Journal of Ubiquitous Systems and Pervasive Networks
Volume 4, No. 1 (2012) pp. 15-20

The protection of privacy in the i-Tour framework

Scott Cadzow[a]*

[a]*Cadzow Communications Consulting Ltd, Sawbridgeworth, England, UK CM21*

Abstract

In this paper we describe the privacy concerns, risks and protection mechanisms within the i-Tour project. The role of legislation for privacy in Europe and other global sectors is examined to describe a privacy protection model that complies with the immediate target of European deployment but that also looks forward to the re-use of the approach across a wider global territory and technical deployment range.

Keywords: *Security; Privacy; Regulation*

1. Introduction

Privacy as a right of citizens is often cited as a key requirement of network and service providers to maintain, however privacy is not a simple tangible entity that lends itself to simple schemes of maintenance and protection. There are a number of ways of viewing privacy and the tolerance of users to release of private information. The approach in i-Tour is to balance the release of private data with rewards or benefits that encourage sharing of some private data in the knowledge that that data is maintained in a restricted space.

Security and privacy are protected in most systems by a combination of technology and process. In recent years there has been significant concerns raised in the press and in a number of privacy forums about the failure of modern systems to adequately preserve user privacy. The goal of the "Design for Assurance" and "Privacy by Design" paradigms is to address both privacy and security at the design stage of a product or system. However whilst the "design for assurance" paradigm can be moved to a set of concrete steps it is less straightforward in the "privacy by design" area.

The fundamental problem of privacy protection is that expectation of privacy is highly dynamic and has deep rooted cultural and societal mores associated to it. As we grow from childhood through teenage and student years to parenthood and beyond our relationships and our expectations of privacy change with us as we develop. The need to separate work relationships from home and play relationships is key to privacy and what is natural in the non-technical domain is difficult to replicate in the connected worlds of the internet and has been complicated by the rush of "social networking" opportunities in which the need to be seen as an early adopter or as a social leader. However the nature of the global internet means that the borders which are inherent in the non-internet world disappear and actions in any geographic area are made visible globally. There are in most inter-personal relationships reasonable expectations of friends keeping confidences and recognizing the scope of such confidences in both time and location.

There has been an ongoing debate on the relevance of privacy protection in the internet world but as privacy regulation is based on principles and not on technology it is essential that technologies do everything to protect privacy. However privacy has many dimensions including data or informational privacy, spatial (location) and temporal privacy, bodily privacy and behavioural privacy of which the current regulation addresses only the first. In the i-Tour project care has been taken to address all of these aspects and to also take the contextual character of privacy into consideration.

Privacy is defined within i-Tour as the right of the individual to have his identity and agency protected from any unwanted scrutiny and interference. It reinforces the individual's right to decisional autonomy and self-determination.

The common approach in privacy protection is to identify the existence of Personal Identifying Information (PII) and to take steps to ensure it is

* Corresponding author. E-mail: scott@cadzow.com

DOI: 10.5383/JUSPN.04.01.003

protected using methods both technical and procedural. However this approach tends to lead to a concentration on data or informational privacy and to avoid the other aspects.

The functional approach to privacy protection has become concentrated in recent years on 4 key areas: Pseudonymity; Anonymity; Unlinkability; and, Unobservability. Of these i-Tour has concentrated on Pseudonymity and Unlinkability, and in doing so it has made steps to separate the core functions of identification and authorization. One of the aims to reinforce privacy is to ensure that the system does not reveal data (and to give guidance to the users on minimizing the amount of personal data they reveal in payload). This means looking beyond the existing Public Key Infrastructures and associated Certificate schemes to ensure all parts of the i-Tour system are privacy protecting.

2. i-Tour overview

i-Tour is very simply a means of optimizing the use of transport networks in urban environments. At the heart of i-Tour is a multi-modal routing model that takes into account the travel preferences of the user to find optimal routes that both satisfy the user and wider society. Whilst i-Tour offers route planning and updates in real time this is insufficient by itself to distinguish it from the herd, this is achieved in large part by introducing a gaming model for rewarding the user to achieve many of the benefits of ITS (see later for a wider analysis of ITS and i-Tour).

In addition to the multi-modal routing and gaming models i-Tour also follows the design approaches of "Design for Assurance" and "Privacy by Design" to maximize security and privacy to i-Tour users.

There are many aspects of i-Tour that reflect the trends in social networking and of Web 2.0 for user generated content and dialogue. The main area of such interaction is in what is called the recommender engine where i-Tour users can attach comment to Points of Interest and events. In addition i-Tour users can integrate their agendas into their route planning and the system can make recommendations for things to do (e.g. identifying PoI or Events that match the user profile that may be on during their trip or which could be accommodated into their trip with some changes).

3. Design for Assurance

The role of design for assurance is a means of answering the age old problem of how to measure the security of a product or system. The scheme used in design for assurance is based on the internationally recognised "Common Criteria for Security Assurance Evaluation" published as ISO 15408 [1] and modified for systems development by ETSI EG 202 387 [2]. The aim is to ensure that a system has been designed such that there is a link between the objectives of the system and the means within the system to achieve these objectives. Primarily this affects the security of the system but consequentially it also impacts the overall system design. Figure 1 shows the way in which the requirements are all built to satisfy the system objectives. It is particularly important that assurance objectives are stated alongside the security objectives as although it is reasonable to say that "all communication between Alice and Bob shall be confidential" it is the assurance requirement that allows this to be refined as "all communication between Alice and Bob shall remain confidential for a period of at least 5 years when subjected to attack by an attacker of class A" where different attacker classes are also defined.

Security mechanisms in most networked environments exist to fulfill a small set of objectives to ensure availability of the network and assure customer confidence. These objectives break down to the following technical security issues for most telecommunications services:

- Prevention of charging fraud;
- Protection of privacy; and
- Assured availability of the offered services.

The following technical objectives for security then have to be upheld:

- Prevention of masquerade
  - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice;
  - applies to both masquerade of the user and of the system or service.
- Ensure availability of the telecommunications services
  - the service must be accessible and usable on demand by an authorized entity.
- Maintain privacy of communication
  - where the parties to a call communicate across public networks mechanisms should exist to prevent eavesdropping;
  - the only delivery points for communication have to be the legitimate parties to the call.

The aim in modern communications systems is to give a measure of what risk is being prevented by security countermeasures thus designing for assurance of security.

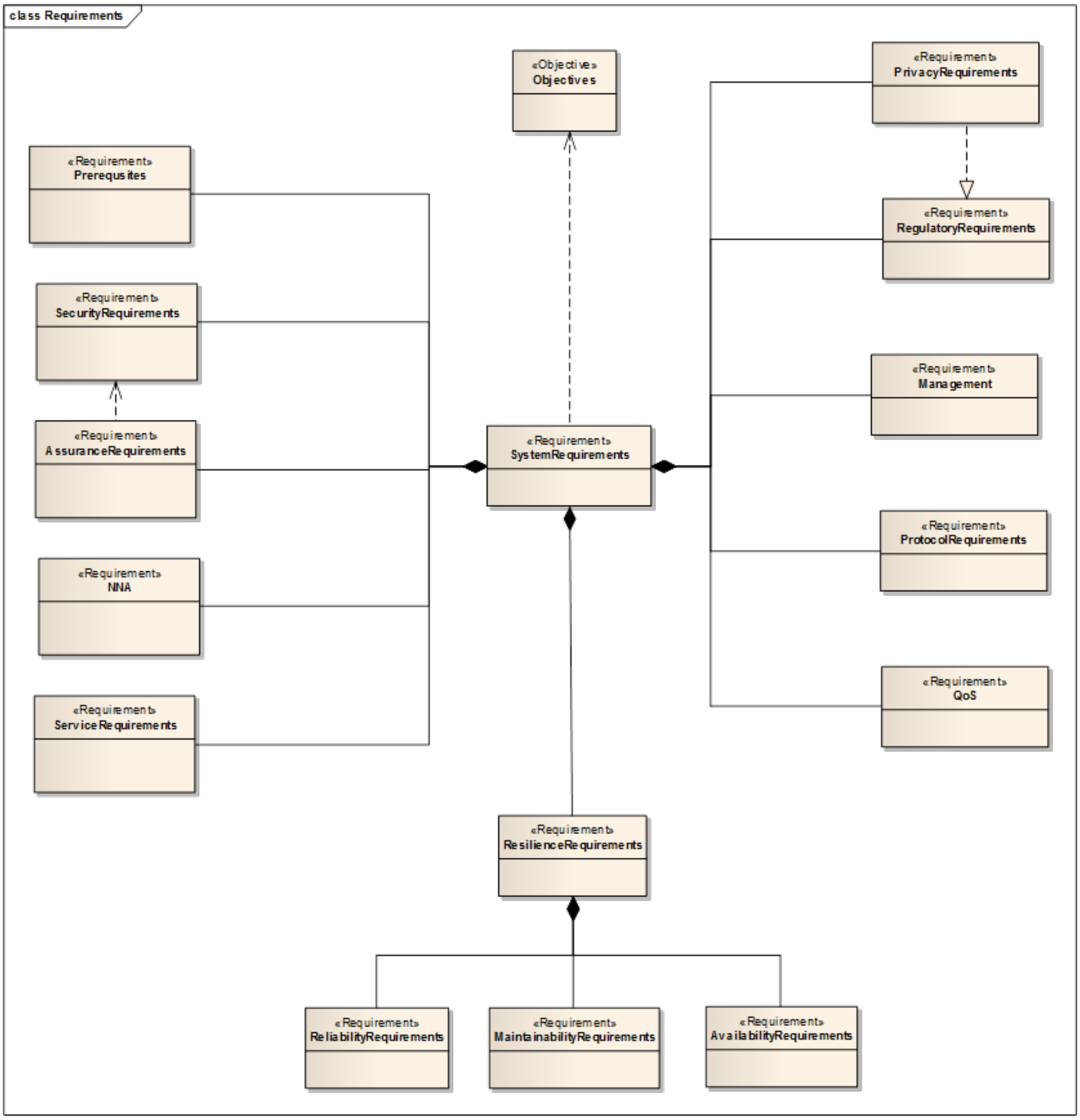
class Requirements
«Objective» Objectives
«Requirement» Prerequsites
«Requirement» SecurityRequirements
«Requirement» AssuranceRequirements
«Requirement» NNA
«Requirement» ServiceRequirements
«Requirement» SystemRequirements
«Requirement» PrivacyRequirements
«Requirement» RegulatoryRequirements
«Requirement» Management
«Requirement» ProtocolRequirements
«Requirement» QoS
«Requirement» ResilienceRequirements
«Requirement» ReliabilityRequirements
«Requirement» MaintainabilityRequirements
«Requirement» AvailabilityRequirements

Figure 1: Requirements to satisfy the system objectives

4. Privacy by Design

Privacy by design is somewhat less mature as a technology but requires the system designer to adopt practices throughout the design, implementation and operation of a system that maximises the privacy of the users. A large part of privacy by design is concerned with identifying data leakage and therefore addresses the human element in system deployment and the policies of the system users, maintainers and managers. Finally privacy by design considers end of life data disposal in which the means by which data stores held on paper and computer disks (or any other media) are disposed of in such a manner that an attacker cannot retrieve personal data from them.

The intent of any privacy protection scheme is to ensure that when data that either identifies a person or which can be directly linked to the person that that data is only available under properly consented conditions. The protection of privacy stems from definitions given in regulation:

- **personal data:** any information relating to an identified or identifiable natural person;
- **privacy:** right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference[1];
- **processing of personal data:** any operation or set of operations which is performed upon personal data, whether or not by automatic means[2].

Within systems personal data should only be processed if the data subjects (i.e. individuals) have unambiguously given their consent. Consent should be explicit and informed and very importantly has to be meaningful to the consenting user.

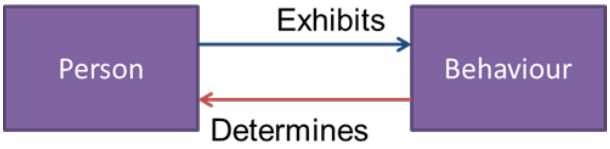

Figure 2: Behavior as personal identifying data

The assertion that a person exhibits behavior is provable by inspection, however the privacy protection problem, and the overall problem, is to give assurance that inspection only of the behavior will not lead to determination of the person (see figure 2).

Behavior is not often thought of as an explicit statement of self but in many inter-personal interactions it is behavior that gives confidence to the involved parties of claims to identity. This is clear in banking where "unusual" transactions are blocked because the behavior is not consistent with the claimed identity.

Whereas risk is relatively straightforward to determine using approaches such as the Threat Vulnerability and Risk Analysis (TVRA) approach described in ETSI TS 102 165-1 [] and the wider Common Criteria approach from ISO/IEC 15408-2 [] these approaches are much less effective in identifying privacy problems in systems. In light of this the recommended approach is to conduct a Privacy Impact Analysis (PIA) of the system.

The benefits of conducting PIAs are numerous. These include helping the i-Tour system and its providers:

- to establish and maintain compliance with privacy and data protection laws and regulations;
- to manage risks to the i-Tour organisations and to the i-Tour users (both privacy and data protection compliance-related and from the standpoint of public perception and consumer confidence); and
- to provide public benefits of i-Tour while evaluating the success of privacy by design efforts at the early stages of the specification or development process.

The PIA process is based on a privacy and data protection risk management approach consistent with the EU legal framework and best practices. The PIA process is designed to help i-Tour operators to uncover the privacy risks associated with the application, assess their likelihood, and document the steps taken to address those risks.

i-Tour uses many forms of personal data within the user profile to determine routing suited to the calendar and desires of the user. As the i-Tour framework is middleware there is a potential risk of that personal data being disseminated to many organisations where there is no direct, consensual relationship to the i-Tour user. Protection of the user data, his PII, is critical to the success of i-Tour and some of the areas in which this protection is focused are described in more depth in the following sections.

5. Intelligent and Sustainable Transport

The i-Tour project lies at the fringe of ITS (Intelligent transport systems) as an example of the more targeted area of Sustainable Surface Transport. The scope of i-Tour is those urban environments where over any reasonable distance a number of transport modes are available, from the simple act of walking, through cycling, public transport by bus, tram, train, ferry, riverboat, and of course private cars and taxis in isolation or combination. The purpose of i-Tour is to provide the traveller guidance in using the modes of transport that

[1] Privacy reinforces the individual's right to decisional autonomy and self-determination which are fundamental rights accorded to individuals within Europe.

[2] Examples of processing are collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

maximize the utility to the traveller, and which makes the options available to the traveller more visible and ultimately more acceptable. By itself ITS has been claimed to promote 5 key societal benefits (see the ITIF report 2010 [2]) and the i-Tour project has direct influence on 3 of them (and indirect influence on the other 2):

1. increasing safety,
2. **improving operational performance, particularly by reducing congestion,**
3. **enhancing mobility and convenience,**
4. **delivering environmental benefits, and**
5. boosting productivity and expanding economic and employment growth

Delivery of the ITS benefits requires changes in behavior and i-Tour uses a gaming model of rewards based on each i-Tour user's contribution to these benefits to assist in their realization.

6. i-Tour characteristics

The i-Tour system is a distributed client server system that broadly follows the Web2.0 model of user as contributor (content provider) thus has prosumers as its end point. The user interface offered to the user is designed to be open and extensible and will initially be offered on the Google Android platform, itself a Java platform closely related to the J2ME (Java edition 2 Mobile Edition) subset, and on conventional web-based clients (including both browser and browser independent applications). The user may be presented to the system by means of credentials whose form is not defined but each form presents a different risk to the user and to the system, examples of credentials include username and password and identity certificates (using asymmetric cryptographic means). In addition the user may be presented to the system using a physical token such as an RFID (Radio Frequency Identification) enabled transport access card (e.g. the Oyster card used in London Transport) or by the ISIM/USIM (IMS Subscriber Identity Module / Universal Mobile Telecommunications Service) identity offered by a mobile phone. [3]

One significant area of i-Tour is the development of a supernetwork to provide multi-modal routing. Each individual transport mode operator is only responsible for maintaining their own unimodal network. i-Tour then provides the supernetwork that combines these in the i-Tour multimodal routing scheme.

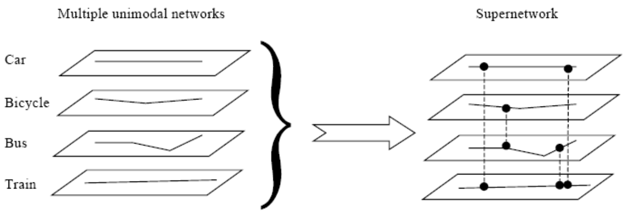

Figure 3: i-Tour model-modal routing supernetwork

Combined with the multi-modal routing i-Tour also introduces as part of the supernetwork algorithms a model to determine the contribution to reducing consumption of resources (fuel, lowering CO_2 &c).

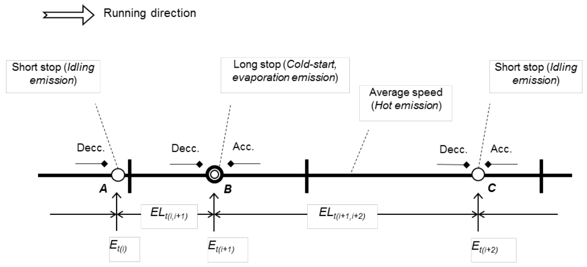
Running direction
Short stop (Idling emission)
Long stop (Cold-start, evaporation emission)
Average speed (Hot emission)
Short stop (Idling emission)
Decc.
Decc.
Acc.
Decc.
Acc.
A
B
C
$EL_{t(i,i+1)}$
$EL_{t(i+1,i+2)}$
$E_{t(i)}$
$E_{t(i+1)}$
$E_{t(i+2)}$

Figure 4: i-Tour consumption calculation model

As each unimodal network is optimized to carry its parameters for the efficiency of each mode, and the gaming goals of the i-Tour user are introduced i-Tour can deliver a personalized model of efficient transport use. As more personal data is given to the system the recommendations of the system can offer greater reward. For example by using the calendar of the i-Tour user as a data source and combining this with the gaming goals, transport timetables, parking availability and tying into social networks i-Tour will aim to offer to use the transport systems in a way to optimize the goals of the user. This could for example tie a lunch reservation with public transport to the restaurant and combine the calendars of all those meeting together for lunch to allow a team game to also get played out.

[3] Where RFID cards are used as access tokens the recommendations made in ETSI TR 187 020 should be taken into account.

The privacy challenge is to ensure that i-Tour is able to meet its goals for extending sustainable surface transport, whilst meeting the ITS benefits, thus i-Tour is being designed to meet the expectations of privacy established in the Organisation for Economic Co-operation and Development (OECD) Declaration of Human Rights [7], the EU Data Protection laws [8], [9] and the EU Convention on human rights [10] and which can be summarised as defining the following top level objectives for the system.

- Access to services should only be granted to users with appropriate authorization;
- The identity of a user should not be compromised by any action of the system;
- No action of the system should make a user liable to be the target of identity crime;
- No change in the ownership, responsibility, content or collection of personal data pertaining to a user should occur without that user's consent or knowledge;
- Personal data pertaining to a user should be collected by the system using legitimate means only;
- An audit trail of all transactions having an impact on personal data pertaining to users should be maintained within the system.

Whilst the i-Tour framework will be mostly based on web-services the underlying architecture is that characterised by SOA (Service Oriented Architecture) approaches based on SOAP (Simple Object Access Protocol). The underlying security mechanisms of SOA/SOAP will be adopted and strengthened as defined in the security and privacy analysis identified from the i-Tour PIA and TVRA documents.

The standardisation framework for the i-Tour system is to be based in part on the ETSI and ISO approaches to security and privacy design, to the work on the IETF (Internet Engineering Task Force) in protocols, and of the work of the OGC (Open Geospatial Consortium Inc. ®) for SOA/SOAP implementations. The models adopted in the main in these areas are based on a Representational State Transfer (REST) model in which the client asserts a state model and the server acts on the assertion. Such models are liable to a number of manipulation attacks that if attempted need to be captured and the impact minimized.

The system architecture of i-Tour is that of a large distributed data driven web-service platform offering many services both discretely and in combination. The semantic and syntactic data definitions for service interactions are fully defined in i-Tour.[4]

ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under the Grant Agreement number 234239. The authors are solely responsible for it and that it does not represent the opinion of the Commission and that the Commission is not responsible for any use that might be made of information contained therein.

REFERENCES

[1] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[2] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables"

[3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[4] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components".

[5] http://www.itif.org/files/2010-1-27-ITS_Leadership.pdf

[6] ETSI TR 187 020: "Radio Frequency Identification (RFID);Coordinated ESO response to Phase 1 of EU Mandate M436"

[7] Universal Declaration of Human Rights

[8] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. .

[10] European Convention on Human Rights (ECHR) (long title: Convention for the Protection of Human Rights and Fundamental Freedoms)

[4] The nature of i-Tour, and of SOA/Web2.0, is that interactions between services will not be known in advance to the developers of each service. This requires that every service is defined with a clear interface specification.