Enabling Privacy Management in Ubiquitous Computing Environments through Trust and Reputation Systems

Jeremy Goecks and Elizabeth Mynatt
GVU Center
College of Computing, Georgia Tech
Atlanta, GA 30332
+1 404 385 1102
{jeremy, mynatt}@cc.gatech.edu

INTRODUCTION

Privacy is a vital and urgent social issue confronting Ubiquitous Computing today. Ubiquitous Computing bicomp) promises a world where computational artifacts embedded in the environment will continuously sense our activities and provide services based on what is sensed [16]. However, such a world presents significant privacy dilemmas [2][9]; for instance, these embedded artifacts may collect data about users and store or share this data without the user's consent. If not addressed, these dilemmas have the potential to turn the utopian vision of Ubicomp into a world where Big Brother is always watching and personal privacy is nonexistent.

We believe that the concepts of trust and reputation are pivotal to understanding privacy and building systems that enable users to effectively manage privacy. Trust and reputation are intimately entwined with privacy in everyday life. The more an individual trusts another person, the more personal information she will likely share with that person and the less privacy she will maintain with that person. Similarly, the better reputation a person has, the more likely and individual will be to trust the person and share personal information with the person. Thus, the connection between trust, reputation, and privacy is clear: people use trust and reputation to manage their privacy.

This connection has inspired us to consider how we might utilize concepts of trust and reputation to enable users to manage their privacy in a Ubicomp environment. We have developed an approach that utilizes trust networks and a reputation system [12] to help users manage how, when, and where they share their personal information. We are integrating this approach with the Augur system, a next-generation group calendaring system that supports informal collaboration [14].

TRUST AND REPUTATION

Sociologists and political scientists have long known that trust is critical for any society to exist [11]. Trust – and its counterpart distrust – profoundly influence many everyday interactions; in particular, the importance of trust cannot be overstated as it relates to and influences interpersonal interactions. We ask people that we trust for information, we collaborate with people that we trust, and we confide in people that we trust.

Despite the fact that trust pervades society, it is difficult to define [11]. For our purposes, we choose to define trust as follows: *An individual's trust is the degree of belief that, for a particular situation, an entity (an individual or a system) has the capacity to harm the individual but is not expected to exercise this capacity*. In other words, if Sarah trusts Adam, Sarah will put herself in a situation where Adam could injure her but is not expected to so. This definition of trust is similar to that in [1] and [7].

Using this definition of trust, we define the concept of reputation: *An entity's reputation is some notion or report of its propensity to fulfill the trust placed in it (during a particular situation); its reputation is created through feedback from individuals who have previously interacted with the entity*. Reputations hold entities accountable for their actions and deter bad behavior by the entity. If an entity consistently violates individuals' trust and gains a reputation for doing so, people are less likely to interact with the entity in the future. Conversely, entities that engage in good behavior build a positive reputation and people will continue to interact with it.

In the physical world, reputations are built either through word-of-mouth or by institutions such as the Better Business Bureau (BBB) [3]. On the Internet, reputation systems have become a popular tool for maintaining reputations in an online community. Reputation systems [12] maintain a history of behavior for individuals in the community. After two individuals interact with each other, each one can submit feedback about the other's behavior to the system; any user can view the feedback submitted about any individual in the system. An individual's accumulated feedback is his reputation. A reputation system may indicate whether a seller at an online auction site accurately describes and delivers advertised goods; alternatively, a reputations system for an online community may denote which community members are most knowledgeable. Perhaps the most famous reputation system is eBay's Feedback Forum [6].

Trust Networks and a Personalized Reputation System

Upon comparing reputations built via word-of-mouth and the reputations created by reputation systems, we found that these two types of reputation were quite different. Word-of-mouth reputations generally consist of only a few data points but are highly valued; reputations generated by reputation systems are based on hundreds or thousands of data points yet they are only valued to a certain degree. For instance, if I need to find a good car mechanic, I will likely ask a few friends to recommend a mechanic. Very often, I will choose a mechanic that my friends recommended, and I will be confident of my choice. Conversely, studies of user behavior on online auction sites suggest that while reputation does impact the auction price a seller can obtain, the impact is somewhat minimal [13].

At first, this analysis appears to be quite paradoxical. Word-of-mouth reputations are highly valued despite the fact they often have few data points, while reputations obtained from reputation systems are only somewhat valued despite the large number of data points that comprise the reputation. What phenomena account for this paradox? The simple answer is that word-of-mouth reputations are generally created based on information from known and presumably reliable sources (e.g. friends in the above example), while the reputations obtained from reputation systems is based on information from strangers. The complex answer led us to develop the concept of trust networks and a personalized reputation system – and towards new methods for managing privacy in a Ubicomp environment.

Trust Networks

The critical difference between word-of-mouth reputations and reputations maintained by reputation systems is the quality of the data points that comprise the reputations. Data points in word-of-mouth reputations are highly reliable because they come from people that the user knows and judges as reliable; in contrast, data points in a reputation system most often come from people that user doesn't know and cannot ascertain is reliable.

In fact, word-of-mouth reputations are built via social networks. Within a community, people form standing relationships with the community members that they interact with on a regular basis. A social network is the interconnected structure that these standing relationships create among the community members; an individual's social network is a network with the individual at the center [15]. Social networks, then, provide the communication channels (the standing relationships) for experiences with an entity to be shared among the community, and these shared experiences are the data points for word-of-mouth reputations.

Although trust is an acknowledged facet of social networks, we are not aware of any work that has focused on trust in particular. However, in order to understand why word-of-mouth reputations are better than reputations maintained by reputation systems, it is necessary to consider trust within a social network. Our definition of trust states that trust is dependent on the situational context. Consider the example discussed above: an individual wants to find a good car mechanic. In this instance, the individual utilized people in his social network – his friends – to find a reputable mechanic. However, an individual almost certainly does not trust all his friends equally in this situation; some friends are likely less knowledgeable about mechanics, and others may not own a car.

An individual's social network, then, morphs to reflect the trust that the individual has in each member of his network for this situation. We define this derived network to be a trust network: *a trust network is the network derived from an individual's social network that represents the degree of trust the individual has in the members of his network for a particular situation.*

Trust networks are the key to understanding why word-of-mouth reputations are so highly valued. Word-of-mouth reputations are built through trust networks; individuals use trust networks to accurately obtain reputations by asking those people they trust most in a particular instance about the reputation of an entity. By virtue of the fact that an individual trusts a group of people, the reputation offered by the group is very highly valued.

A Personalized Reputation System

As described above, the reason that reputations generated by reputation systems are not highly valued is that users cannot assess the trustworthiness of those people providing an entity's reputation, and this makes it difficult to evaluate the entity's reputation. We can solve this problem by employing a user's trust network to personalize a reputation system's data for the user. We are developing a system that implements this solution; and we have named this novel system a Personalized Reputation System (PRS).

Reputation systems weigh all reputation data about an entity equally when creating the entity's composite reputation. In contrast, a PRS weighs an entity's reputation data based on the user's trust network; the data of those people that a user trusts will contribute more to entity's reputation that data from people that the user doesn't trust. Hence, an entity's reputation in a PRS is shaped more by the people that a user trusts and less (or not at all) by people that she doesn't trust. Observe that a PRS builds reputations the same way that word-of-mouth builds reputations: via feedback from people that the user trusts.

Consider a simple, qualitative example. Imagine that a user trusts person A and person B, but doesn't know nor trust person C or person D. Now assume that all four individuals have provided feedback about an entity; persons A and B provided positive feedback, but persons C and D provided negative feedback. In a normal reputation system, the entity's reputation would be neutral and the user wouldn't be able to determine whether to trust the entity. However, a PRS would generate a positive reputation for the entity by weighing the feedback of persons A and B more heavily than the feedback of persons C and D. In the next section we discuss a system that enables users to manage their personal information in a Ubicomp environment using trust networks and a PRS.

MANAGING PRIVACY IN UBICOMP ENVIRONMENTS

One common definition of privacy is the control of personal information [17]. The goal of our approach is to empower users with this type of privacy. Personal information may take on many forms in a Ubicomp environment. For example, media spaces [8] use audio and video recording devices to capture and share what a user says or is doing. Alternatively, some Ubicomp applications identify and share a user's location [5].

Our approach utilizes trust networks and a PRS to provide a simple and intuitive method for users to manage their personal information in a Ubicomp environment. We introduce our approach by discussing its application in a particular Ubicomp system. Augur is a next-generation group-calendaring system that employs calendars as sensors [14]. Augur uses artificial intelligence methods to predict how likely a user is to attend events that he has scheduled on his calendar; the user's colleagues can utilize this information to identify where the user is likely to be during the day. Workers can use the information that Augur provides to find colleagues and engage in short, information conversations just before or after events. Of course, numerous privacy concerns arise from the data that Augur provides. A user may want to limit who can view his predicted attendance at events or she may want to limit who can view his calendar at all.

We are building an interface for Augur that enables users to specify a list of people that she trusts. When she adds a person to her list, she also specifies the degree of trust she has in the person. We have mapped degrees of trust to the type of calendar information that Augur shares so that users can clearly understand the implications of trusting another person. There are currently three levels of trust and one level of distrust (Table 1). If a user distrusts a person, then the system doesn't share any of the user's calendar information with the user. When the person requests the user's calendar data, Augur will show only the information that the user has indicated is acceptable to show. Of course by referring to groups of people (e.g. names in a group email alias), the user could minimize the overhead of entering trust levels for numerous individuals.

Table 1. Mappings from degree of trust to shared personal information in Augur system.

Degree of Trust	Shared Personal Information
very much	calendaring events and predictions
Somewhat	calendaring events only
Little	free/busy blocks
Distrust	none

These trust listings are not sufficient for managing the flow of personal information in Augur. There will be instances in which a person who is not in the user's trust network requests the user's information. In these instances, the user must decide how much information to share with this person, and the person's reputation can help the user make this determination. We are building a PRS into Augur that will enable users to obtain the reputation of an individual.

The data for Augur's PRS is stored in personal trust networks. If an individual is in a user's personal trust network, this entry speaks to the reputation of an individual in the eyes of the user. Thus, we can mine personal trust networks to obtain a reputation for an individual. When an individual requests information about a user, we create a reputation using the following process:

1. Build a personal trust network for the user. This operation requires two steps:
    a. Connect the user to the individuals on his trust list.
    b. For each individual on the user's list, connect the individual to the people on the individual's trust list.

    The resulting trust network (Figure 1, next page) places the user at the center and extends out two relationships: user – those he trusts – those they trust.
2. Infer the individual's reputation by examining this network and determining who in the network trusts the individual and how much they trust the individual. We are still developing the algorithm that will compute an individual's reputation based on this network.

Consider a simple example. Steve, Quan, and Jeremy are in Amy's personal trust network and they are each trusted 'very much.' Kris is not in Amy's trust network, but she is in Steve's, Quan's and Jeremy's trust network. If Kris requests information about Amy, the PRS can compute Kris's reputation by considering how much Steve, Quan, and Jeremy trust Kris. If they all trust Kris very much, then Kris's reputation will be very good.

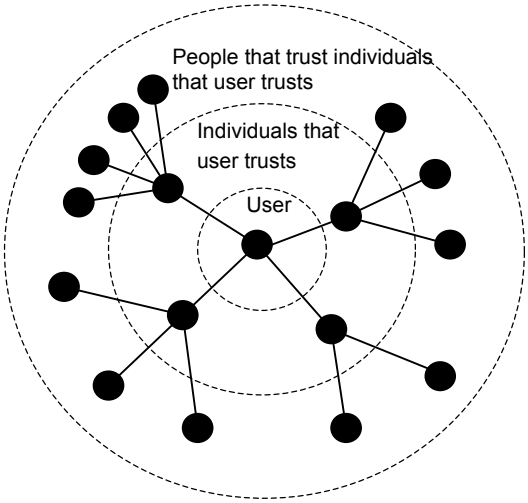

Figure 1. A simple personal trust network.

Using trust networks and a PRS to help users manage personal information flow in an Ubicomp environment offers many advantages to the user. We believe that two advantages are especially compelling: adaptivity and flexibility. Privacy is a dynamic metric that changes over time, and a privacy management system should support such changes. Trust networks and reputation systems are fluid entities that naturally evolve to reflect current levels of trust and reputation; hence, by using these tools, our approach naturally adapts to the current privacy trends of users.

Our approach provides significant flexibility to the user by enabling her to specify an information sharing policy on a per-entity basis. The current privacy specification, P3P [4] and Langheinrich's Privacy Awareness System [10], the only Ubicomp privacy management system that we know of, both assume that the user maintains only one privacy policy and this policy is applicable to all entities. Providing the user with the flexibility to create entity-specific privacy policies is critical because users often want to share significant personal information with one entity (e.g. a family member) but less information with another entity (e.g. a coworker).

REFERENCES

1. Abdul-Rahman, A. and Hailes, S. Supporting Trust in Virtual Communities. Hawaii Int'l. Conf. System Sciences 33, 2000, Maui, HI.
2. Bellotti, V. and Sellen, A. Design for Privacy in Ubiquitous Computing Environments. Proceedings of ECSCW '93, Milan, Italy, p. 77-92.
3. Better Business Bureau website: http://www.bbb.org
4. Candor, L., Langheinrich, M., Marchiori, M., and Reagle, J. The platform for privacy preferences 1.0 (P3P1.0) specification. W3C Recommendation, HTML Version at http://www.w3.org/TR/P3P/, April 2002.
5. Dey, A., Futakawa, M., Salber, D., and Abowd, G. The Conference Assistant: Combining Context-Awareness with Wearable Computing. Proceedings of the 3rd International Symposium on Wearable Computers, San Francisco, CA, 1999. p. 21-28.
6. The Feedback Forum, eBay. http://pages.ebay.com/services/forum/feedback.html
7. Friedman, B, Kahn, P Jr., and Howe, D. Trust Online. *Communications of the ACM*, 43(12):34-40, 2000.
8. Harrison, S., Bly, S., Anderson, S., and Minneman, S. The Media Space In K.E. Finn, A. J. Sellen, and S.B. Wilbur (eds.) *Video-Mediated Communication.* Lawrence Erlbaum Associates, NJ, 1993, p. 273-300.
9. Langheinrich, M. Privacy by Design – Principles of Privacy Aware Ubiquitous Systems. Proceedings of Ubicomp 2001, Atlanta, GA, p. 273-291.
10. Langheinrich, M. A Privacy Awareness System for Ubiquitous Computing Environments. *To Appear in* Proceedings of Ubicomp 2002, September 2002.
11. Misztal, B. *Trust in Modern Societies*. Polity Press, Cambridge, MA, 1996.
12. Resnick, P., Zeckhauser, R., Friedman, E., and Kuwabara, K. Reputation Systems. *Communications of the ACM*, 43(12):45-48, 2000.
13. Resnick, P., Zeckhauser, R.,, Swanson, J, Lockwood, K. The Value of Reputation on eBay: A Controlled Experiement. *Working Paper*. http://www.si.umich.edu/~presnick/papers/postcards/
14. Tullio, J., Goecks, J., Mynatt, E., and Nguyen, D. Augmenting Shared Personal Calendars. *To Appear in* Proceedings of UIST 2000, October 2002.
15. Wellman, Barry and S.D. Berkowitz (eds.) *Social structures: A network approach* Cambridge University Press, Cambridge, MA, 1988.
16. Weiser, M. The Computer for the Twenty-first Century. *Scientific American, 265, 3* (September 1991), p. 94-104.
17. Westin, Alan, *PRIVACY AND FREEDOM*. Atheneum Press, NY, 1967.