A Privacy Preserving Access Control Scheme using Anonymous Identification for Ubiquitous Environments

Nguyen Ngoc Diep*, Sungyoung Lee*, Young-Koo Lee*, HeeJo Lee**
*Dept. of Computer Engineering, Kyung Hee University
**Dept. of Computer Science and Engineering, Korea University
*{nndiep, sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr, heejo@korea.ac.kr

Abstract

Compared to all emerging issues, privacy is probably the most prominent concern when it comes to judging the effects of a wide spread deployment of ubiquitous computing. On one hand, service providers want to authenticate legitimate users and make sure they are accessing their authorized services in a legal way. On the other hand, users prefer not to expose any sensitive information to anybody. They want to have complete control on their personal data, without being tracked down for wherever they are, whenever and whatever they do. In this paper, we introduce an anonymous identification authentication and access control scheme to secure interactions between users and services in ubiquitous environments. The scheme uses anonymous user ID, sensitive data sharing method, and account management to provide a lightweight authentication while keeping users anonymously interacting with the services in a secure and flexible way.

1. Introduction

Ubiquitous computing integrates computation into environment, rather than having computers which are distinct objects. This environment consists of thousands of transparent devices and sensors surrounding users with a convenient, information-rich atmosphere. These gadgets will be everywhere, performing regular tasks, providing new functionality, extending the reach of traditional computing to physical spaces, allowing users to interact seamlessly with the surrounding environment.

In this smart world, data about individuals is constantly generated, transmitted and stored. Computational artifacts embedded in the environment will continuously sense our activities and provide services based on what is sensed. However, such a world presents significant privacy dilemmas [2][3]. On one hand, people can enjoy using variety useful services anywhere, in anytime and at any situation in a seamlessly way. On the other hand, they fear for the risk of exposing sensitive private data because their personal data is collected by the environment for wherever they are, whenever and whatever they do. Users want to have a complete control about their privacy. They need a claim "to determine for themselves when, how and to what extent information about them is communicated to others" [1].

User privacy issues have been pointed out in [4][5], but we still need to further clarify definition of privacy in ubiquitous environment in scope of this paper, as follows.

- Anonymity: The real identity of a user should never be revealed from the communications exchanged between the user and a server unless it is intentionally disclosed by the user. Different communication sessions between the same user and service should not be linkable [6]. Different devices of user should not be linkable.
- Context privacy: Except users want to disclose their context information (location, time, preference, name of services, etc), no one can know about such information even system administrator or service providers they interact with.
- Confidentiality and integrity: system should provide protection measures on the communication channels while users are interacting with services in order to protect sensitive information from eavesdroppers.

In reality, the quests for authentication/access control and user privacy protection conflict with each other in many aspects, and the problem is highly complex in ubiquitous computing as the context

13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications(RTCSA 2007)
0-7695-2975-5/07 $25.00 © 2007 IEEE

information of users is more of a concern. On one hand, the service generally depends on the user identity information and corresponding pre-established trust relationship as well as the service contract between them to accomplish user authentication and conduct access control. On the other hand, the user does not want to be tracked by the service for wherever he is and what ever he does. The trade off between the two thus poses a great challenge to security designers [6]. Beside that, these environments present more privacy concerns to users as there is no existing trust relationship between the user and the environment's owner. So, providing flexibility as personalizing services from these environments is difficult because users must provide information to the system without breaching their required levels of privacy [13].

This paper provides us a scheme to protect privacy of users and to maintain the flexibility for users while using available service in ubiquitous environments. The ultimate goal is anonymity which keeps the users anonymously interacting with the services, through that, preserving context privacy of users. And also it keeps confidentiality and integrity on communication channels.

The proposed schemes is at application level without relying on any underlying system infrastructure such as "light house" or "Mist router" in [7]. It is much easier in implementation compared to other anonymizing technique using Mix concept [8] like Onion Routing [9], SG mixes [10]. This scheme possesses many desirable security properties, such as anonymity, nonlinkability, risk mitigation, etc.

The rest of this paper is organized as follows. In section 2, we describe system architecture. Then we present in detail the proposed scheme in section 3. Next, we discuss about the security features and performance of proposed scheme in section 4. Section 5 is related work and we conclude the work in section 6.

2. Proposed scheme

2.1. System architecture

Our given system architecture (Fig. 1) basically consists of four types of entities: users, services, authentication server and database server.

We are considering a scenario that a user want to access to available services in a ubiquitous environment. User with handheld device comes to a smart office. When he registers with the system here, his context information will be collected by many sensors deployed in the environment. He wants to access available services in this ubiquitous environment. In order to protect the system, users must be authorized before using services.

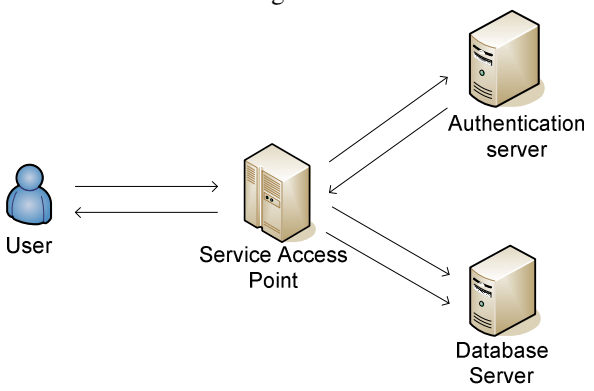

Fig. 1: System architecture

Meanwhile, the user does not want to expose his context information. He does not want to be tracked down for where they are, when and what they are doing. He needs full control of context privacy, that means: Except users want to disclose their context information (location, time, preference, name of services, etc), no one can know about such information even system administrator or service providers they interact with. In order for an environment to provide a personalized service to a user, it must be able to record a user's interests and behavior over time. And because of a large number of services in ubiquitous environments, users usually have their preference and other private data saved on server at service-side. But even when he needs to expose some sensitive information when interacting with services, he still wants to use them anonymously. So, how to keep users interacting with services in ubiquitous environments anonymously while keeping their data on servers at service-side? Here, we assume that users can manipulate their IP address or MAC (Media Access Control) address. This is a prerequisite for anonymous communication because someone can easily find the real identity of the users using services by linking their unique IP/MAC address to the owner.

2.2. Anonymous identification based scheme

This section presents our user privacy preserving scheme using anonymous identification. The scheme consists of two sessions: session 1 is for getting user's data and anonymous ID (temporal ID), session 2 is for anonymous authorization and interacting with service.

Before presenting the scheme, we need to have some assumptions as follows. Users need to register

themselves as legal users of the system first. User's sensitive data is stored in database server at server side and it is encrypted by user before sending and storing in database. This ensures that no body at service side can know about these data, so privacy of user is guaranteed. We do not mention about encryption of the communication channels in the scheme but we suppose we have that by symmetric key cryptographic method to ensure confidentiality of the system.

The scheme can be conceptually described by Fig. 2 and Fig. 3.

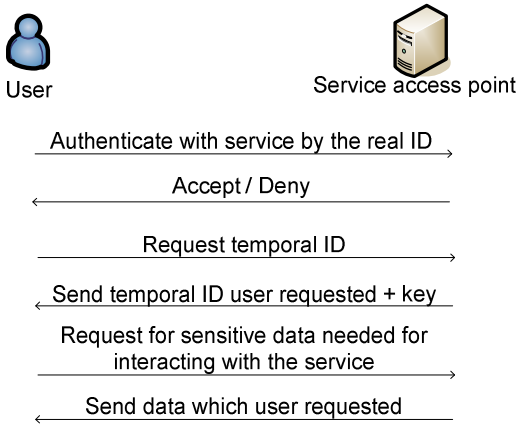

Fig. 2: Session 1

a) For detail, session 1 can be described as follows. Firstly, user needs to authenticate with the service by his real user ID. In this step, the system can use a traditional authentication protocol like Kerberos to authenticate the user, which uses an authentication server in the backend. After user is authorized, he sends a request for a temporal ID in order to use the service anonymously. Note that the temporal ID is not unique so no one can link this ID to the real user ID. Beside that, temporal ID is usually updated to guarantee confidentiality. If this user has right to use the service (e.g.: printing) anonymously, service access point will send back a user a temporal ID and a key to use in the next session. The key is not unique and usually changed in a short time. The temporal ID which user received has at least same rights as rights of real user ID. The level of temporal ID depends on user's request. The reason is to mitigate the risk, users should have right to choose the suitable ability of temporal ID. The less ability of temporal account, the less risk will occurs in transactions. In the next step, user requests for sensitive data stored in service side. Sensitive data can be preference data or personal data like email address, etc. The request is sent to service access point and service access point will get requested data from database server. Then it sends those data back to user. The data is decrypted on user's device to use in the next session (these data is encrypted by user as assumption). This activity makes a little burden for the system but it is necessary. Because if the service requires some sensitive information from user (such as email address) to send back to user some information later and if user show the link to database on the server, the system will easily know the true identity of user. (Note that, these data only consist of sensitive information like user preferences or personal information, so it is not much.) And suppose that user sends some sensitive information to the service; if that data in database on server is not encrypted, the system can easily link them to the user's true identity because those data is often unique.

b) In session two, the user had temporal ID, key and he uses it to access the corresponding service.

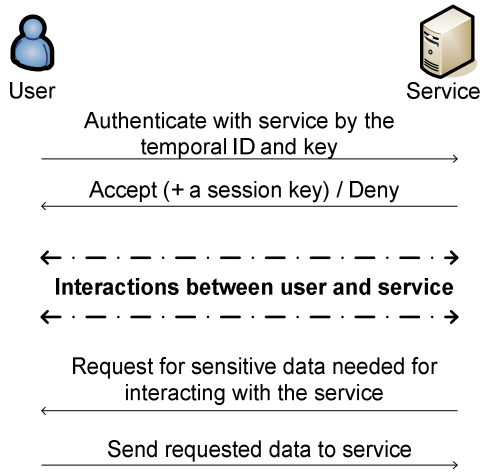

Fig. 3: Session 2

The user authenticates with service by using the temporal ID and the key he got in the previous session. The key here and its changing-in-a-short-time property (the time is enough for the user finishes session 1, plus a delay time between two sessions and time for doing authentication step in session 2) are to make sure that if some one has temporal ID, he can not bypass session 1. Note that we need to define a time-out value between session 1 and session 2, and the delay time between to sessions is not fixed. If the time is out, users can not perform authentication step in session 2. So, only registered user can use the service. If the user is authorized then he can start using service with legitimate actions within his rights he has for his temporal ID. The session key is used for encrypting the communication channel. Whenever the service requires

data, the user will send it without fear for exposing sensitive data or being disclosed his real identity.

2.3. Improvement – Account Management

For better supporting user's flexibility and controlling interactions between users and services as well as privacy disclosure level of users, we need a method called Account Management.

Before describing the method, we need to modify our above proposed scheme as follows. In session 1, when the user sends request for temporal ID to service access point, service access point will check if user has right to use service anonymously. If the user has that right, service access point will send back a set of rights that current real user ID has in the service. For example, in FTP service, user has rights like read, write, update, create folder, etc. After receiving rights, user chooses a suitable number of rights in the set corresponding with his wish when using the service (for example, user just use two rights: read, update), then sends that subset of rights (e.g. read, update) with a request for corresponding temporal ID. Based on this subset of rights, service access point will send back user a corresponding temporal ID (which has set of rights as requested). This temporal ID is not unique. This method mitigates the risk for users as well as the system.

Each above subset of rights is saved as a configuration that can be used for the next time the user uses service. So, for each service, users have some configurations of temporal user ID.

Beside that, by allowing users to control over what information they share with intelligent environments, they can effectively control their involvement and interaction with this emerging form of computing. For information services, users will be able to automate information gathering and service usage, like receiving updates on public transport schedule and new bulletins while traveling to work, etc. So, we provide user accounts which contain information of configuration of temporal user ID (set of rights), information of user's preferences, and user's habit for setting up working environment of users in the service. These accounts even contain template that describes the information required to access services available in ubiquitous environments, for example, context information. All the user accounts are stored in account manager and saved in database at server side.

This approach gives users flexibility to use ubiquitous environments as they wish. Users can personalize interactions when using services. Of course, we need a user interface for doing all these works: managing user accounts and information sharing with services available in the environment. This interface will manage privacy preferences which are responsible for selecting account to be used in any services in any given intelligent environment.

3. Security analysis of proposed scheme

Our proposed scheme has some nice security properties as follows.

Anonymity: Our proposed scheme provides anonymity to users. Firstly, users are anonymously authorized by the corresponding service. Secondly, real identity of users can not be known by linking sensitive data collected by the service through interaction with users because these data is encrypted in database on the service side. Note that we have assumption that users can manipulate their MAC/IP addresses so that no one can find the real identity of the users using services by linking their unique IP/MAC address to the owner.

Protection of User Context Privacy and User Preference: all context privacy and preference data of the user is protected by the proposed scheme. Only necessary data is disclosed to the service and it is under control of user. For example, in authorization process, only type of service is known by service, or while interacting with service, only some required sensitive information is disclosed. Through authorization process, users could be authenticated anonymously without disclosing any other information. All the service side knows is some legal users are using the service. Outsiders can not extract any information because the communication is well protected.

Integrity and Confidentiality: because each session has one session key for encryption of all interaction data traffic between users and service, system ensure the integrity and confidentiality. This process can be archive by using symmetric cryptography.

Nonlinkability: Ideally, nonlinkability means that, for both insiders (i.e., service) and outsiders, 1) neither of them could ascribe any session to a particular user, and 2) neither of them could link two different sessions to the same user [11]. In this scheme, nonlinkability is achieved for both insiders and outsiders. For each session, every user has the same temporal account (for a particular role) but has different session key. Therefore, there is no relationship among user and session.

Risk mitigation: our scheme provides a set of temporal user ID in which no one has more rights than current real user ID. That means rights of temporal ID in this set are subset of rights in current real user ID. Users can choose any set of rights that is reasonable in

order to mitigate risk. That is the reason why users do not often choose account Administrator for normal operations.

One feature we need to improve is *Untraceable Routing:* Suppose that the user is in collaborative environment, and he uses location services in parallel. If the system is compromised, the user is easily known by other users by linking the user's location to the owner. To prevent this situation, user should not use location services in parallel with collaborative services. Or the system may use some anonymous routing technique like [7][8].

4. Related work

Research on privacy and anonymity can be roughly classified into two categories: anonymous communication and user anonymity. User anonymity aims at providing the users anonymity while they are using the network by letting them hide their identity from the services. Anonymous communication focuses on providing a communication channel that is immune to traffic analysis so that the communicating parties can be anonymous against the eavesdroppers.

The first category consists of researches focused on designing specific security infrastructure to protect context privacy like location information from service providers. They are "Mist router" [7], Onion routing [8], SG mixes [9]. These works have to trade off privacy with performance because the overhead of packets is high. Another kind is proxy-based. Users can use it to hide real identities form web servers they access. Anonymizer [12] is a one of them. Users can enjoy anonymity by rerouting their HTTP packets through the Anonymizer, which replaces the information in the packet headers so that the websites cannot infer the user's identities. This approach has the problem of a centralized trusted entity. The Anonymizer site can track all the anonymous user's activities and is also a single point of failure.

The second category mainly focuses on identity manipulation. Craig et al. [13] introduce a method using pseudonyms that allows users to manage their identity in ubiquitous environments. This method helps users maintain their desired level of anonymity. Similarly, Jendricke et al. [14] introduced an identity management system where a user is issued multiple identities, and the user uses them depending on applications. These works can mitigate the risk of exposing user privacy but can not provide a true anonymity.

He et al. [15] presented a simple anonymous ID scheme, which is a direct application of Chaum's blind signature technique [8]. However, the scheme neither provides nonlinkability nor ensure about user anonymity when users expose data to services.

Kui Ren et al. [6] also proposed an anonymous ID scheme based on blind signature technique. This work provides a flexible and lightweight authentication and key establishment protocol based on hash chain. It achieves many nice security features. The drawback is it did not consider the scenario that users have to disclose some necessary sensitive context information to services without affecting user privacy. In that case, service side may link sensitive information to real identity of the user. They can not guarantee privacy of users when they have to interact and to share information with the services.

5. Conclusion

As ubiquitous environments become more prevalent they will cover more and more of our public and private life. So, the success of these environments will be dependent on user's willingness to accept and manage the privacy risks of exposing their personal information to the environments. The intelligent environments that provide benefits to the user without invading their privacy will be much more useful than the traditional security and sensing environments currently under development.

This paper has described a scheme allowing users to interact with services anonymously while still maintaining the flexibility by using the concepts of temporal ID (anonymous user ID), sensitive data sharing method and user account management. The temporal ID allows users to access services anonymously. Sensitive data sharing method helps users interact with services but the real identity of user can not be revealed. User account management allows users to control risks to their privacy and security of system, giving them better flexibility when using services in these environments. This scheme also possesses many desirable security properties, such as anonymity, nonlinkability, risk mitigation, etc. With the proposed scheme, we are able to provide users with complete control over their privacy while allowing the administration to authenticate legitimate users and keeping interactions between users and services running without limitation.

6. Acknowledgment

This research was supported by the MIC (Ministry of Information and Communication), Korea, Under the ITFSIP (IT Foreign Specialist Inviting Program)

supervised by the IITA (Institute of Information Technology Advancement).

7. References

[1] Alan F.Westin, “Privacy and Freedom”, Atheneum, New York NY,1967.

[2] Bellotti, V. and Sellen, “A. Design for Privacy in Ubiquitous Computing Environments”, Proceedings of ECSCW ’93, Milan, Italy, 1993, pp. 77-92.

[3] M. Langheinrich, “Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems”, Proc. Ubicomp 2001, Springer-Verlag LNCS 2201, 2001, pp. 273-291.

[4] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M. Dennis Mickunas, and Seung Yi. “Routing through the mist: Privacy preserving communication in ubiquitous computing environments”, In proceedings of IEEE International Conference of Distributed Computing Systems (ICDCS), Vienna, Austria, 2002, pp. 65--74.

[5] Ernesto Damiani, Sabrina De Capitani di Vimercati and Pierangela Samarati, “New Paradigms for Access Control in Open Environments”, Signal Processing and Information Technology, Proceedings of the Fifth IEEE International Symposium, 2005, pp. 540- 545.

[6] Ren K., Wenjing Lou, Kwangjo Kim, and Deng R., “A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments”, IEEE Transactions on Vehicular Technology, 2006, vol. 55, pp. 1373-1384.

[7] J. Al-Muhtadi, R. Campbell, A. Kapadia, D. Mickunas, and S. Yi, “Routing through the mist: Privacy preserving communication in ubiquitous computing”, Proc. ICDCS,Vienna, Austria, 2002, pp. 65-74.

[8] Chaum D., ”Blind Signatures for Untraceable Payments”, Advances in Cryptology: Proceedings of CRYPTO'82, Plenum Press, 1983.

[9] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding Routing Information," R. Anderson, editor, Information Hiding, LLNCS 1174, Springer-Verlag, May 1996, pp 137-150.

[10] D. Kesdogan, J. Egner, and R. Buschkes, "Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System", Information Hiding 1998, LNCS 1525, Springer Heidelberg, 1998, pp 83-98.

[11] S. Xu and M. Yung, “K-anonymous secret handshakes with reusable credentials”, in Proc. ACM Conf. CCS, 2004, pp.158-167.

[12] Anonymizer, http://www.anonymizer.com

[13] Craig Chatfield and René Hexel, “User Identity and Ubiquitous Computing: User Selected Pseudonyms”, in Workshop on UbiComp Privacy: Privacy in Context, Tokyo, Japan, September 2005.

[14] U. Jendricke, M. Kreutzer, and A. Zugenmaier, “Pervasive privacy with identitymanagement”, in Proc. 1st Workshop Security, UbiComp, 2002.

[15] Qi He, Dapeng Wu, P. Khosla,”The Quest for Personal Control over Mobile Location Privacy”, Communications Magazine, IEEE, 2004, vol. 42, pp. 130-136.