一种面向信任管理的委托授权模型及其在 P2P 安全中的应用

张志勇[1,2] 裴庆祺[2] 杨 林[3]
(河南科技大学电子信息工程学院 洛阳 471003)[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[2]
(中国电子设备系统工程总公司研究所 北京 100141)[3]

摘 要 在信任管理中现有的委托授权模型并未涉及对角色、匿名用户等实体间信任关系的定义与度量,且缺少相关的细粒度形式化模型和委托授权安全协议其无法有效地满足信任管理系统的应用需求。现面向信任管理提出了一种能够刻画实体间信任关系的形式化委托授权模型 DAM for TM(Delegation Authorization Model for Trust Management),通过引入信任罚函数对实体的信任度量值加以动态调整。同时给出了支持可信计算的信任委托与角色委托等安全协议,以及在 P2P 安全中的应用实例。该实例表明,所提出的模型及安全协议构建了 Peer 间的信任委托关系,并通过终端完整性的远程证明确保了计算平台与共享资源的安全性。

关键词 信任管理,委托授权,远程证明,P2P 安全
中图法分类号 TP309 **文献标识码** A

Delegation Authorization Model for Trust Management and its Application in Peer-to-Peer Security

ZHANG Zhi-yong[1,2] PEI Qing-qi[2] YANG Lin[3]
(Electronic Information Engineering College, Henan University of Science & Technology, Luoyang 471003, China)[1]
(Ministry of Education Key Laboratory of Computer Network & Information Security, Xidian University, Xi'an 710071, China)[2]
(The Research Institute, China Electronic Equipment & Systems Engineering Corporation, Beijing 100141, China)[3]

Abstract In trust management existing delegation authorization models were not involved with the definition of trust relations and the trustworthiness measurements among entities, such as roles and anonymous users, and a fine-grained formalized model and relevant delegation authorization security protocols were also absent, as could not effectively satisfy the requirements of trust management system applications. A trust management oriented formalized model that depicts trust relationships among entities, which is called DAM for TM, was presented and trustworthiness measurement metrics of entities could be dynamically adjusted through introducing the trust punishment function. Also, the trust computing-enabling trust delegation and role delegation security protocols, and an application case in P2P security were also addressed. The case shows that the proposed model and security protocols constructed peers' trust delegation relations, and ensured the security of computing platforms and shared resources by the remote attestation on the terminal integrity.

Keywords Trust management, Delegation authorization, Remote attestation, Peer-to-Peer security

作为分布式计算环境下的访问控制研究对象,信任管理依赖于证书链机制与可传递性委托授权实现了系统对匿名、未知用户信任关系的管理和共享资源的访问控制,并支持分布式应用可伸缩的特点[1,2]。面对着大规模未知用、户开放、动态的公共访问和计算服务模式,委托授权和基于角色的策略的结合则是分布式计算机环境下解决集中式授权服务器负荷过重的有效方案[3]。

现有的基于角色的委托模型在分布式环境下基于认证用户的访问控制中得到了深入研究[4,5],尤其是在委托周期性[6]、委托约束[7]、角色的安全属性等方面进行了不断的扩展和完善。此外,Li 提出了一种描述信任管理中委托授权的逻辑语言[8]和基于角色的信任管理框架 RT[9]。然而,上述模型及架构并未涉及匿名的、未知用户之间委托授权的信任关系问题,因此不能有效地应用于信任管理系统中。文献[10]提出的基于信任度的委托授权模型 TBAD,使用信任度来刻画授权实体和被授权实体之间的信任程度,能够满足分布式开放环境中的信任管理,并有效地解决委托的深度控制问题。但是该模型缺少完整的委托授权形式化定义,同时并未涉及角色与信任度的关系,信任度仍然是和用户直接关联的,这在应用中无法体现角色实体的意义。因此,在信任管理中,一种

到稿日期:2008-11-11 返修日期:2009-08-04 本文受国家自然科学基金项目(60803150,60633020)资助。
张志勇(1975-),博士生,副教授,CCF 高级会员,主要研究方向为访问控制与信任管理、可信计算与可信网络,E-mail:xidianzzy@126.com;裴庆祺(1975-),博士,副教授,主要研究方向为无线网络安全与可信计算;杨 林(1970-),博士,研究员,博士生导师,主要研究方向为信息安全与系统安全。

具有实体信任度量的较为完备的委托授权模型是必要的。

1 形式化的面向信任管理的委托授权模型

1.1 DAM for TM 模型

DAM for TM 在基于角色的委托模型基础上,引入了对实体的信任度量以适用于信任管理系统,并将委托具体区分为信任委托和角色委托两个概念。前者是信任管理系统中所特有的,主要用于对匿名实体的授权过程中,基于信任和委托关系,从可信的第三方实体中获取对匿名实体的信任关系,以用来辅助决策,完成角色授权过程;而后者则类似于集中式系统中的委托机制,获得授权的实体可以进一步将授权转让,以完成角色和能力(权限)的传播。DAM for TM 中的角色授权及委托都是基于角色粒度的,这简化了基于许可或基于能力的授权的复杂性,减轻了服务器或授权实体的负担,更适用于开放的分布式计算系统。该模型如图 1 所示。

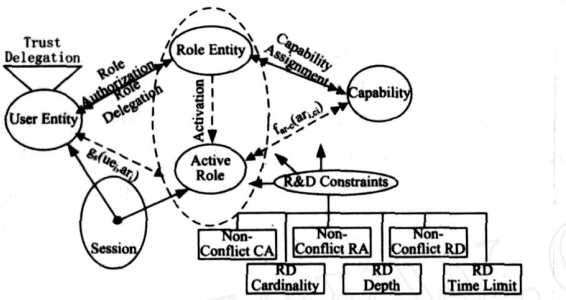

图 1 面向信任管理的委托授权模型(DAM for TM)

1.2 DAM for TM 基本组件

本节采用基本的集合论和谓词逻辑形式化模型。定义用户实体集 UE、角色实体集 RE、能力集 C、授权与委托约束集 RDC、会话集 S。

定义 1(用户实体 User Entity) 在分布式计算环境下,按照资源的所属关系,用户可分为服务提供者(Service Provider)和服务请求者(Service Demander);按照实体的可信关系可区分为可信用户(Trusted User)和非可信用户(Untrusted User),可信的度量见第 3.3 节。UE 可以为自然人 Usr、智能 Agent 或对等实体 Peer 等。

$$UE=\{ue \mid ue\in SP\vee SD\in UE, ue\in Usr\vee ue\in Agnt\vee ue\in Peer\}$$

或

$$UE=\{ue \mid ue\in TU\vee UU\in UE, ue\in Usr\vee ue\in Agnt\vee ue\in Peer\}$$

定义 2(能力 Capability) UE 对访问客体 Obj(如共享电子数据、Web 服务等)可施加的操作 Opr 的集合,记为 C。这里的操作既可以定义为实际的读、写、执行和查找,也可以为抽象的动作,这满足了基本安全需求中的"数据抽象"原则。例如在 Web 服务中,操作可以定义为系统认证服务、审计服务等。能力 C 与操作 Opr 之间的指派和映射关系,可以体现在普通授权模型中,本文作为委托模型不作讨论,这里约定两者的关系已事先建立。

定义 3(角色 Role) 具有相同服务请求和能力的一类用户实体 ue 的抽象集合。ue 在一次服务请求中所激活的角色称为活跃角色(Active Role),这里 $AR(x)$ 表示实体 x 的活跃角色集。并且,AR 和 C 之间满足多对多的映射关系。

$$RE\in 2^{UE}(ue\in UE), ar\in AR(ue)\text{ 且 }ar\in re$$

$$f_{arc}(ar_i): ar_i\rightarrow c_i(ar_i\in RE, c_i\in C)$$

定义 4(会话 Session) 会话是 ue 通过活跃角色 ar 完成一次服务的过程,ue 和 ar 之间存在一一映射关系,记为 $g_s(ue, ar)$。

$$g_s(ue_i): ue_i\rightarrow ar_j(ue_i\in UE, ar_j\in AR(ue))$$

定义 5(能力指派与撤销 Capability Assignment & Revocation) 指派 ca 是一个三元组 $(re_i, c_j, ncca_k)$,其中 $ncca_k$ 为无冲突能力指派约束(见 1.4 节)。该三元组的语义解释为在满足 $ncca_k$ 的前提下可以将能力 c_j 分配给角色 re_i。指派 ca 在 re_i 与 c_j 之间满足多对多的关系。当角色 re 的能力动态改变或安全策略发生变化时,系统可以依据 ACR 机制指派给 re 能力回收的动作,即 ACR 是指派的逆过程,两者同属于系统动作。记 $(ca)^{-1}$ 为能力回收。

$$CA\subseteq RE\times C\times NCCA\text{ 且 }CA\neq\varnothing$$

定义 6(角色授权与撤销 Role Authorization & Revocation) RA 表示 SP 在每次会话开始时根据用户 SD 的信任程度、无冲突角色授权约束特征 NCRA,以及不同的服务请求等安全策略来决策为其分配相应的角色,记为 $(sp_i, sd_j, re_k, ncra_l)$。$RA$ 发生在每次会话起始时间,具有动态性和即时性,其逆过程 $(ra)^{-1}$ 体现在下一次会话时 RA 的改变,在会话过程中不能执行 $(ra)^{-1}$。

$$RA\subseteq UE\times UE\times RE\times NCRA\text{ 且 }RA\neq\varnothing$$

定义 7(信任委托 Trust Delegation) SP 对于未认知的匿名 SD,将信任判定(Trust Determinability)委托给其他的和 SD 具有某种信任关系的 TU,由 TU 根据已知的信任关系,给出信任度量并返回给 SP,再由 SP 根据本地安全策略判定是否进行角色授权 RA。

$$TD=(sp_i, tu_j, Tru\text{-}Dtrm)$$

定义 8(角色委托与撤销 Role Delegation & Revocation) 委托者 Dlgtor 在满足无冲突角色委托约束 NCRD 的基础上,可以将获得的角色子集再次分配给其他的信任用户 dlgtee,使其可以共享所具有的数据资源,表示为七元组 $(dlgtor_i, dlgtee_j, re_k, ncrd_l, RDC, RDD, RDTL)$。$TD$ 具有静态性,得到委托角色的 TU 在每次会话时可通过角色委托凭证 RDC 直接共享访问资源。当系统安全策略动态变化或委托超出时限约束时,委托者或系统可以显式、实时、或自动地执行 $(rd)^{-1}$ 动作,回收已委托的角色。

$$RD\subseteq Dlgtor\times Dlgtee\times RE\times NCRD\times RDC\times RDD\times RDTL\text{,且 }RD\neq\varnothing\vee RD=\varnothing$$

1.3 DAM for TM 信任度量及相关性质

定义 9(信任特征值 Trust Metric) 在信任管理中,TM 表示系统对实体或实体与实体之间的信任度量关系,该值为 0～100 之间的某个整数值。其中,用户实体信任特征值 $UTM_{ue1}(ue_2)$ 是表示用户 ue_2 对 ue_1 的信任度量值;能力信任特征值 CTM 是系统对该能力访问资源或实施服务所信任的程度;角色信任特征值 RTM 是由该角色所属能力的信任特征值所决定,通常不大于其中的最小值。这些特征值根据安全策略及实体关系的改变,在信任系统中具有动态性。

$$\forall c_i, re(c_i\in C(i=1,2\cdots n), re\in RE)\ \bigcup_{i=1,2\cdots n}c_i\in CA(re_k)\Rightarrow RTM_{re}\leq\min(CTMc_1, CTMc_2, \cdots, CTMc_n)$$

定义 10(信任阈值 Trust Threshold) 在信任管理中,系

统对两类实体所预设的信任程度的门限值,该值为 1～100 之间的某个整数值。用户信任阈值 UTT 是系统设定的最低信任门限;角色信任阈值 RTT 是系统对该角色设定的最低信任程度。TT 在信任系统中具有稳定性,并且为可编程的。

性质 1(信任的判定 Trust Determinability) TM 低于信任阈值的实体则被判定为不信任的,同时不能获得信任委托和(或)角色授权。低于 UTT 的用户实体属于不信任实体且不具备受托的资格,即不能获得信任委托或角色委托;低于 RTT 的角色将不能被授权给可信用户实体。

$\forall ue_1, ue_2 (ue \in UE)\ UTM_{ue1}(ue_2) < UTT \Rightarrow TD(ue_1, ue_2, Tru\text{-}Dtrm) = \varnothing$

$\forall ue_1, ue_2, re(ue \in UE, re \in RE)\ UTM_{ue1}(ue_2) < UTT \Rightarrow RD(ue_1, ue_2, re) = \varnothing$

$\forall ue_1, ue_2, re(ue \in UE, re \in RE)\ RTM_{re} < RTT \Rightarrow RA(ue_1, ue_2, re) = \varnothing$

定义 11(信任域 Trust Domain) 相互信任的用户实体间所构成的局部的信任组织关系。位于同一信任域的可信用户实体间,具备信任委托关系。

定义 12(信任罚函数 Trust Punishment Function) 罚函数是根据用户实体实施能力的行为日志,动态实时地调整用户实体的信任特征值的非线性单调增幂函数 $P(n, p) = n^p$,这里 n 为迭代的次数,常数 p 为信任罚因子,且 $p > 0$。

用户的信任特征值由用户的信任阈值和罚函数值构成,初始 UTM 为最大 UTT 阈值。

$$\begin{cases} UTM_{n+1} = |UTM_n - P_n(p)|, n = 0, 1, 2, \cdots \\ UTM_1 = UTM_0 = \max(UTT) \end{cases} \quad (1)$$

性质 2(信任惩罚 Trust Punishment) 根据信任罚函数的定义和幂函数性质得知,当用户实体多次实施非可信能力(操作)时,UTM 将迅速下降(信任惩罚的幅度逐渐增大),直到低于 UTT 时,该用户将成为不可信实体。

1.4 DAM for TM 委托约束特征

DAM for TM 约束能够加强角色授权和委托机制,同时也满足了模型自定义安全策略的需求。特定的信任管理系统可以根据本地的实际安全策略,自定义完整的约束规则集,从而实施更为完备的指派和委托关系。

定义 13(冲突能力 Conflicting Capability) 如果 c_i, c_j 不能同时指派给同一角色 re_k,则称 c_i, c_j 为冲突能力,记为 $Conf\_C(c_i, c_j)$。

约束规则 1(无冲突能力指派约束 Non-Conflict CA) 对同一角色的能力指派中,不能包含两两冲突的能力。

$\forall c_i, c_j, re_k (c_i \in C, c_j \in C, re_k \in RE)\ c_i \in CA(re_k) \wedge c_j \in CA(re_k) \Rightarrow \neg Conf\_C(c_i, c_j)$

定义 14(冲突角色 Conflicting Role) 如果 re_i, re_j 不能同时指派给同一实体 ue_k,则称 re_i, re_j 为冲突角色,记为 $Conf\_RE(re_i, re_j)$。

约束规则 2(无冲突角色授权约束 Non-Conflict RA) 对同一用户实体的角色指派中,不能包含两两冲突的角色。

$\forall re_i, re_j, ue_k (re_i \in RE, re_j \in RE, ue_k \in UE)\ re_i \in RA(ue_k) \wedge re_j \in RA(ue_k \Rightarrow \neg Conf\_RE(re_i, re_j)$

约束规则 3(无冲突角色委托约束 Non-Conflict RD) 对同一用户实体的角色委托中,不能包含两两冲突的角色。

$\forall re_i, re_j, ue_k (re_i \in RE, re_j \in RE, ue_k \in UE)\ re_i \in RD(ue_k) \wedge re_j \in RD(ue_k) \Rightarrow \neg Conf\_RE(re_i, re_j)$

约束规则 4(角色委托基数约束 RD Cardinality) 角色 re_i 所能够委托的最大用户实体数不能超过委托基数 c(c 为自然数)。

$\forall ue_1, ue_2, \cdots, ue_m, re_i, \exists c \in N(ue_1 \in UE, ue_2 \in UE, \cdots, ue_m \in UE, re_i \in RE)\ re_i \in RA_1(ue_1) \wedge \cdots \wedge re_i \in RA_m(ue_m) \Rightarrow m \leq c$

约束规则 5(角色委托深度约束 RD Depth) 角色 re_i 所能够级联委托的最大用户实体数不能超过委托深度 d(d 为自然数,显式给出)。当 $d = 1$ 时,称为单步委托;当 $d > 1$ 时,称为多步委托。

$\forall ue_1, ue_2, \cdots, ue_d, re_i, \exists d \in N(ue_1 \in UE, ue_2 \in UE, \cdots, ue_m \in UE, re_i \in RE)\ re_1 \in RD_1(ue_i) \wedge \cdots \wedge re_i \in RD_d(ue_d) \Rightarrow d \leq c$

2 支持可信计算的委托协议实现

本节所述的协议是基于文献[11]中的可信计算平台体系架构提出的,但在协议描述上则依据 DAM for TM 增加了用于信任管理的相关协议子集,如信任委托、角色委托和角色授权协议等,并改进了其中的策略分发协议和完整性实施协议。本文研究的委托策略是基于角色粒度的委托,密码机制采用公钥、非对称密码体制。这里约定 SP, SD 及 TU 所在的工作站点分别为 WSP, WSD 和 WTU,$WSP.TRM$,WSD. TRM 和 WTU. TRM 是各自站点上的可信引用监视器(Trusted Reference Monitor),SK(Secure Kernel)为安全的操作系统内核。

协议 1(信任委托) 服务提供者 SP 对于非同一信任域内的 SD 服务请求,依据所在信任域中其他可信实体 TU 的信任特征值,选取其中特征值大于信任阈值的 TU,验证其站点的完整性,然后通过信任委托证书 TDC(Trust Delegation Credential),委托 TU 判定服务请求者 SD 的可信性;TU 根据和 SD 的可信关系签发安全的信任证书 TRC(Trust Recommendation Credential),做出信任推荐,再将其返回给 SP,从而完成信任委托过程。此后,由 SP 做出服务请求的角色授权。具体交互如图 2 所示。

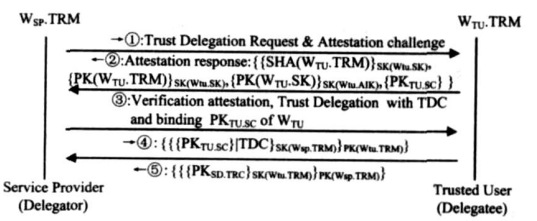

图 2 SP 与 TU 的信任委托协议

(0)协议预备过程:SP 根据所在信任域的 TU 的信任特征值 UTM,选取其值大于 UTT 的 TU_i($i = 1, 2 \cdots n$)。

(1) SP 所在的 $W_{SP}.TRM$ 向 $W_{TUi}.TRM$ 发出信任委托请求和验证挑战(Attestation Challenge);

(2)如果 $W_{TUi}.TRM$ 接收委托请求,则将签名后的平台完整性信息、相关公钥信息以及 TU 的安全凭证 SC(Security Credentail)$\{PK_{TU.SC}\}$ 发送给 $W_{SP}.TRM$,接受验证;

(3) $W_{SP}.TRM$ 收到受托者平台完整性信息后,验证 TU 的平台是否可信;如果可信,则签发信任委托证书 TDC,然后绑定到 TU 的安全凭证;

(4) $W_{SP}.TRM$ 将上述绑定后的证书,使用 $W_{SP}.TRM$ 的私钥签名,然后用 $W_{TUi}.TRM$ 的公钥加密后,发给受托者 TU_i;

(5) 由 TU_i 根据和 SD 的可信关系签发安全的信任凭证,再将其返回给 SP。

(6) 返回第 2 步,继续获取其它的 TU 信任凭证。

协议 2(角色委托) SD 根据资源共享的需求选择可信的 SP 请求委托角色 $dlgt\_role(s)$,SP 验证请求者的信任域和角色的 UTM 后,发出平台验证挑战,再验证请求者站点的完整性,然后在满足 SP 端本地委托策略的基础上,将写有委托角色子集的角色委托证书(Role Delegation Certificate)绑定到受托者的安全凭证。最后由委托者签名后发给受托者,从而完成角色委托过程,如图 3 所示。

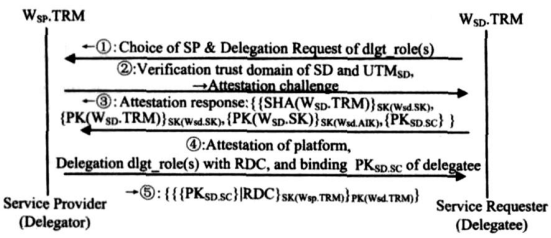

图 3 可信实体间的角色委托协议

(0) 协议预备过程:某个用户实体 SD 在其信任域内选择 UTM 高于 UTT 的 SP;

(1) SD 向选取的 SP 请求委托角色(集) $dlgt\_role(s)$ 以共享资源。

(2) SP 接受请求后,判定请求者 SD 是否属于本身信任域内的用户实体,以及 $RTM_{dlgt\_role(s)}$ 是否不低于 RTT。如果不在同一信任域内,则先执行协议 1,根据间接信任关系判定 SD 的信任度;如果 $RTM_{dlgt\_role(s)}$ 低于 RTT,则协议终止,本次角色委托请求失败。否则,根据已有的 SD 信任特征值判定信任程度,如果 SP 信任 SD,则发出验证挑战;

(3) 如果 $W_{SD}.TRM$ 接收委托请求,则将签名后的平台完整性信息、相关公钥信息以及 SD 的公钥证书{$PK_{SD.SC}$}发送给 $W_{SP}.TRM$,接受验证;

(4) $W_{SP}.TRM$ 收到受托者平台完整性信息后,判定是否可信;如果可信,则根据本地委托策略和约束特征,将角色委托相关安全策略(委托的角色 $Role$ 及所属能力)写入 RDC 后和 SD 安全凭证 SC 绑定;

(5) $W_{SP}.TRM$ 将上述绑定后的凭证,使用 $W_{SP}.TRM$ 的私钥签名,然后用 $W_{SD}.TRM$ 的公钥加密后,发给受托者 SD,此后委托者可依据 RDC 上的委托角色行使资源共享能力。

3 Peer-to-Peer 安全应用实例

P2P 系统中的对等实体具有开放性、分布性、动态性和匿名性[12],Peer 间的匿名资源访问不同于传统的已知用户身份的资源共享方式,由此所引起的实体信任问题则不能采用现有的访问控制机制加以解决[13]。因此本文提出了基于 Peer 间信任管理和可信计算平台的安全架构,有效地解决了 P2P 开放环境下对等实体平台的完整性验证和共享资源的安全问题。其中的信任委托和交互协议分别采用第 1,2 节给出的 DAM for TM 模型和相关的支持可信计算的协议集。图 4 描述的是无线局域网络下基于信任管理和可信计算模块(TPM)的 P2P 资源共享的安全架构,主要涉及在不同信任域内、Peer(可信的与不可信的)之间的服务请求、平台验证以及通过签发 TDC、TRC、RDC、SC 实现信任委托、角色委托、角色授权等协议,并通过委托及授权约束规则、信任特征的度量实现 Peer 间的信任授权关系。

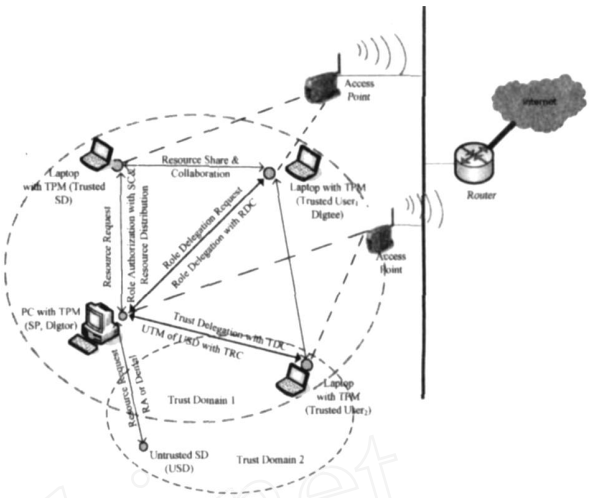

图 4 基于信任管理和可信计算平台的 P2P 资源共享

在信任域 1 中,包括通过无线访问点 AP 接入互联网络并嵌入 TPM 芯片的可信 PC 以及移动终端 Laptop 等,它们彼此具有一定的信任关系。作为可信任的服务请求者 SD 使用安全凭证向 PC 属主 SP 请求资源共享,由于两者之间的信任关系,SP 在验证 SD 的平台完整性后,为其进行角色授权,签发安全凭证 SC,并将共享资源分发到 SD 的 Laptop 平台,满足其访问请求,此后 SD 可以在本地访问共享资源。当 Laptop 用户 TU_1 根据信任域中的可信关系向 SP 请求委托某个角色时,SP 在验证 TU 身份及其平台的可信性后,在满足全部委托约束规则的前提下,可以为其签发角色委托证书 RDC 并分发共享资源,完成整个角色委托过程,使得 TU_1 可以通过委托角色共享资源,进而和 SD 之间也可以完成协作。然而,当信任域 2 中的一个不可信服务请求者 USD 向 SP 请求服务时,鉴于两者不在同一信任域内,SP 需先向信任域 2 内的可信实体 TU_2 通过 TDC 进行信任委托,使其给出对 USD 的信任特征值,然后由 SP 进行访问决策。若 TU_2 返回的 TRC 中 UTM_{USD} 不低于 SP 预设的用户信任阈值 UTT,并在验证 USD 平台后,则进行角色授权和资源分发。这样 USD 便可以共享不在同一信任域内的实体所具有的资源。该架构所关注的是无线网络环境下对等实体间的信任管理和移动平台的可信赖性,有关无线网络通信中的其他安全问题则不属于本文所讨论的范畴。

结束语 本文所提出的 DAM for TM 模型引入了形式化描述信任委托、角色委托和授权,并通过引入信任罚函数对实体间的信任度加以动态调整。依据该模型同时给出了支持可信计算的相关安全协议以及基于可信计算平台的 P2P 网络资源共享安全架构,解决了平台和资源的可信赖和完整性问题。关于 DAM for TM 的角色层次关系,以及委托撤销的协议与实现机制将是本文进一步的研究工作。此外,所提出协议的可证安全性也将是今后待解决的主要问题。

参 考 文 献

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C] //1996 IEEE Symposium on Security and Privacy. Washington DC, USA, 1996: 164-173

[2] 徐锋, 吕建. Web 安全中的信任管理研究与进展[J]. 软件学报, 2002, 13(11): 2057-2064

[3] 张志勇, 黄涛. 信任管理中基于角色的委托授权研究进展[J]. 计算机应用研究, 2008, 25(6): 1601-1605, 1610

[4] Barka E, Sandhu R S. Framework for role-based delegation models[C] //The 6th Annual Computer Security Application Conference. New Orleans, Louisiana, USA, 2000: 168-176

[5] Zhang X W, Oh S, Sandhu R. PBDM: A flexible delegation model in RBAC[C] //The 8th ACM Symposium on Access Control Models and Technologies. New York, USA, 2003: 149-157

[6] 张宏, 贺也平, 石志. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报, 2006, 29(8): 1427-1437

[7] 徐震, 李斓, 冯登国. 基于角色的受限委托模型[J]. 软件学报, 2005, 16(5): 970-978

[8] Li N H, Feigenbaum J, Grosof N B. A logic-based knowledge representation for authorization with delegation[C] //The 12th IEEE Computer Security Foundations Workshop. Mordano, Italy, 1999: 162-174

[9] Li N H, John C M, William H W. Design of a Role-based Trust-management Framework[C] //2002 IEEE Symposium on Security and Privacy. Berkeley, California, USA, 2002: 114-130

[10] 廖俊国, 洪帆, 朱更明, 等. 基于信任度的授权委托模型[J]. 计算机学报, 2006, 29(8): 1265-1270

[11] Sandhu R S, Zhang X W, Kumar R, et al. Client-side access control enforcement using trusted computing and PEI models[J]. Journal of High Speed Network, 2006(15): 229-245

[12] 高迎, 程涛远, 王珊. 对等网信任管理模型及安全凭证回收方法的研究[J]. 计算机学报, 2006, 29(8): 1282-1289

[13] Shane B, Amit D L, Kenneth G P. Trusted Computing: Providing Security for Peer-to-Peer Networks[C] //The 5th IEEE International Conference on Peer-to-Peer Computing. Konstanz, Germany, 2005: 117-124

(上接第 71 页)

[6] Ekert A. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663

[7] Bennett C H, Brassard G, Mermin N D. Quantum Cryptography without Bell's Theorem[J]. Physical Review Letters, 1992, 68(5): 557-559

[8] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution schemes[J]. Physical Review A, 2002, 65(3): 032302

[9] Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution[J]. Physical Review A, 2003, 68(4): 042315

[10] Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses[J]. Physical Review A, 2004, 70(1): 012311

[11] Yang Y G, Wen Q Y, Zhu F C. An efficient two-step quantum key distribution protocol with orthogonal product states[J]. Chinese Physics, 2007, 16(4): 910-914

[12] Yang Y G, Wen Q Y. An efficient quantum key distribution protocol with orthogonal product states[J]. Chinese Physics, 2007, 16(8): 2215-2218

[13] Beige A, Englert B G, Kurstsierer C H, et al. Secure Communication with a Publicly Known Key[J]. ACTA PHYSICA POLONICA A, 2002, 101(3): 357-368

[14] Deng F G, Long G L. Secure direct communication with a quantum one-time-pad[J]. Physical Review A, 2004, 69(5): 052319

[15] Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons[J]. Physics Letters A, 2006, 358(4): 256-258

[16] 王剑, 陈皇卿, 张权, 等. 多方控制的量子安全直接通信协议[J]. 物理学报, 2007, 56(2): 673-677

[17] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902

[18] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Physical Review A, 2003, 68(4): 042317

[19] Deng F G, Li X H, Li C Y. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs[J]. Physics Letters A, 2006, 359(5): 359-365

[20] Hwayean L, Jongin L, Hyungjin Y. Quantum direct communication with authentication[J]. Physical Review A, 2006, 73(4): 042305

[21] 吕欣, 马智, 冯登国. 基于量子 Calderbank-Shor-Steane 纠错码的量子安全直接通信[J]. Journal of Software, 2006, 17(3): 509-515

[22] Gao T, Yan F L, Wang Z X. A Simultaneous Quantum Secure Direct Communication Scheme between the Central Party and Other M parties[J]. Chinese Physics Letters, 2005, 22(10): 2473-2476

[23] Gao T, Yan F L, Wang Z X. Deterministic secure direct communication using GHZ states and swapping quantum entanglement [J]. Journal of Physics A: Mathematical and General, 2005, 38(25): 5761-5770

[24] Man Z X, Xia Y J, Nguyen B A. Quantum secure direct communication by using GHZ states and entanglement swapping[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2006, 39(18): 3855-3863

[25] Wang H F, Zhang S. Quantum Secure Direct Communication by Using a GHZ State[J]. Journal of the Korean Physical Society, 2006, 49(2): 459-463

[26] Cao H J, Song H S. Quantum Secure Direct Communication with W State[J]. Chinese Physics Letters, 2006, 23(2): 290-292

[27] Dur W, Vidal G, Cirac J I. Three qubits can be entangled in two inequivalent ways[J]. Physical Review A, 2000, 62(6): 062314

[28] Bennett C H, Brassard G, Popescu S, et al. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels [J]. Physical Review Letters, 1996, 76(5): 722-725

[29] Deutsch D, Ekert A, Jozsa R, et al. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels[J]. Physical Review Letters, 1996, 77(13): 2818-2821

[30] Cirac J I, Gisin N. Coherent eavesdropping strategies for the four state quantum cryptography protocol[J]. Physics Letters A, 1997, 229(1): 1-7

[31] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge, England: Press of the University of Cambridge, 2000