普适计算的信任认证*)

郭亚军[1,2] 洪 帆[2] 叶俊民[1] 邱珊珊[1] 宋建华[2] 洪 亮[2]

(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 在普适计算环境中,用户能够在任何时间、任何地点访问资源,获得服务。但是这种无处不在性和移动性的环境带来了新的安全问题。资源的拥有者和请求者一般互相不知道。认证是安全的基石,没有认证,系统的保密性、完整性和可用性都将受到影响。可是传统认证是基于身份的认证,不适合普适环境中对陌生实体的认证。本文在分析普适计算的认证要求后,指出了在普适计算环境中应该先在陌生的实体间建立信任关系,然后可以用几乎所有的标准密钥交换协议进行安全认证。提出了用资源限制信任协商技术在陌生人之间建立信任关系。由于它避免了大量的公钥密码操作所带来的计算负担,因此比较适合计算能力有限的设备之间建立信任关系。

关键词 普适计算,资源限制信任协商,认证

Trust Authentication in Pervasive Computing

GUO Ya-Jun[1,2] HONG Fan[2] YE Jun-Min[1] QIU Shan-Shan[1] SONG Jian-Hua[2] HONG Liang[2]

(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 Users can access resources and obtain services anytime and anywhere in pervasive computing environment. However, the ubiquitous and mobile environment presents a new security challenge. The resource owner and requestor do not foreknow each other. Authentication is the footstone of security. Without authentication, confidentiality, integrality and availability of a system will be affacted. It is unsuitable for pervasive computing environment which entities are strangers to use traditional identity-based authentication. In this paper, after analyzing the requirements of authentication that pervasive computing need, we indicate that authentication in pervasive computing is firstly to establish trust relationship. Then secure authentication is achieved using almost any traditional authentication key exchange protocols. The resource-constrained trust negotiation method is presented to established trust relationship among strangers. Owing to avoiding the heavy computational demands the public key cryptography operations bring about, resource-constrained trust negotiation is well-suited for resource constrained devices to negotiate trust in pervasive computing environment.

Keywords Pervasive computing, Resource-constrained trust negotiation, Authentication

普适计算[1]环境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、透明地获得数字化的服务。但是在这种具有无处不在性和移动性的环境带来了新的安全问题。在该环境中资源的拥有者和请求者一般互相不知道。传统的安全机制是针对静态网络或者封闭系统,系统中已经明确了授权的用户,建立了这些用户的权限与系统资源的关系,阻止没有授权的用户访问这些资源。它基本上假设系统中的实体已经知道,所以根据每个实体的身份很容易建立起信任。这种系统的认证可以建立在资源请求者的身份基础上。如果当双方互相不知道时,基于身份的安全认证显然是不可行的。本文在分析普适计算的认证要求后,指出了在普适计算环境中应该先在陌生的实体间建立信任关系,再用几乎所有的标准密钥交换协议进行安全认证。自动信任协商[9~12]是一种新的基于属性认证的访问控制技术。陌生的双方之间通过反复呈现信任书(credential)和要求信任书逐步建立信任关系。但是信任协商使用公开密钥密码体制,不适合计算能力有限的普适计算设备。在此基础上我们提出了资源限制信任协商(RCTN)方法,陌生的双方仅仅交换一次信任书,用 hash 函数验证信任书中的属性,用对称密码保护敏感属性。它避免了大量的公钥密码操作所带来的计算负担,比较适合普适计算的认证要求。

1 普适计算的认证要求

普适计算环境与传统的计算环境的本质区别是:前者是动态的系统,后者是静态、封闭的系统。在封闭的系统中,已经知道授权的用户,并建立了这些用户的权限与系统资源的关系,在这样的系统中实际上已经存在了信任关系。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。显然在普适环境中不能用同样的身份信息来进行实体间的认证。下面我们借助两个普适计算环境实例说明普适计算环境的认证要求。

第一个例子是我们使用 Balfanz[2] 的例子。假设用户在公共环境使用 PDA 无线连接一台公用打印机,打印一份机密文件。它的安全要求是:

· 用户的 PDA 传输的加密文件只能传给用户选择的打

*)基金项目:国家自然科学基金项目(60403027),湖北省自然科学基金项目(2005ABA243)。

印机；

• 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，传统的认证要求用户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，并且有你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。这种基于名字解析的认证方法不适合于普适环境。对于第二个要求的关键是打印机应该是值得信赖的，但知道打印机的名字不能确保设备是否可信。

第二个例子是不同的用户用自己的 PDA 构成一个安全无线自组网。问题是：

• 事先不认识的用户如何构成一个安全的网络；

• 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。

• 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。

上面的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 3 个问题。通过上面两个应用实例我们认为普适计算的认证需要达到下面的要求：

• 普适计算的认证是信任的认证。认证是建立在信任的基础上，陌生的实体之间首先要建立充足的信任。只是认证不能保证自己的安全，安全还取决于实体的信任程度。用户通过认证后可以访问机密数据，但数据是否安全取决于用户是不是可以信赖的。

• 普适计算的认证是基于属性的认证。在普适环境中信任是与属性（如位置、时间、设备类型等）相关的，与身份联系很少。通过认证各种属性，确定设备能够做什么。例如知道一个人的毕业学校和所学的专业（属性）可以判断他能够做什么，但知道一个人的名字（身份）不能判断他的能力。

• 普适计算中大量使用的设备是移动设备和嵌入式设备，这些设备具有有限的计算能力，因此普适计算的认证尽量少使用计算任务大的公开密钥算法。

2 相关工作介绍

Kerberos[3] 是典型的认证协议，使用对称密码的间接认证方法，可预防客户方和服务方身份的伪造，能够检测重放攻击，并且可以相互认证。但 Kerberos 是基于身份的认证，用户必须登录网上的一些工作站，通过工作站访问分布式服务。Kerberos 假设客户机是值得信任的，容许客户机存储和使用用户的通行票，没有考虑用户的隐私，显然不适合普适环境中的认证。

Pirzada 等[4] 扩展了 Kerberos 协议，使之适合无线自组网的安全认证。该协议使用分布式认证方法，防止了 Kerberos 协议单点失效问题。所有的服务器都保存了所有用户的口令的 hash 值，所有的服务器共享同一个密钥，它们定期地相互复制所有用户的口令的 hash 值。但它是基于用户身份的认证，不适合普适计算的认证。

Asokan 等[5] 回答了在一个封闭的会议室建立无线自组网的认证问题。它首先利用大家一致同意的一个口令（弱密码），然后把口令输入他们的 PAD 中，使用协议产生一致的密码（强密码）。这是通过物理接触获得共同的口令，再得到一致的密码。这里的信任来自于大家都在一个房间里，彼此可以看见。信任是基于位置和人的接触，不是基于身份。陌生人加入该网需要认证，需要提供关于自己和设备的证书。它巧妙地把人类的信任转化为电子信任，适合小范围的认证。

Stajano 的复苏小鸭子安全模型[6,7] 中，基本认证问题是在两个实体间建立主仆关系的安全短暂联系。该模型中，小鸭子是从设备，母亲鸭子是主控制器，小鸭子被它的母亲通过安全通道传送密钥来识别，如用物理接触，这个过程称为烙印（imprinting）。小鸭子总是服从它的母亲。它适合计算能力较弱的设备进行公钥交换。该模型由主仆关系构成树型拓扑结构。树根是人类，它控制所有设备，中间结点控制其子树的所有设备。这种由全局母亲鸭子和局部母亲鸭子构成的层次结构类似于公钥基础设施，也存在与 PKI 类似的优缺点。

Smetters 等[2] 提出了类似复苏小鸭子安全模型的认证方法。该认证方法使用两个通道：一个称为位置限制通道，这个通道的认证过程称为预认证；另一个是主通道，完成数据交换。首先与待认证的设备进行物理接触（位置限制通道），交换公钥，然后用 PDA 通过无线网（如 Bluetooth or IEEE 802.11）与设备执行标准的 SSL/TLS 密钥交换协议。由于安全地鉴别了设备的公钥，因此数据是发往指定的设备，并建立起秘密通道。该方法是设备通过辅助通道交换有限的公钥信息，然后通过无线连接完成认证密钥交换协议。所以它不需要公钥基础设施，但其本质是基于身份的认证，不能保证设备本身的可信性。

Kagal 等[8] 没有明确提出认证概念，陌生的用户必须与已经注册的用户建立信任关系，然后已经注册的用户通过基于信任书的委托允许未注册的用户访问某些资源。认证是通过已经注册用户和陌生用户之间的信任关系实现。但没有说明如何建立两者之间的信任关系。

自动信任协商[9~12] 能够认证陌生用户。交互的双方为建立足够的信任，相互多次向对方呈现自己的数字信任书。信任书包含某些属性。自动信任协商是基于对方有什么（即有什么属性），而不是基于对方是谁（身份），因此信任协商是基于属性的认证。信任书由信任书发行者签名，证明信任书的拥有者具有哪些属性。访问控制策略控制访问服务、信任书或者策略本身等敏感资源。协商策略指明要访问一个特殊资源，对方应该呈现哪个信任书。由于协商的双方可能有敏感的证书和访问控制策略，因此信任协商可能需要多次要求证书和证书交换。所以称之为信任协商。由于信任协商是基于公钥体制，信任协商中使用的算法要求大量的密码计算，因此不适合计算能力较弱的普适计算设备。

Hess 等[10] 认为在 Internet 的商业交易中，交易的双方在大多数情况下是不认识的，TLS 是基于身份的认证，不适合陌生人之间的认证，因此他把信任协商应用到 TLS 中，集中了两者的优点，但是它需要更多的公钥密码计算，不适合普适计算认证。

Al-Muhtadi 等[13] 使用不同的可穿戴的或者嵌入式认证设备提供方便的保护用户隐私的认证。认证设备能够进行多

级信任度的认证，该认证主要是设备对用户的直接认证。

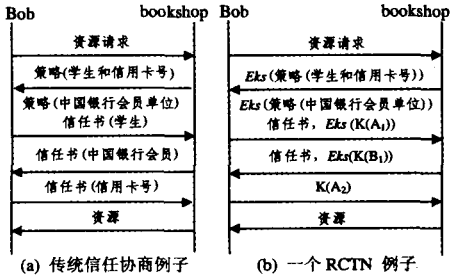
综上所述，目前的认证方法只能部分满足普适计算环境的认证要求，并且适用范围受到限制。

3 资源限制信任协商

传统的信任协商在陌生双方之间要进行多次的交换信任书和访问控制策略，因此信任书的验证和策略的一致性检验需要完成大量的计算任务。资源限制信任协商方法在陌生的双方仅仅交换一次信任书，随后多次交换对称密钥(用于解密敏感属性)。双方使用椭圆曲线密钥交换算法产生共同的会话钥 Ks，用该会话钥加密双方传输的信任书。但椭圆曲线密钥交换算法中公开的数字容易受中间人攻击，文[15]提出的方法可以借鉴用来防止对公开的数字进行中间人攻击。资源限制信任协商(RCTN)中的数字信任书与传统的信任协商中使用的信任书类似，用 X.509v3 证书实现。X.509v3 扩展提供了能够将多个属性绑定给一个证书。但是在资源限制信任协商的信任书中绑定的是加密属性，用随机产生密码 K_i 对信任书中每个敏感属性 A_i 加密，即 $EK_i(A_i)$。信任书用信任书发行者的私钥签名，由发行者的共钥验证。为了保证用户提供的加密属性的完整性，签名方需要对信任书中的属性进行如下验证：

- 用户用单向 hash 函数作用于加密后的属性 $E_{ki}(A_i)$，输出固定大小的 hash 码，即 hash($E_{ki}(A_i)$)。
- 用户向签名方传送 $EK_i(A_i)$和 hash($E_{ki}(A_i)$)。
- 签名方用同样的单向 hash 函数作用于 $EK_i(A_i)$；
- 签名方比较接收到的 hash 值和自己计算的 hash 值，二者相等，则可以验证属性的合法性。

下面的例子说明了传统信任协商和资源限制信任协商的区别。假设在线书店对高校学生提供打折销售。访问者 Bob 要求得到学生折扣，在线书店事先没有访问者 Bob 的信息。在线书店的安全策略是只给高校学生优惠，因此在线书店请求对方出具有高校学生的学生号以及银行信用卡号的信任书。Bob 的安全策略是信用卡号只能给中国银行会员单位看，因此 Bob 也要求对方显示具有该银行会员的信任书。对于传统信任协商而言，双方需要多次交换信任书，验证信任书以及判断信任书是否满足自己的安全策略，如图 1(a)所示。资源限制信任协商在双方交换一次信任书后，接着多次交换对称密码，用于逐步向对方显示自己的属性。如图 1(b)所示。



(a) 传统信任协商例子　(b) 一个 RCTN 例子

图 1

资源受限信任协商与传统的信任协商主要有如下区别：

- 在资源受限信任协商中双方只交换一次信任书，而传统的信任协商中双方需要经过多次交换信任书，因此资源受限信任协商所需要的计算任务小于传统的信任协商。
- 资源受限信任协商多次交换密钥是逐步向对方显示属性，因此在传统的信任协商中与信任书相关的访问控制策略和协商策略都改变成与属性相联系。

4 一种认证协议

资源限制信任协商能够在陌生实体间建立信任关系。当信任关系建立起来后，就可以使用一些安全密钥交换协议(如 TLS[14])建立安全通道：

A↔B：资源限制信任协商

A↔B：密钥交换协议

下面用 TLS 来说明这个过程。由于已经对 TLS 进行了扩充，因此容易将资源限制信任协商融合到该协议里。

TLS 支持保密性、数据完整性以及客户端和服务器端的认证。TLS 握手协议提供双方认证和安全参数的协商。2003 年 7 月传输层安全工作组对 TLS 进行了扩充[14]，扩展的目的是让 TLS 也能有效地工作在无线网络环境。TLS 扩充主要提供 client hello 和 server hello 消息的一般扩充机制，以及基于它的特殊扩充。一般扩充机制是为了使客户端和服务器端能够协商是否使用特殊的扩充以及如何使用特殊的扩充。在 client hello 消息里增加了 client_hello_extension_list 这个字段，它包含一个扩充列表。同样，在 server hello 消息里也增加了 server_hello_extension_list 与客户端相对应。我们使用这个扩充的 hello 消息，将资源限制信任协商融合到 TLS 中。扩展后的握手协议描述如下：

当一方(客户端)向另一方(服务器端)要求访问资源。如果客户端没有满足服务端的访问控制策略，服务器端向客户端发送 TrustNegotiationRequest 消息。如果客户端的 TLS 不支持信任协商，客户端将会终止协商。如果客户端接受信任协商，客户端向服务器端放送 ClientHello，在 client_hello_extension_list 这个字段增加协商同意以及协商策略列表。服务器端响应一个 ServerHello 消息，决定在会话中设置必要的参数。随后双方进行多次协商，服务器端向客户端发送 Credential，Policy，CredentialVerify 和 ServerDone 等消息。信任书是资源限制信任协商里使用的加密后的信任书。客户端向服务器端发送 Credential，Policy，CredentialVerify 和 ClientDone 等消息。这一轮以后双方交换密钥(用于解密敏感属性)，双方互相发送消息 Key，Policy，和 ClientDone(ServerDone)。由于双方只交换一次信任书，在后面协商阶段不必再次验证信任书。这个过程直到协商成功或者失败。随后由服务器方发送 TrustNegotiationDone 消息，表示协商结束。最后阶段，双方互相发送 ChangeCipherSpec 和 Finished 消息，建立安全的会话通道。与资源信任协商相关的，主要在握手协议的第一和第二阶段，如下所示：

阶段 1：建立安全能力

1. Client→Server：Resource Request
2. Server→Client：TrustNegotiationRequest
3. Client→Server：ClientHello
4. Server→Client：ServerHello

阶段 2：服务器端和客户端信任协商、互相认证以及交换密钥

5. Server→Client：Credential
6. Server→Client：CredentialVerify
7. Server→Client：Policy
8. Server→Client：ServerDone
9. Client→Server：Credential
10. Client→Server：CredentialVerify

(下转第 183 页)

Engine: Algorithm and Examples. Artificial Intelligence, 1989, 41:1～63
6 Lakoff G. The Contemporary Theory of Metaphor. In: Ortony A, ed. 2nd ed. Metaphor and Thought. Cambridge: Cambridge University Press, 1993. 202～251
7 Ahrens K. When Love is not Digested: Underlying Reasons for Source to Target Domain Pairing in the Contemporary Theory of Mataphor. In: Proceedings of the first Cognitive Linguistics Conference, Taipei, 2002
8 Searle J R. Metaphor. In: Ortony A, ed. 2nd ed. Metaphor and Thought. Cambridge: Cambridge Universtiy Press, 1993. 83～111
9 林书武. 国外隐喻研究综述. 外语教学与研究, 1997:1～12
10 冯晓虎. 隐喻——思维的基础 篇章的框架. 北京: 对外贸易大学出版社, 2004
11 胡壮麟. 认知隐喻学. 北京: 北京大学出版社, 2004
12 汤志群. 对一种比喻性语言:隐喻的理解机制的研究:[博士学位论文]. 北京: 北京师范大学, 1998
13 张威. 汉语语篇理解中元指代和隐喻的机器消解研究:[博士学位论文]. 杭州: 浙江大学, 2003
14 张威,周昌乐. 汉语隐喻理解的逻辑描述初探. 中文信息学报, 2004,18:23～28
15 杨芸,周昌乐. 基于机器理解的汉语隐喻分类研究初步. 中文信息学报, 2004. 18:31～36
16 Wilks Y. A preferential pattern-seeking semantics for natural language inference. Artificial Intelligence, 1975,6:53～74
17 Fass D. Met*: A Method for Discriminating Metonymy and Metaphor by Computer. Computational Linguistics, 1991,17:49～90
18 Fass D, Wilks Y. Preference Semantics, Ill-Formedness, and Metaphor. American Journal of Computational Linguistics, 1983, 9:178～187
19 Weiner E J. A Knowledge Representation Approach to Understanding Metaphors. Computational Linguistics, 1984,10:1～14
20 Martin J H. A Computational Model of Metaphor Interpretation. Boston: Academic Press, 1990,8
21 Martin J H. Representing UNIX Domain Metaphors. Artificial Intelligence Review, 2000,14:377～401
22 Veale T. Metaphor, Memory and Meaning: Symbolic and Connectionist Issues in Metaphor Interpretation: [PhD. Thesis]. Dublin: Trinity College, 1995
23 Sun R. A Microfeature Based Approach Towards Metaphor Interpretation. In: Proceedings of The International Joint Conference on Artificial Intelligence(IJCAI'95). California: Morgan Kaufmann, 1995. 424～430
24 Steinhart E C. The Logic of Metaphor: Analogous Parts of Possible Worlds. Dordrecht: Kluwer Academic Publishers, 2001
25 Kintsch W. Metaphor comprehension: A computational theory. Psychonomic Bulltin & Review, 2000,7:257～266
26 Kintsch W. Predication. Cognitive Science, 2001,25:173～202
27 Mason Z J. CorMet: A Computational, Corpus-Based Conventional Metaphor Extraction System. Computational Linguistics, 2004,30:23～44
28 Goatly A. The Language of Metaphors. London: Routledge, 1997
29 Fellbaum C. WordNet: an electronic lexical database. Cambridge: MIT Press, 1998
30 Russell S W. Book Review: A computational Model of Metaphor Interpretation. Metaphor and Symbolic Activity, 1996,11:169～174
31 周昌乐. 隐喻、类比逻辑与可能世界. 外国语言文学研究, 2004, 4:10～12
32 Fillmore C J. The Case for Case. In: Bach E, Harms R., Eds. Universals in Linguistic Theory, 1968. 1～88
33 Holyoak K J, Thagard P. Analogical Mapping by Constraint Satisfaction. Cognitive Science, 1989,13:295～355
34 Resnik P. Selection and Information: a Class Based Approach to Lexical Relationships: [PhD. Thesis]. Pennsylvania: University of Pennsylvania, 1993

(上接第 94 页)

11. Client→Server: Policy
12. Client→Server: ClientDone
13. Server→Client: Key
14. Server→Client: Policy
15. Server→Client: ServerDone
16. Client→Server: Key
17. Client→Server: Policy
18. Client→Server: ClientDone

13～18 步可能来回多次,直到满足各自的访问控制策略。

19. Server→Client: TrustNegotiationDone

5 安全性能分析

认证过程主要分两个阶段,即协商信任阶段和密钥交换阶段,协议的性能也取决这两个阶段。这里将不对具体的密钥交换协议进行分析。

对于资源信任协商而言, hash 函数具有单向性,所以属性不能伪造。另外对属性使用对称密码进行加密,属性具有保密性。在向对方出示第一个解密属性的密钥以后,接收方不能知道其他的属性值,接收方只能在发送方控制下逐步计算出属性值,因此双方可以控制自己的属性值的出示,保护自己的敏感属性。由于双方交互的消息是保密的,因此 RCTN 也防止了传统信任协商存在的中间人攻击问题。

该认证协议与传统认证协议主要区别是多了一个建立信任的过程,主要是由于传统认证协议是基于已经存在了信任关系这个隐含的条件。因此该认证过程要增加一定的计算量。但是在上面的例子里,在 TLS 中引入资源限制信任协商基本上没有增加额外的负担。

参 考 文 献

1 徐光祐,史元春,谢伟凯. 普适计算. 计算机学报, 2003, 26(9): 1042～1050
2 Balfanz D, Smetters D K, Stewart P, Wong H C. Talking to strangers: authentication in Ad-hoc wireless networks. In: the 9th Annual Network and Distributed System Security Symposium. San Diego, California, Feb. 2002
3 Kohl J, Neuman S. The kerberos network authentication service. IEIF RFC 1510, 1993
4 Pirzada A A, McDonald C. Kerberos assisted authentication in mobile Ad-hoc networks. In: Castro EV, ed. the 27th Conference on Australasian Computer Science. Dunedin, New Zealand, 2004, 26: 41～46
5 Asokan N, Ginzboorg P. Key agreement in Ad-hoc Networks. Computer Communications, 2000, 23(17):1627～1637
6 Stajano F, Anderson R. The resurrecting duckling: security issues for Ad hoc wireless networks. In: Christianson, B, Crispo B, Roe M, eds. The 7th IntL Workshop on Security Protocols, LNCS 1796, Springer-Verlag, 1999. 172～194
7 Stajano F. The resurrecting duckling - what next? In: The 8th IntL Workshop on Security Protocols, LNCS 2133, Springler-Verlag, Berlin Germany, April 2000. 204～214
8 Kagal L, Finin T, Joshi A. Trust-based security in pervasive computing environments. IEEE Computer, 2001, 34(12): 154～157
9 Winslett M, Yu T, Seamons K, Hess A, Jacobson J, Jarvis R, Smith B, Yu L. Trust negotiation on the Web. IEEE Internet Computing, 2002, 6(6): 30～37
10 Hess A, Jacobson J, Mills H, Wamsley R, Seamons K E, Smith B. Advanced client/server authentication in TLS. Network and Distributed System Security Symposium, San Diego, California, Feb. 2002
11 Hess A, Holt J, Jacobson J, Seamons K E. Content-triggered trust negotiation. ACM Transactions on Information and System Security, 2004, 7(3): 428～456
12 Jarvis R. Selective disclosure of credential content during trust negotiation. Master thesis, Department of Computer Science, Brigham Young University, 2003
13 Al-Muhtadi J, Ranganathan A, Campbell R, Mickunas MD. A flexible, privacy-preserving authentication framework for ubiquitous computing environments, In: the 22nd Intl Conference on Distributed Computing Systems Workshops 2002. 771～776
14 Blake-Wilson S, Nystrom M, Hopwood D, Mikkelsen J, Wright T. Transport layer security(TLS) extensions. IETF RFC 3546, June 2003
15 肖道举,郭杰, 陈晓苏. 一种对中间人攻击的防范策略的研究[J]. 计算机工程与科学, 2004, 26(9): 7～8