TRUST-BASED MODEL FOR PRIVACY CONTROL IN CONTEXT-AWARE SYSTEMS

Waleed Wagealla, Sotirios Terzis and Colin English

The Smartlab research group
Department of Computer and Information Sciences
University of Strathclyde, Glasgow, Scotland.
waleed.wagealla@cis.strath.ac.uk

Abstract. In context-aware systems, there is a high demand on providing privacy solutions to users when they are interacting and exchanging personal information. Privacy in this context encompasses reasoning about trust and risk involved in interactions between users. Trust, therefore, controls the amount of information that can be revealed, and risk analysis allows us to evaluate the expected benefit that would motivate users to participate in these interactions. In this paper, we propose a trust-based model for privacy control in context-aware systems based on incorporating trust and risk. Through this approach, it is clear how to reason about trust and risk in designing and implementing context-aware systems that provide mechanisms to protect users' privacy. Our approach also includes experiential learning mechanisms from past observations in reaching better decisions in future interactions. The outlined model in this paper serves as an attempt to solve the concerns of privacy control in context-aware systems. To validate this model, we are currently applying it on a context-aware system that tracks users' location. We hope to report on the performance evaluation and the experience of implementation in the near future.

1. Introduction

Recent advances in networking, handheld computing and sensor technologies have led to the emergence of context-aware systems. This new technology makes it possible to collect assorted contextual sensing information, such as computing context, user context, and physical context [1]. In this paper, a narrow definition of context information is used, referring only to location information. In location-aware systems, sensors are usually allocated in various places to facilitate the collection of users' location information in as accurate a manner as possible. The sensed data is processed by the context information servers (CIS), and then disseminated to users on demand.

1.2 Motivation

The vast amounts of personal information collected by such systems has led to growing concerns about the privacy of their users. Users concerned about their private information are likely to refuse participation in such systems because they prefer not to be tracked by anyone at anytime. The way location information is exchanged between users classifies them as either *information owners*, those who are tracked, or *information receivers*, those who would like to use the sensed location information.

Privacy control, as the term states, encompasses the notion of privacy and the notion of control. A good privacy solution should combine these two notions.

According to Alan Westin [2] “privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information is communicated to others”. Privacy on it is own is about protecting users’ personal information. On the other hand, control is about justification of privacy and plays a role in the management of privacy [3].

In the location-aware systems we consider, *information owners* are willing to disclose personal location information if this disclosure is potentially beneficial. Therefore, it is quite clear that location-aware systems raise an important concern about users’ privacy. Accordingly, for any location-aware system to be acceptable to the users, mechanisms for controlling access to personal information are desirable system features. This implies that the acceptance of any location-aware system depends on the provision of mechanisms for fine-grained control of the disclosure of personal information incorporating an explicit notion of benefit.

The position we take in this paper is that trust could be exploited to protect users’ privacy, in the sense that reasoning about the trustworthiness of *information receiver*s allows us to decide the amount of information that can be disclosed to them. The general rule regarding users’ trustworthiness is that trusted users tend to behaviour in a positive manner, whereas distrusted users tend to behaviour negatively. This use of trust to estimate future behaviour mandates the need for incorporating an explicit notion of risk. Reasoning about the risk involved in interactions between users allows us to adjust the amount of disclosed information according to the expected benefit from providing the information. For example, information could only be revealed to trustworthy users, i.e. users that are expected to provide significant benefits to the *information owner*. Furthermore, our model supports learning from past interactions. We observe the outcomes of each interaction and we change our opinion of the *information receiver*’s trustworthiness to reflect our observations.

The structure of this paper is as follows; section 2 describes the trust-based model for privacy control in location-aware systems. Conclusions and further work are discussed in section 3.

2. The Trust-based Model

The aim of the trust-based model is to provide solution that would help developers to address the issues regarding privacy concerns in general and how to control privacy in particular. The model outlined below are set out to address the question of how to supply users with ability to have the control over their contextual information and who may gain access to it.

2.1 Risk Evaluation

In attempting to deal with risk in location-aware systems, one must first identify the nature and impact of risk in disclosing personal information. The nature of the risks can be represented by determining the possible outcomes of the specific interaction. The risks that stem from the disclosure of personal information in location-aware systems are centred on privacy violations, such as propagating information to a third party without permission. The risk of an outcome is a function of its likelihood and its impact in terms of cost or benefit.

Risk analysis allows users to develop an understanding of risk for the specific situation. An interaction involving risk can be seen as one in which a probability distribution for cost/benefit of outcomes can be made dependent on subjective parameters. Such parameters indicate, for example, the direct sensitivity of personal information. After identifying the set of possible outcomes involved, it is important to estimate the possible costs and benefits (speculative risk) of each outcomes of the disclosure of personal information. This must include direct, indirect costs and benefits. The subjective costs/benefits for each outcome, as determined by the *information owner*, can be represented cost-probability density function (cost-pdf). The parameters of the interaction determine the exact nature of the cost-pdf. This can therefore be viewed as one cost-pdf parameterised by the interaction parameters, or as a set of cost-pdfs, one of which is selected based on the interaction parameters. The chosen cost-pdf reflects the probabilities of specific costs of these outcomes occurring. In other words, the cost-pdf gives an indication of the specific users' profile and their expected behaviour (i.e. how the user is likely to exploit the disclosed information).

It is necessary to provide a means of determining the probabilities that occur in the chosen pdf. For this purpose, the trustworthiness of the *information receiver* can be used, i.e. knowing the trustworthiness of users enables full assessment of risk.

2.2 Trust Representation

Trust is inherently linked to risk; there is no reason to trust if there is no risk involved. This relationship is defined such that low trust implies higher risk and means cooperation is less likely to occur unless the benefits of disclosing location information are worth the risk.

The first step in structuring a representation of trust for the potentially interacting users is to specify a range of values for users' trustworthiness (trust values). In large location-aware systems there is a possibility of not knowing all of the users and as such, the range should address this possibility by including a trust value for unknown users. In principle, this range of trust values will be a totally ordered set. It is then possible to assign values from this set to other users, assigning the upper element of the range to known users of maximum trustworthiness and allocating minimally trusted users the lower element for the range.

The inclusion of the notion of risk implies uncertainty because it considers situations in which we cannot be certain of the outcome (the whole risk analysis based on probability theory). This relationship between risk and uncertainty poses the need for representing the latter within the representation of trustworthiness. This should be considered as a second step after constructing the basic range of trust values. The manner in which we cater for uncertainty is to allow the specification of an interval on the ordered set of trust values, within which one can be confident that the exact trust value of a user lies. In this way, trustworthiness of users can be viewed as a hierarchy, the root of which is the interval containing all possible trust values, and hence representing full uncertainty in trustworthiness. Further up the hierarchy are smaller intervals, which represents a decrease in uncertainty of trustworthiness and as such an increase in the precision of the opinion. Following this technique, we are able to represent the notion of uncertainty. If a user is completely unknown to us, we are now able to represent this uncertainty by

allocating the full interval of trust values, thus differentiating unknown users from those that are not trusted or even distrusted.

2.3 Privacy Management Policy

After the explicit reasoning about risk and trust, it is clear that the users will be able to set out the rules by which they can specify their privacy management policy. In privacy management policy, users can articulate their preferences (risk thresholds, in terms of the maximum cost they can accept) for the possible outcomes of interactions. Allowing *information owners* to specify their own privacy policy is very important because users have significantly different attitudes towards privacy.

The decisions regarding the disclosure of personal information could be reach under the light of what are the access rights that are specified in the privacy policy. Therefore, the decisions that can be reached are:

- Yes, reveal the location information to the *information receiver*.
- No.
- Ask for more information, i.e. asking about the purpose of requesting the location information.

2.4 Adjustment of the Privacy Management Policy

The most important step after observing number of interactions is to clear the fog of uncertainty by learning from past experiences. The accumulated evidence, from past experiences, appears to provide more information that we might learn from it in both risk evaluation and trust evolution. As mentioned above, risk analysis is based on probability distribution since we are uncertain about the likelihood of the outcomes. There is a possibility of reaching a precise risk analysis when the accumulated evidence aids us in predicting certain behaviours of the interacting users. Accordingly, observations help in adjusting the privacy management policy (i.e. having direct mapping between cost-pdf and users' trustworthiness).

3. Conclusion and Further work

The purpose of this paper is twofold. On the one hand, is to give an insight view about privacy concerns in location-aware systems and, on the other hand, to propose a new model in addressing the privacy concerns for them.

The issue of privacy concerns in ubiquitous computing in general attracts number of researchers. The angles from which they tackled these concerns are totally different [4,5,6] from ours, to the best of our knowledge.

The conclusion to draw from our ongoing work is that privacy of context information depends on the level of trust between the parties involved (*information owner* and *information receiver*) and the benefits to the individual in revealing information.

We are currently applying the outlined model in a smart space scenario. The scenario looks at a university department equipped with a context information server, which tracks the location of users and can provide location information on demand. The access to the location information is controlled by the tracked user's privacy policy (*information owner*), which is expressed in terms of the

trustworthiness of the requesting users (*information receivers*). The primary investigations of our model to this scenario were promising and we hope to report on this work and performance evaluation in the near future.

References

[1] Bill Schilit, Norman Adams, and Roy Want. Context-aware computing applications. In Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pages 85-90, Santa Cruz, California, December 1994. IEEE Computer Society Press.

[2] Alan F. Westin. Privacy and Freedom. Publisher: Bodley Head.

[3] Tavani, H.T.: 1999, "Informational Privacy, Data Mining, and the Internet." Ethics and Information Technology, vol. 1, 2.

[4] Xiaodong Jiang and JA Landay. Modelling privacy control in context-aware systems. IEEE Pervasive Computing, 1, 3, pp. 59-63, 2002.

[5] Moamo Wu and Adrian Friday. Interacting privacy enhancing services in ubiquitous computing environments. Ubicomp2002, Security Workshop, 2002.

[6] Marc Langheinrich. Privacy by design--principles of privacy-aware ubiquitous systems. In Proceedings of UbiComp 2001: International Conference on Ubiquitous Computing, volume 2201 of Lecture Notes in Computer Science, pages 273 291. Springer-Verlag, 2001.