Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 3 / DECEMBER 2007 / 1 - 17
© 2007 Universidad de Talca - Chile

This paper is Available online at
www.jtaer.com

Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering

Lothar Fritsch

Norsk Regnesentral - Norwegian Computing Center, Oslo, Norway and Johann Wolfgang Goethe – Universität Frankfurt am Main, Germany, lothar.fritsch@nr.no

Received 11 January 2007; received in revised form 14 September 2007; accepted 7 October 2007

Abstract

This article presents an approach for the design of location-based information systems that support privacy functionality. Privacy-enhancing technology (PET) has been available for a considerable amount of time. New online applications and infrastructures for mobile and ubiquitous use have been installed. This has been done without usage of available PET, although they are favored by data protection experts. Designers of location-based services (LBS) create infrastructures for business or application specific purposes. They have profit-oriented views on the rationale for PET deployment. Finally, users have requirements that might be neither on the PET community's nor on the business people's agenda. Many disciplines provide knowledge about the construction of community-spanning information systems. The challenge for designers of infrastructures and applications is to find a consensus that models all stakeholders' interests – and takes advantage all involved community's knowledge.

This paper groups LBS stakeholders into a framework based onto a sociological knowledge construct called "boundary object". For this purpose, a taxonomical analysis of publications in the stakeholder communities is performed. Then the paper proposes a socio-technical approach. Its goal is to find a suitable privacy design for a LBS infrastructure based on the boundary object. Topics for further interdisciplinary research efforts are identified and proposed for discussion.

Key words: Privacy design, location, mobile infrastructures, requirements engineering, boundary objects.

1 Introduction

The purpose of this work is to show how to design mobile communication infrastructures in a way that they respect privacy and fulfill user and operator requirements. In particular, the process focuses on the interdisciplinary feasibility of the resulting infrastructure with respect to the business model.

Information systems cross one more border into our personal and private lives by measuring our personal context. In providing context-based, situation-dependant services, human beings are being equipped with technology measuring their daily lives to provide computerized services to them. One kind of context information collected and used in such services is a person's location, determined through the position of the person's mobile telephone. Location-based services (LBS) based on wireless networks can position users with their mobile equipment. LBS business models are seen as an important application for mobile operators and the online services industry. A new challenge is the ubiquity of the infrastructure. By positioning a mobile phone, users can be tracked and profiled all day in all places with network coverage. This poses new service opportunities, but also creates a new class of risk towards privacy. Now many service providers can track an individual, while the existing data protection laws were drafted for protection against centralized infrastructures. As an approach to the privacy dilemma, cryptographers and data protection specialists suggest the use of privacy-enhancing technology (PET). PET development has been technology-centric, detached from business requirements and cost-of-ownership. With the deployment of ubiquitous infrastructures, the analysis and deployment of privacy-friendly infrastructures might stimulate adoption of the new applications against strong privacy concerns that are being voiced by researchers and privacy advocates.

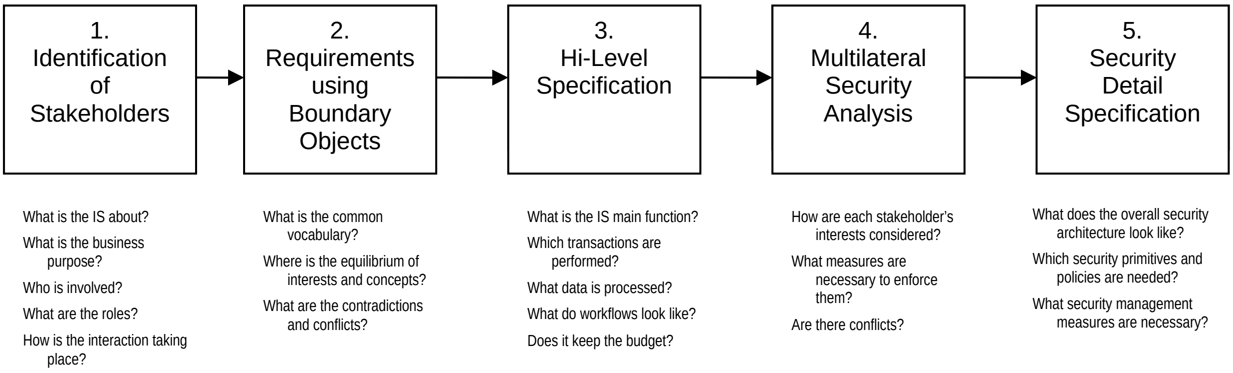
1. Identification of Stakeholders
2. Requirements using Boundary Objects
3. Hi-Level Specification
4. Multilateral Security Analysis
5. Security Detail Specification
What is the IS about?
What is the business purpose?
Who is involved?
What are the roles?
How is the interaction taking place?
What is the common vocabulary?
Where is the equilibrium of interests and concepts?
What are the contradictions and conflicts?
What is the IS main function?
Which transactions are performed?
What data is processed?
What do workflows look like?
Does it keep the budget?
How are each stakeholder's interests considered?
What measures are necessary to enforce them?
Are there conflicts?
What does the overall security architecture look like?
Which security primitives and policies are needed?
What security management measures are necessary?

Figure 1: Design process for Privacy Infrastructure Design

This text presents a process about how design a privacy-friendly on-line infrastructure. This process is to be used for information infrastructure development. The example for such information systems will be LBS. The focus of my analysis is the intersection of economic theory, system design and PET to create information systems that have the properties of privacy-friendliness, efficiency, and value creation. In
Figure 1, the steps of the design process are introduced.

An important tool to be used is the creation of a Boundary Object [6] as a tool for reaching equilibrium between the stakeholders of a mobile business model and its infrastructure. This article will review the state of the art of privacy design for location-aware applications, and then introduce the stakeholders and the respective Boundary Object. It will conclude with an outlook on the design process.

2 Research methodology

This research follows the approach of design science. Design science, as described in [19], is a research paradigm for information systems research. Design of information systems, according to [19], is both a process and a product – or artifact. The progress of design science is to execute a number of steps that lead to an artifact. According to [31], the two principal processes of design science are BUILD and EVALUATE. Resulting from these activities, four kinds of artifacts can be created: CONSTRUCTS MODELS, METHODS, and INSTANTIATIONS. Design research is conducted along seven guidelines, as illustrated in Table1.

Table 1: Design science research guidelines, from [19]

Guideline	Description
1: Design as an artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2: Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3: Design evaluation	The utility, the quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4: Research contributions	Effective design-science research must provide clear and verifiable contributions in the area of the design artifact, design foundations, and/or design methodologies.
5: Research rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6: Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7: Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

For the evaluation of design science research, five principal methods are suggested. The methods can be employed using several evaluation techniques or tools that are appropriate for the research to be evaluated. In Table 2, evaluation techniques in design science are summarized.

Table 2: Design science evaluation methods, from [19]

Evaluation method	Techniques & tools
Observational	Case study, field study
Analytical	Static analysis, architecture analysis, optimization, dynamic analysis
Experimental	Controlled experiment, Simulation
Testing	Functional testing, structural testing
Descriptive	Informed argument, scenarios

For the research in this text, the construction process for privacy-respecting information systems will be the design artifact. As evaluation methodology, observational and descriptive methods will be used.

2.1 Feasibility of Design Science

Design science provides various ways to work with business-related research on information systems. By definition in [19], design science has the objective to "… develop technology-based solutions to important and relevant business problems". Its focus on design artifacts in environments with dynamic context makes design science attractive for the scientific investigation of construction processes of information systems infrastructures with particular properties.

2.2 Limitations of Design Science

Two major difficulties can arise in the application of design science on information systems design. The artifact for a problem in a particular environment for a current technology can be subject to outdating in a close future. Therefore, results from design science might have a shorter relevance – until the next major changes in the environment of the design artifact.

Another issue are metrics for evaluation. Metrics for evaluation may be hard to find, while some changes in the design artifact environment can effectively render metrics inappropriate. An evaluation without metrics – for example of the descriptive kind mentioned in Table 2 – much effort in scientific discourse can be necessary to evaluate the creation of new knowledge.

3 State of the Art

The main focus of the state of the art analysis is privacy support for mobile applications in research and practice. It will be complemented by a view on software design with focus on privacy. Finally, an introduction to the knowledge construct of Boundary Objects will be presented as a foundation of the coming sections.

An important aspect of this section will be the review of privacy enhancing technologies (PET), as they are important building blocks for privacy friendly mobile systems. Since their appearance in 1981 [9], much work has been done to elaborate PET. A practical overview over them can be found in [3].

3.1 Privacy Enhancing Technology in M-Commerce in Theory and Practice

This section will present a brief overview of the state of the art in privacy technology research, e.g. from the PRIME and FIDIS research initiatives and other scientific efforts. It also reviews the technology available and used in practice. The protection against location profiling has three components: identity protection, camouflage and a legal and social framework for technology regulation. Each of the items will be discussed below. Following the distinction in section 2.2 of [13], protective measures are divided in opacity tools and transparency tools. Opacity tools serve the purpose of hiding personal information to enable unobservable, individual freedom. Transparency tools are used to create open, understandable and fair practices when dealing with personal information.

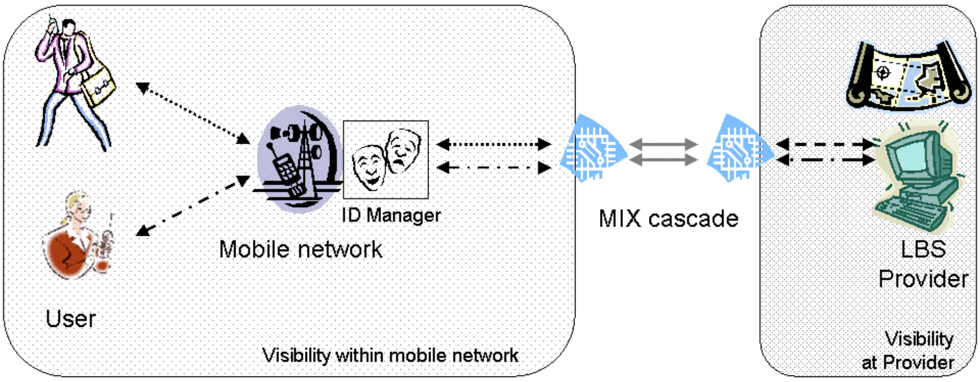

Figure 2: Minimalist Mobile Network Identity Management approach

3.1.1 Identity protection

A person's identity should be protected while using location-based services. If the location track is not personalized, it cannot be combined with any other personal data. Furthermore, the amount of data that can be accumulated about a person should be limited. This prevents identity guessing from movement patterns, as described in [16]. Identity management systems with frequent pseudonym changes and anonymous access to services provide to reach these goals. The simplest form of identity management occurs in Figure 2. Here, the mobile operator offers pseudonym translation services for the user before the application data traffic is forwarded into cascades of anonymizing MIX [9] nodes (a form of router that denies observers from observing the content and the end points of data communication.

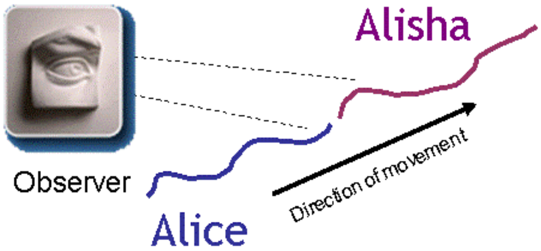

Figure 3: Naive pseudonym change reveals pseudonym connection

The use of several serialized MIX nodes as a cascade protects the communication from a corrupt single MIX. More advanced identity management approaches introduce policy management. Here, a user can set policy about location forwarding at her mobile operator, and at the same time issue anonymous credentials that identify the policy. The credential then is given to the LBS provider as a voucher Please note that naïve use of pseudonym change mechanisms can reveal all your pseudonyms used with a service though, as illustrated in Figure 3. To prevent this from happening, MIX-Zoning will be discussed later in this text (see Figure 6). Identity Management can be either an opacity or a transparency tool, dependent on its particular deployment in a context.

3.1.2 Camouflage

The generation of false information about identity, identifiable movement patterns and time disturbances will provide to protection from unauthorized geographic profiling. Camouflaging technologies exist for a long time, e.g. for MIX technologies with dummy traffic [11]. Early location hiding concepts have been suggested by Gruteser and Grunwald in [18]. Concepts include:

Temporal cloaking: the time intervals for location queries are regulated to avoid micro-measurement of a user's position. The concept is illustrated in Figure 4.

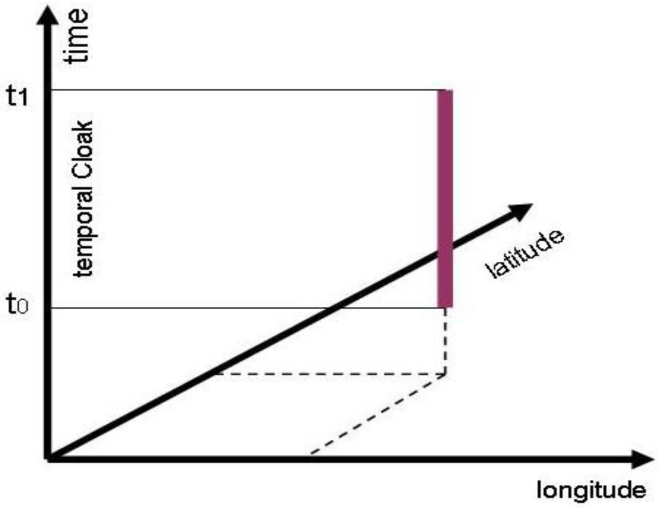

Figure 4: Temporal cloaking

Spatial cloaking: precision of location information is reduced to a level tolerable by the application, but will not be delivered too precise. This intentional degradation of position precision prevents too precise information collection about a person's movements on a high-resolution level. Spatial cloaking is illustrated in Figure 5.

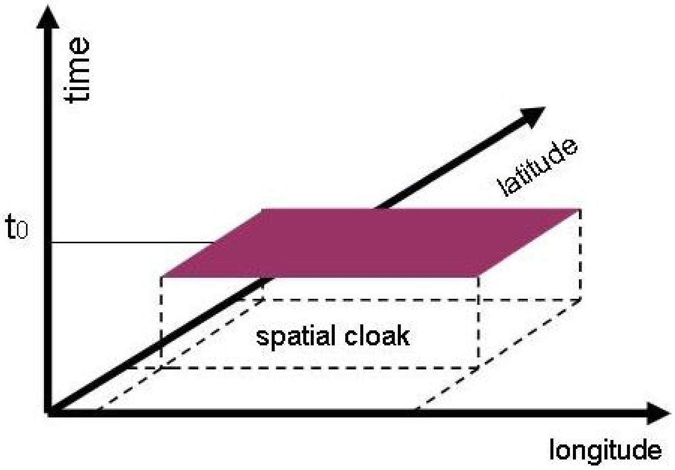

Figure 5: Spatial cloaking

MIX-zoning: To allow for unobservable change of pseudonyms (and solve the problem from Figure 3 with naïve pseudonym change), a zone of unobservability is created where users can go to perform their pseudonym change. As soon as many users do this simultaneously, an anonymity set is created. The concept is inspired by Chaum's MIX [9]. An example of MIX zoning for the purpose of pseudonym change protection is shown in Figure 6. Temporal cloaking ads uncertainty to the point in time the position or a person was measured. The relying service using the data does receive a position datum, but only knows this is not the person's current position but from some time in the past. The usefulness of this approach is limited in terms of privacy protection. Only in contexts where a service tracks a person frequently (e.g. a pollen warning scenario, as used in [27]), but with coarse requirements on resolution and timing, temporal cloaking seems applicable. Spatial cloaking is effective in circumstances where a tracking service doesn't require high-resolution position information (e.g. for pollen warning). Here, the information is intentionally degraded to a degree where no daily routine is contained anymore.

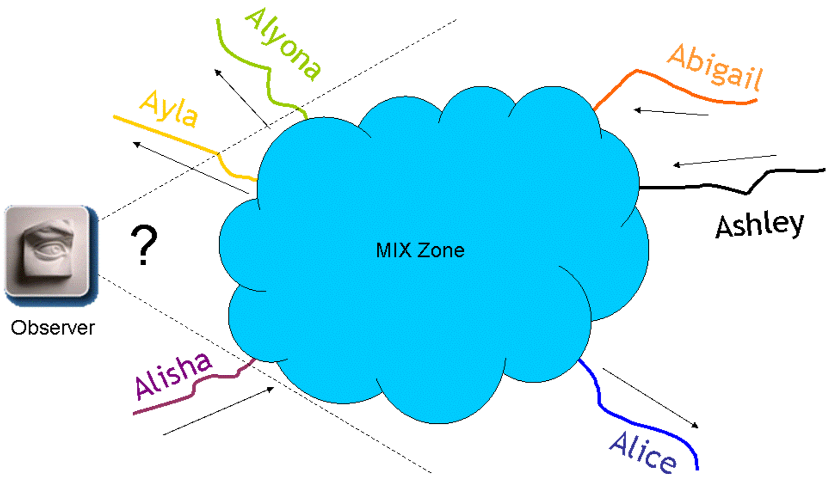

Figure 6: A MIX zone

Location dummy traffic: MIX zones are effective to protect and obfuscate pseudonym changing event. Unfortunately, MIX zones might not always have enough people in them just at the moment when they are used. To improve on this problem, the concept of dummy traffic in MIX communication can be adapted. Location track dummy traffic is performed with dummy users that are artificially generated location tracks with a certain non-compromising behavior. The dummy pseudonyms are registered with the LBS application, and will be used for pseudonym changes. When a user wishes to change to a different pseudonym, the dummy system ensures that some of his alternative or dummy pseudonyms will cross the user's path at a rendezvous point, where the change will happen.

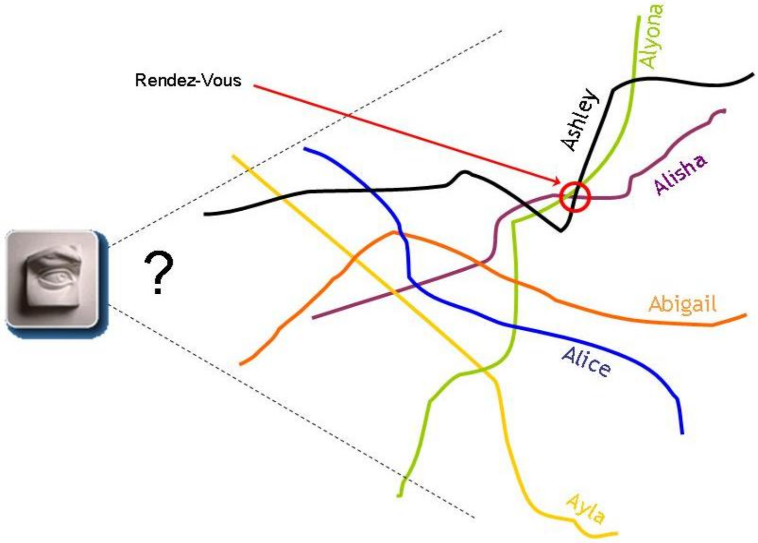

Figure 7: Location dummy traffic, Rendezvous point

The now unused pseudonym takes up a dummy life of its own, in temporary or permanent continuation of the previous path. Figure 7 illustrates the concept. This mechanism can take up a used pseudonym and carry it around the town virtually. The challenge here is the generation of realistic movement patterns that do not compromise the pseudonym owner by, e.g., entering the town's red light district. The application of this protection measure is restricted to LBS infrastructures that allow for injection of artificially created position data (e.g. the GPS device scenario or some special instance of the intermediary scenario described in [15]). A model and a prototype have been described in [35].

All camouflage technologies are opacity technologies.

3.1.3 Privacy & Identity Protection in Practice

Location information today is acquired in one of three ways. Either, the mobile computer has access to a satellite navigation receiver (e.g. GPS) to read position information using satellite signals – functioning only outdoors. Indoors, special sensors can interact with short-range communication to gather a position. And finally, with the use of a mobile telephony networks based on cells, the telephony network can provide location information about the phone's whereabouts using the cell broadcast units [41]. The privacy implications of monitoring positions depend strongly on the application design and the frequency the positions are acquired. Potentially problematic applications include centralized processing and storage of people's positions, possibly with other people being able to access this data [2]. Looking at the current state of deployed technology, mostly the mobile telephony networks and the application platforms can usually monitor people's movements whilst possessing identifying data about the persons. Some efforts for improving this situation are on the way. Most mobile network operators work use the subscriber number IMSI as a pseudonym, which unfortunately contains the subscriber's phone number. More elaborated approaches enable the use of several pseudonyms, which in turn are used for different service provider's identification needs. In [33], a solution prototype with cryptographic privacy protection, pseudonym management and a high level of privacy protection against the application providers is presented. The concept introduces an identity intermediary between the positioning system and the application providers. The intermediary follows user-defined policies for the service provider's access to the user's location. Additionally, the intermediary provides pseudonym management for the users.

3.2 Designing Security & Privacy for Information Systems

This section will present approaches for security and privacy engineering for information systems. It will lay the foundation for the approach in section 3.

Few complete frameworks or approaches have been published, namely KPMG's model in [25], a security framework in [42], and a design process in [17]. The work on risk modeling in [20] also provides insight on requirements engineering. In particular, the interdisciplinary nature calls for a model that provides a frame for knowledge in important disciplines as well as a way of integration of application-specific knowledge. Several approaches towards 4th-generation design methods for IT security in information systems exist. Siponen describes the requirements engineering and design process as a socio-technical process in [38]. Beyond security, Sommerlatte describes in [39] the concept of Maieutik. Here, a process with strong user interaction and rapid prototyping cycles is used to ensure that information systems match their user's requirements. The lack of metrics for privacy in information systems as well as the lack of standards (there are some ISO activities, but so far the application of ISO 15408 'Common Criteria' for privacy evaluation is only under research in [28] and in ISO/IEC/JTC1/SC27/WG3 [7]). A suitable approach to collect interdisciplinary security requirements is Multilateral Security [34], applied by Fritsch and Scherner in [36]. It is applied according to the application requirements and the first high-level design of an information system is made. Its goal is to develop multilaterally satisfying security and privacy requirements. Several research groups have proposed platforms to manage privacy, for example [21], [23], and [27]. These architectures were specified for a specific application purpose, but solely from a technician's view.

3.3 Transcending Knowledge Boundaries: The Boundary Object concept

The concept of Boundary Objects was developed by Bowker and Star. It is a model for the knowledge boundaries that exist between different disciplines or communities of practice when they collaborate on a certain topic. The concept originated in the observation of different communities that are connected to a Natural History Museum – and their respective views on and uses of the institution [40]. Boundary objects have proven to be a useful model for sorting out stakeholder interests, their terminology and their understanding of certain subjects that might be used by all involved communities, but interpreted in very different ways.

The ambiguity of such contextual interpretation of concepts requires the definition of a common terminology for any information systems specification project that involves several communities of practice. The approach to solve terminological ambiguity in requirements collection aims at creating a boundary object. A boundary object is a construct that expresses knowledge in a meaningful way for several communities of practice. Boundary objects were introduced in [6]. Boundary Objects *"... are those objects that both inhabit several communities of practice and satisfy the informational requirements of each of them. Boundary objects are thus both plastic enough to adapt to local needs and constraints of the several parties employing them, yet robust enough to maintain a common identity across sites. They are weakly structured in common use and become strongly structured in individual-site use. These objects may be abstract or concrete... Such objects have different meanings in different social worlds but their structure is common enough to more than one world to make them recognizable, a means of translation. The creation and management of boundary objects is a key process in developing and maintaining coherence across intersecting communities*." (in [6] p. 297).

Based on Bowker's and Star's concept, observations and applications of Boundary Objects to production, terminology and software engineering have been performed. In [8], a technical drawing is conceptualized as a boundary object for several departments that are involved in product development. The existence of the drawing is identified as the knowledge object that allows all participants to communicate about production. In [43], the role of taxonomy on a subject is identified to be that of a Boundary Object between involved stakeholders. Thus, a textual exploration and definition of a topic can construct a form of Boundary Object. Finally, in [1], the authors use Boundary Objects as a tool for bridging communication gaps between experts in "domain-oriented design environments". In their analysis, Boundary Objects are represented by prototypes, and models documentation (e.g. project web sites). Finally, work applying the concept to requirements definition and software engineering appeared in some research, such as [26] with the analysis of a common terminology for telecommunications applications, and in [29] where the e-government design process is conceptualized with Boundary Objects.

The role of a boundary object as a taxonomy object will be used below for the specification of a privacy-respecting infrastructure for location-based services (LBS) on a wireless telephony network.

4 Stakeholder analysis

Stakeholder analysis will be used to identify the parties involved in a particular business model, and the construction of the mobile communications infrastructure that will be used to implement the business application. The stakeholders need to be identified as a base for further work, e.g. the requirements specification. Stakeholder analysis is a tool to identify stakeholders and their specific role. It has been described in [10]. An application of stakeholder analysis to information privacy has also been described in [32].

4.1 Modeling Stakeholders in Location-Based Services

This section will present a stakeholder model for LBS. It describes the communities involved and describes their interconnection with focus on privacy management in LBS. The core communities involved are telecommunications business, economics, and data protection (here called by the name of the scientific subject of study – privacy-enhancing technology). This is based on a general stakeholder analysis performed in [30].The fields of law, market and end-user psychology have been modeled as influence factors on the core communities. The communities have different views on concepts present in LBS. To efficiently communicate between the communities, they have to be aware of their different use of terms and concepts. In [26], a short presentation of the communities' different views on LBS is presented. The communities have been selected from publications concerning LBS business models and LBS privacy issues.

Table 3: Taxonomy of communities of practice in LBS [26]

Taxonomy of the communities of practice in LBS	
Community	***Description***
Privacy Enhancing Technology (PET)	People in data protection, IT research, cryptography and other academic disciplines care for this area of knowledge. They answer questions like: • How can a user browse the web without being observed all the time? • Who can access a mobile user's location data? • What data can be collected by what party? • Is a user anonymous? If so, under what circumstances? • How long will personal data be kept? • How will personal data be passed on? • What other purposes is location data used for besides the LBS application? • Does a policy exist concerning private data processing, and is it followed by the information system? • Will the user be advised about data processing? Did he consent to processing of his personal data?
Telecommunications Industry	A large, traditional community. Involves equipment vendors, mobile operators, network operators, re-sellers and telecommunications engineers. The community is strongly oriented towards technological questions in telecommunications. Typical topics are: • Which new functionalities can be implemented on the network? And how? • How will position data be gathered? Which mobile terminals support LBS? Which modifications result to network operations, billing ad other processes? • Are all regulatory requirements met? Are the data protection requirements met economically? • What cost will occur upon the implementation of certain functionality?
Economy	This community of knowledge focuses on economy theory, economic numbers, optimization, market theories, diffusion of innovation and other research topics. In economic literature, topics discussed are: • What business models can be used for LBS? • How is the Value Chain of LBS going to look like? • What is the right pricing model for LBS? • What is the optimal supply chain / service level agreement?

Different views on a subject lead to different interpretation of requirements, e.g. for privacy protection. Therefore, a boundary object can help to find mutual understanding of a complex knowledge topic over community boundaries.

How boundary objects can be used to describe a taxonomy of LBS that recognizes these conflicting definitions from communities of practice has been shown in [26]. Approximately 200 scientific publications have been classified with regard to their community background. Thereafter, the use of terms that are relevant for LBS has been studied. The resulting community-specific terms have been identified and sorted as independent or community-spanning terms (the latter with either coherent or conflicting interpretation by the communities).

5 A Boundary Object for Location Privacy Requirements

Telecommunications terminology sometimes is conflicting in terms and semantics of words. The semantics depend on a particular group's view. For example, "data protection" has very different semantics for either a telecommunications executive or a data security specialist. The former will regard data protection as a source of operational cost, while the latter will very likely think in terms of cryptographic mechanisms and system configuration against data theft. The description is based on the taxonomic analysis presented in [26]. At first, a model of communities of practice involved in LBS has been found using stakeholder analysis (see section 4). Next, using scientific publications originating from the respective communities, their use of terms has been analyzed and compared to each other. Finally, the resulting common terms, their interpretations and their differences among the communities are used to construct the boundary object.

5.1 Assessment of Community-Specific Knowledge

An analysis of approx. 200 scientific articles from the communities in 2.1 is summarized. The analysis focused on the communities' usage of terms. The frequency of occurrence and the community-specific interpretation of the terms are analyzed. Insightful excerpts from the analysis are presented.

First, the publications have been analyzed for important terms. The terms have been categorized according to their community semantics and the frequency of their appearance. The resulting table offers an overview on the importance of the terms (by frequency per community) and also a key to equal of different interpretation of the term by the communities.

The next step of the analysis selects terms available in several communities – which creates the common vocabulary for the LBS project. The resulting boundary spanning terms are those of particular interest in system analysis and specification, as they are the common – and potentially misinterpreted – vocabulary of the involved stakeholders.

Table 4: Term classification into boundary-spanning character [26]

Type	Description
Regular language	No specific meaning of the term for any of the communities can be found.
Technical term	The term is specifically used by one community.
Weak Boundary Spanner	The term is seldom used in several communities.
Medium Boundary Spanner	The term is used in several communities, with a high frequency in one community.
Strong Boundary Spanner	The term is frequently used in several communities.

Table 5: Selected Terms and their community usage frequency [26]

Term	PET Community	Telecommunications Community	Economy community
anonymity	360	6	2
anonymous payment	3	0	0
business model	38	124	869
identity	647	36	21
identity management	201	0	0
m-commerce	45	195	181
pseudonymity	58	0	0
value chain	0	49	327

To illustrate different term usage, selected terms are shown in Table 5. While "anonymity" appears in publications of all three communities, mainly the PET community seems to use the term frequently. In contrast, "pseudonymity" seems exclusive to the PET community. Is "anonymity" possibly used but interpreted as "pseudonymity" by the other communities? As shown in Table 5, telecommunications people and economists might, at a first meeting, be very ignorant about the concept of "anonymous payment", as it is not used in publications concerning LBS. The same might apply for "identity management", which in scientific publications usually appeals to the PET community. Most interestingly, "business model" is hardly mentioned in PET publications, while there is a clear use in business papers, and a strong representation in the economy community. This indicates that business considerations upon deployment of an infrastructure could be an area of conflict between the communities.

After the identification of the boundary-spanning terms, they can be grouped into their communities, and used as interfaces between the communities they belong to. For finding these interfaces, the visualization shown in Table 6 is used. It shows the type of boundary spanner, and the community border it transcends. For example, “accuracy” is a weak interface between the PET and Telecom communities. The information from Table 6 will be used to map out the Boundary Object for LBS.

Table 6: Example Classification of boundary spanning terms according to Table 4.
* = weak, **=middle, ***=strong. + = Appears in respective community. [26]

Terms				
	Type	**PET**	**Telecom**	**Economics**
acceptance	*	+	+	+
access to data	**	+	+	+
access to information	**	+	+	+
accessibility	**	+	+	+
accountability	*	+		
accuracy	*	+	+	
added value	**	+	+	+
aggregation	**	+	+	+
angulation	**	+	+	
anonymity	***	+	+	+
anonymous payment	**	+	+	+
location	**	+	+	
location aware	***	+	+	
location determination	**	+	+	
location enabled	***	+	+	
location identification	***	+	+	
location management	**	+	+	
location privacy	**	+	+	
location sensing	***	+	+	
location sensitive	***	+	+	
location tracking	***	+	+	
manipulation	*	+		

The examples above illustrate the use of a systematic taxonomy in form of a boundary object. With the documented interpretations of terms, it seems mandatory for any LBS project to define a common knowledge object before proceeding with the specification of requirements and information systems. The total amount of boundary spanning terms was 136, of which 37 were strong Boundary Spanners. Please refer to Table 7 for further details.

Table 7: Some numbers about analyzed terms & publications [26]

Some numbers	**total**	**Communities**		
		PET	**Telecom**	**Economics**
Analyzed publications	**209**	88	61	28
Candidate Terms	**150**			
- Technical terms	**7**	3	3	1
- General terms	**7**			
- Strong Boundary Spanners (***)	**37**			
- Medium Boundary Spanners (**)	**58**			
- Weak Boundary Spanners (*)	**41**			
- Boundary Spanners total	**136**			

5.2 Construction of the Boundary Object for Location Privacy

This paragraph will show the construction of a boundary object that represents the results from 2.2. In particular, the intersections, complementary knowledge and confusing use of terminology and concepts of the communities will be presented. The result is a knowledge object creating mutual understanding for terminology, concepts and interests.
In our case for privacy in LBS, the application specific communities have been identified as telecommunications, PET and Economics (see Figure 8). The graphical representation of the terminology Boundary Object will be done in the form of two diagrams. Figure 9 shows a detailed representation of the taxonomical aspects, while Figure 8 shows a simplification that represents a framework for negotiating the interdisciplinary requirements for LBS in requirements engineering and privacy infrastructure specification.

Figure 9 shows the boundaries between PET, Telecommunications and Economics. The three communities are draws as areas with borders. The areas intersect in such a way that each community has intersecting borders with each other community – and in the center of the diagram with all others. These intersections represent the boundary spanning interfaces between the communities. To conceptualize the common terminology (which represents a Boundary Object, as stated in [43]), the boundary spanning terms identified in section 5.1 will be placed in their respective intersection areas. The type of boundary spanner directly refers to the type of intersection: Weak boundary spanners appear in a community's exclusive area. Medium boundary spanners usually appear in a 2-community intersection, while strong boundary spanners and some medium boundary spanners appear in the 3-community intersection of all communities. Technical terms belong to their respective community only, and could be written into the respective community's area. In Figure 9, the technical terms have been left out for clarity.

For example, in Figure 9 the term "Cell-ID" in "Telecom Business" is a weak boundary spanner. The term "m-commerce" interfaces the Telecom and Economics community. Finally, in the center of all three communities, the term "identity" represents a strong boundary spanner. This resulting taxonomical Boundary Object represents the common language for location-based services. This form of the object will help within the requirements engineering phase by enabling the participants from all communities to understand the implications of terms used when specifying location privacy needs of a new mobile infrastructure or application.

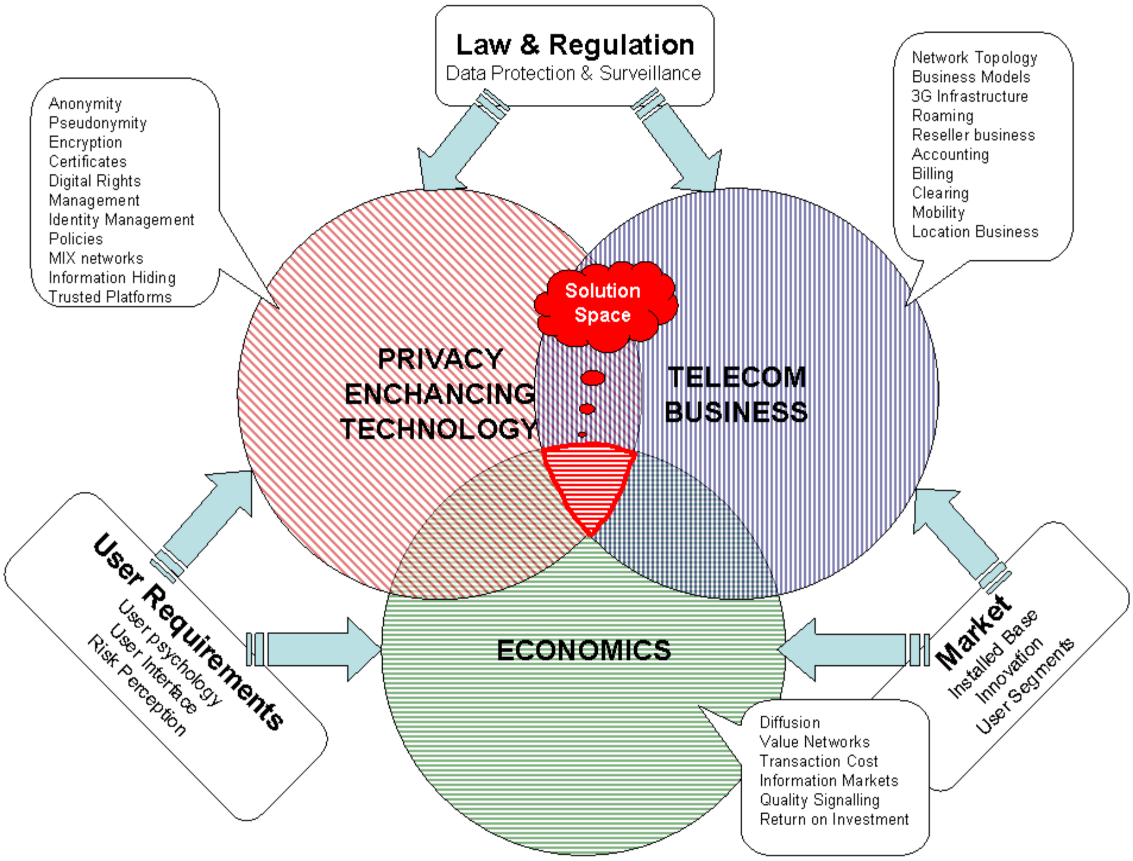

Figure 8: Boundary Object for privacy requirements analysis for Location-based Services

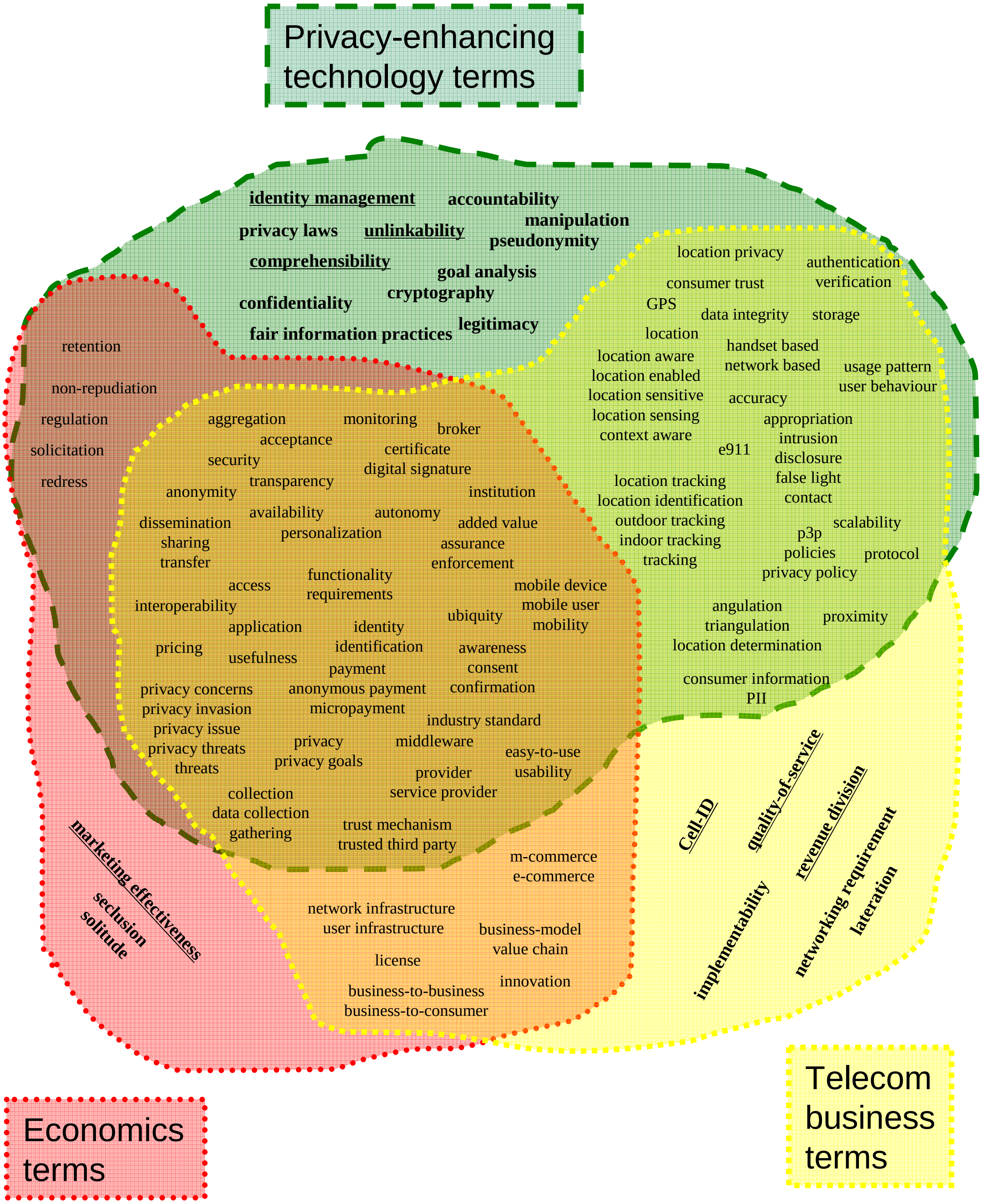

Figure 9: The Taxonomy Boundary Object for Location-based Services [26]

A simplification of the intersecting communities can be used to visualize the possible solution space. By omission of the terms in Figure 9, the resulting diagram in Figure 8 represents the communities and their common borders. The center represents the solution space that will represent the area where the communities' interests intersect, and where a win-win situation for all stakeholders can be negotiated. Each community provides its most important topics, technologies, standards, procedures and requirements to their respective area.

These communities are influenced by law and regulation, by the situation on the market of needs and related products, as well as by the user requirements from various disciplines respectively. To facilitate important influencing subjects that might not entirely be part of the community, an additional object may be attached to the diagram and be connected to the community that is influenced by it. For example, in Figure 8, “law & regulation” have been identified as providing to the PET and Telecom communities. A further elaboration of each communities’ interest leads to a Boundary Object that represents all stakeholders requirements – and by using the taxonomical Boundary Object from Figure 9 to express their requirements, the other stakeholders are put into a position to interpret the requirements in a correct way.

The construction of these two Boundary Objects requires communication, analysis and negotiation between the involved stakeholders. But by the execution of this negotiation process, a clearer understanding of each community’s language and their requirements is possible. Additionally, the resulting Boundary Objects can be used as a reference for various purposes in the development project following the specification phase (see also [29]). The Boundary Objects in requirements engineering are then to be used as a reference to each communities’ understanding, and as a base for evaluation of the performed steps on the early design phases.

6 Next: Toward Privacy-Respecting, Mobile Location Infrastructures

This section will show how to use the boundary object results to reach a multilaterally satisfying privacy design for LBS. The resulting workflow approach for Boundary Object requirement engineering and privacy specification has been designed as illustrated in the 5 steps of the process in Figure 1:

Step 1: Identification of Stakeholders: With the input being the desired business case and use case of a new online business, a stakeholder analysis is performed in the first step. This identifies the stakeholders and their respective business and other interests in the use case that is to be implemented.

Step 2: Requirements using Boundary Objects: From the stakeholders and the discovered interests, the development a boundary object that spans all involved communities with their needs and terminologies is the next step. This identifies language and conceptual conflicts. The Boundary Object helps to find a common terminology, and visualizes the community-spanning intersection of terms, concepts and interests that will be the framework for design.

Step 3: High-Level Specification: Building on the knowledge gathered in step 2, a high-level specification of the infrastructure and business logic is made. The specification is performed in standardized software and business process modeling languages [4], [12].

Step 4: Multilateral Security Analysis: The next step proceeds with a Multilateral Security Analysis [34] on the high-level specification- Its goal is to gather security and privacy requirements for the infrastructure in question, and to make suggestions for improvement of the specification. Multilateral security analysis takes under account all stakeholder’s requirements relevant to security and privacy issues.

Step 5: Security Detail Specification: Using the output of step 4, a detailed specification of security properties is performed. This will provide the required technical details for the implementation of the infrastructure. Security and privacy properties can be specified according to assurance standards (such as [22]) or according to the UMLSec extension [24].

Evaluation: Following the five steps, a cycle of socio-technical evaluation in accordance with Sommerlatte [39] or to one of the 4th generation approaches in [38] will be carried out. The evaluation ensures the conformance of the detail specification with privacy functionality and with the original requirements. This is of particular importance with regard to the business and user requirements.

An example application of the design process has been done for the LBS application of mobile disaster warnings on mobile phones in [37], [14] and [36]. After requirements identification, a thorough multilateral security analysis has led to a security and privacy concept that implements the stakeholder’s requirements on all parts of the infrastructure. A brief summary of the approach and the results is provided below. The diagrams are taken from [14].

6.1 The Disaster Warning Infrastructure

The high penetration of the population with mobile phones makes GSM/UMTS a high-bandwidth channel for disaster management. Citizens can be informed selectively after being localized by the mobile network to avoid blocking of critical resources. Furthermore, the localization of all mobile phones in a disaster area can be used by the disaster manager to survey the situation and plan the next steps. By pre-registering disaster specialists (e.g. firemen, police forces), they can be identified and notified by the disaster manager. For risk reduction, registered users can monitor their property or family members and receive notification in case of a disaster warning in an area-of-interest. Here, for example neighbors could be asked to secure property before a storm reaches the property. See Figure 10 for an illustration of the scenario.

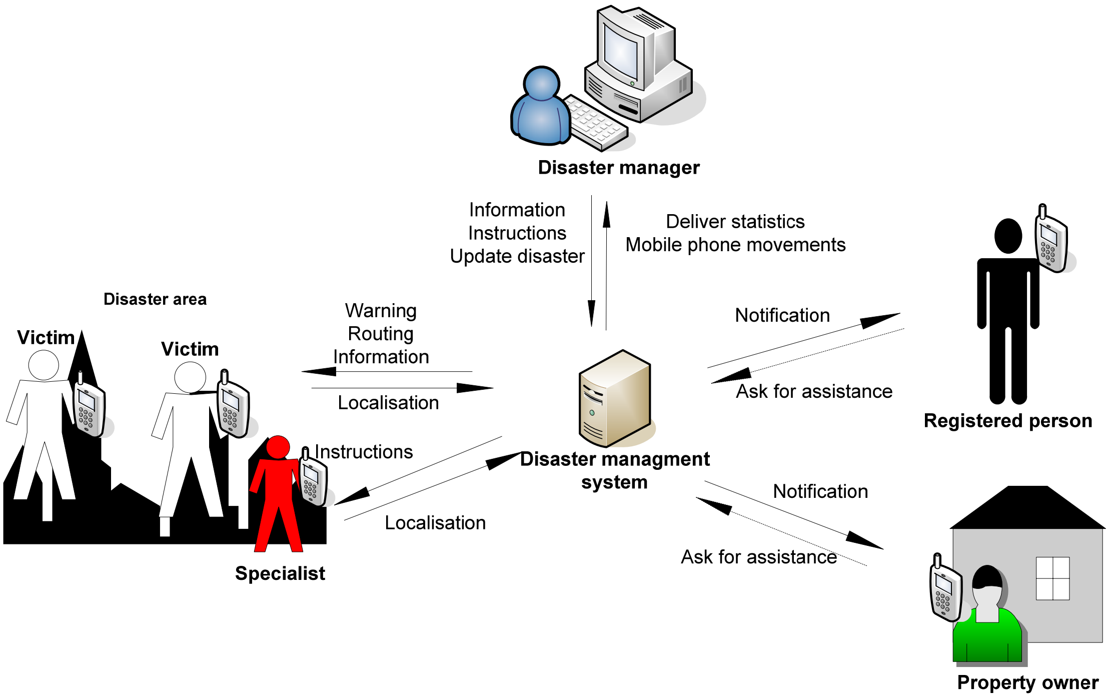

Figure 10: Disaster Management basic scenario [14]

Summarizing the main system features, the LBS disaster management system is responsible for these functions:

- Geographical administration of disaster areas including weather and traffic data;
- Localization of mobile phones within the disaster area;
- Reporting of statistics of phones, phone movements, population density based on LBS to disaster manager;
- Identification of disaster specialists among the citizens with mobile phones;
- Delivery of messages to mobile phones (either for evacuation, or containing instructions for disaster specialists);
- Notification about citizens threatened by disasters to registered next-of-kin.
- Notification about area threatened by disaster to property owners or persons in charge for areas of interest (e.g. chemical facilities).

The scenario contains several flows of information that is regarded private by some of the participants. Our infrastructure solution provides mechanisms to keep the data private as a measure to ensure high participation rates of the population. But there are obvious conflicts in requirements, too. The use of a Boundary Object here defines a language of expectations and requirements that creates clarity about the semantics of particular stakeholder's interests. Privacy is threatened in several places in our scenario. An observer configuration can reveal social networks of registered users. The whereabouts of off-duty disaster specialists can be retrieved with the system. Also, no localization of citizens should happen unless there is a real disaster. Furthermore, the location of citizens within a disaster area is information only relevant for the disaster manager. It must be impossible to find persons in charge of particular facilities unless there is a disaster.

In our solution we suggest a middleware system with front-end support to control the flow of information and to protect the interests of every party. This system consists of three components shown in Figure 11:

- Matcher: Manages locating the citizens in the disaster area. Matches the disaster area with observation rules of the users. Protects the persistent store of observation rules on behalf of the distinct user. Matches profiles of threatened person with their registered contact person.
- Identity management system: Steers information exchange of the disaster management with mobile operator and the citizen in an emergency case. This is similarly described in [5].

- Process control: Controls the disaster management system, represents an interface to the disaster manager and is responsible for temporal storage disaster data (observation rules and position information).

The warnings of victims and instructions to specialists are to be transmitted via cell broadcast. This bypasses the performance limitations of point-to-point technologies like short message services. Notifications for specialists are encrypted. Unlike the warning mass broadcast, this notification will be sent point-to-point. To be able to use the whole bandwidth of the suggested system it is necessary to register as a user and to deposit observation rules and specialist status including verification of status and claims. Unregistered users are only able to receive warnings and get localized. After a disaster user-specific information will be deleted or anonymously stored. Only the user himself will be able to find out when and how often he was located.

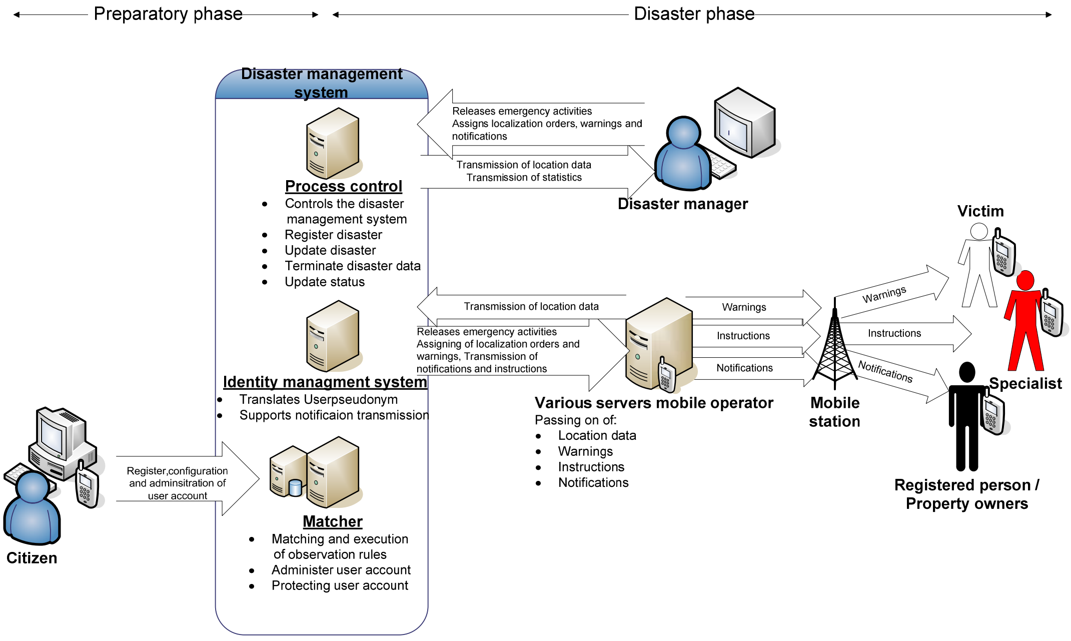
Preparatory phase
Disaster phase
Disaster management system
Process control
Controls the disaster management system
Register disaster
Update disaster
Terminate disaster data
Update status
Identity managment system
Translates Userpseudonym
Supports notificaion transmission
Matcher
Matching and execution of observation rules
Administer user account
Protecting user account
Citizen
Register,configuration and adminsitration of user account
Releases emergency activities
Assigns localization orders, warnings and notifications
Transmission of location data
Transmission of statistics
Disaster manager
Transmission of location data
Releases emergency activities
Assigning of localization orders and warnings, Transmission of notifications and instructions
Various servers mobile operator
Passing on of:
Location data
Warnings
Instructions
Notifications
Warnings
Instructions
Notifications
Mobile station
Warnings
Instructions
Notifications
Victim
Specialist
Registered person / Property owners

Figure 11: Disaster Management solution overview [14]

However, to ensure that the high-level design that was performed and resulted in the specification of system properties in Figure 11 still matches the stakeholders' understanding of the system's security properties, an evaluation against the initial understanding of the security & privacy requirements must be made. For this reason, the original stakeholder's interests concerning their privacy stakes will be reviewed against the high-level specification. This is done by the systematic analysis of the transactions with personal data that can occur on the system. For each transaction, the involved stakeholder's interests are extracted from the Boundary Object. Here, the important point is that the interests are interpreted in the way the stakeholder is used to in his community, as many misinterpretations happen when members of a different community of practice interpret the other community's concepts. When this cycle of checking is finished, the specification proceeds to the multilateral security analysis.

The resulting security detail specification for the disaster warning system is shown in overview in Figure 12. It attributes the necessary security and privacy functionality to the system entities and communication links. To ensure conformance with the stakeholders, once again this specification is to be matched with the initial requirements using the Boundary Object to ensure interpretation of requirements within the initial community.

7 Conclusion

When designing mobile information systems that process personal location information, it seems advisable to go through the effort of developing a common understanding of terms and concepts in the sense of a boundary object. With changing application contexts, deployment of systems over several cultures in a globalized context and with a business perspective, there will be hardly any static privacy engineering process possible. Therefore, the value of privacy and the effort for its protection in information systems are relative. The construction of a set of Boundary Objects can help mapping out the whole space of requirements and possible solutions, thus helping software engineers to grasp the breadth of possible solutions – and pick a multilaterally sufficient solution approach. The particular degree of privacy protection results from a socio-technical process that balances interests of users, law, business and infrastructure depending on the application of the information system in question. With the approach presented in this paper, multilaterally satisfying design of the privacy infrastructure in information systems can be found. By executing a multilateral security analysis on the first design, a detailed privacy design according to the community requirements can be achieved. The approach has been tested with promising results on the disaster warning application scenario, and will be further used for other application contexts.

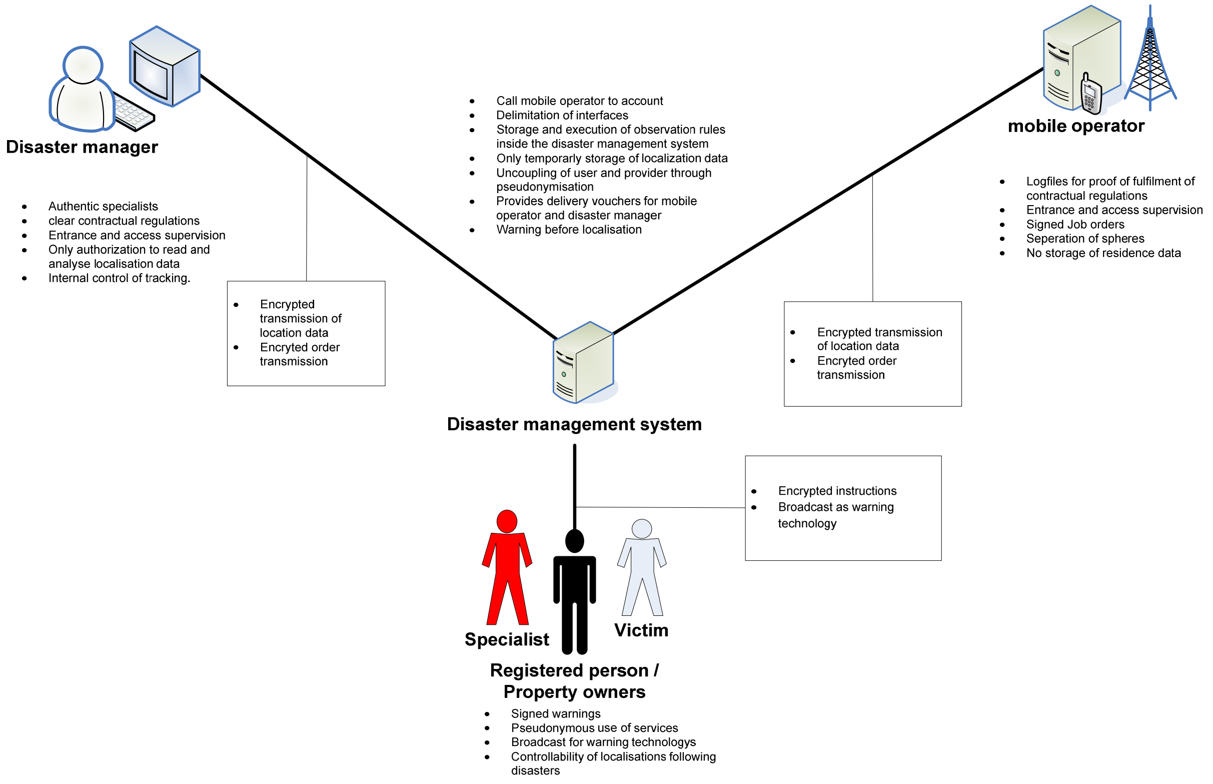
Disaster manager
Authentic specialists
clear contractual regulations
Entrance and access supervision
Only authorization to read and analyse localisation data
Internal control of tracking.
Encrypted transmission of location data
Encryted order transmission
Call mobile operator to account
Delimitation of interfaces
Storage and execution of observation rules inside the disaster management system
Only temporarly storage of localization data
Uncoupling of user and provider through pseudonymisation
Provides delivery vouchers for mobile operator and disaster manager
Warning before localisation
mobile operator
Logfiles for proof of fulfilment of contractual regulations
Entrance and access supervision
Signed Job orders
Seperation of spheres
No storage of residence data
Encrypted transmission of location data
Encryted order transmission
Disaster management system
Encrypted instructions
Broadcast as warning technology
Specialist
Victim
Registered person / Property owners
Signed warnings
Pseudonymous use of services
Broadcast for warning technologys
Controllability of localisations following disasters

Figure 12: Security & privacy properties of the disaster management system [14]

Acknowledgments

Part of this research was funded by the European Union IST projects FIDIS and PRIME; however it reflects the author's opinion only. I thank Prof. John Leslie King for his valuable hint about "Sorting things out" for privacy.

References

[1] E. G. Arias and G. Fischer, Boundary Objects: Their Role in Articulating the Task at Hand and MakingInformation Relevant to It,in Proceedings of the International ICSC Symposium on Interactive & Collaborative Computing (ICC'2000) Wetaskiwin, Canada: ICSC Academic Press, 2000, pp. 567-574.

[2] L. Barkhuus, Privacy in location-based services: Concern vs. coolness, in Mobile HCI 2004 Workshop on Location Systems Privacy and Control, Glasgow, 2004.

[3] G. W. Blarkom, J. Borking, and J. Olk, Handbook of Privacy and Privacy-Enhancing Technologies. The Hague:College bescherming persoonsgegevens, 2003.

[4] G. Booch, J. Rumbaugh, and Jacobson, I., The unified modeling language for object-oriented development, Rational Software Coorperation, Santa Clara, USA, 1996.

[5] J. Borking, Der Identity Protector, Datenschutz und Datensicherheit (DuD), vol. 20, no. 11, pp. 654-658, 1996.

[6] G. C. Bowker, and S. L. Star, Sorting things out: classification and its consequences. New Baskerville:MIT Press, 1999.

[7] S. Brand, (2006, November) ISO/IEC/JTC1/SC27/WG3 COMMITTEE MEETING. [Online]. Available: http://www.incits.org/tc_home/CS1/2005docs/cs1050163.htm.

[8] P. R. Carlile, A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development, Organization Science, vol. 13, no. 2, pp. 442-445, 2002.

[9] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM, vol. 4, no. 2, pp. 84-88, 1981.

[10] B. L. Crosby, Stakeholder Analysis: A vital tool for strategic managers, USAID IPC Technical Notes, no. 2, 1991.

[11] C. Diaz and B. Preneel, Taxonomy of Mixes and Dummy Traffic, in Proceedings of the 18th IFIP World Computer Congress, Toulouse, France, 22.-27. August 2004, 2004, pp. 215 - 230.

[12] H. Eriksson, and M. Penker, Business Modeling with UML: Business Patterns at Work. New York:John Wiley & Sons, Inc., 1998.

[13] FIDIS, FIDIS Deliverable D7.2: Descriptive analysis and inventory of profiling practices, European Union IST FIDIS Project, 2005.

[14] L. Fritsch and T. Scherner, A Multilaterally Secure, Privacy-Friendly Location-based Service for Disaster Management and Civil Protection,in Networking - ICN 2005 - Proceedings of the 4th International Conference on Networking, Reunion Island (LNCS 3421), France, April 17-21, 2005(P. Lorenz and P. Dini, Eds.). Berlin, Heidelberg, New York: Springer, 2005, pp. 1130-1137.

[15] L. Fritsch, Economic Location-Based Services, Privacy and the Relationship to Identity, in 1st FIDIS Doctoral Consortium, IST FIDIS Network of Excellence, Riezlern, Austria, 2005.

[16] L. Fritsch, Profiling and location based services, in D7.5: Profiling the European Citizen. Cross-disciplinary perspectives (M. Hildebrandt and S. Gutwirth, Eds.). 2007.

[17] L. Fritsch, T. Scherner, and K. Rannenberg, Von Anforderungen zur verteilten, Privatsphären-respektierenden Infrastruktur, Praxis in der Informationsverarbeitung und Kommunikation (PIK), vol. 29, no. 1, pp. 37-42, 2006.

[18] M. Gruteser and D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking, in First International Conference on Mobile Systems, Applications, and Services (MobiSys'03), 2003, pp. 31-42.

[19] A. R. Hevner, S. T. March, J. Park, and S. Ram, Design Science in Information Systems Research, MIS Quarterly, vol. 28, no. 1, pp. 75-105, 2004.

[20] J. Hong, J. Ng, S. Lederer, and J. Landay, Privacy risk models for designing privacy-sensitive ubiquitous computing systems, in Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques(D. Benyon, P. Moody, D. Gruen and I. McAra-McWilliam, Eds.). New York:ACM Press, 2004, pp. 91-100.

[21] M. Huber, T. Dietl, J. Kammerl, P. Dornbusch, Collecting and providing location information: The location trader, in MoMuc'2003, München, 2003.

[22] ISO, ISO 15408 The Common Criteria for Information Security Evaluation, 1999.

[23] O. Jorns, PRIVES: A privacy enhanced location based scheme, in Mobile HCI 2004 Workshop on Location Systems Privacy and Control, Glasgow, 2004.

[24] J. Jürjens, Secure Systems Development with UML. Berlin:Springer, 2005.

[25] KPMG Canada, A Retailer's guide to Privacy Risk Management, KMPG LLP, Canada, 2003.

[26] C. Koch, Taxonomie von Location Based Services, Lehrstuhl für M-Commerce & Mehrseitige Sicherheit, Johann Wolfgang Goethe - Universität, Frankfurt am Main, 2006.

[27] T. Koelsch, L. Fritsch, M. Kohlweiss, and D. Kesdogan, Privacy for Profitable Location Based Services,in Security in Pervasive Computing - Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2005) (LNCS 3450)(D. Hutter and M. Ullmann, Eds.). Boppard:Springer, 2005, pp. 164-179.

[28] M. Kohlweiss, L. Fritsch, M. Radmacher, M. Hansen, and H. Krasemann, Overview of existing assurance methods, EU IST PRIME Project, 2004.

[29] A. Kühn, Boundary Objects for E-Government, Department of INformation Technology, University of Zürich, Zürch, Switzerland, 2006.

[30] F. Lehner and R. T. Watson, From E-Commerce to M-Commerce: Research Directions, Wirtschaftsinformatik, Universität Regensburg, Regensburg, 2001.

[31] S. March and G. Smith, Design and Natural Science Research on Information Technology, Decision Support Systems, vol. 1995, no. 15, pp. 251-266, 1995.

[32] A. Pouloudi, FOCUS: Conflicting Concerns over the Privacy of Electronic Medical Records in the NHSnet, Business Ethics - A European Review, vol. 6, no. 2, pp. 94-101, 1997.

[33] M. Radmacher, J. Zibuschka, T. Scherner, L. Fritsch, and K. Rannenberg, Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen,in Proceedings of the 8th conference "Wirtschaftsinformatik 2007" Karlsruhe:2007.

[34] K. Rannenberg, Multilateral Security - A concept and examples for balanced security, in Proceedings of the 9th ACM New Security Paradigms Workshop, Cork, Ireland:ACM Press, 2000, pp. 151-162.

[35] T. Rensmann, Eine Tarnkappe für Location-based Services, Lehrstuhl für M-Commerce & Mehrseitige Sicherheit, Abteilung Wirtschaftsinformatik, Johann Wolfgang Goethe - Universität, Frankfurt am Main, 2007.

[36] T. Scherner and L. Fritsch, Notifying Civilians in Time,in Proceedings of the Eleventh Americas Conference on Information Systems (AMCIS 2005)(AIS, Eds.). Omaha: Nebraskam USA, 2005, pp. 1611-1619.

[37] T. Scherner, Mehrseitige Sicherheit bei Katastrophenschutzanwendungen, Lehrstuhl für M-Commerce & Mehrseitige Sicherheit, Johann Wolfgang Goethe-Universität, Frankfurt am Main, 2004.

[38] M. Siponen, Designing Secure Information Systems and Software, Department of Information Processing Sciece, University of Oulo, Oulo, Finland, 2002.

[39] T. Sommerlatte, Angewandte Systemforschung: ein interdisziplinärer Ansatz. Wiesbaden:Gabler, 2002.

[40] S. L. Star, and J. R. Griesemer, Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology 1907-39, Social Studies of Science, vol. 19, no. 3, pp. 387-420, 1989.

[41] V. Zeimpekis, G. M. Giaglis, and G. Lekakos, A Taxonomy of Indoor and Outdoor Positioning Techniques for Mobile Location Services, ACM SIGecom Exchanges, vol. 3, no. 4, pp. 19-27, 2003.

[42] A. Zuccato, Holistic Information Security Management Framework. Karlstadt:Karlstadt University Universitetstrycjeriet, 2005.

[43] P. van Dijck, (2005, July) Taxonomy is a boundary object. [Online]. Available: http://www.poorbuthappy.com/ease/archives/2003/10/31/1860/taxonomy-is-a-boundary-object.