudonyms, applications do not process tickets of anonymous users but rather of pseudonymous users which allows applications to recognize users without the need to learn about their true identity. This however requires applications to additionally request the translation of non-persistent pseudonyms to the respective persistent one.

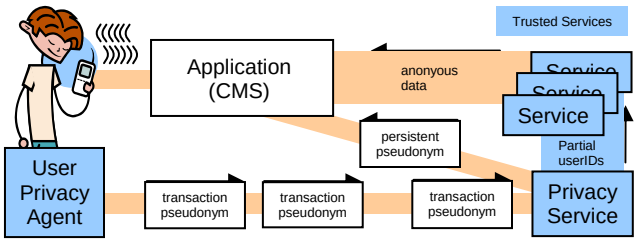

Figure 4. Transaction Pseudonyms translated to User Identities and Persistent Pseudonyms

Recapitulatory, one characteristic of the privacy enhancing protocol is that it allows applications to process tickets of users that are totally anonymous. Another one is that the privacy enhancing protocol can be configured in such a way that applications that are given persistent pseudonyms may recognize users and therewith better utilize resources on behalf of the pseudonymized user.

In regard to the CMS, the privacy enhancing protocol further allows secure and privy content-based user subscriptions [7]. This means that user who configured and ordered a ticket from the application simultaneously initiate the application logic to translate the raised ticket request into a specific subscription language that can later be interpreted by the CMS. With the help of a subscription language, even complex event requirements as well as their relations among each other can be expressed in an interpretable form. Such personalized expressions of events and their relations allows the CMS to fully map the functional set and modalities of real world tickets to virtual ones with the advantage to react on external influences such as traffic conditions.

4. CONCLUSIONS

Context-aware digital tickets for public transport as described above have several advantages in comparison to physical tickets. Since a digital ticket's content is dynamic, it can be easily transferred and additional information such as elapsed time, information about when to change for the next transportation as well as other kind of information can also be part of a ticket.

An advantage of the public transport domain is that the system can assume a closed world (i.e. the transportation network and its users). Therefore the underlying context model has limited complexity which makes context-aware ticketing feasible: time and semantic location can be derived from infrastructure context (e.g. nearest stationary access point), the wider world context from the state of the transportation network, and user aims and preferences from personal settings and usage history. However, capturing and storage of such sensitive user data raises issues of privacy and security which we solve through the use of a privacy enhancing protocol which is based on easy to compute transaction pseudonyms. In addition to secure transmission of sensitive data such as information about the user's identity, this protocol further enables non-trusted 3rd party applications to utilize sensitive context-data such as user profiles and interaction histories while at the same time maintaining anonymity.

5. ACKNOWLEDGMENTS

The work presented here is part of the projects X0 and SUPRA at the Telecommunications Research Center Vienna (ftw.). The work is supported by the Kplus program of the Austrian Federal Government.

6. REFERENCES

[1] Bhrat P., and Crowcroft J. Ticket Based Service Access for the Mobile User, *Proc. MobiCom'97*, Budapest, Hungary

[2] Boehm A., Leibner, T., and Reufenheuser B. Trust and Transparency in Location-Based Services, *MobileHCI'04*, Glasgow, Scotland, September, 2004.

[3] Burak, A., and Sharon, T.. Usage Patterns of FriendZone – Mobile Location-Based Community Services. *Proc. CHI2005*, 2005.

[4] Chen, G. and Kotz, D. *A survey of context-aware mobile computing research*, Technical Report TR2000-381, Dartmouth College, Hannover, NH, 2005.

[5] Dourish, P., What we talk about when we talk about context, *Personal and Ubiquitous Computing*, 8(1): 19-30, 2004.

[6] Erickson, T. Some Problems with the Notion of Context-Aware Computing, *Communications of the ACM*, Vol. 45, No. 2 , pp 102-104. February, 2002 (Technical Opinion).

[7] Eugster P. Th., Felber A. P., Guerraoui R. and Kermarrec A.-M., The Many Faces of Publish/Subscribe, *ACM Computing Surveys (CSUR)*, Volume 35, Issue 2, Pages 114-131, (June 2003), ISSN: 0360-0300.

[8] Jorns O., Jung O., Gross J., and Bessler S. A Privacy Enhancement Mechanism for Location Based Service Architectures using Transaction Pseudonyms, *Second International Conference on Trust, Privacy, and Security in Digital Business, (TrustBus' 05)*, Copenhagen, Denmark, August, 2005.

[9] Mobile Electronic Transaction, Ltd., 2003. *MeT White Paper on Mobile Ticketing*, http://www.mobiletransaction.org/pdf/R200/white_papers/MeT_White_paper_on_mobile_ticketing_v1.pdf

[10] Oulasvirta, A., Tamminen, S., Roto, V., and Kuorelahti, J. Interaction in 4-second bursts: The fragmented nature of attention in mobile HCI, *Proc. CHI 2005*, Portland, Oregon, ACM Press, 2005, pp. 919-928.

[11] Quirchmayr G. Adaptive Context Aware Legal Work Environments - Basis for Developing Legal Live Spaces on the Web, *Proc. of the 2nd Intl. Conference on Web Information Systems Engineering*, Volume 2 (Workshops), December 2001, Kyoto, Japan

[12] Schmidt, A., Beigl, and M., Gellersen, H. W. There is more to Context than Location, *Proc. of the Intl. Workshop on Interactive Applications of Mobile Computing (IMC98)*, Rostock, Germany, November 1998.

[13] Schmidt, A., and Van Laerhoven, K. How to build smart appliances?, *IEEE Personal Communications*, 8 (4), 2001, 66-71.

[14] Tamminen, S., Oulasvirta, A., Toiskallio, K., and Kankainen, A. Understanding mobile contexts. *Personal and Ubiquitous Computing*, 8 (2), 2004, 135-143.