一种不依赖于协商策略的信任协商协议

李 开 李瑞轩 鲁剑锋 卢正鼎
(华中科技大学计算机科学与技术学院智能与分布计算实验室 武汉 430074)

摘 要 自动信任协商为开放环境中希望进行资源共享或业务协作的陌生双方提供了一种灵活的信任建立方法。然而现有自动信任协商系统之间不具备可互相操作性,首要原因是缺少一个统一的信任协商协议。提出了一种不依赖于协商策略的信任协商协议,将协议消息划分为资源请求、信息披露和终止协商3种类型并定义了消息的格式,阐明了协商过程的3种状态及状态之间的转化关系,同时给出了协议实现算法。分析表明,该协议支持包括多种格式信任证在内的数字断言和不同策略语言描述的访问控制策略的披露,允许在一次协商过程中使用多种协商策略进行协商,以满足不同应用场景的协商需求,因而具有明显的通用性。

关键词 自动信任协商,协商协议,协商策略,可互操作性
中图法分类号 TP309 **文献标识码** A

Strategy-independent Trust Negotiation Protocol

LI Kai LI Rui-xuan LU Jian-feng LU Zheng-ding
(Intelligent and Distributed Computing Laboratory, College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Automated trust negotiation is a flexible approach to establish mutual trust between strangers that wish to share resources or conduct business transactions in open environments. However, existing automated trust negotiation systems cannot interoperate with each other. The main reason is lack of a unified trust negotiation protocol. A strategy-independent trust negotiation protocol was presented. In the protocol, message was classified into three categories: resource request message, information disclosure message and ending negotiation message, and their form was defined. Three states of the negotiation process and the transformation between them wre illustrated, and the protocol algorithm was expressed using pseudo codes. The analysis indicates that the protocol supports the disclosure of digital assertions including credentials with various formats and access policies specified with different policy languages, and allows adopting manifold strategies in one negotiation process, and satisfies to negotiate in various application scenes, and is provided with distinct generality as a result.

Keywords Automated trust negotiation, Negotiation protocol, Negotiation strategy, Interoperability

1 引言

适应于Internet的发展趋势,跨越组织边界进行资源共享的大规模开放系统成为越来越普遍的计算模式,比如P2P网络、网格计算、机构重组的虚拟组织、电子商务、电子医疗保健等。与传统的分布式系统不同的是,开放系统中的资源是公共可访问的,系统的用户不再是特定的群体。由于潜在用户的规模巨大,而且用户与系统之间没有预先存在的信任关系,传统的基于身份的授权方法不适用于开放系统的授权服务[1]。自动信任协商(automated trust negotiation, ATN)技术以解决开放系统授权问题为目标,引起研究人员的广泛关注而成为当前研究的热点。目前,已经提出的具有代表性的几种ATN系统原型和框架有TrustBuilder[2], Trust-X[3], PeerTrust[4], COTN[5]等。这些系统各具特色,不同程度地体现了ATN系统的保密性、完备性和高效性。然而,由于所采用的协商策略各不相同,并且缺乏一个统一的协商协议,现有ATN系统之间无法相互操作。例如假定Alice和Bob是参与协商的两个实体。如果Alice和Bob使用相同的ATN系统,那么他们能够顺利进行协商,甚至最后可能建立某种级别的信任关系;如果Alice和Bob分别使用当前不同的ATN系统,那么他们之间根本无法进行协商。

ATN系统现有的研究通常都以这样一种假设条件为支

到稿日期:2010-01-12 返修日期:2010-03-04 本文受国家自然科学基金项目(60873225, 60773191, 70771043),国家高技术研究发展计划(863计划)项目(2007AA01Z403),软件工程国家重点实验室开放基金项目(SKLSE20080718),华中科技大学自主创新基金项目(01-09-210014)资助。

李 开(1968—),男,讲师,主要研究方向为分布式系统安全,E-mail:kli@hust.edu.cn;李瑞轩(1974—),男,博士,副教授,主要研究方向为分布式计算、分布式系统安全;鲁剑锋(1982—),男,博士生,主要研究方向为分布式系统访问控制;卢正鼎(1944—),男,教授,博士生导师,主要研究方向为分布式计算、软件集成环境、数据库系统、信息安全。

撑：协商双方使用相同 ATN 系统。显然，这种假设是不符合实际情况的。日益增长的网络服务以及数以亿计的网络用户，由于实体的高度自主性和需求的差异性，他们之中任何陌生双方为交互敏感信息而进行信任协商时大都会凭经验和喜好来选择使用自认为合适的 ATN 系统。为保证不同 ATN 系统能够进行交互，并且不影响协商结果（也就是说，双方采用同一种 ATN 系统能够成功建立信任的协商，不会因双方采用不相同的 ATN 系统而失败，反之亦然），首要工作是必须制定一个统一的协商协议。本文提出了一种不依赖于协商策略的信任协商协议，分析表明本协议独立于具体的协商策略，具有明显的通用性。为了叙述方便，本文将资源请求方称为用户，其协商代理称为用户系统；将资源提供方称为服务器，其协商代理称为服务器系统。

2 问题的提出

2.1 ATN 工作原理

为寻求在开放环境中的陌生实体之间建立信任关系的方法，2000 年 Winsborough 等人提出了 ATN 的概念[6]，随即引起研究人员的广泛关注。在大量的理论研究和技术探讨的基础上，研究人员提出了多个 ATN 系统原型和框架。总体来说，一个 ATN 系统主要包括 3 个部分：1）证书库、资源访问控制策略库及对证书库和访问控制策略库的读写进行安全保护的模块；2）协商策略模块；3）协商协议模块。

ATN 系统采用对等的体系结构，用户和服务器之间能否建立信任关系不由可信第三方（trusted third party，TTP）决定。虽然在验证信任证时需要 TTP 提供服务，但最终的信任决策由双方自主作出。ATN 系统工作原理如图 1 所示。

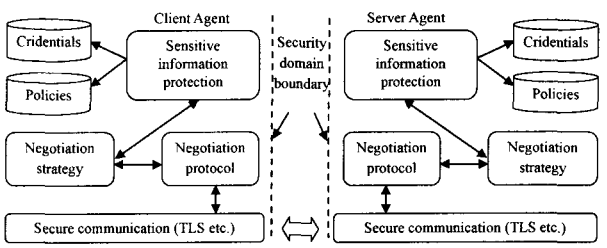


图 1 ATN 工作原理

2.2 协商策略与协商协议

协商策略用来控制所发送消息的具体内容，比如披露哪些信任证、在什么情况下披露它们以及何时终止协商等。

协商协议定义消息中所包含信息的类型以及消息发送的次序。

2.3 存在的问题

现有研究大多集中在协商策略的保密性和协商效率方面，而对协商协议的研究非常有限。协商协议的论述只是在分析所提出的协商策略性能时简单提及，协议定义的消息类型仅限于该协商策略所用，因而协商协议不能独立于所讨论的协商策略，不具备通用性。

3 不依赖于协商策略的信任协商协议

3.1 会话安全

本信任协商协议在通信上使用 TLS 协议作为传输层支撑，用户系统和服务器系统之间所有交互信息以数据篡改验证（tamper-proof）方式在 TLS 隧道内进行安全传送，以确保协商过程中会话内容的机密性和完整性。

3.2 消息类型

为控制用户系统和服务器系统之间敏感信息的流动，本协议支持 3 类消息：资源请求（Resource Request，RR）消息、信息披露（Information Disclosure，ID）消息和终止协商（Ending Negotiation，EN）消息。

每条消息由多个 ASCII 码文本行组成，消息长度不固定。每个文本行以一个换行符（'\n'，0x0a）作为结束标志，连续两个换行符（即一个空行）表示整条消息结束。消息的第一个文本行表明消息的类别，其余文本行为消息体。消息基本格式为：

```
TYPE={RR|ID|EN}
〈message_body_line_1〉
.....
〈message_body_line_n〉
〈blank line〉
```

下面分别说明 3 类消息的功能。

（1）RR 消息

RR 消息是协商过程的第一条消息，由用户系统发给服务器系统，起到触发协商开始的作用。

RR 消息中包含一个通用资源标志符（Universal Resource Identifier，URI）和一系列可选的用来描述用户所请求资源属性的〈属性名、属性值〉对。URI 命名机制极具灵活性，足以描述广泛多样的资源。被描述的资源可以是互联网上的任何一个子网，可以是任何域内的一个或多个角色，可以是某个主机或者部署在此主机上的一个或一组服务，也可以是方法调用等。RR 消息采用以下格式：

```
TYPE=RR                          //消息类型为 RR
〈resource URI〉                  //所请求资源的 URI
ATTRIB=(〈attribute〉,〈value〉)   //资源的属性
.....
ATTRIB=(〈attribute〉,〈value〉)
〈blank line〉
```

RR 消息中的 URI 指定了用户想要访问的资源。尽管 URI 可以采用 URN（Uniform Resource Name，统一资源名称）形式来描述更多种类的资源，但大多情况下，这里的 URI 采用 URL（Universal Resource Locator，统一资源定位符）来指定一个网络服务。

（2）ID 消息

ID 消息用来封装协商过程中一方披露给另一方的信息，对协商进程起到实质性的推进作用。

分析现有协商策略，协商过程中所披露的信息分为 4 种：1）用来证明持有人具有某种身份、属性、能力、声誉等特征的数字断言，包括各种类型的信任证及从信任证中提取出来的部分属性值等；2）协商对方所请求资源的访问控制策略；3）隐藏证书；4）协商约定，包括协商过程相关要求的约定（如信任证格式、最大协商轮数、可容忍的协商时间、可采用的加密算法及密钥等）。

一条 ID 消息中可以封装零条到多条上述 4 种类型的信息，每条信息的种类用 KIND 消息行来区分。以某协商方向对方披露一个信任证和一条访问控制策略为例，相应的 ID 消息内容如下：

```
TYPE=ID                          //消息类型为 ID
```

```
KIND=1                    //信息类型为数字断言
BEGIN_DECLARE
SORT=〈Credential〉        //数字断言为信任证
〈credential_data〉
……
〈credential_data〉
END_DECLARE
KIND=2                    //信息类型为访问策略
BEGIN_POLICY
LANGUAGE=〈DTPL〉          //策略语言为 DTPL
〈policy_content〉
……
〈policy_content〉
END_POLICY
〈blank line〉
```

不包含披露信息的 ID 消息表示没有进一步披露信息，这种空消息是必要的。大部分协商策略用一个或两个空消息表示协商失败。

(3) EN 消息

EN 消息是协商过程的最后一条消息，用来结束协商进程，返回协商结果。

协商成功时，服务器发给用户的 EN 消息中封装了准予用户访问所请求资源的授权，用一张票据(Ticket)来表示授权内容。授权内容与具体应用相关，一般包括用户的主体标志、所请求资源的 URI、对所请求资源的访问权限、权限的有效期以及服务器对授权内容的数字签名和签名证书等。例如，一次成功的协商最后的 EN 消息可表示为

```
TYPE=EN              //消息类型为 EN
BEGIN_TICKET
CLIENT_ID=〈ID of the client〉
URI=〈resource URI〉
PERMISSION=〈accessible〉
PERIOD_OF_VALIDITY=NOT BEFORE〈xxxx-xx-xx xx:xx:xx〉 NOT AFTER〈xxxx-xx-xx xx:xx:xx〉
ISSUER_ID=〈ID of the server〉
SIGNATURE=〈signature〉
END_TICKET
〈blank line〉
```

协商成功后，用户向服务器出示自己的信任证和从 EN 消息中解封的票据就可以访问所请求的资源。

如果协商失败，EN 消息中仅包含消息类别。

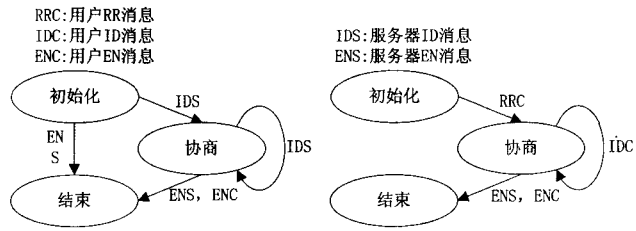
```
TYPE=EN
〈blank line〉
```

协商失败的 EN 消息既可以由用户发给服务器(用户认为服务器是虚假的，决定终止协商)，也可以由服务器发给用户(用户所请求资源的 URI 不正确，或用户披露的证书不满足所请求资源的访问控制策略，或用户披露伪造证书等)。

3.3 系统状态

协商过程中，系统的状态分为 3 种：初始化协商状态、协商状态和协商结束状态。从初始化协商状态开始，随着消息的发送和接收，系统的状态发生改变，直到协商结束状态。对系统而言，一个从初始化协商状态到协商结束状态的转变过程就是一次信任协商。

图 2 示例了系统状态变化和消息之间的关系。用户系统状态变化图中，ID_S 和 EN_S 分别表示从服务器系统收到 ID 消息和 EN 消息，EN_C 表示用户向服务器系统发送 EN 消息。服务器系统状态变化图中，RR_C、ID_C 和 EN_C 分别表示从客户系统收到 RR 消息、ID 消息和 EN 消息，EN_S 表示服务器向客户系统发送 EN 消息。由图 2 可以看出，用户系统和服务器系统处于协商状态时，都可以发送 ID 消息和 EN 消息；ID 消息不改变协商状态，而任何一方发出 EN 消息都可以使双方系统进入协商结束状态。



(a) 用户系统状态变化图　　(b) 服务器系统状态变化图

图 2 系统状态变化图

3.4 协议算法

算法 1 用伪代码描述了协议实现算法。其中调用了 3 个函数：*ReceiveMsg*()用来接收对方发送的消息，*SendMsg*(m)将消息 m 发给对方，*LocalStrategy*(M,L,R,m,A)使用本地协商策略生成回复消息。

算法 1 协议实现算法

```
NegotiateAgent(L,R,A)
输入：L 是本地资源集，包括本地可访问资源，信任证和相应访问控制策略
      R 是用户请求访问资源，服务器系统中初值为 Ø
      A 是本地协商配置参数表
输出：成功时返回授权票据，失败时返回 FAIL
变量：M 存放信息披露序列，初值为 Ø
      state 系统状态标志，取值 INIT，NEGO 和 ENDN
      m 存放接收和发送消息
1：state←INIT；//置初始化协商状态
2：If (R=Ø){ //对方是资源请求方
3：    m←ReceiveMsg()；//接收消息
4：    If (m.type=RR and m.URI∈L){//合法 RR 消息
5：        R←m.URI；
6：        state←NEGO；//置协商状态
7：        m←LocalStrategy(M,L,R,m,A)；}
           //调用本地协商策略生成回复消息
8：    Else{                    //不是合法 RR 消息
9：        m.type←EN；          //生成终止协商消息
10：       m.content←Ø；}
11：   If (m.type=EN) state←ENDN；
       //若回复消息类型为 EN 则置协商结束状态
12：   SendMsg(m)；} //发送回复消息
13：Else{ //本方为资源请求方
14：   m.type←RR；//生成资源请求消息
15：   m.URI←R； //用 URI 描述 R
16：   SendMsg(m)；//发送资源请求消息
17：   m←ReceiveMsg()；//接收消息
18：   If (m.type=ID){ //收到信息披露消息
19：       state←NEGO；//置协商状态
20：       m←LocalStrategy(M,L,R,m,A)；
           //调用本地协商策略生成回复消息
```

```
21:        If (m.type=EN) state←ENDN;
     //若回复消息类型为 EN 则置协商结束状态
22:        SendMsg(m);} //发送回复消息
23:    Else                    //收到终止协商消息
24:        state←ENDN;}    //置协商结束状态
25:While (state=NEGO){     //在协商状态
26:    m←ReceiveMsg();     //接收消息
27:    If (m.type=ID){     //收到信息披露消息
28:        m←LocalStrategy(M,L,R,m,A);
29:        SendMsg(m);
30:        If (m.type=EN) state←ENDN;}
31:    Else state←ENDN;}
32:If (m.content=∅) //终止协商消息内容为空
33:    return FAIL;//返回协商失败
34:Else
35:    return m.ticket;//返回授权票据
END of NegotiateAgent.
```

以上算法时间复杂度为 $O(M+N)$，其中 M 和 N 分别为双方最大信认证个数和访问控制策略条数。

4 分析与讨论

本协商协议的优越性主要体现在以下几个方面：

(1) 适用于不同应用场景的协商

现有研究中应用场景大部分是用户为请求访问某个单一的、离散的和具体的资源而展开协商。而实际应用中，服务器提供连续的、相互关联的和整体资源服务的情形并不少见。比如，开放系统在用户登录时需要先经过协商来确定用户能够访问哪些资源，然后将用户有权访问的资源组合起来，由用户选择访问，而不是在用户要求访问一个个具体资源时一次次地进行协商。本协议 RR 消息中用 URI 和一系列可选的属性可以描述广泛多样的不同规模和粒度的资源，可适应不同应用场景的协商需求。

(2) 支持多种协商策略和访问控制策略描述语言

本协议 ID 消息中封装的 4 种格式披露信息，能够描述现有协商策略所能处理的各种披露信息。比如，文献[5,7,8]中分别提出的契约、隐藏证书和 DL-TNL 语义身份断言等这些特定协商策略披露的信息都可以按 4 种格式分类描述并封装到 ID 消息中。同时，第三种格式披露的信息能够表达不同种类访问控制策略语言描述的访问策略。

(3) 允许在协商过程中同时使用多种协商策略

本协议对多种协商策略的支持不仅使不同协商策略之间的协商成为可能，而且允许协商策略模块在一次协商过程中灵活切换多种协商策略，可满足协商中随信任级别提升而调整协商性能的需求。

此外，由于协商成功后授权票据中包含了有效期，用户可以“一次协商多次使用”。而授权票据与用户主体标志进行绑定并提供服务器对授权的数字签名，一方面能防止授权票据被滥用，另一方面可保护用户免遭抵赖和欺骗。

结束语 本文提出的信任协商协议将消息分为 3 类，采用极具灵活性的 URI 命名机制描述广泛多样的资源，4 种披露信息格式能完全区分和表示现有协商策略所能处理的各种信息，因而使协议独立于具体的协商策略而具有明显的通用性。

参 考 文 献

[1] Lee A J, Winslett M, Basney J, et al. The Traust Authorization Service [J]. ACM Transactions on Information and System Security, 2008, 11(2): 1-33

[2] Smith B, Seamons K E, Jones M D. Responding to policies at runtime in TrustBuilder[C]// Proc. of the 5th Int'l Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2004: 149-158

[3] Bertino E, Ferrari E, Squicciarini A C. Trust-X: A Peer-to-Peer Framework for Trust Establishment[J]. IEEE Trans. Knowledge and Data Eng, 2004, 16(7): 827-842

[4] Nejdl W, Olmedilla D, Winslett M. PeerTrust: Automated trust negotiation for peers on the semantic Web[C]// Proc. of the Workshop on Secure Data Management in a Connected World (SDM 2004). LNCS 3178. Springer-Verlag, 2004: 118-132

[5] 李建欣，怀进鹏. COTN：基于契约的信任协商系统[J]. 计算机学报，2006，29(8)：1290-1300

[6] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation[C]// DARPA Information Survivability Conf. and Exposition. New York: IEEE Press, 2000: 88-102

[7] Holt J, Bradshaw R, Seamons K E, et al. Hidden credentials[C]// Jajodia S, Samarati P, Syverson PF, eds. Proc. of the 2003 ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2003: 1-8

[8] 张妍，冯登国. 吝啬语义信任协商[J]. 计算机学报，2009，32(10)：1989-2003

(上接第 6 页)

[37] Sjöberg M, Laaksonen J, Honkela T, et al. Inferring semantics from textual information in multimedia retrieval[J]. Neurocomputing, 2008, 71(13-15): 2576-2586

[38] Urban J, Jose J M. Adaptive image retrieval using a graph model for semantic feature integration[C]// 8th ACM International Workshop on Multimedia Information Retrieval MIR '06. Santa Barbara, CA, USA, October 2006: 117-126

[39] Luan Xi-dao, Xie Yu-xiang, Ying Long, et al. SATS: A News Story Detection Method Based on Multi-feature Fusion[J]. Journal of Information and Computational Science, 2008, 5(1): 267-274

[40] Liu Yuchi, Luan Xidao, Wu Lingda, et al. Narrative structure analysis of lecture videos with hierarchical hidden markov model for e-learning[C]// Technologies for E-Learning and Digital Entertainment. First Internation Conference, Edutainment 2006. Hangzhou, China, April 2006: 429-437

[41] 栾悉道，谢毓湘，应龙，等. 基于 EDU 模型的新闻视频摘要技术研究[J]. 系统仿真学报，2007，19(16)：3770-3774

[42] 庄越挺，吴聪苗，吴飞，等. 多媒体交叉参照检索系统研究[J]. 计算机辅助设计与图形学学报，2005，17(4)：834-839

[43] 鲍永生，任建峰，郭雷. 支持语义的图像检索[J]. 南京航空航天大学学报，2005，37(1)：75-78

[44] 丁国祥，吴仁炳，张振亚，等. 一种用于 MAM 的语义可扩展视频编目与检索方法[J]. 中国图象图形学报，2005，10(8)：1036-1041