User requirements and Protection Profile for secure location sharing

Julie Facon, Ben Fetler, and Carlo Harpes, *itrust consulting* (1)

***Abstract* – Several location sharing services for vulnerable people compliant with a high level of data privacy and data integrity requirements are currently under development. This paper presents an analysis of user requirements and a proposal of a protection profile for a location sharing application of a mobile device. This protection profile, compliant with ISO 15408 should prepare a secure design, enable certification and thus contribute to make customer confident in the system.**

Keywords – Location sharing, privacy, vulnerable people, Protection Profile, Smartphone.

I. INTRODUCTION

Location sharing services are becoming very popular. Google Latitude [1] and GPSLite [2] are examples of location sharing based services. These services are highly attractive for communities of young people who like to share live experiences. These services are offered free of charge on the Internet.

The main objective of a recently announced FP7 project called Liveline [3] is to develop a commercial, secure location sharing service. "Secure" means that only authorised parties can access the location data and "sharing" means that location data are sent via an external component to other persons. The Liveline project starts from the observation that there are people whose unexpected absence immediately creates high level of concern and anxiety at the side of their close relatives and caretakers, as they may not be able to find their way back home and they may become easy victims of accidents or crime. Examples of such groups of people are children, epileptic people, elder people suffering from various types of mental absences and mentally disabled people. In regrouping these people under the common denominator: 'vulnerable' people, it is possible to state that Liveline aims at protecting vulnerable people. It is immediately clear that this is not a closed category of people: in a certain way everybody can be vulnerable to some extent and in some circumstances.

Their status puts them in a direct protective relationship towards their close relatives, tutors, caretakers, etc. In case this protective relationship is known and recognised, these relatives, tutors, etc. may need to know the vulnerable person's position in case of an unexpected absence. Being able to track a vulnerable person's position immediately has several advantages: it saves critical search time, it takes away unnecessary worries and it reduces unnecessary police interventions.

According to their website, the Liveline consortium plans to develop from an existing technology a private platform for secure location sharing of the vulnerable people, only accessible to their authorised and authenticated close relatives [3].

II. PRIVACY THREATS AND PRIVACY PRESERVATION IN LOCATION-BASED SERVICES

Since the flourishing of Location-based services, in 2004 [4], operators which wanted to offer this kind of services were mainly exposed to three major difficulties: find the best and cheapest technology to use, develop location based-services where the users see the need to use it, and finally find solutions for solving the security and privacy concerns of the end-users [5].

In this paper we will concentrate on the security and privacy aspects which are a part of the flagships of future location-based services. Location data, combined with personal information of a user represent in a lot of different scenarios serious privacy threats. The disclosure of these sensible data could cause, amongst others, economic damages, provoke location-based spam, harm the reputation of a person [6] or promote criminality [4], [7]. All the enumerated threats for privacy can even be aggravated if children are concerned, which is the case for the Liveline system.

All those threats lead to the need to find solutions which preserve the privacy of location-based service users. Preserving privacy starts by the choice of the positioning technology because the choice between handset-based positioning or network-based positioning plays a role in privacy. In the handset- or client-based approach, the location data are computed on the handset itself and only disclosed to the network with the users consent. However in the network-based approach, the computation of the raw location data are computed by the service provider and thus the potential loss of privacy are greater [4], [6].

Several other propositions were made, concerning the preservation of privacy, like Pseudonymisers, Anonymisers Obfuscation-based methods [7] or web service privacy, where either larger amounts of location data are downloaded and later on filtered on the device of the user, such that if data is revealed, the location data is not precise enough to locate the user precisely [5], [6] or the users identity is tried to be obscured such that an identification of a user is not possible.

Because of the fact that people rather trust transparent systems, where they see who uses their data and where their data is stored [8], we have to consider not only technological solutions. The proposed solution in this paper is to follow a

(1) J. Facon, trainee of University of Technology of Troyes, facon@itrust.lu, B. Fetler, trainee of University of Luxembourg, fetler@itrust.lu, Dr. C. Harpes, Managing Director at itrust consulting, 6891 Berbourg, Luxembourg, harpes@itrust.lu. This paper has been co-funded by the European commission within the FP-7 Framework.

norm, where people can clearly see how the system is designed and how data is treated by the system.

III. User requirement

A main focus of a location-sharing service is to find user requirements, expressed by people who fit into the target group of the offered service.

However, to prepare the discussion with target user group of vulnerable people and their relatives and to collect requirements of stakeholders which do not explicitly fit in the target user group, the service has been demonstrated to visitors at the Galileo Application Days from 3-5 March 2010 in Brussels. A questionnaire was worked out, containing 9 general questions chosen to cover important parts of typical requirement on a location sharing service.

Visitors had the possibility during the demonstration to respond to the questions and express their personal requirements on the system. These questionnaires were evaluated and the result of the evaluation, on the one hand, confirmed the state of the knowledge on location-based systems and, on the other hand, provided further refinements on costumers needs.

In total, 32 questionnaires have been filled out and evaluated. As the respondents were visitors of a technical exposition, we have to clarify that this is not a representative study. It nevertheless helps to face a future service design on user requirements.

The questions, covering the expectancies of the respondent, revealed that people want to have a fast and easy to handle, service with high accuracy (between 1 meter (38%) and 10 meters (44%)), which could be installed on the most popular mobile phones like Nokia (24%) and the Apple iPhone (21%).

People agree to use a location sharing service as a commercial service (73%), with cost between 3 and 5 Euro per month (34%).

The target use is the family environment (60%). That people would use the system primarily in their family environment could be explained by the fact that people trust mainly their family in emergency situations and they trust their family to not use the service in an abusive way.

To get a more precise idea to whom in the family users would recommend to use Liveline, people answered that they would use it for localisation of their young children (40%) and of their elder family members (21%).

The evaluation also showed that the main obstacle why people would not use such a service, is the concern that their data could be shared with other parties (39%), followed by the concern that they can get localised with or without their consent (31%). This feedback, together with the feedback that people want their data to be stored securely and that the operator of such data be put under supervision of a Data Protection Authority (66%), shows that people have large concerns on their privacy.

This result seems to be in contradiction with the current popularity of unsecured social networks, and the willingness of peoples to share very private information. But it is consistent with the current public debates and the raised concerns on privacy issues.

The increasing awareness encourages service providers to conceive a secure system, to make a secure design, and to be prepared for certification and operational audits of the service delivery. An excellent basis for such independent certification is ISO 15408, generally called common criteria, in which security requirement are defined in a document called Protection Profile.

IV. Common Criteria

Common Criteria is the standard method to ensure product security and communicate on the security of software of hardware component. The same method has also been used in the FP7-project MICIE [11] to define security requirements of a gateway sharing risk information among operators of critical infrastructure. In general, the method is state-of-the-art for high security components like electronic signature cards or crypto servers.

A. Common Criteria

Common Criteria (ISO 15408) formalise the way to integrate security in a product. The main purpose is to define a security profile called protection profile for a product called target of evaluation. A protection profile can be applied to different products of the same type. The certification evaluate that the security of a given product has been implemented according to the formal requirements and good practices as it is described in the protection profile. Such evaluation is generally made by independent, accreditated labs. The depth of this evaluation is the so-called evaluation Assurance Level

Note that common criteria does not provide certification that a product is secure in all circumstances; it can certifythat a product was designed and developed following transparent requirements and that it is secure to use it in the conditions that it has been designed for.

B. Location sharing context

the secure location service that we adresse here consists in making available to authorised persons on a web server through the Internet network location data with a given accuracy collected by some means of localisation, mainly GSP. The localisation device can be a mobile phone, a smartphone or a location tracker.

The system is composed by two parts: one is the application installed on the mobile device and the other one is the web server which receives the location data, authenticates the user and provides the location data.

Location sharing is a sensitive exchange of information especially through public network as Internet. Web applications are common applications that are attacked by non specialist hackers. That is why people should not trust a location sharing service without some guarantees that their private data are protected.

A dedicated approach for assurance of the web server security will be not be defined here. In this paper, we focus on the security of the Smartphone application and the communication towards the server.

The application on the mobile phone is a key application from the security point of view, because it collects and sends location data from and to some other parties. It represents a starting point to define and implement the security

requirements which are needed to protect personal data in a location sharing application.

For the second key component, the web server collecting the location data and providing access to authenticated and authorised users, approaches different than common criteria seems to be more appropriate. A quite recent approach for this is the European Privacy Seal, defined in 2008 [12].

C. Protection Profile

Protection Profiles are used as part of the certification process according to the Common Criteria (ISO 15408). It is a document which describes the security requirements of a product without describing how these requirements will be implemented. It describes an overview of a product named Target of Evaluation (TOE) and his functionalities. Then, it describes the assets that should been protected and the assets that the TOE should protect. After that, it describes the threats and the assumptions about the TOE and his environment. Assumptions permit to define the right context to use the products in good condition. To finish, it describes the security objectives of the TOE and his environment to take care about the identified threats. All these features are used to define the security functional requirement and the security evaluation assurance that the product reach or have to reach.

Moreover, the Protection Profile helps to develop the application in accordance with data privacy and data integrity requirements. It demonstrates that the product has been developed following the security requirements defined on it, so people can be confident on the product.

V. Protection Profile for a Mobile Location Sharing Application

This part presents the Protection Profile for a mobile location sharing application.

A. TOE overview

This part describes the main functions of the TOE.

1) TOE type

The TOE is a software component which can be installed on different kind of equipment such as Smartphone. Its objective is to read location information provided by a GPS chipset on the smartphone, and to send it regularly to a web server. Moreover, it may provide the location of other devices by retrieving the information from the web server.

2) Usage and major security features of the TOE

The TOE is used to collect and send location data about people. These data are considered as personal data so that it is necessary to assure their confidentiality during the entire process.

B. TOE description

This part describes the TOE and how it interacts with its environment.

1) Physical scope

The TOE is software.

2) Logical scope

The TOE is composed by the application process and its configuration data. It has five interfaces with its environment:

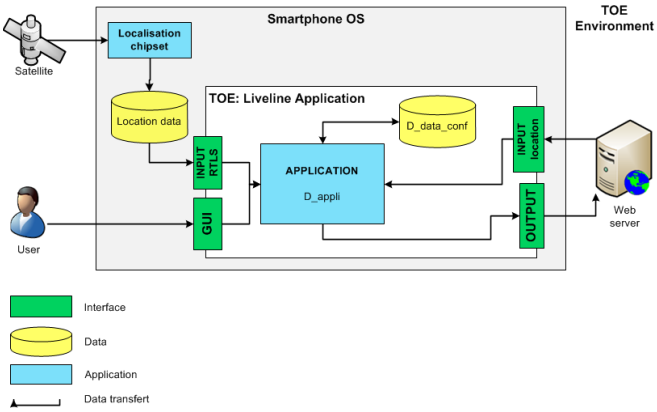

Figure 1: Target of Evaluation Environment

1. Input RTLS (Real Time Locating System) is used to collect location data from the location system;
2. GUI is used to interact with the user of the application. He can activate the system by entering his password and see other people localisation;
3. Output is used to send location data to the web server by public networks;
4. Input location is used to request a location data from the web server to see someone's location through the GUI;
5. The operating system in which it is installed.

Figure 1 represents an overview of the TOE, its environment and the interactions between it.

3) Security objectives for the operational environment

The correct operation of the TOE depends on the operating system on which it is installed, on the hardware, on the visibility of satellite signals, and on the GSM network for external communication.

C. Assets

The description of each asset of the TOE also gives the type of protection required.

D_Data: Location data which are transferred through the application from the GPS chipset to the web server. Protection: Confidentiality, Integrity.

D_Data_Conf: Configuration data of the application. Protection: Confidentiality, Integrity.

D_Software: The application which is installed on the smartphone. Protection: Integrity.

D. Threats

The threats are evaluated in accordance with the type of potential impact on the information transmitted and to their criticality.

T_Confidentiality: Access to the location data by an unauthorized person or program by listening to the message or by accessing to configuration data through a second application. Assets threatened: D_data, D_Data_Conf.

T_Integrity: Modification of the application configuration. The application can be modified to send location data to a wrong server or to send wrong location data. Assets threatened: D_Data, D_Data_Conf.

E. Assumptions

A_User: The user is a person with honest intentions. He does not switch off the device or leave it at a wrong place.

F. Security Objectives

This section defines security objectives of the TOE and its environment. These security objectives are required to cover the threats defined previously.

1) Security objectives of the TOE

OT_Confidentiality: The location data has to be protected against access from unauthorized person.
OT_Software_Integrity: The application should not be modified by a malware or an unauthorized person.
OT_Data_Integrity: The data send by the software should not be manipulated before reception by the web server and vice versa.
OT_Configuration_Integrity: The password should not be modified by an unauthorized person.

2) Security objectives of the environment

OE_Access: The Smartphone has to be protected by a password such as a SIM code or a password to open the application.
OE_Smartphone_Integrity: The Smartphone has to be protected against malware, virus and worms which can alter its process.
OE_Data_Integrity: The environment should verify that the location data has not been corrupted.
OE_Availability: Communication devices and networks which are used to transfer the location data by the application should be available.

VI. Conclusion

Several initiatives intend to offer a secure location sharing service. Because location data are personal data, it is important to proof that the customer privacy protection is assured by the service. Our questionnaire on user requirements showed that people are concerned by the protection of their private data. The Protection Profile defined with help of the common criteria methodology prepares for secure implementation of a software for location sharing, and allows an independent certification of the Smartphone application including the communication protocol if this external verification is required by the market.

During a pilot phase in 2011, itrust will try to assess whether these features contribute to gain the confidence of vulnerable people and their care takers.

Acknowledgment

The authors thank B. Krüger (SRC-GmbH) for his help on common criteria certification, and Th. Petitgenet and M. Aubigny (itrust consulting) and a multitude of reviewers for useful comments.

References

[1] Google Latitude, Available: http://www.google.com/latitude [Accessed: May 11, 2010]
[2] GPSLite of Motion X, Available: http://motionx.com/ [Accessed: May 11, 2010]
[3] Liveline project, Available: http://www.liveline-project.eu [Accessed: May 11, 2010]
[4] Maya Gadzheva, *Privacy concerns pertaining to location-based services, Int. J. Intercultural Information Management*, Vol. 1, No.1, pp.49-57, 2007.
[5] Jason Hong, Gaetano Borriello, James Landay, David McDonald, Bill Schilit, and Doug Tygar, *Privacy and Security in the Location-enhanced World Wide Web*, Seattle, WA. October 2003.
[6] Bill Schilit, Jason Hong, and Marco Gruteser, *Wireless Location Privacy Protection*, vol. 36, no. 12, Computer, pp. 135-137, December 2003.
[7] Agusti Solanas, Josep Domingo-Ferrer, and Antoni Martínez-Bassesté, *Location Privacy in Location-Based Services: Beyond TTP-based Schemes*, October 2008
[8] Louise Barkhuus, *Privacy in Location-Based Services, Concerns vs. Coolness*, Workshop paper in Mobile HCI 2004 workshop: Location System Privacy and Control, Glasgow, UK, September 2004
[9] *Common Criteria for Information Technology Security Evaluation*, V3.1, July 2009
[10] BSI, *The PP/ST Guide*, V1, *August 2007*
[11] MICIE project, Available: http://www.micie.eu/ [Accessed May 11, 2010]
[12] European Seal, Available: https://www.european-privacy-seal.eu/ [Accessed: May 11, 2010]