普适计算的隐私保护协议①

贾宗璞 冯倩倩 (河南理工大学 计算机科学与技术学院 河南 焦作 454000)

摘 要: 改进了一个用于保护用户隐私的安全协议。该协议引入了服务发现者，用户并不直接与服务提供者进行通信，而是通过服务发现者来完成用户的需求。通过对协议的安全分析，可以看出：该协议保护了用户的隐私，也防止了用户被跟踪，并且减少了原有协议的计算量，更适合普适计算。该协议可以很好的保护用户的隐私，并且能够防止重放攻击。

关键词: 普适计算；隐私保护；认证；攻击；安全

A Privacy Protocol for Pervasive Computing

JIA Zong-Pu，FENG Qian-Qian

(Department of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: In this paper, a secure protocol to protect user privacy is improved. In this protocol the users does not directly communicate with the service provider, instead, the user connects through the service discoverers to complete their needs. Through analysis of the security system in the protocol, it becomes clear that this protocol protects users' privacy, and prevents users from being tracked at the same time. The protocol reduces the computational complexity of the original protocol, and it is more suitable for ubiquitous computing. The protocol may very well protect users' privacy, and can also prevent replayed attack.

Keywords: pervasive computing; privacy protect; authentication; attack; secure

1 引言

普适计算是继主机计算、桌面计算之后的第三类计算模式。其思想最早是在 1991 年由 MarkWeiser[1] 根据人机交互、网络技术、计算技术演化以及图形化用户接口的前期研究基础上提出的。他强调把计算机嵌入到环境或日常工具中去，让计算机本身从人们的视线中消失，让人们注意的中心集中到要完成的任务本身。徐光佑[2]给出的定义是“普适计算是信息空间与物理空间的融合，在这个融合的空间中人们可以随时随地、透明地获得数字化服务。”可见，普适计算最本质的特点就是融合、透明、以人为本。

普适计算的提出受到很多人的关注，已经成为一个非常有活力的研究领域。目前业界及众多高校都开展了普适计算研究项目。例如：麻省理工学院计算机科学实验室和人工智能实验室于 2000 念启动的 Oxygen，该项目使人可以像呼吸氧气般轻松地使用计算机；Microsoft 的 Esay Living 项目，旨在研发建立智能环境的原型体系结构及技术；清华大学的 Smart Platform 等等。但是，随着深入研究，人们发现普适计算的安全性是实施阶段所面临的最大困难。由于普适计算的一些固有特性使得传统的安全机制不能适用于普适环境。普适计算需要有新的技术来保障其安全性。

保证普适计算的安全需要解决下面几个关键问题[3]：①动态信任模型；②认证；③访问控制；④隐私保护；⑤安全均衡。隐私保护是普适计算一个非常重要的方面。保护用户的隐私主要是保护“5W”信息，即 who，what，where，when，why。这些都是用户的隐私。普适计算在为人们提供服务的同时，又要对用户进行认证，尤其是一些特殊的服务，需要用户提供更多的

① 基金项目:河南省重点科技攻关项目(072102210058)
收稿时间:2010-01-22;收到修改稿时间:2010-03-07

认证信息。如何保证这些信息不会泄露是一个很重要的问题。而且由于普适环境的分布性等特性，就使得普适环境中的隐私问题比传统环境更复杂。在普适环境中常用的是使用假名来保护用户隐私，但是攻击者可以跟踪并统计假名用户来分析出其真实身份，用户需要频繁的更换假名来避免跟踪，这增加了用户的工作量，也是不现实的。任娟等人[4]将普适计算中的隐私问题划分为物理层、链路层和应用层来解决，为系统提供了灵活的隐私保护方案。Shin[5]等人针对匿名和未授权提出了可保护隐私的访问控制协议，该协议运用 Schnorr 零知识验证算法和 Diffie-Hellman 算法保证密钥的交换是安全的，该模型还支持异构的信任框架。

郭亚军等人[6]利用盲签名提出了一种普适计算的隐私安全保护协议。该协议由服务发现者对用户进行认证和盲签名，随后用户以匿名的方式访问服务提供者提供的资源。通过匿名攻击模型分析可以看出，隐私保护安全协议不仅允许服务提供者对用户的认证，同时也可以保护用户隐私，并能够防止重放攻击和设备间的恶意串通。该协议使用的是盲签名来保护用户的隐私，盲签名分为对消息的盲化和脱盲两步，计算量比较大。由于在普适环境中存在很多计算和存储能力比较低的设备，所以不适合做大量的计算。本文对该协议进行了改进，利用服务发现者作为信息传输的中转站来保护用户的隐私。该协议只是通过普通的加密算法来实现，方便简单，不需要很大的计算量，因此适合普适环境。

2　协议设计

在普适环境中，设备的计算能力和存储能力都是有限的，直接由用户发现服务然后与服务提供者进行信息交互会给用户设备带来很大的压力。所以引入服务发现者，这些服务发现者具有很强的计算和存储能力，可以减少用户和服务提供者的负担。用户 U 与服务发现者 SD 通过资源限制信任协商[7]来建立它们之间的信任关系。资源信任协商就是用来建立两个陌生实体间的信任关系。通过协商服务发现者 SD 知道用户 U 的一些属性，用户 U 可以知道服务发现者 SD 的公钥 PK_{SD}。用户可以获取服务列表。服务发现者 SD 和服务提供者 SP 可以建立信任的公钥基础设施，它们互相知道对方的公钥。

协议的相关符号符号：

ID_U：用户 U 的 ID 号；

ID_{SP}：用户所需要的服务提供者的 ID 号；

ID_S：用户所需要的服务的 ID 号；

PK_U：用户 U 的公钥；

PK_{SP}：服务提供者的公钥；

PK_{SD}：服务发现者的公钥；

K：用户与服务提供者之间的会话密钥；

||：连接符。

① $U \rightarrow SD$：$\{ID_U \| ID_{SP} \| PK_U\}_{PK_{SD}}$；

② $SD \rightarrow U$：$\{ID_{SP} \| N_1 \| PK_{SP}\}$；

③ $U \rightarrow SD$:$\{N_1 \| ID_{SP} \| ID_U\}_{PK_{SD}} \| \{ID_S \| N_2 \| PK_U\}_{PK_{SP}}$；

④ $SD \rightarrow SP$：$\{\{ID_S \| N_2 \| PK_U\}_{PK_{SP}} \| ID'\}_{PK_{SP}}$；

⑤ $SP \rightarrow SD$：$\{\{N_2 \| K\}_{PK_U} \| ID'\}_{PK_{SD}}$；

⑥ $SD \rightarrow U$：$\{N_2 \| K\}_{PK_U}$。

第一步中用户向服务发现者索要服务提供者的公钥。第二步服务发现者用用户的公钥对 $ID_{SP} \| N_1 \| PK_{SP}$ 进行加密，其中 N_1 为服务发现者产生的随机数。用户收到后用自己的私钥脱密，用户得到了服务提供者的公钥。在第三步中服务发现者收到后先用自己的私钥脱密，通过 N_1 对用户进行认证，同时防止重放攻击。服务发现者重新选择随机数作为用户的 ID 号记为 ID'，并将用户的 ID 号与新的 ID 号记入服务发现者的表中，该对应会随着服务的完成而自动删除。服务发现者服务发现者将新的 ID 连同$\{ID_S \| N_2 \| PK_U\}_{PK_{SP}}$ 用自己的私钥加密发送给服务提供者。服务提供者收到信息后，将会话密钥和 N_2 用用户的公钥加密之后连同 ID'用服务发现者的公钥加密发送给 SD。SD 收到后进行脱密，得到$\{N_2 \| K\}_{PK_U}$，发送给用户。用户收到后用自己的私钥脱密，N_2 完成了用户对服务提供者的认证。同时用户与服务提供者交换了会话密钥，用户可以用会话密钥获得需要的服务。

3　安全分析

(1) 信任关系的建立：在该协议中，用户与服务发现者是通过资源信任协商来建立信任关系的，服务发现者与服务提供者之间的信任是建立在公钥基础设施的基础上的，所以具有很高的安全性。

(2) 保密性，在这个协议中使用的是 RSA 加密算法，RSA 加密算法的安全性基于大合数的难分解性，

易于实现，安全性比较高。

(3) 重放攻击：该协议中随机数的选择与发送可以很好的防止重放攻击，而且随机数的选取也可以完成在信息传送过程中身份的认证。由此可见随机数的选取保证了协议的安全性

(4) 跟踪分析：在协议第 3 步中由服务发现者给用户设置了新的 ID，通过新的 ID 可以很好的防止信息被跟踪。假设敌对的观察者可以监视网络信道中传输的所有信息，他可以获得用户所发送的消息，并计算该信息的杂凑值。然后他可以获取服务发送者到服务提供者的消息，并计算其杂凑值。若杂凑值相等，则对该消息进行跟踪。在该协议中，服务发送者对消息进行了重新包装，所以即使监听到消息，根据杂凑函数的特点，不可能得到相等的杂凑值。所以观察者并不知道哪条是用户所发送的信息，就无法发选择对的信息进行跟踪，从而保护了用户的隐私不会泄露。而且这个 ID 号是随机的，在用户获取服务之后会直接删除这个 ID 的对应，下次用户申请服务可能会得到不同的 ID 号。

(5) 篡改：第 3 步中由于服务发现者不知道服务提供者的私钥，所以并不能对用户发送的信息进行篡改。而且在协议中使用了加密，不知道私钥无法脱密对消息进行篡改。

在该协议中通过加密手段使服务发现者也并不知道用户所要求的服务。由于用户并不直接和服务提供者进行通信，服务提供者并不知道用户的信息，不知道为谁提供服务，从而保证用户的隐私安全。在消息的发送过程中是连同 ID 号和随机数一起进行加密发送的，这就在一定程度上抵制了第三者攻击。

4 结束语

本文设计了一个适用于普适计算环境的隐私保护协议，在协议中，通过使用第三者来转发消息来保护用户的隐私。在原协议中使用盲签名时首先将所要签名的消息盲化，盲化过程需要用户先与服务发现者建立连接，向服务发现者索要一些信息用于消息的盲化。在本文提出的协议中减少了这一步的通信，更适合普适计算无人干预的特点。以 RSA 和基于 RSA 算法的盲签名为例，在原协议的第一步用户将消息盲化和本文协议的第一步所使用的加密方法在难度上并没有太大的区别。在原协议中用户收到服务发现者的的消息后，用户除了脱密还要对签名脱盲。在本文所提出的协议中仅仅需要脱密，这样接减少了用户的计算量。在本协议中主要工作都是由服务发现者来做，减轻了用户和服务提供者的负担。该协议中通过服务发现者对消息进行转发来保护用户的隐私，而且服务发现者对用户的 ID 进行重新分配来防止跟踪。通过随机数的发送来防止重放攻击。该协议在保护用户隐私的同时又完成了认证，保证了数据的完整性和保密性。该协议可以满足那些对安全要求不太高的用户的隐私保护，对于那些要求比较高的用户的隐私保护，还需要进一步的研究。

参考文献

1 Weiser M. The computer for the twenty-first century. Scientific American, 1991,265(3):115－124.

2 徐光祐,史元春,谢伟凯.普适计算.计算机学报, 2003, 26(9):1042－1050.

3 郭亚军,洪帆,沈海波,陈利,王琴,徐芬.普适计算面临的安全挑战. 计算机科学, 2007,34(6):1－3.

4 任娟,裘正定.普适计算中的隐私保护.信息安全与通信保密, 2006,5:74－76.

5 Shink, Yasuda H. Provably secure anonymous access control for heterogeneous trusts. Proc of the 1st Intemational Conference on Reliability and Security. Washington DC:IEEE Computer Society, 2006:24－33.

6 郭亚军,何炎祥, 齐梅.普适计算的隐私保护安全协议.华中科技大学学报:自然科学版, 2007,35(11):103－105.

7 洪帆,郭亚军.资源限制信任协商.华中科技大学学报:自然科学版, 2006,34(5):23－25.