Journal of Network and Computer Applications 35 (2012) 1839–1846

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments

Zuowen Tan *

School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330032, Jiangxi Province, China

ARTICLE INFO

Article history:
Received 27 January 2012
Received in revised form
14 May 2012
Accepted 3 July 2012
Available online 13 July 2012

Keywords:
Privacy-preserving
Authentication
Accountability
Pervasive computing environment
Access control

ABSTRACT

In pervasive computing environments, the users can get access to the services from the service providers in a highly desirable way. But the security of the user's authentication is a challenging field. Pervasive computing environments must provide the service to only legitimate users. On the other hand, some users attempt to keep their anonymity without revealing their identities while using some privacy-related services such as location information, printing, buying shares, etc. In this paper, we propose a conditional privacy-preserving authentication and access control scheme for pervasive computing environments, called *CPriauac*. Compared with the previous schemes in the literature, registration servers and authentication servers in the proposed scheme need not maintain any sensitive verification tables. The management of public keys is easier. Furthermore, the anonymity of the user can be removed efficiently once the dispute happens. The proposed scheme provides user anonymity against outside and inside parties, mutual authentication, accountability and differentiated access control.

1. Introduction

Pervasive computing environments (PCEs) are an important application of wireless networks, computers and mobile computing, which make mobile users have seamless access to various services such as Auction, e-Learning, GPS and accessing wireless LAN by using low-cost, handheld devices, anytime and anywhere. The dynamic PCE has the unique characteristics, such as user mobility and open communication channels (Ye et al., 2012). Furthermore, the traditional security mechanisms will not be adapted in PCEs. All these characteristics lead to some new security issues which will affect their convenience.

Entity authentication and access control are two basic requirements for the dynamic PCE. In many situations, user privacy is also one of the biggest challenges. In essence, the protection of identity and other context information is regarded as an important criterion for PCEs (Beresford and Stajano, 2003). On one hand, the different kinds of threats exist in the dynamic open PCE. On the other hand, the computing devices have the limited communication range and computing power. Due to these inherent properties, security and privacy mechanisms must be efficient in terms of storage, communication and computation. So far, access control with authentication and privacy preservation in PCEs is still an open research area (Juels, 2006; Ren et al., 2006; Ren and Lou, 2007).

Based on Ren et al. (2006) and Magkos and Kotzanikolaou (2011), we highlight the security requirements which access control scheme in the PCE system should satisfy.

(1) *Unforgeability*: It is computationally infeasible to forge a valid credential. Any insiders even including a trusted third party (TTP) in collaboration with the service provider (SP) are not able to create a valid credential without the participation of users. Therefore, unforgeability implies the non-frameability.
(2) *Implicit mutual authentication*: Messages transmitted between the entities should be authenticated and provided with the protection of integrity. *SP* requires user authentication anonymously to prevent service abuse. Likewise, the user authenticates *SP*.
(3) *Conditional anonymity*: Any entities except TTP are not able to trace the real identity of the user. In case of dispute or service abuse, TTP can reveal the real identity of the user through the credential and transaction information. Obviously, Conditional anonymity implies the non-repudiation.
(4) *Unlinkability*: None of entities but the trusted third party can link different transactions with the same user unless the system policy explicitly permits it.
(5) *Accountability*: Users can acquire differentiated service access control. Thus, the system can prevent the double spending problem.
(6) *Scalability*: The system allows many users and service providers to join it without the reduction of its efficiency.

Security and privacy preservation in PCEs is essential. Many papers have been published to address the security and privacy

* Tel.: +86 791 83910192.
E-mail address: tanzyw@gmail.com

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.07.008

preservation challenges in PCEs (Beresford and Stajano, 2003; Ackerman, 2004; Myles et al., 2003; Kapadia et al., 2007; Li et al., 2009). Some researchers focus on construction of security infrastructures to protect user context privacy such as location information from the service provider. Hashem and Kulik (2011) proposed a MIST system to protect the user's privacy. LEXP (Burnside et al., 2002) is another infrastructure-based approach via proxy.

Another direction of the research on security and privacy preservation in PCEs is to find manipulation approaches. Jendricke et al. (2002) established a framework in which a user is given multiple virtual identities that can protect user privacy. He et al. (2004) applied Chaum's (1982) blind signature technique to present an anonymous ID scheme. However, the scheme (He et al., 2004) cannot prevent the double spending problem. Gruteser and Grunwald (2003) proposed a method for hiding users' MAC address with anonymous IDs so that the user cannot be tracked in a wireless LAN environment. Recently, Lu et al. (2008) proposed an efficient conditional privacy preservation protocol based on group signature scheme for secure vehicular communications. However, Jung et al. (2009) pointed out that Lu et al.‘s scheme does not provide unlinkability. Jung et al. (2009) proposed a robust conditional privacy-preserving authentication protocol in VANET.

Ren et al. (Ren et al., 2006; Ren and Lou, 2005) combined blind signature with hash chains to propose new schemes. Their schemes solve the double spending problem. Moreover they do not rely on underlying system infrastructure. However, the schemes in Ren et al. (2006), Ren and Lou (2005) and Kim et al. (2007) cannot provide strong unlikability against the *AP*s. The insider entity such as the service provider or authentication server can link different sessions with a user. Li et al. (2008) pointed out that an impersonation attack is possible in the scheme (Ren et al., 2006). Some work is done in the line of efficient protocols for privacy-preserving access control in PCEs (Ren and Lou, 2005; Ren et al., 2006; Kim et al., 2007; Ren and Lou, 2007; Li et al., 2008; Magkos and Kotzanikolaou, 2011). However, the existing privacy-preserving access control schemes do not fully satisfy the requirements.

Motivated by their work, we propose a lightweight conditional privacy-preserving authentication and access control (*CPriauac*) scheme in PCEs. Although each service provider has their public key, the scheme does not require public key for every different service. Since one service provider can provide many kinds of service, the management of public keys is easier. Authentication servers need not maintain any sensitive verification tables, which will enhance the security of the system. The proposed scheme provides user anonymity against both outside and inside parties, accountability, mutual authentication, and differentiated access control.

The rest of this paper is organized as follows. In Section 2, we describe the system architecture of a PCE and a cryptographic primitive. Section 3 describes *CPriauac* in detail. The analysis of the security properties and the performance analysis of *CPriauac* are provided in Section 4. Finally, Section 5 concludes the paper.

2. Background

2.1. System architecture of PCE

In a PCE, a mobile user accesses a service of many types. The system of PCE is involved with five kinds of participants: users *U*, registration servers *RS*, authentication servers *AS*, access points *AP* and a trusted third party TTP. Fig. 1 shows the basic system architecture of a PCE in our *CPriauac*.

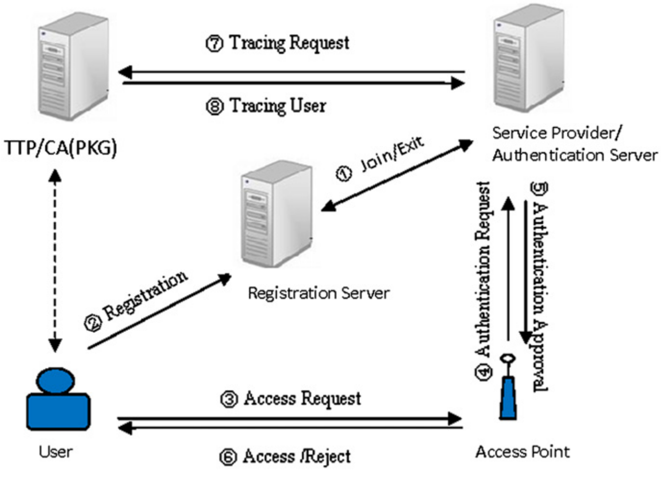

Fig. 1. System architecture.

- Users access different authorized services anytime anywhere via some resource-limited devices. After a user *U* subscribes a service with an identifier *SID*, *U* can get access to the service with the identifier *SID* through any *AP*.
- Registration servers are responsible for the registrations of all the users about all the kinds of services. Meanwhile, if a new type of service requests to join the system, *RS* will add it to the system. *RS* also manages the services to remove from the system.
- Authentication servers authenticate the authorized user for service request. In the system architecture of a PCE, we assume that authentication servers *AS* will also act as service providers *SP*. *SP* has the task to provide authorized users with the service data. In many cases, *AS* and *SP* are the same or controlled by the same entity. Different users can get access to the same *SP* through various *AP*s.
- Access points *AP* receive the service request message and forward the message to the authentication server *AS*. Upon obtaining the access grant from *AS*, *AP* allows the users to access the service.
- Trusted third party TTP is an offline authority and is invoked only when dispute resolution or anonymity revocation happens. TTP also acts as the CA (certification authority) or PKG(Private Key Generator) in our *CPriauac* scheme.

Now we compare the above system architecture of a PCE with the system architecture in the literature. Firstly, in Kim et al. (2007) and Ren and Lou (2007), *RS*, *AS* and *SP* is the same. However, *AS* and *SP* is the same party in our *CPriauac*. We add registration servers which are responsible for the user registration. Secondly, the system architecture of a PCE in Kim et al. (2007) includes a database server (*DS*). But no database server (*DS*) is required in our *CPriauac*.

Compared with other system architectures of PCE, the system architecture of a PCE in our *Cpriauac* is more reasonable. First, a registration server *RS* can manage many authentication servers. In the actual situations, in order to get access to different services from the servers, a mobile user only needs to register with one department called *registration* department in advance. Our *CPriauac* is an analog to the situations. Secondly, every service provider also acts as an authentication server to authenticate the users before the service provider permits the user to access it. Third, TTP in our *CPriauac* is offline. TTP is required only when dispute happens. In addition, our *Cpriauac* requires no *DS* to store the related or partial information for user authentication, which can avoid the potential insider attacks.

The communication models in the system are as follows. All the communication channels between an entity and the user are