普适计算面临的安全挑战*)

郭亚军[1,2] 洪 帆[2] 沈海波[2] 陈 利[1] 王 琴[1] 徐 芬[1]
(华中师范大学计算机科学系 武汉 430079)[1] (华中科技大学计算机学院 武汉 430074)[2]

摘 要 分析了普适计算面临的安全挑战,给出了普适计算需要解决的几个安全问题,它们分别是:动态信任模型、认证、访问控制和隐私保护。并指出了这些安全问题的一些解决思路。

关键词 普适计算,安全,信任

Security Challenges in Pervasive Computing

GUO Ya-Jun[1] HONG Fan[2] SHEN Hai-Bo[2] CHEN Li[1] WANG Qin[1] XU Fen[1]
(Department of Computer Science, Central China Normal University, Wuhan 430079)[1]
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)[2]

Abstract This paper analyzes some security challenges the pervasive computing will meet, and examines several key security problems that are barriers to pervasive computing. They are: dynamic trust model, authentication, access control and privacy protection. In addition, some directions to settle them are indicated.

Keywords Pervasive computing, Security, Trust

1 普适计算

普适计算[1,2](Pervasive/Ubiquitous Computing)是继主机计算、桌面计算之后发展起来的一种新的计算模式。普适计算的思想最早是1991年由Weiser[1]提出的,其目标是要建立一个充满计算和通信能力的环境,同时使这个环境与人们逐渐地融合在一起。在这个环境中,人们使用计算机就如同使用水、电一样方便,像呼吸空气一样不知不觉。清华大学徐光祐教授将普适计算[2]定义为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、透明地获得数字化的服务。

一个普适计算环境主要是由移动用户、系统的服务、嵌入在物理环境的传感器和资源等组成的联合环境。用户在这个环境中只需要把注意力集中在他的工作上,无需关心如何使用设备。一个普适计算环境可能是一个会议室(如美国国家标准技术局的Smart Space),能够自动地为演讲者提供对投影仪和计算机的访问,能够记录会议资料,接受演讲者的命令,并能够根据不同的演讲者提供不同的应用环境。一个普适计算环境也可以是一个办公室网络(如MIT的Office Network),用户能够容易地定位移动的同事,并方便地与同事通信。用户也能够使用便携移动设备轻松地访问文件、电子邮件、软件以及使用打印机、传真机等。一个普适计算环境也可能是一个智能教室,教师可以通过自己的PDA向学生的PDA发送电子课件。当教师走近学生讨论组时,其PDA会动态加入该组,下载该组的讨论材料。普适计算环境也可能是Weiser设想的一个生活环境。当女士Sal早上起床后,计算系统已经按照Sal的习惯为她准备好了咖啡;当Sal向与周围环境关联的"windows"望去时,计算系统可以让Sal了解当时周围的环境;当Sal向与孩子们关联的"windows"望去时,计算系统可以让Sal了解孩子们此时的活动情况。

2 普适计算研究的内容

从技术发展上讲,普适计算是从分布式系统和移动计算的影响下发展而来的。但是普适计算研究的还涉及许多新的内容[8],如图1所示。

该图显示了普适计算与分布式计算以及移动计算研究内容的关系。图中自左至右出现一些新的研究问题,而且前面出现的问题到后面会变得更复杂。这种复杂性的增加是以乘法(×)而不是加法(+)的形式来体现的。分布式系统是由第一组(图1①)远程通信、容错处理、高有效性、远程信息存取和分布式安全性等技术发展而来;移动计算研究问题除包括分布式系统外,还包括第二组移动网络、移动信息存取、可适应性应用、能源觉察系统、位置敏感性等技术。普适计算研究内容包括移动计算以及第三组的四个额外技术(图1③),包括智能空间、不可见性、局部可扩展性、非均衡条件等技术。

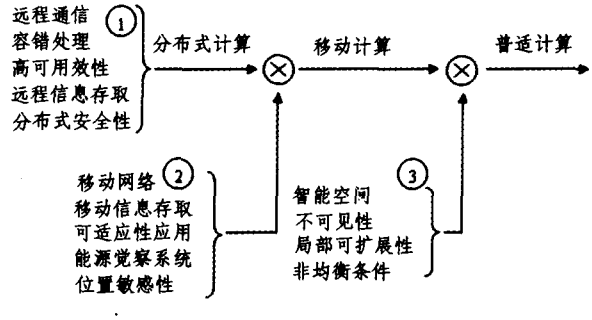

图1 普适计算的研究内容

从图中可以看到,普适计算需要研究的新内容包括:

(1)智能空间:智能空间是指特定的封闭区域(如会议室)或定义明确的开放区域(如一个庭院),并且它可以不断连接扩大至全球。美国国家标准和技术学会(NIST)给出的智能

*)国家自然科学基金(60403027);湖北省自然科学基金(2005ABA243)。

空间的定义是一个嵌入了计算、信息设备和多模态的传感器的工作空间。其目的是使用户能非常方便地在其中访问信息和获得计算机的服务[9]。

智能空间通过将计算设施嵌入建筑设施，融合了信息世界和物理世界。智能空间的研究最终目标是使之能够理解用户的意图，变为我们生活的一个组成部分。具体地讲，智能空间应具备的功能和为用户提供的服务包括：

·能识别和感知用户以及他们的动作和目的，理解和预测用户在完成任务过程中的需要；

·用户能方便地与各种信息源进行交互；

·用户携带的移动设备可以无缝地与智能空间的基础设施交互；

·提供丰富的信息显示；

·提供对发生在智能空间中的经历(experience)的记录，以便在以后检索回放；

·支持空间中多人的协同工作以及与远程用户的协同工作。

(2)不可见性：这是 Weiser 所指的用户意识上的“消失”，也就是减少用户在完成任务时精力的分散。让用户几乎可以在下意识水平上进行交互。当前的计算模式，计算机仍然是关注的焦点，这时的计算机不是一个好的工具。一种好的工具是不可见的工具，其含意是这一工具并不进入你的意识，你只是专注于任务而非工具。当然，工具本身不是不可见的，它只是使用工具这一场景中的一个部分。

(3)局部可扩展性：随着智能空间复杂程度的提高，用户个人计算空间与其周围环境的交互作用密度增加。对无线移动用户存在严重的带宽、能耗和精力分散等问题，多用户的存在更增加了问题的复杂性。因此，从广义上讲，可扩展性是普适计算的关键问题。以前关于可扩展性研究是不考虑物理距离的，但普适计算不同，交互密度应该随用户的移出必须降低。

(4)屏蔽非均衡条件(Masking Uneven Condition)：将普适计算技术渗透到基础设施中，很大程度上取决于一些非技术因素。例如取决于组织结构、经济和商业模型等。完全融合入需要一个过程，目前将会出现的不同环境的“智能性”存在巨大的差别。这种“智能性”的差别会影响普适计算实现不可见的目标，因此需要屏蔽这种不均衡状态。

3 普适计算的特点

普适计算的本质就是全面实现计算技术的“以人为本”，使计算像“空气”一样无处不在地融入人们的生活之中。普适计算具有以下特点：

(1)扩充了计算界限：传统的计算包括软硬实体，而普适计算扩充了计算界限，它包括物理空间，建筑软件基础设施以及所包含的设备。

(2)看不见和无干扰：当前的计算模式，计算机仍然是关注的焦点，普适计算环境中，计算设备是不可见的，并且是无干扰地使用这些设备，也就是人们能将自己的精力集中在完成自己的任务上，而不是集中在如何使用计算机上。

(3)无所不在性：用户可以随地以各种接入手段进入同一信息世界。无处不在的计算设备广泛分布在我们生活和工作环境的周围，无声无息地为人们提供服务。

(4)移动性：用户和计算均可按需自由移动。

(5)自适应的：计算和通信服务可按用户需要和运行条件提供充分的灵活性和自主性；它能够自己适应资源缺乏的环境，并且当更多的资源可以获得时，也能够进行扩展。

(6)永恒的：系统在开启以后再也不会死机或需要重起。

(7)智能空间：看不见的嵌入设备和传感器的联合使物理空间变为智能空间，智能空间能够看见、听见和感知空间内发生的事情，最终并能够理解用户的意图。

(8)上下文感知：一个普适计算环境能够获得不同的上下文和状态信息，这是普适计算能够理解用户意图和服务于用户的必要条件。

4 普适计算面临的安全挑战

从普适计算固有的特性看，传统的安全机制将不能适用于普适计算环境。下面用三个普适计算的场景来说明这个问题。

场景一：教授 Bob 回到自己的办公室，办公室的门检测到 Bob 的移动设备和设备的使用者后自动打开。同样，办公室里的设备通过认证 Bob 会主动提供一些服务，如打开桌上台灯，给 Bob 订购咖啡等等。Bob 也可以使用自己的移动设备通过无线连接，“命令”室内打印机帮自己打印一份文件。当教授 Bob 走出办公室，他得到的服务会受到限制，如不能使用打印机。当学生 Alice 使用 Bob 的移动设备时，她不能得到一些服务，如办公室的门不会为她打开，但她可以获得基本的服务，如使用移动设备订购免费咖啡。

这个场景描述了普适服务和受限的普适服务。它的安全要求是：

(1)能够保护教授 Bob 的个人隐私。

(2)能够认证用户以及对用户进行自动动态授权。

系统对教授提供服务，必须检测教授的上下文信息，但是这个上下文信息可能对教授的个人隐私造成了潜在的威胁。能否保证这些信息不被恶意地利用是普适计算成功实施的一个关键问题。在普适环境中，对用户提供的普适服务是动态的，传统的访问控制无法满足这个要求。

场景二：假设教授 Bob 在飞机场使用 PDA 无线连接一台公用打印机，希望打印一份机密文件。它的安全要求是：

(1)Bob 的 PDA 传输的加密文件只能传给教授所选择的打印机；

(2)打印机能够保证不让其他用户访问该数据，打印结束后应该立即删除该机密文件。

对于第一个安全要求，传统的认证要求 Bob 必须知道打印机的公钥，或者通过确定打印机的名字，然后从 CA 签发的证书中得到打印机的公钥。也就是说在任何地方必须有公钥基础设施，每个设备都有唯一的名字，并且有信任的权威机构签署的证书，这是极端不现实和不可能的。即使有这样的基础设施可以发现你需要的打印机的名字，也很难确保一个任意设备所声称的名字的真实性。对于第二个要求的关键是打印机应该是值得信赖的。知道打印机的名字不能确保设备是否可信。

场景三：教授 Bob 和一些行业代表用移动设备构建 Ad Hoc 网，传输一些机密文件。它的安全问题是：

(1)事先不认识的用户如何构成一个安全的网络；

(2)当一个用户在任意一个地方使用不同的设备，如何判断该设备不会泄露用户的秘密。

(3)同一个用户可能与不同的用户组成几个不同的自组网，如何安全地保证该用户与不同的用户交换不同的数据。

第一个问题涉及如何在陌生人之间建立信任关系；第二

个问题是如何判断设备的可信性;第三个问题是如何建立不同的信任关系。传统的认证无法回答这三个问题。

从上面三个场景可以看到,保证普适计算的安全是普适计算成功实施的关键。普适计算的安全问题具有新的特点,它需要新的方法来解决。传统的安全机制不适用的主要原因是它只是针对一个封闭的中心管理的安全域而言,系统根据访问策略和用户身份给予或者拒绝用户访问某些资源。它的基本假设是系统中的主体已经知道,所以信任根据每个主体的身份很容易建立起来。而普适计算环境是变化的和预先不可知的,如(1)环境对用户不熟悉,用户与环境的拥有者不存在信任关系;(2)数据常常动态地产生;(3)用户的访问权限动态变化;(4)系统是典型分散的。显然基于中心管理的安全机制不再适用。当前信任管理系统通过使用信任书委托权限来管理大规模分布式网络的安全,它直接将完成特定任务的权限与公钥绑定,不要求知道公钥的持有者是谁。但是这些系统实际上已经蕴涵了信任关系。当前一些信任模型能够解决一些特殊的应用安全问题,但它们不能很好地适用于普适计算环境。它们或者不能反映信任的动态性;或者已经蕴涵了信任;或者不能回答如何在陌生主体之间建立最初的信任;或者存在可操作性差等问题。

5 普适计算安全的关键技术

保证普适计算安全需要解决下面几个关键问题:

(1)动态信任模型

安全服务均建立在信任的基础上。经典安全模型主要依赖周边防御措施以及静态的信任关系。它定义了一个严格的网络边界,使用防火墙加强这个边界的安全,并且系统中的用户是假设事先登记注册的,因此认证和访问控制是以用户的身份为中心的。在普适环境中,上面的假设不能成立。普适计算扩展了传统计算的界限,并且信任关系是动态的,用户社区可能是匿名的、经常变化的,这些特点使预先登记注册方式是不能工作的,用户的身份不可能知道。普适计算不存在周边安全防御机制和静态的信任关系,因此建立动态信任关系是保证普适计算安全的最关键要求。普适计算信任模型至少应该能够体现信任的动态性,能够解决陌生实体之间的信任问题。

(2)认证

进行安全通信的前提是要保证双方的身份是合法的和真实的,这样才能在彼此信任的基础上开展对话,才能保证相互间信息传输的保密性和安全性。传统的认证是基于信任的第三方,认证的目的是区分授权的和没有授权的用户。因此可以用一些身份信息,如用户名、口令或者身份证书来认证一个实体是否应该信任。但是普适计算中不存在事先的关系。

普适环境的认证机制还应该权衡认证强度和无干扰性,如一个智能徽章能够广播近距离的射频信号,它是一个很好的无干扰的认证机制。但是它只能提供弱认证,一个 challenge-response 机制能够提供强认证。但是也带来了额外的交互代价。传统认证机制对用户干扰性较大,如常常需要用户输入口令。普适计算的宗旨是使人的注意力集中在用户的任务上,尽量不分散人的注意力。因此,普适计算的认证需要能以透明、非干扰性的方式来认证用户。传统认证方法建立在已经存在的信任基础上,普适计算不存在事先的信任关系,因此将动态信任模型与传统认证方法相结合是普适计算认证的一个解决思路。

(3)访问控制

普适计算一个主要特征是用户和资源之间有更丰富的交互界面,可以使用多种多媒体的输入输出方式,参与智能空间的运行操作和管理维护。由于用户交互方式的性质,智能空间不太可能轻易地防止用户"看见"和"听到"空间中所发生的与该用户无权访问的信息和资源。因此,在设计访问控制机制时必须考虑用户交互问题。需要实施适当的访问控制策略,防止非授权的资源被使用。访问控制机制应该同时考虑信息空间和物理空间的特点,这里的访问控制决定还可能依赖于时间或者其他特别的情况,也就是说访问控制决定常常是动态的。另外访问控制在某种程度上来说也应该是透明的,它的引入不会过分地引起用户太多的注意。基于角色的访问控制是比较有效的访问控制方法,但它的前提条件也是实体之间已经存在信任关系,如果将动态信任模型与基于角色的访问控制模型结合,用信任动态调整角色的权限将可能是一种解决普适计算访问控制的一个方向。

(4)隐私保护

普适计算环境要为在其中的用户提供服务,首先要作的就是收集用户相关的信息。这些信息就是所谓的"5W"信息,即 who, what, where, when, why。这些信息对用户来说是他们的隐私信息。如果计算系统的安全性得不到保证,就会导致用户隐私暴露给系统入侵者。如果不能解决这个问题,整个普适计算系统就成了一个分布式监视系统,跟踪捕获用户的所有隐秘信息。保护用户隐私又带来新的问题,普适环境中的智能设备并不是对任何用户提供所有的服务,有些服务只能提供给授权的用户,因此智能设备必须对用户进行认证,认证又需要用户的一些信息,因此认证和用户隐私保护常常是对立的,并且由于普适环境的分布性,异构性以及存在大量的不同应用,因此在普适环境中的隐私问题比传统环境更复杂。在两个设备之间同时进行认证和隐私保护是很困难的,如果借助一个第三方(如普适服务发现者)就可能满足要求。如用服务发现者对用户进行认证,然后用户使用服务发现者提供的凭证访问服务,这时服务提供者不能获得用户的信息。

(5)安全均衡

在保证普适计算安全的同时也要考虑其他的一些问题。一方面要考虑安全与资源限制的均衡。普适计算中的操作是常常是资源受限的,普适计算环境传感器众多,并且很大程度依赖无线通信。传感器计算平台是资源限制的,如限制的计算能力,限制的能量以及限制的存储设备。无线媒体具有很有限的带宽和吞吐量。这些因素严重地限制了安全机制中使用的密码操作的类型、安全协议以及安全机制。另一方面要考虑安全和其他服务的均衡。普适计算包含多种类型的应用以及数据处理要求。每个应用领域应该提高多种服务属性的权衡,如这些属性包含安全、隐私、可用性、服务质量以及代价,因此设计安全模型是应该考虑这些属性的权衡。

结论 安全是普适计算能否成功实施的关键问题。普适计算具有的无处不在性和移动性决定了传统安全机制不能用于普适环境。本文分析了普适计算面临的安全挑战以及需要解决的关键问题。但是这些关键问题并不是独立的,它们是紧密相关的。动态信任模型是安全服务的基础,认证、访问控制和隐私保护是建立在信任的基础上的。如何有效地把它们联合起来,提供一体的安全机制是将来要研究的问题。

(下转第 12 页)

面对的难题，为此应该对现有的各种覆盖多播路由协议和算法进行全面的、定量的比较研究，以便在性能和开销之间寻找最佳平衡点；其次，目前的覆盖多播路由协议和算法所涉及的路由性能参数相对比较简单，还缺乏对多 QoS 约束的覆盖多播路由问题的研究。特别是，当考虑到系统的异构性时，上述问题将更为复杂；最后，覆盖多播路由的可用性问题（例如，如何适应网络环境的动态变化、如何快速修复路由分裂以及防范恶意攻击等）也同样需要重视并进一步研究。

参 考 文 献

1 Diot C, Levine BN, Lyles B, et al. Deployment Issues for the IP Multicast Service and Architecture [J]. IEEE Network, 2000, 14 (1): 78～88

2 El-Sayed A, Roca V. A Survey of Proposals for an Alternative Group Communication Service [J]. IEEE Network, Jan/Feb 2003. 2～7

3 Banerjee S, Bhattacharjee B. A Comparative Study of Application Layer Multicast Protocols [A]. In: submitted for review, 2002

4 Hassin R, Tamir A. On the minimum diameter spanning tree problem [J]. Inform Processing Lett, 1995, 53: 109～111

5 Wang Z, Crowcroft J. QoS Routing for Supporting Resource Reservation [J]. IEEE Journal on Selected Areas in Communications, 1996, 14(7): 1228～1234

6 Salama H F, Reeves D S, Viniotis Y. The Delay-constrained Minimum Spanning Tree Problem [A]. In: Proceedings of the International Symposium on Computers and Communications (ISCC '97) [C], June 1997

7 Garg N, Khandekar R, Kunal K, et al. Bandwidth Maximization in Multicasting. In: Proceedings of the 11th Annual European Symposium on Algorithms, September 2003. 242～253

8 Banerjee S, Kommareddy C, Kar K, et al. Construction of an Efficient Overlay Multicast Infrastructure for Real-time Applications [A]. In: Proceedings of the IEEE INFOCOM [C]. San Franciso, 2002. 1521～1531

9 Shi S, Turner J. Multicast Routing and Bandwidth Dimensioning in overlay networks [J]. IEEE Journal on Selected Areas in Communications, 2002, 20(8): 1444～1455

10 Bauer F, Verma A. Degree-constrained multicasting in point-to-point networks [A]. In: Proceedings of IEEE Infocom'95 [C], 1995. 369～376

11 吴家皋，叶晓国，姜爱全. 一种异构环境下覆盖多播网络路由算法. 软件学报，2005，16(6)：1112～1120

12 Malouch N M, Liu Z, Rubenstein D, et al. A Graph Theoretic Approach to Bounding Delay in Proxy-Assisted, End-System Multicast [A]. In: Proceedings of ACM NOSSDAV' 02 [C], 2002

13 Pendarakis D, Shi S, Verma D, et al. ALMI: An Application Level Multicast Infrastructure [A]. In: Proceedings of the 3rd USENIX Symposium on Internet Technologies & Systems [C], San Francisco, 2001. 49～60

14 Chu YH, Rao SG, Zhang H. A Case for End System Multicast [A]. In: Proceedings of the ACM SIGMETRICS [C]. Santa Clara, 2002. 1～12

15 Chu Y H, Rao S G, Seshan S, et al. Enabling Conferencing Applications on the Internet using an Overlay Multicast Architecture [A]. In: Proceedings of ACM SIGCOMM [C], 2001. 55～67

16 Chawathe Y. Scattercast: An Architecture for Internet Broadcast Distribution as an Infrastructure Service: [Ph D Thesis]. University of California, Berkeley, 2000

17 Francis P. Yoid: Extending the Multicast Internet Architecture: [Technical Report]. Berkeley: AT&T Center for Internet Research at ICSI (ACIRI), 2000. http:// www. aciri. org/yoid/

18 Jannotti J, Gifford D, Johnson K, et al. Overcast: Reliable Multicasting with an Overlay Network [A]. In: Proceedings of 4th Symposium on Operating Systems Design and Implementation [C], 2000. 197～212

19 Kim M S, Lam S S, Lee D Y. Optimal Distribution Tree for Internet Streaming Media [A]. In: Proceedings of the 23rd IEEE ICDCS [C], May 2003

20 Helder DA, Jamin S. End-host Multicast Communication Using Switch-trees Protocols [A]. In: Proceedings of 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'02) [C], 2002. 419～424

21 Zhang B, Jamin S, Zhang L. Host multicast: A framework for delivering multicast to end users [A]. In: Proceedings of the IEEE INFOCOM 2002 [C], New York, 2002. 1366～1375

22 Li Z, Mohapatra P. HostCast: A New Overlay Multicasting Protocol [A]. In: Proceedings of IEEE Int. Communications Conference (ICC) [C]. Alaska, 2003. 702～706

23 Mathy L, Canonico R, Hutchison D. An Overlay Tree Building Control Protocol [A]. In: Proceedings of 3rd Int Workshop on Networked Group Communication [C], London, 2001. 78～87

24 Banerjee S, Bhattacharjee B, Kommareddy C. Scalable Application Layer Multicast [A]. In: Proceedings of ACM SIGCOMM '02 [C], 2002. 205～217

25 Tran D A, Hua K A, Do T T. ZIGZAG: An Efficient Peer-to-Peer Scheme for Media Streaming [A]. In: Proceedings of IEEE INFOCOM 2003 [C], 2003

26 Druschel P, Castro M, Kermarrec A, et al. Scribe: A large-scale and decentralized application-level multicast infrastructure [J]. IEEE Journal on Selected Areas in Communications, 2002, 20 (8): 1489～1499

27 Ratnasamy S, Handley M, Karp R, et al. Applicationlevel multicast using content-addressable networks [A]. In: Proceedings of 3rd Int. Workshop on Networked Group Communication [C], London, 2001. 14～29

28 Zhuang S Q, Zhao B Y, Joseph A D, et al. Bayeux: An architecture for scalable and fault-tolerant widearea data dissemination [A]. In: Proceedings of Eleventh International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2001) [C], 2001. 14～29

29 Roca V, El-sayed A. A host-based Multicast (hbm) Solutionfor Group Communications [A]. In: Proceedings of 1st IEEE Int Conf Networking [C], 2001. 610～619

30 Kwon M, Fahmy S. Topology-Aware Overlay Networks for Group Communication [A]. In: Proceedings of ACM NOSSDAV' 02 [C], 2002. 127～136

（上接第 3 页）

参 考 文 献

1 Weiser M. The computer for the twenty-first century. Scientific American, 1991, 265 (3): 94～104

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 Coen MH, Phillips B, Warshawsky N, et al. Meeting the computational needs of intelligent environments: the metaglue system. In: Nixon P, Lacey G, Dobson S eds. Proceedings of the 1st International Workshop on Managing Interactions in Smart Environments. Berlin: Springer-Verlag, 1999. 201～212

4 Iachellov G, Abowd G D. Security requirements for environmental sensing technology. In: Proceedings of the 2nd Workshop on Ubicomp Security, Seattle, USA, 2003

5 Ranganathan K. Trustworthy pervasive computing: the hard security problems. In: Proceedings of the 2nd IEEE Conference on Pervasive Computing and Communications Workshops. Washington: IEEE Computer Society, 2004. 117～121

6 Lahlou S, Langheinrich M, Röcker C. Privacy and trust issues with invisible computers. Communications of the ACM, 2005, 48 (3): 59～60

7 Creese S, Goldsmith M, Roscoe B, et al. Research directions for trust and security in human-centric computing. In: Proceedings of the First Workshop on Security and Privacy in Pervasive Computing. Vienna, Austria, 2004

8 Satyanarayanan M. Pervasive computing: vision and challenges. IEEE Personal Communication, 2001, 8(4): 10～17

9 Rosenthal L, Stanford V. NIST information technology laboratory pervasive computing initiative. In: Proceedings of the IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Washington: IEEE Computer Society Press, 2000. 30～36