Privacy Enhancing Factors in People-Nearby Applications

Sehrish Malik and Jong-Hyouk Lee*
Sangmyung University, Cheonan, Republic of Korea
{serry, jonghyouk}@pel.smuc.ac.kr

Abstract

People-Nearby Applications (PNAs) are becoming popular day by day. People try to find new ways for increasing their social circle according to their interests. PNAs provide people with a best way to find new people within one's physical vicinity by applying activities and interests filters. A large number of people using PNAs complain about privacy issues and fake users. Another big concern of people is the trustworthiness of a person they are going to meet, i.e., whether the person is a good person to meet or can be harmful. In this paper, we target to address a few privacy issues by proposing a four step approach to keep permissions limited so that everyone using PNA can enjoy the experience without having to care about privacy issues and other threats.

Keywords: People-Nearby Applications, Physical vicinity, Privacy, Trust

1 Introduction

Expanding and strengthening social relations is considered important in every age. People-Nearby Applications (PNAs) like other social networking sites are type of virtual communities which are growing with the passage of time. On such sites millions of users create online profiles and share their personal information with extensive networks of people who are often strangers. People are becoming more concerned about privacy now. People seem to appreciate sites which fulfil privacy needs of every type of users. Most of the social networking sites provide many privacy options and different ways to communicate to cover people of all types. PNAs on the other hand have been following a particular set of rules which is a problem to many people. There are huge number of people who want to meet new people but also want to have different privacy options and trust insurance factors at the same time.

Privacy is personal information of a person and it is also the right of a person to disseminate this information according to his will (1). Trust is blindly putting your best expectations in another person and allowing him to make decisions or actions on your behalf which will influence you on personal level. Trust is defined as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster, irrespective of the ability to monitor or control that other party. One of the major factors of meeting someone face to face and sharing personal information is trust. Trust is a foundation for successful online interactions (2).

Relation between a person and social networking sites is two facade. At times we want to reveal our personal information to only our closely related people and not to strangers and at times we feel free to reveal our personal information to strangers but want to hide it from people who know us better (3). This dual human nature demands all type of privacy options. The fact that often we are willing to share our personal information to completely strangers eventually brings out the trust issue. In dealing with dating sites or PNAs more than 80 percent of people feel the need of some trust mechanisms and use their own ways to find trust factors (4). In this paper, we present a new methodology for PNAs to make it easy for users to know who they should trust or not. The proposed methodology consists of five steps — ping

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 2, pp. 113-121
*Corresponding author: Protocol Engineering Lab., Sangmyung University, Cheonan, Hannuri Building 708, Dept. of CSE, Sangmyung University, Cheonan, 330-720, Republic of Korea, Tel: +82-(0)41-550-5487

messages, trust measure, have met measure, reported/blocked measure, and recommendations — that enhance privacy and trust in PNAs.

The rest of this paper is organized as follows: Section 2 presents related work. In Section 3, we present the proposed methodology for privacy in PNAs. Section 4 shows analysis results and we conclude this paper in Section 5.

2 Related Work

2.1 Previous Work

Privacy is always an issue in social networking sites where people have information to share or hide and have to make decisions about it. Some past work such as (5), (6) and (7) has found that privacy is an obstacle to the acceptance of location sharing applications. Different factors are likely to drive information revelation in online social networks. Since creating an online relation with someone is very risky especially when it comes to strangers whom you have never met before. While privacy may be at risk in social networking sites, information is still willingly provided. Many people despite of all the suspected risks still experiment with such services to find out more about them and gain something useful out of them. But many bad cases such as sexual assaults on Skout (8) make people worry about trust and privacy.

Another study on location presents a series of insights relating to location-sharing practices. It highlights the use of third person scenarios as a useful method for eliciting privacy concerns and potentially educating users. Application which provide combination of virtual and physical interactions to users, all the risks regarding abusive language and trust are enlarged and are combined with more factors like online privacy risks (9).

Study in (10) shows that what users are willing to disclose their location to social relations. The most important factors found by authors are who was requesting, why the requester wanted the participant's location, and what level of detail would be most useful to the requester. After determining these, participants were typically willing to disclose either the most useful detail or nothing about their location.

In (11) and (12) authors have shown how information sharing matters when being shared to some closely related people like friends or family or a desired group. How it can be useful or can be turned into a complete joy. Whereas (13) has given a detail study on which features of interpersonal relationships influence sharing. They show that self-reported closeness is the strongest indicator of willing to share and also individuals are more likely to share when they find common behaviors.

The research work done in (14) describes how a user using PNA navigates between risk and opportunity. It provides a qualitative analysis of usage patterns of PNAs. Further role of locality in the user experience is studied along with the dynamics of privacy.

2.2 People-Nearby Applications

PNAs as defined by (4) are mobile systems that allow users to discover new people using geographical proximity search and online communication. A PNA searches for the users based on their location. Each user has own profile to show information and interest and users can communicate with each other. Some commonly used PNAs are Badoo, Banjo, Blendr, Circle, Highlight, Grindr, SayHi and Skout. These all are social networks to meet new people, make friends, find friends nearby helping to learn more about people. Circle and Skout do not have any location visibility control. Banjo gives location blocking option and Grindr gives hiding user distance option. Banjo, Circle and Highlight have a Facebook login option.

3 Proposed Methodology

Normally in PNAs location, profile information, and message option are open to all users. We propose the five steps which enhance privacy and trust.

1. Ping messages
2. Trust measure
3. Have met measure
4. Reported/Blocked measure
5. Recommendations

A user can keep its location, profile, and messages open for any level he/she wants but in a normal case exact location will be after chat is opened or in some cases after trust is added if the user wants.

3.1 Ping message

An unknown user can only ping another user. If the user gets a response back only, chat is allowed; else not. Figure 1 shows a user X sends the ping message to another user Y. When a user X receives a response of ping from user Y then chat is opened between X and Y.

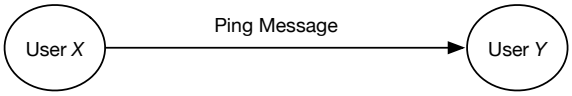

Figure 1: Ping Message

3.2 Trust measure

Trust can be one sided or mutual. A user can associate full trust to another while other might associate partial or no trust to it. Figure 2 shows an example of the trust graph of a user V.

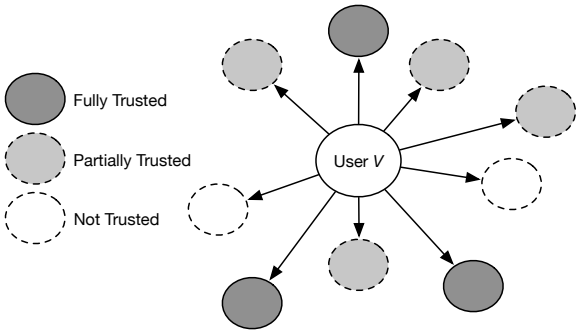

Figure 2: Trust Graph

3.3 Have met measure

Have Met is the check by which users help each other to increase their credibility. The more people a user has personally met, the more authentic the user is considered. Have Met check will be done after mutual consent as shown in Figure 3.

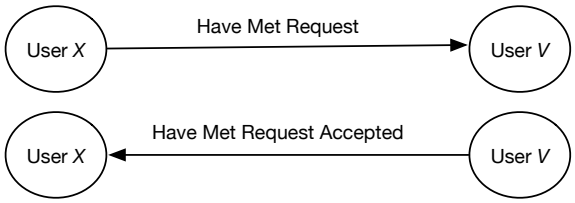

Figure 3: Have Met messages

3.4 Blocked measure

If a person X is approached by a person Y which has been reported or blocked ever by any of the trusted friends of X then X will be informed about the event. If Y does not fall in the threshold value of being trustworthy then also its status will be notified to all others it tries to makes contact with. Ratio in Eq. (1) will be used to judge the trustworthiness of a user i.e. if a person X is blocked in more than 10% of his interactions then X is not trustworthy enough.

$$\frac{\text{No. of times that } X \text{ is blocked}}{\text{No. of times that } X \text{ opened chat}} >= 0.1 \tag{1}$$

3.5 Recommendations

Recommendations of a node V are done on basis of how much it wins other people's trust. Recommendations are forwarded to links of only those who trust V and themselves are also equivalently trusted among their links. Recommendations are not forwarded to those who are one sided trusted by V but do not trust V in response shown in Figure 4.

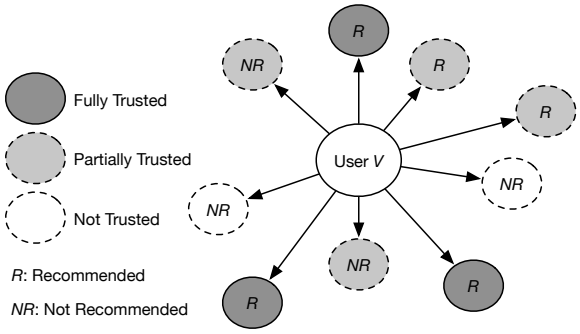

Figure 4: Recommendations Graph

Following formulae are used for recommendations. Recommendations to trust will be forwarded to links of those who strongly trust X in Eq. (2), recommendations to trust will be forwarded to links of

those who strongly trust X and also those weekly trust in Eq. (3), and recommendations to trust will be forwarded to all in user's proximity with matching interests in Eq. (4).

$$\frac{\text{No. of times that } X \text{ is trusted}}{\text{No. of times that } X \text{ opened chat}} >= 0.5 \tag{2}$$

$$\frac{\text{No. of times that } X \text{ is trusted}}{\text{No. of times that } X \text{ opened chat}} >= 0.67 \tag{3}$$

$$\frac{\text{No. of times that } X \text{ is trusted}}{\text{No. of times that } X \text{ opened chat}} >= 0.85 \tag{4}$$

Attributes of a person X will contain the number of people that X is fully trusted by, the number of people that X is partially trusted by, the number of people that X has met personally, the number of people X is blocked or reported by, and the number of people X has opened the chat with.

4 Performance Analysis

Among people using PNAs or any dating apps of similar kind, more number of female members report that they have encountered offensive or abusive language at least once, whereas male members experience it very less as compared to female. According to (15), 80% people do deceptive self-presentation to some scale at such sites. From a survey done in (4), 57% of female users report experiencing verbal violence whereas about 20% male users report verbal violence. Overall 52% people report doubting other person's motives and integrity. Those are summarized in Figure 5.

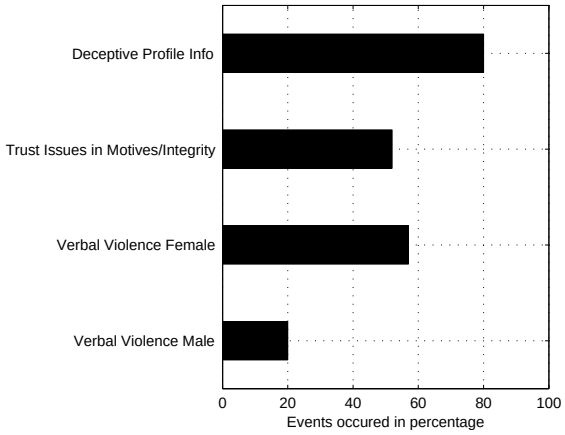

Figure 5: Percentages of threats encountered

4.1 Simulation Setup

In order to perform experiments of proposed methodology some assumptions are made and an event-driven simulation considering the time period of one year is done. A person with intention to use abusive language would not be able to open the chat in α of times. Assuming that despite of all the authenticity measures β of the fake profile users manage to have impressive profile measures. Here we set values of α and β from the range 10-90% to see effect of user behaviour at different scenarios.

Let π be the number of persons who intend to use abusive language, ϖ be the umber of persons projecting fake profiles and ρ be the number of persons trying to meet someone in person with harmful intentions. We assume that every 6 hours π persons use abusive language to someone in initial message, every 24 hours ϖ fake profile person try to make contact with someone, and every 48 hours ρ harmful persons try to meet someone. π is randomly chosen from the range 5 to 16, ϖ is randomly chosen from the range 2 to 11, ρ is randomly chosen from the range 1 to 6. The number of times that the chat will be opened for threats is taken randomly from the given range. 10% of times are taken as when warning messages propagation informed users of threat.

With the above assumptions, event-driven simulations were performed for both the ordinary PNA case (where only blocking threat by user on right time probability is considered) and for the proposed approach. Simulations are ran of 100 times and then the average is taken for best results.

4.2 Simulation Results

Three main cases have been considered which are abusive language messages, fake profile dealings, and meet in person threat. The open chat request option will play role in reducing number of abusive language messages. Fake profiles will be easier to recognize since all the factors will help to improve authenticity of a person and be a proof of it. The meet in person threat again will be reduced by profile judgment factors as well as warning messages. The recommendations process will make sure that most trustworthy users are recommended with best effort of minimizing all the threats.

In Figure 6 the difference in abusive language messages is shown. It is quite evident that the proposed approach reduces the number of such messages to half even in worst case.

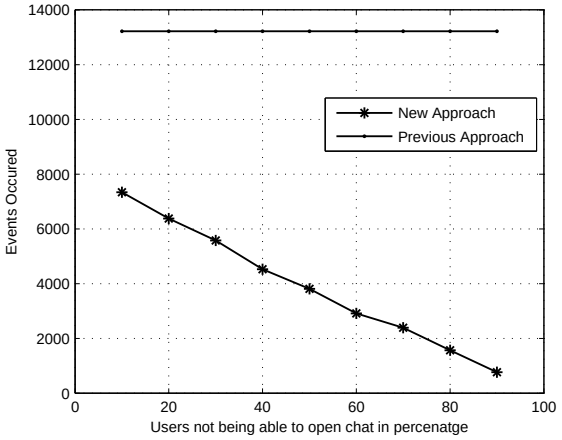

Figure 6: Abusive Language Messages

Figure 7 shows the comparison with respect to fake profile dealings, while Figure 8 shows the comparison of meet in person threats. We can see that fake profiles events are decreased about 40% at least and 95% at maximum, meet in person threats are decreased 77% at least and 99% at maximum in best case. In the same way the recommendation by the proposed methodology will also be 60% more authentic by taking out the probability of 40% fake ones.

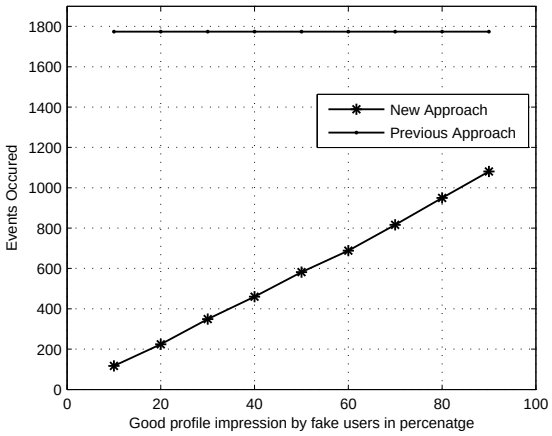

Figure 7: Fake Profile Interactions

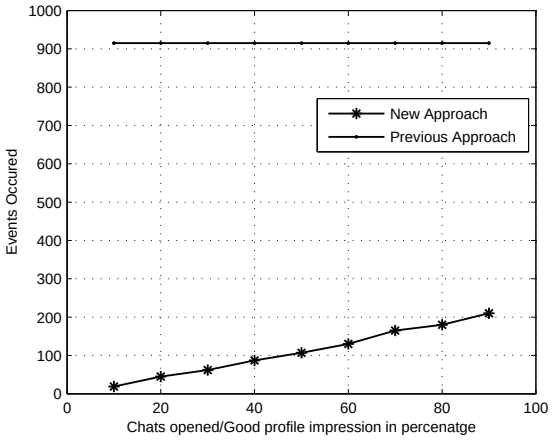

Figure 8: Recommendations Graph

5 Conclusion

In this work, a methodology consisting of five factors has been proposed in order to reduce privacy and trust concerns of users using PNAs. The three tests have shown a great decrease in the threats. Though users always have huge concerns about privacy and giving out their location but at the same time too many changes on privacy are also not welcomed by users. Trust factors might be more welcome by users in comparison to privacy factors. In future further study can be done on the implementation of such a methodology that how well PNA users take inclusion of such privacy and trust factors in PNAs. Research on popular factors among privacy and trust can be done to see which way users are more willing to see the change.

Acknowledgments

This work was supported by a 2014 research grant from Sangmyung University (2014-A000-0287).

References

[1] D. M. Timm and C. J. Duven, "Privacy and social networking sites," *New directions for student services*, vol. 2008, no. 124, pp. 89–101, 2008.

[2] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in *Proc. of the 13th Americas Conference on Information Systems (AMCIS'07), Colorado, USA*, August 2007, p. 339.

[3] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proc. of the Workshop on Privacy in the Electronic Society (WPES'05), Alexandria, USA*. ACM, November 2005, pp. 71–80.

[4] E. Toch and I. Levi, "Locality and privacy in people-nearby applications," in *Proc. of the 15th International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'13), Zurich, Switzerland*. ACM, September 2013, pp. 539–548.

[5] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? privacy preference determinants in ubiquitous computing," in *Proc. of the 21st Conference on Human Factors in Computing Systems (CHI'03), Florida, USA*. ACM, April 2003, pp. 724–725.

[6] S. Patil and A. Kobsa, "Privacy considerations in awareness systems: designing with privacy in mind," in *Awareness Systems*, ser. Human-Computer Interaction Series, P. Markopoulos, B. D. Ruyter, and W. Mackay, Eds. Springer London, June 2009, pp. 187–206.

[7] X. Page, A. Kobsa, and B. P. Knijnenburg, "Don't disturb my circles! boundary preservation is at the center of location-sharing concerns." in *Proc. of the 6th International Conference on Weblogs and Social Media (ICWSM'12), Dublin, Ireland*. AAAI, June 2012.

[8] E. Bradner and G. Mark, "Why distance matters: effects on cooperation, persuasion and deception," in *Proc. of Conference on Computer Supported Cooperative Work (CSCW'02), New Orleans, USA*. ACM, November 2002, pp. 226–235.

[9] D. Wagner, M. Lopez, A. Doria, I. Pavlyshak, V. Kostakos, I. Oakley, and T. Spiliotopoulos, "Hide and seek: location sharing practices with social media," in *Proc. of the 12th international conference on Human computer interaction with mobile devices and services (MobileHCI'10), Lisboa, Portugal*. ACM, September 2010, pp. 55–58.

[10] N. Perlroth, "After rapes involving children, skout, a flirting app, bans minors," *New York Times Blog Post*, 2012.

[11] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations: why, when, & what people want to share," in *Proc. of the 23rd Conference on Human Factors in Computing Systems (CHI'05), Portland, USA*. ACM, April 2005, pp. 81–90.

[12] F. R. Bentley and C. J. Metcalf, "Sharing motion information with close family and friends," in *Proc. of the 25th Conference on Human Factors in Computing Systems (CHI'07), San Jose, USA*. ACM, April 2007, pp. 1361–1370.

[13] L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers, "From awareness to repartee: sharing location within social groups," in *Proc. of the 26th Conference on Human Factors in Computing Systems (CHI'08), Florence, Italy*. ACM, 2008, pp. 497–506.

[14] J. Wiese, P. G. Kelley, L. F. Cranor, L. Dabbish, J. I. Hong, and J. Zimmerman, "Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share," in *Proc. of the 13th International Conference on Ubiquitous Computing (UbiComp'11), Beijing, China*. ACM, September 2011, pp. 197–206.

[15] C. L. Toma, J. T. Hancock, and N. B. Ellison, "Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles," *Personality and Social Psychology Bulletin*, vol. 34, no. 8, pp. 1023–1036, 2008.

Author Biography

Sehrish Malik received her B.S. in Computer Science from National University Of Computer and Emerging Sciences (NUCES-FAST), Pakistan. In September 2014, she moved to Republic of Korea for M.S. studies and started working in the Protocol Engineering Laboratory (PEL). Research interests include privacy, trust, and communication systems.

Jong-Hyouk Lee received the M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea, in 2007 and 2010, respectively. Dr. Lee was a researcher at INRIA, France and was an Assistant Professor at TELECOM Bretagne, France. Since September 2013, he has been with Sangmyung University, Cheonan, Korea. Dr. Lee won the Best Paper Award at the *IEEE WiMob 2012* and was a tutorial speaker at the *IEEE WCNC 2013* and *IEEE VTC 2014 Spring*. He was introduced as the Young Researcher of the Month by the *National Research Foundation of Korea (NRF) Webzine* in November 2014. He is an associate editor of *Wiley Security and Communication Networks*, *Springer Annals of Telecommunications*, and *IEEE TRANSACTIONS ON CONSUMER ELECTRONICS*. Dr. Lee is an IEEE senior member. Research interests include authentication, privacy, and Internet mobility management.