Toward unlinkable ID Management for Multi-service Environments

Nohara, Yasunobu
Kyushu University

Inoue, Sozo
Kyushu University

Yasuura, Hiroto
Kyushu University

出版情報：Proc. 3rd Int'l Conf. Pervasive Computing and Communications(PerCom) Workshops, pp.115-119, 2005-03. IEEE Computer Society
バージョン：
権利関係：

Toward unlinkable ID Management for Multi-service Environments

Yasunobu NOHARA, Sozo INOUE, Hiroto YASUURA
Kyushu University
6-1 Kasuga-koen, Kasuga-shi
Fukuoka, 816-8580 Japan
{nohara,sozo,yasuura}@c.csce.kyushu-u.ac.jp

Abstract

As pervasive computing environments become popular, ID devices, such as smart cards and RFID tags, introduce multi-service environments, in which a user can receive multiple services by one ID device. However, there exists a problem that service providers can trace a user's behavior by linking the user's access history, if only one ID is assigned to the user.

In this paper, we propose an unlinkable ID management scheme for multi-service environments. Our scheme provides unlinkability of users' accesses against third-party service providers, by preparing different user IDs for each service, and by using cryptographic protocol to exchange the ID between a user and a service provider, while linkability is assured between the user and the involved provider.

1 Introduction

With pervasive computing environments becoming popular, *ID devices*, such as smart cards and RFID tags, are introducing multi-service environments, in which a user can receive multiple services by one ID device. However, there exists a problem that service providers can trace a user's behavior by linking the user's access history, if only one ID is assigned to the user.

The concept of unlinkability, that third parties cannot link multiple accesses by the same user[3][4], and some technology which realizes unlinkability has been proposed[5]-[7]. However, these technologies have a problem that multi-service environments are not assumed or that service providers cannot offer customized services for each user.

In this paper, we propose an unlinkable ID management scheme for multi-service environments. Our scheme is based on PID system [1][2], which is proposed as a social infrastructure system for electronic services. Our scheme provides unlinkability of users' accesses against third-party service providers, by preparing different user IDs for each service, and by using cryptographic protocol to exchange the ID between a user and a service provider, while linkability is assured between the user and the involved provider.

The remainder of this paper is organized as follows: Section 2 explains unlinkability, and describes the related work. Section 3 presents the proposed scheme. Section 4 evaluates the proposed scheme. Section 5 concludes this paper with summary.

2 Motivation

It is possible to make a device's ID such that it does not include personal information. However, there exists a problem that third parties such as third-party service providers can trace a user's behavior by linking the user's access history, if anyone can read the ID of a device unrestrictedly. Therefore, it is important to clarify the concept of unlinkability, that third parties cannot read the ID of a device unrestrictedly and cannot link the user's access history.

2.1 Definition of Unlinkability

In [3], unlinkability is defined as a property which ensures that a user may make multiple uses of resources or services without others being able to link those uses together.

In [4], unlinkability of two or more items is defined as a property that, within the system, those items are no more and no less related than they are related concerning the a-priori knowledge.

In this paper, we define *unlinkability* as follows: let I^n_{AX} be the n-th information that a person X gets from user A's ID device, then we say that *user A's information is unlinkable against X*, if X cannot recognize whether I^n_{AX} and $I^m_{AX} (m \neq n)$ are sent by the same user. It means that X cannot distinguish I^n_{AX}, I^m_{AX} and user B's information I^l_{BX}.

Proceedings of the 3rd Int'l Conf. on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops)
0-7695-2300-5/05 $20.00 © 2005 IEEE

If a person X and Y share user's information and cannot recognize whether I^n_{AX} and I^k_{AY} are sent by the same user, then we say that *user A's information is unlinkable among X and Y*.

2.2 Related Work

In RFID systems, schemes which realize unlinkability against third parties are Randomized Hash Lock scheme[5] and one time ID scheme[6]. In these schemes, ID devices send hashed or encrypted value of ID and random number. The value which an ID device sends is not fixed, and only the service provider who knows the secret information can generate the ID from the values. Therefore, these schemes realize unlinkability against third parties. However, these schemes do not assume multi-service environments.

An information systems using smart card is anonymity authentication system[7] using group signature. In these systems, unlinkability is realized not only against third parties but also against the involved service provider using the nature of group signature that restricts even involved service provider to identify users. However, the involved service provider can verify who the regular users are, and the administrator can link the user's access history. Therefore, service providers can deal with services that need accountability. This system satisfies unlinkability against the involved service provider. Therefore, this system enables high level protection of user's privacy. However, there exists a problem that the provider cannot offer customized service for each user.

2.3 Unlinkability in Multi-service Environments

As it is addressed in previous section, there exists discussion of unlinkability in single service environment. However, it was rare for the literature to discuss unlinkability in multi-service environment.

As a recent problem in multi-service environments, there is linkability among third-party service providers. A conventional ID device has only one ID, and the ID is used by multiple service providers. Therefore, service providers can link a user's history of each service. There exists a privacy problem that third-party service providers can trace user's behavior if user's access history is shared among third-party service providers. In multi-service environments, it is important to realize unlinkability among third-party service providers.

3 Proposed Scheme

3.1 System Model

In this section, we describe the model of the ID management scheme. This model is based on PID system[1][2]. In the model, there are three entities and an individual ID called *PID* (Personal IDentifier)[2].

Three entities are User, Issuer, and Service provider, and these are defined as follows.

- *User* : The one who receives services. Multiple users can exist.
- *Issuer* : The one who issues and manages PID. Only a single issuer is assumed to exist. The issuer must be trusted socially.
- *Service provider* : The one who deal with services to users. Multiple service providers can exist.

PID is a long bit sequence which an issuer issues to a user. A subsequence of PID is called *subPID*, and this subPID is assigned to each service provider. The technique of generating subPID from PID enables flexible ID issue. For example, the length of subPIDs can be changed for every service provider.

PID issued to user i is PID_i. sid_{ij} is a subsequence of PID_i issued to service provider j. ID_j is the ID that identifies the service provider j. f is a function which gives sid_{ij} from PID_i and ID_j. For example, f is given as lookup table of ID_j and sid_{ij}'s address of PID_i.

User i's subPID is a unique value in the service provider j. It means $sid_{ij} \neq sid_{i'j}$ for arbitrary $i \neq i'$ and j.

Each subPID, which is issued to service providers are distinct. It means $sid_{ij} \neq sid_{ij'}$ for arbitrary i and $j \neq j'$.

The process for a service provider providing services to users is as follows.

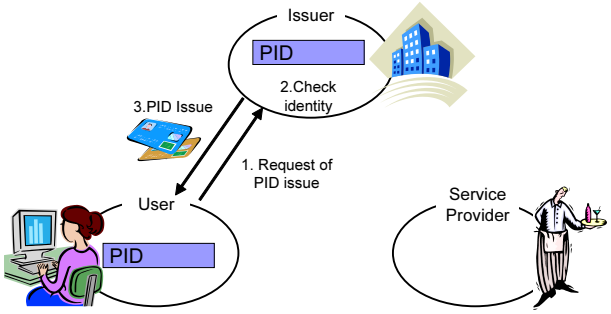

Figure 1. The process of PID issue

STEP1: The issuer examines the user's personal identity, and gives a PID to the user(See Figure1). The

PID is stored in an ID device and the device is issued to the user. The issuer stores the PID into a database.

STEP2: When a service provider wants to provide service to users, the service provider applies to the issuer for permission of using the PID system. The issuer provides a list of subPIDs : $SID_j = \{sid_{1j}, sid_{2j}, \cdots, sid_{nj}\}$ to the service provider j(See Figure2). The service provider stores subPIDs into a database. The issuer certifies a user's identity and subPID.

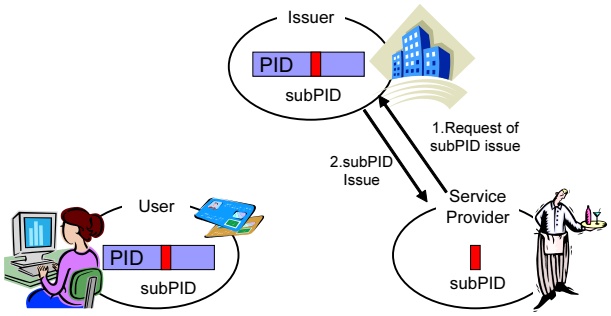

Figure 2. The process of services taking out subPID

The channel of these steps is authentic and encrypted. Thus, user and service provider can share the subPID, which is a part of PID. A user and a service provider identify each other by *ID matching*, which is a process to confirm that both of them have the same subPID and is shown in the following paragraph. After the ID matching, normal service such as authentication, data access in ID device is provided.

If a user or a service provider abuses the system, the issuer investigates their responsibility.

The information that a user and a service provider have are as follows(See Figure3):

- User : PID and $f(PID_i, ID_j)$
- Service provider: Service ID and a list of subPIDs

3.2 ID Matching Protocol

In this section, we explain *ID matching protocol*, which a user and a service provider can identify and authenticate each other without leaking user's ID to third parties.

In conventional authentication protocols, an ID exchange is done before an authentication. Therefore, they cannot satisfy unlinkability against third parties. In our protocol, mutual authentication is done without leaking ID to third parties as follows(See Figure4).

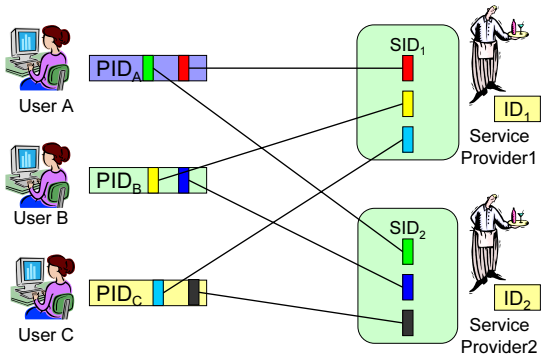

Figure 3. The information that users and service providers have

STEP1: The ID device sends an authentication request to the service provider.

STEP2: The service provider sends the provider's ID_j and a random number R_s to the ID device.

STEP3: The ID device calculates $sid_{ij} = f(PID_i, ID_j)$ from PID_i and ID_j. Then, the ID device sends $H_u = H(R_s||R_u||sid_{ij})$ [1][2] and a random number R_u to the service provider.

STEP4: The service provider computes $H(R_S||R_u||sid_{ij})$ for all sid_{ij} in the SID_j. If the service provider finds a match such that $H_u = H(R_S||R_u||sid_{ij})$, the provider sends $H_s = H(sid_{ij}||R_u)$ to the ID device.

STEP5: The ID device verifies whether $H(sid_{ij}||R_u)$ becomes H_s.

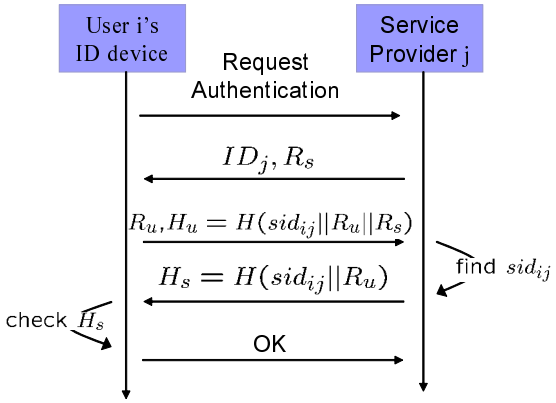

Figure 4. ID Matching protocol

[1] $H(X)$ means hashed value of X.
[2] $X||Y$ means combined valued of X and Y.

Our protocol can satisfy unlinkability against third parties, because the value ID device sends is hashed of user's ID and is not fixed. But the involved service provider can link the user's information using the searched sid_{ij}, so the involved service provider can offer a customized service for each user.

In our protocol, not encryption function unit but hash function unit is implemented in ID devices, so the cost of devices can be reduced. But a service provider needs to hash all users' subPID (STEP4). The more the number of user increases, the more the load of the service provider increases. Therefore, it is not easy to apply this scheme in very large-scale systems.

If a user sends $E_u = E_{KS_j}(R_s||R_u||sid_{ij})$ [3] instead of H_u and R_u in STEP3, a service provider can get sid_{ij} by decrypting E_u in STEP4. The cost of decrypting E_u is constant even if the number of users increases. Therefore, the problem of user increasing is solved by the public key scheme. However, ID device needs public key encryption unit, therefore it is necessary to consider the cost of device. Moreover key management scheme should be also considered.

To solve these problems, we proposed *K-ID matching protocol*, which is using hash function but the load of the service provider can be reduced[8].

4 Discussion

4.1 Unlinkability of our scheme

Our scheme satisfies unlinkability against third parties, because the value which ID device sends is hashed of user's ID and is not fixed. Therefore, our scheme prevents third parties from tracing users' behavior.

The involved service provider can know user's ID by using the list of subPIDs, and then the involved provider can link the user's access history. However, third-party service providers cannot link the user's history among the third-party service providers, because different subPIDs are issued to each provider. Therefore our scheme satisfies unlinkability among third-party service providers. A service provider can offer customized services for each user, but cannot link user's information among third-party service providers.

When a problem occurs, the issuer can investigate the user's responsibility by linking user's history, since the issuer holds PID including whole subPIDs.

Thus, our scheme satisfies unlinkability which is suitable for multi-service environments.

[3] $E_{KS_j}(X)$ means encrypted valued of X by S_j's public key.

4.2 Attacks against ID Matching

This type of attack is that an attacker sends a value as a hash value H_u to a service provider and receives to services by disguising someone. The more number of users N increases, the more the possibility of matching a value to the value, which is hashed of someone's subPID increases. It means the attacker's possibility that attack success increases.

In order to maintain the safety, our protocol should use the length of a subPID increased by $\log_2 N$ [bit] than a key of conventional authentication protocols.

4.3 Attacks against Unlinkability among third-party service Providers

Our scheme has unlinkability among third-party service providers as described in section 4.1. However, if multiple service providers share a list of subPID, unlinkability among third-party service providers may be broken through the following attacks although there are restrictions for attacking.

4.3.1 Sharing subPIDs

This type of attack is that multiple service providers offer services using only one shared subPID list. In this case, there exists a problem that the providers must provide single service to a user.

4.3.2 Multiple subPID Matching

In this attack, firstly service providers perform ID matching using one shared subPID list. After that, the service providers perform ID matching using other shared subPID list. If the interval of these ID matchings is short enough, it can be said that the ID device does not move between them. And then the service provider can recognize the information which can be gotten by subPID lists of each providers are send by the user. Therefore, the service providers can break unlinkability among third-party service providers. However, the third-party service providers must be share the subPIDs, which might be not only IDs but also the keys of mutual authentication to realize the attack.

For the countermeasure of this attack, it could be thought that the ID device rejects to response if multiple ID matching is requested in short period.

5 Conclusion

In this paper, we proposed an unlinkable ID management scheme for multi-service environments. Our scheme realizes unlinkability among third-party service providers, and is suitable for multi-service environments.

The next challenge is to discuss the method of reducing the amount of calculation required for the server in ID matching.

Acknowledgment

We thank Dr. H. Morita, Dr. K. Baba, Mr. Y. Hamasaki and Mr. S. Noutomi for their help of preparation of this article. Thanks are also due to all of members System LSI Research Center of Kyushu University.

This work has been supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 and for Young Scientists No.15700100 of the Ministry of Education, Science, Sports and Culture(MEXT). We are grateful for their support.

References

[1] Hiroto Yasuura, "Towards the Digitally Named World -Challenges for New Social Infrastructures based on Information Technologies-", Proceedings of Euromicro Symposium on Digital System Design -Architectures, Methods and Tools-(DSD2003), pp.17-22, Sep.2003.

[2] Yoichirou Hamasaki, Hiroto Yasuura, "A Proposal of Secure Information Infrastructure based on PID", DICOMO2002 Symposium, Jun.2002. (in Japanese)

[3] "ISO/IEC 15408 - INTERNATIONAL STANDARD Information technology - Security techniques - Evaluation criteria for IT security - Part2: Security functional requirements", Dec.1999.

[4] Andreas Pfitzmann, Marit Hansen, "Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology", http://www.freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf, May.2003.

[5] Stephan A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels,"Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", International Conference on Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, 2004.

[6] Kenji Imamoto, Kouichi Sakurai, "A Key Agreement Protocol With Users' ID Protection Using Trusted Third Party", Computer Security Symposium 2003, Oct.2003. (in Japanese)

[7] Takehisa Kato, Koji Okada, Takuya Yoshida, "Development of Anonmous Authentication System for Personal Data Protection", Computer Security Symposium 2003, Oct.2003. (in Japanese)

[8] Yasunobu Nohara, Sozo Inoue, Kensuke Baba, Hiroto Yasuura,"Unlinkable ID Matching Protocol for Large-scale RFID Systems", Symposium on Cryptography and Information Security 2005, in press. (in Japanese)