ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

An Automated Consent for Privacy Preservation in Peer to Peer Networks using Agent Technology

K.Govinda
Assistant Professor (SG)
SCSE, VIT University,
Vellore-India,
kgovindha@vit.ac.in

R.Sujatha
Assistant Professor
SITE, VIT University,]
Vellore-India
r.sujatha@vit.ac.in

S.Prasanna*
Assistant Professor (Sr)
SITE, VIT University,
Vellore, India
sprasanna@vit.ac.in

Abstract **:** Privacy is a complex and multi-faceted notion, both from social and legal point of view which is interpreted in different ways among different times, cultures and individual perception. Here in this paper we propose agents based mechanism to make the mobile computing more popular and safer than before in order to give technological advancement to the users. The transaction of personal data over the internet and for other services without any notification to the user is a huge compromise with privacy of the person in concern. The Location Based Services over mobile phones often try to access personal information of the user for their database and thus provide services which are of user's interest. The LBS Server is more prone to attack from unauthorized people and therefore the databases including the personal information about the customers are also equally threatened. This personal data can be easily used to figure out information about the user which he/she does not intend to disclose. Hence implementing a Privacy Agent in order to make Pervasive Computing more safe and secure so that users can easily rely on the mobile phones for any kind of transaction whether financial or personal data.

Keywords**:** privacy agents, pervasive computing, controller agent, auditor agent, data manager.

I. INTRODUCTION

The latest information technologies like pervasive computing in which the privacy of the user is at utter risk as the data regarding the user is used without taking his consent. Privacy is a complex and multi-faceted notion, both from social and legal point of view. Privacy is interpreted in different ways among different times, cultures and individual perception. Despite of strong legal protections, many citizens feel that technologies – especially information technologies – have invaded so many aspects of their lives that they no longer have suitable guarantees about their privacy. This all has lead to two kinds of attitudes, most people think that privacy is the price they have to pay for the new facilities while others people oppose to pay this price in return of inessential services or facilities and compromise one of their fundamental rights.

A reassessment of all the legal documents and necessary papers of the people being send and received should be a multidisciplinary endeavour because privacy can neither be apprehended nor guaranteed by exclusively legal, social or technical approaches, in particular in the context of the fast development of new information technologies [3].

An explicit concern with the subject of the data being dealt with has to be considered as it is a cornerstone most data protection regulations. A personal data may be processed only if the data subject has unambiguously given his consent. And so the controller must provide sufficient information about the data subject to the user, including ''the purposes of the processing for which the data are intended''. But after all this many aspects of new information technologies render privacy protection – and especially informed consent – difficult to put into practice. Data communication over internet is now taking place without any notification to user or to the person to whom so ever this information may concern and this is going to get worse with the invention of technologies in the form of "pervasive computing" and "ambient intelligence"[2]. These expressions refer to environments where individuals are surrounded by small devices with capabilities for collecting and communicating data, computing and reasoning. Such devices include sensors, actuators, mobile phones, communicating personal digital assistants (PDAs), etc. They communicate through various wireless protocols such as Bluetooth, Wi-Fi, WLAN, GPRS, etc. This paper discusses the legal aspects of the privacy issues in such scenarios and proposes to deal with the automated technologies like pervasive computing in automated ways like using the so called privacy agents.

II. ISSUES RELATED TO PRIVACY

The first and the foremost issue we are dealing with are the protection and privacy of the user. The transaction of personal data over the internet and for other services without any notification to the user is a huge compromise with privacy of the person in concern. The Location Based Services over mobile phones often try to access personal information of the user for their database and provide

services which are of user's interest. The LBS Server is more prone to attack from unauthorized people and therefore the databases including the personal information about the customers are also equally prone to the attack [7]. These personal data can be easily used to figure out information about the user which he/she does not intend to disclose.

In order to save the privacy rights from being jeopardized by the highest level of automation provided in the form of pervasive computing a notion called "Privacy Agent" is coined, a dedicated software which would act as a ''surrogate'' of the subject and automatically manage on his behalf his personal data. The role of the Privacy Agent includes the decisions to refuse or accept to disclose personal data of the subject depending on the current context and the information provided by the entity requesting the data.

Further, and more importantly, the issues regarding the deployment of privacy agents are discussed because as the agent is a piece of software its liability in case of failure of any sort and its capabilities need to be discussed both in legal and architectural terms so that proper laws and architecture for deployment be framed. The nature of consent in legal terms has been discussed and the two views i.e. unilateral and contractual. In the contractual view the consent is regarded as an agreement between at least two entities like some contract whereas in the unilateral view consent is regarded completely as an individual's will or freedom to decide whether he wishes to give or share the information or not.

The paper supports the later view of consent and the European data protection laws that are actually being used there are quoted as an argument in support of the unilateral view of consent [2]. The features of consent as per the Directive 95/46/EC have been defined."Freely given" is the feature that ensures that the data or information is being taken from the subject unsolicitly and he is not in a situation of compromise."Specificity" is the feature that at the time of taking consent from the user the boundaries of usage should be clearly defined and the information seeker should strictly adhere to the constraints of data usage or he may be liable to legal action. The "unambiguous and informed" feature says that the subject should readily be informed regarding the methods of processing, third partier's involvement, etc. Even though the above features are well defined and implemental but when using privacy agents there can be exceptional situations like there being a bug in the coding of the privacy agents that causes privacy breach or incorrect privacy parameters being supplied by the subject to his privacy agent. In such situations the consent of the subject becomes null and the subject has to either stop further processing of his data or could ask for compensation from the institution responsible for creating the privacy agent.

Another significant issue is the liability of the Privacy Agent provider in case of undesired disclosure of personal data due to the misbehaviour of a Privacy Agent. Sometimes, unprofessionally Privacy Agent provider may make some amendments in the software in order to disclose the private and personal information about the user to some unauthorized person. Now, this is a liability and has to be taken care of.

Again, enforcing liability involves both legal and technical issues: the scope of the liability must be stated precisely in the software license agreement of the Privacy Agent and this agreement must be complemented by technical measures (such as secure log management) to make it possible to establish liabilities after the facts. Formal semantics can also play an instrumental role to this respect, to help defining and establishing liabilities without ambiguity. The extension of formal methods to the definition of a software liability framework is studied in the multidisciplinary project LISE (Liability Issues in Software Engineering).

III. ARCHITECTURE AND IMPLEMENTATION

The privacy agents have three major parts, the user interface for taking keywords as the input from the user, the sendSms part which is used for sending messages and last part is receives which is used for receiving messages. All three of these parts should be designs so that they are completely in agreement with the features and legal bounding regarding consent defined above. The data manager used in this is solely responsible for the management of consent. It is the responsibility of the data manager to ensure that only the data rendered as disclosable by the subject should be send or received by the user from the mobile or seeker and all other data at all other times should be restrained from disclosure. Before sending any data the data manager should cross check the sharability of the data with the choices entered into the system by the subject through the user interface at an earlier point in time [6]. After receiving messages the data manager should again check the data for the keywords given by the user and prompt the user if the keywords are found so that the keywords should not go unnoticed. In case of any discrepancy the data should be kept as undisclosable and should not be send as per the user desire. In case the nature of information that the controller is seeking is not clear to the privacy agent it should be able to send information seeking messages to the controller so as to get a more accurate perception of the nature of the data that the controller is requesting. Also the data manager can issue a warning if it finds that the controller is requesting for information that the subject has defined as undisclosable.

The user interface is a key component because its usability and flexibility of the user interface that decides the precision with which the subject can define the constraints on information sharing. If the user interface is properly designed there will be very less chance that the privacy agent doesn't totally understand the privacy requirements of the subject and hence provide some information rendered as sensitive by the subject. Also the user interface should be able to warn the subject in case of any divergence of interpretation.

All pervasive computing environments will have three kind privacy agents installed at the three important objects involved in the whole process i.e. the subject ,the controller and the certified authorities that audit the logs created by the agents installed both at the subject's and the controller's end.

Every transaction through mobile communication is carried through a particular port. These ports are designated for specific type of communication such as http communi cation, stream-based socket communication, datagram-based socket communication, serial port communication and file I/O communication. Similarly, for messaging also there is a designated port which carries out all the communication [8].

In J2ME, Connection class is responsible for all kinds of communication, It's extended classes handle the specific communication for example http connection etc.

Actually, once a port is used it can never be referred again for any purpose so under this constraint we have designed a new messaging instance in which an additional technique of scanning the message for the unsharable data is included.

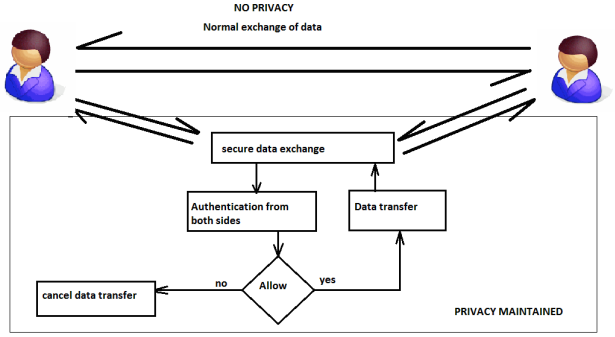

Figure1. Comparison between peer to peer data transfer in the presence of privacy agent and in absence of privacy agents.

Implementation details

Module1 (Subject Agents):

Subject agents: These are installed on the devices that are responsible for the data communication between the subject and the controller like the user's PDA or his mobile. This agent is responsible for applying the policies defined by the user using his GUI and thus stop the disclosure of non-permitted information. These agents allow users to define their policies using the GUI with the help of a "restricted natural language" called SIMPL (Simple Privacy Language).The user can define his choice through wizards and menus which is automatically converted to SIMPL form and is displayed which is to be approved by the user before it can become effective. This provides total flexibility to the user in terms of defining privacy policy and minimizes the chances of any discrepancy or misunderstanding [2].

Module 2 (Controller agents):

Controller agents: These are installed on the site of the controller and they are responsible for ensuring that they meet all standard rules for protection of privacy of the users and also avoid misuse of the information collected from the users.

Module 3(Auditor agents):

Auditor agents: These are run by certified data protection agencies that check whether the controller agents are adhering to the policies that the subject agents have defined. They are like the cross checking police agents and thus increase and ensure trust in the system.

The implementation in this paper consists of three modules as stated above. The working of these application is based on the information provided by the user which he/ she does not wants to be disclosed to the undesired people. Using the user interface component of the application we can easily retrieve this information from the user and store these keywords in a database. Whenever any information is being retrieved from the mobile device then this application reads this information from the port which is being used for transfer of information and checks for the information that the subject has defined as disclosable. If the controller agents find some information subjected to the concern of the user then it alerts the user about the transaction taking place and then with the consent of the user the transaction takes place. The application supports the various aspects of the security which are to be considered when dealing with pervasive computing.

The user interface module of this application has been already completed. In this all the keywords or the information which the user desires not to be disclosed are entered into the text box with comma as a separator. The application stores these keywords in the database and searches the incoming and outgoing information for these keywords. When the application is installed on the device then only the user enters these keywords and can also add these keywords as per his convenience later during the use of this application. The user also has the facility to delete or update the keywords as his priorities keeps on changing. Thus making this application total flexible is our primary concern.

IV. CONCLUSIONS

Before concluding, we would like to emphasize the need for a pragmatic approach to privacy protection. The fact of consent makes us familiar to two options which are:

A. Either, we refrain from resorting to Privacy Agents and stick to the rule that subjects should give their consent before each single disclosure of personal data; the likely result will be that, overwhelmed by repeated requests for consent, individuals will end up accepting systematically and thus giving up any privacy protection.
B. Or we accept the risk of delegating our consent to a Privacy Agent which meets strong legal and technical requirements, even though we are aware of the fact that software may contain bugs and the risk of mistake is not null.

At the end of all what really matters is the choice we make as the main conclusion is that with appropriate technical and legal frameworks we can easily implement Privacy Agent which can efficiently improve the level of privacy and protection of our rights. Along with the methods and tools designed by the Computer Science Community, the emergence certification mechanism can be instrumental in the development of Privacy Agent and its worldwide acceptance.

The misbehaviour of Privacy Agent provider in case of disclosing the undesired data is also a liability. But again with proper precautions such as mentioning all the liabilities in the license agreement document of the software these liabilities can be easily overcome.

V. FUTURE WORKS

Upcoming technologies will surely make mobile devices most sought for in secure financial transactions. Currently mobile devices are used for accessing bank accounts only but possibly cannot take out transaction but this will not be the future scenario. Pervasive Computing can be made so secure that financial transaction will not be a dream then. This work is a step forward to this.

VI. REFERENCES

[1] V.-S. Wong and V. Leung, "Location management for next generation personal communication networks," IEEE Network, vol. 14, no. 5, pp.8–14, Sep./Oct. 2000.

[2] S. Tabbane, "Location management methods for third generation mobile systems," IEEE Commun. Mag., vol. 35, no. 8, pp. 72–78, 1997.

[3] (2001) TS 33.102: Security architecture, version 4.2.0, release 4. Third Generation Partnership Project - Technical Specification Group.

[4] (2000) TR 33.902: Formal analysis of the 3G authentication protocol.Third Generation Partnership Project - Authentication and Key Agreement(AKA).

[5] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 734–742, Mar. 2005.

[6] Q. He, D. Wu, and P. Khosla, "Quest for personal control over mobile location privacy," IEEE Commun. Mag., vol. 42, no. 5, pp. 130–136,2004.

[7] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," J. Cryptology, vol. 1, no. 1, pp. 65–75, Jan. 1988.

[8] D. A. Cooper and K. P. Birman, "Preserving privacy in a network of mobile computers," in Proc. IEEE Symposium Research Security Privacy, 1995, pp. 26–38.

[9] S. Hoff, K. Jakobs, and D. Kesdogan, "Anonymous mobility management for third generation mobile networks," in Proc. IFIP Commun. Multimedia Security, 1996, pp. 72–83.

[10] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," IEEE Network, vol. 8, no. 2, pp. 26–34, Mar./Apr. 1994.1042 IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 3, MARCH 2008.

[11] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in Proc. International Conf. Mobile Computing Networking, 1995, pp. 26–36.

[12] A. Herzberg, H. Krawczyk, and G. Tsudik, "On travelling incognito," in Proc. IEEE Workshop Mobile Systems Applications, 1994, pp. 205–211.

[13] M. J. Beller, L.-F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," IEEE J. Select. Areas Commun.,vol. 11, no. 6, pp. 821–829, Aug. 1993.

[14] C. Tang and D. O. Wu, "An efficient mobile authentication for wireless networks," to be published.

[15] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," IEEE Trans. Wireless Commun., vol. 4, no. 1, pp. 57–64, Jan. 2005.

16] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc. 3rd ACM CCS, 1996, pp. 48–57.

[17] T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signature for smart card," in LNCS 1729. Spinger-Verlag, 1999, pp. 247–258.

[18] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong nondesignated proxy signature," in LNCS 2119. Springer-Verlag, 2001, pp. 474–486.

[19] G. Wang, F. Bao, J. Zhou, and R. H. Deng, "Security analysis of some proxy signatures," in Proc. Inform. Security Cryptology (LNCS 2971). Springer-Verlag, 2004, pp. 305–319.

[20] K. Zhang, "Threshold proxy signature schemes," in Proc. 1st International Inform. Security Workshop, 1997, pp. 191–197.

[21] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International J. Inform. Security, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[22] A. M. Odlyzko, "Discrete logarithm in finite fields and their cryptographic significance," in Proc. Eurocrypt. Spinger-Verlag, 1985, pp. 224–314.

[23] C. Pomerance, "Analysis and comparison of some integer factoring algorithms," in Computational Methods Number Theory. H. W. Lenstra, Jr., and R. Tijdeman, eds. Mathematisch Centrum, Amsterdam, 1982, pp. 89–139.

[24] E. Teske, "Square-root algorithms for the discrete logarithm problem," in Public - Key Cryptography Computational Number Theory. Walter de Gruyter, Berlin - New York, 2001, pp. 283–301.

[25] J. Zagami, S. Parl, J. Bussgang, and K. Melillo, "Providing universal location services using a wireless E911 location network," IEEE Commun.Mag., vol. 36, no. 4, pp. 66–71, 1998.

[26] L. C. Godara, "Application of antenna arrays to mobile communications, part ii: Beam-forming and direction-of-arrival considerations," Proc. IEEE, vol. 85, no. 8, pp. 1195–1245, Aug. 1997.