Addressing User Privacy and Experience in Distributed Long Lifetime Systems

Scott W. Cadzow

Cadzow Communications Consulting Ltd.
(as partner to European Research projects i-Tour and i-SCOPE)
scott@cadzow.com

Abstract. Very large distributed systems that aim to offer natural interaction with their human users fail to address the everyday nature of trust and its establishment at their peril. In human interactions trust builds slowly, it builds contextually, and it builds by association. In contrast most software systems make assumptions regarding user behaviour and do little to learn at the natural pace of the user, this leads to an unnatural relationship between the user and the software, system or service they are using. The claims of social networking to address this only go so far as in many cases the objectives of the service and those of the user do not align or one melds to the other – treating a person as a social network entity quite distinct from that same person as a natural person. What this paper intends to show is how the privacy and security problem is being addressed across the smart city projects in Europe with particular emphasis placed on material from case studies taken from the i-Tour and i-SCOPE projects.

1 Introduction

Colouring almost all of human interaction is trust. This assertion covers every aspect of human endeavour whether that be in work, sport, parenting, …, in fact it is difficult to identify a single relationship that does not depend to some extent on trust. As we move our lives to an increasingly virtual world and to greater reliance on software and machines we need to also re-evaluate trust and how to engage our human instincts for trust in the machine world. Trust, by colouring human interaction, also determines to some extent how we experience an event as trust and confidence become synonymous.

2 i-Tour and i-SCOPE Project Goals

A very simple list of *i-Tour*'s functional goals are the following:

- Multi-modal personalised urban route planning and route maintenance
- Goal based rewards for using the system and thus the public transport resources of the host
- Point of interest recommender engine

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 297–305, 2013.

i-SCOPE extends this list by adding capabilities of individuals to upload noise maps and the routing model is extended with detail architectural models written in cityGML to enable, in particular, multi-modal routing for wheelchair users and to address solar potential of the host city.

3 Challenges

The challenge for both privacy and security is in both the conflict between privacy and security and in the conflict in managing privacy and security with the personalisation at the core of *i-Tour*'s and *i-SCOPE*'s functionality.

The core model in i-Tour and i-SCOPE for security and privacy is based on the simple access control model: *Entity "A" allows entity "B" to process data from "A" only under the agreed constraints "C"*. This introduces another problem for design as stated by Donald Rumsfeld "*… there are known knowns … there are known unknowns … there are also unknown unknowns …*" which whilst being unwieldy political speak points to a key problem in security work, that of establishing (and proving) a security and privacy boundary. As systems become more complex, and interactions with them become more developed over time, the establishment of that boundary become increasingly crucial in establishing the security, privacy and trust relationship.

The role of privacy as an attribute in trust is well understood in human relationships. However much of the technical work in protecting privacy has been addressed from a security standpoint, i.e. assuring confidentiality of data or providing complex access control models. Trust and privacy are in practice softer technologies that provide reinforcement that privileged information given is enacted on within the bounds of a mutually agreed policy (the "C" in the generic access control statement). The approach of developing non-repudiation of consent structures within a policy driven processing engine allows for contraction and expansion of the allowed policy as the relationship evolves allowing a more natural development of a relationship.

The human model of trust is complex, slow, and expensive, but it is also ultimately resilient. This compares quite badly to the normal trust models used in computing systems where the model is often reduced to trust for a single transaction with third parties brought into the loop to give validation. In human terms this is like saying “you can trust Angela, David does, and you trust David”, so trusting David establishes the model for trusting Angela. The problem here is that you may trust David on a tennis court as a reliable partner but may not trust his financial judgement and you are asking Angela for financial advice. It is this very contextual nature of trust that is natural in human interactions but that is notoriously difficult to make work for machine interactions.

There are specific privacy issues raised by i-Tour that need care in handling to ensure i-Tour is acceptable both from a regulatory viewpoint and from a user viewpoint. An example is taken from the "bootstrapping" sequence in the "trust based

recommender system" in which the initial hypothesis is that the system "doesn't know what I like, but does know where I live, where I work, when I travel and how (e.g. from Oyster card data)". The privacy challenge is to ensure that the hypothesis can build communities and make recommendations without allowing unauthorized parties to make assertions related to the person.

4 Developing Contextual Trust

In the i-Tour project contextual trust in recommender systems and in the privacy model has been key to the basic design. For example when reading reviews and recommendations for hotels you may be more likely to trust the opinions of real travellers who have actually stayed at the hotel than employees of the hotel or competitors to the hotel. We understand trust as incremental, contextual and relationship centred. In building a framework built from conventional asymmetric and symmetric cryptographic security modules to meet the requirement of incremental, contextual and relationship centred trust one of the keys is to develop policy as testable statements. In itself this step is still in development by taking TPlan as a candidate language and extending it to the new language ExTRA.

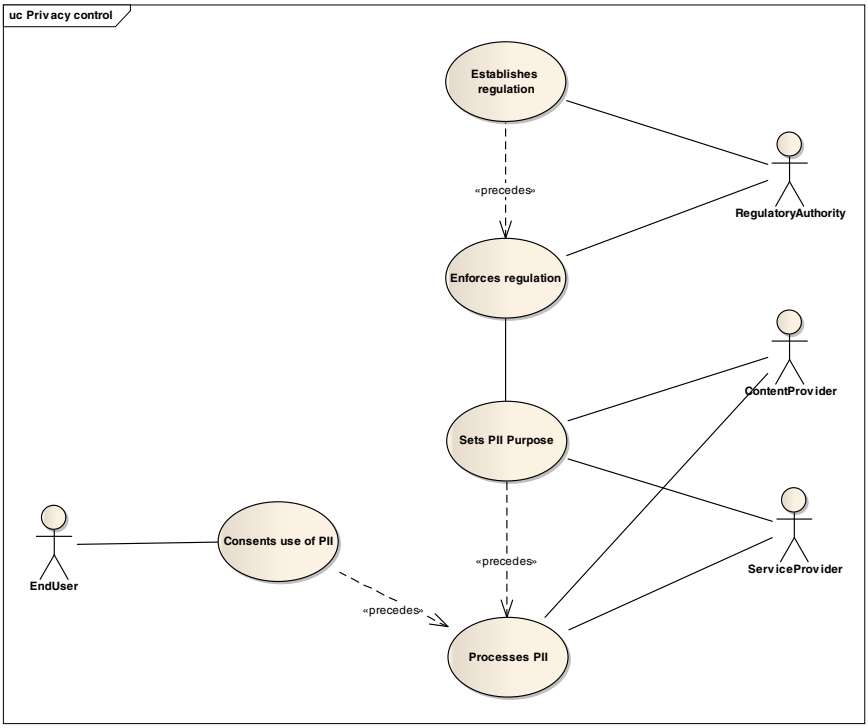

Fig. 1. Use cases for use of Personal Identifiable Information (PII)

It is important to note that privacy is a protected right and there is a significant body of legislation in Europe that applies to organisations seeking to gather personal data with consequences including criminal prosecution for failure to properly maintain the right to privacy of those they interact with. This is a very "hot" topic in society with high stakes in both the protection of the rights to privacy and the use of the same data to build business. In approaching this topic i-Tour is taking the view that it has to be open about the risks and impacts of its design on privacy and security.

Many of the privacy concerns raised by consumers regarding the use and deployment of any new technology surround the uncertainty of the system design, its operation and its intent. An increasingly prevalent privacy concern is that of the system's capability to track individuals. For i-Tour tracking is core as this is required to make routing decisions and to offer recommendations to users, thus it is essential that such tracking information is not open to exploit of the i-Tour users.

i-Tour and i-SCOPE when deployed have to meet the expectations of privacy established in the Organisation for Economic Co-operation and Development (OECD) Declaration of Human Rights, the EU Data Protection laws, and the EU Convention on human rights 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.

Core to both i-Tour and i-SCOPE is that an increasing amount of people are living in cities and, by 2030, the number will be close to 5 billion (United Nations 2008). Therefore, it is essential to develop efficient techniques to assist the management of modern cities. It behoves researchers across many disciplines to pay attention to smart cities, as technologies associated to smart cities are part of knowledge-based economies with a key being development of socially inclusive but socially responsible services. In this regard addressing privacy and trust is essential in providing the platform for social integration by citizens of future smart cities.

Smart cities are an example of a multi-variable multi-scenario system whose purpose is to assist citizens in their daily life and to also assist the administrators of cities to run their cities without hindrance. In such systems the complexity of the trust/privacy/security model becomes apparent. Smart city systems and their providers

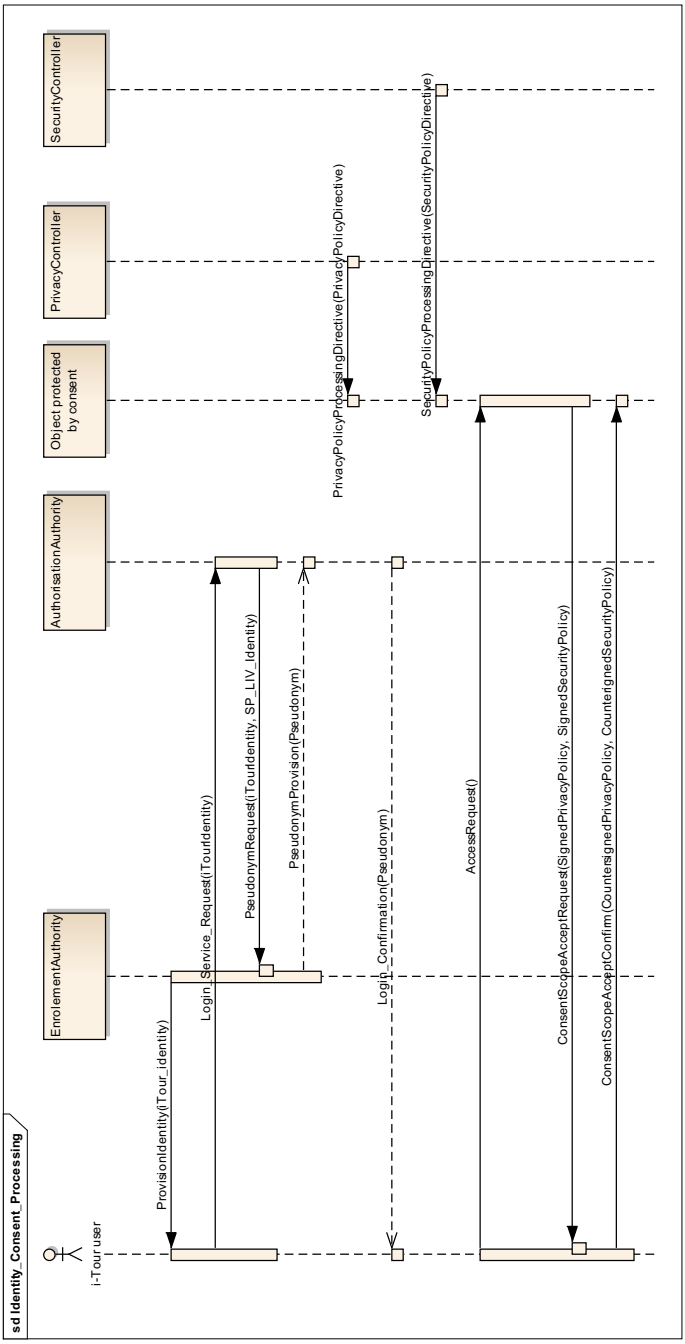

Fig. 2. Simplified processing to allow non-repudiation of consent

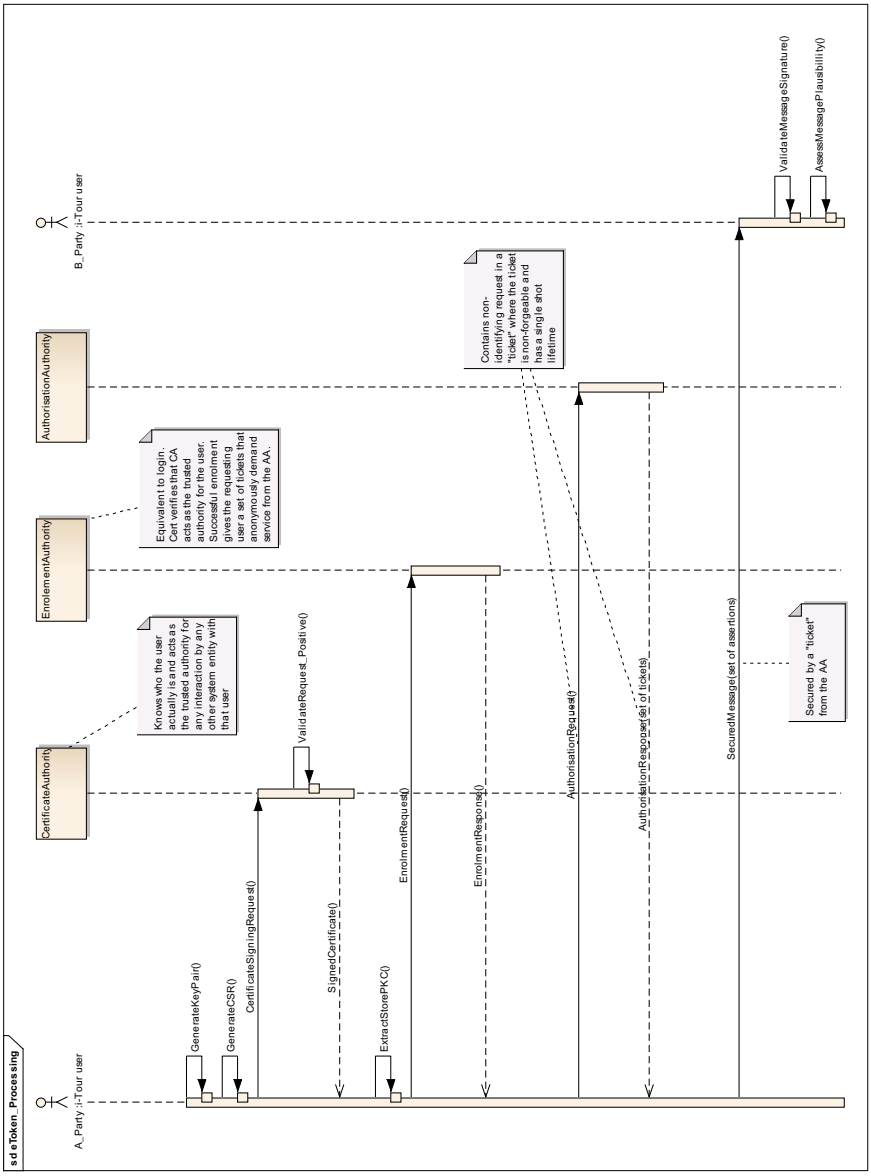

Fig. 3. Registration and authorisation ticket model

have to work with the citizens, employers, visitors to ensure they all work together. The systems themselves will evolve over time gathering data and capability as they grow. If growth is unconstrained it may damage the users the systems are intended to serve therefore we have to be able to bring growth and education into the lifecycle of our systems. Without intending to anthropomorphize systems lending them some of

the characteristics of human nature regarding relationships with their users is part of the path to make systems that appear as partners. As trust is established over a long period of time in normal human relationships, and where introductions form part of normal relationship establishments, so should the relationships of users and systems. As an example using a mobile phone as a sensor in gathering noise data may use the mobile phone operator as the party that introduces the user to the noise measurement agency, but once the initial introduction is achieved and the new relationship established there is no need for details of the relationships to be shared. Whilst this form of introduction and use of trusted third parties has been used to underpin much of the public key cryptography at the heart of digital signature it has not been developed to assist in the business and social interactions at the heart of smart cities.

What i-Tour and i-SCOPE have introduced is an extension of non-repudiation to consent. The aim in general is that policy has to be properly machine processable and in i-Tour and i-SCOPE we are taking the step of extending the test notation TPlan to cover assertions and requirements.

5 Summary and Conclusions

In summary the role of privacy as an attribute in trust is well understood in human relationships. However much of the technical work in protecting privacy has been addressed from a security standpoint, i.e. assuring confidentiality of data or providing complex access control models. Trust and privacy are however considered in this work as softer edged to provide reinforcement that privileged information given is enacted on within the bounds of a mutually agreed policy. The approach allows for contraction and expansion of the allowed policy as the relationship evolves allowing a more natural development of a relationship.

6 Definitions and Abbreviations

Confidentiality: The process of ensuring that information is accessible only to those authorized to have access

Privacy: Right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference

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

References

1. ETSI EG 201 940: Human Factors (HF); User Identification solutions in converging networks
2. ETSI EG 202 067: Universal Communications Identifier (UCI); System framework

3. ETSI TR 187 011: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples
4. ETSI TR 187 020: Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436
5. 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
6. ETSI TS 187 001 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements
7. Clark, R.V.: UK Home Office; Hot Products: understanding, anticipating and reducing demand for stolen goods, ISBN 1-84082-278-3
8. ITU-T Recommendation X.509 (11/2008): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
9. ISO/IEC 15408-1: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
10. SO/IEC 15408-2: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
11. ISO/IEC 17799 2005: Information technology - Security techniques - Code of practice for information security management
12. 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
13. 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)
14. Recommendation of the OECD Council in 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data (the OECD guidelines for personal data protection
15. European Convention on Human Rights (ECHR) (long title: Convention for the Protection of Human Rights and Fundamental Freedoms)
16. Universal Declaration of Human Rights
17. David, C.: Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto 82(3), 199–203 (1983)
18. Article 29 of Directive 95/46/EC Working group (an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC): Opinion 15/2011 on the definition of consent (adopted on July 13, 2011)
19. Article 29 of Directive 95/46/EC Working group Opinion 13/2011 on Geolocation services on smart mobile devices (adopted on 16 May 2011)
20. Privacy Impact Assessment Handbook, `http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf`
21. Fletcher, G.: Identity in practice blog: Privacy across Social Network aggregation, `http://practicalid.blogspot.com/2010/09/privacy-across-social-network.html`
22. Shannon, C.E.: A Mathematical Theory of Communication. Bell System Technical Journal 27, 379–423, 623–656 (1948)

23. ISO/IEC 15408: Information technology - Security techniques - Evaluation Criteria for IT security
24. ISO/IEC 10181-3: Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework
25. ISO 14977: Extended Backus-Naur Form (EBNF) syntactic meta-language
26. Kerckhoffs, A.: La cryptographiemilitaire. Journal des Sciences Militaires IX, 5–38, 161–191 (1883)
27. Computer Misuse Act 1990: An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes, http://www.legislation.gov.uk/ukpga/1990/18/contents