

支持属性委托模型中委托撤销研究

叶春晓¹ 符云清²

(重庆大学计算机学院 重庆 400044)¹ (重庆大学软件学院 重庆 400044)²

摘 要 支持属性的委托模型(ABDM)中,受托者必须同时满足委托先决条件(CR)和委托属性表达式(DAE)才能获得委托权限或角色。在该模型中,委托撤销完成将委托出去的权限收回到委托者处的工作。首先介绍了 ABDM 提出的两种新的撤销模式及其带来的多步委托中委托与撤销的优先级问题。然后详细讨论了委托与撤销的关系,对两种解决办法:“先来先响应”和“先撤销后委托”进行了分析,提出了两种方法的适应场合。

关键词 访问控制, RBAC, 委托, 撤销, 属性

中图分类号 TP301 **文献标识码** A

Study on Delegation Revocation in Attribute Supported Delegation Model

YE Chun-xiao¹ FU Yun-qing²

(College of Computer Science, Chongqing University, Chongqing 400044, China)¹

(College of Software Engineering, Chongqing University, Chongqing 400044, China)²

Abstract In Attribute Supported Delegation Model (ABDM), delegatee must satisfy both delegation prerequisite condition (CR) and delegation attribute expression (DAE) when assigned to a delegation role. In ABDM, revocation focuses on how to revoke those delegated roles or permissions from delegatee. This paper first introduced two new sorts of revocations, which bring about priority between multi-step delegation and revocation. Then analyzed the relation between delegation and revocation and proposed two solutions: “first request first response” and “revocation first then delegation”. We also discussed different situations fitting these two solutions.

Keywords Access control, RBAC, Delegation, Revocation, Attribute

1 引言

委托(delegation)可实现将委托者(delegator)的全部或部分权限指派给受托者(delegatee),撤销是委托的逆过程,其作用是将受托者获得的委托权限收回。

在 RBAC^[1]中,URA97 定义了撤销关系,该撤销关系主要针对 URA 过程。由于委托过程与 URA 过程类似,因而委托模型中的撤销与之类似。在现有的委托模型中,RBDM^[2,3]提出了基于角色的委托模型,首次将角色概念引入到委托模型中。RBDM 详细讨论了委托撤销,将其分为系统撤销和用户撤销两种。前者指撤销操作由系统条件自动触发,后者指撤销操作由用户手工完成。RBDM 对后者又进行了进一步分类。

RDM2000^[4]模型支持层次角色和多步委托。该模型详细讨论了不同的委托和撤销方式,将委托分为初始用户委托(Original User Delegation)和受托者委托(Delegated User Delegation)两种。同时,将委托撤销分为由委托期限约束条件引起的撤销(Revocation using duration-restriction constraint)和用户撤销(User revocation)。并且将用户撤销分为非级联撤销(Non-cascading revocation)和级联撤销(Cascading revocation)^[5],以及由委托者自己撤销(can-revokeGI)和

由委托者及拥有比委托者级别高的角色的其他用户撤销(can-revokeGD)。PBDM^[6]是为解决权限的部分委托而提出的模型,支持部分委托模式。但该模型主要针对委托操作,对委托撤销未做深入研究。

RPRDM^[7]主要就 RBDM 和 RDM2000 中不能进行重复和部分权限委托进行改进和扩展,定义了 4 种委托撤销:只有委托者才能完成撤销、具有委托角色的用户均可完成撤销、系统自动撤销和系统管理员撤销。该模型对前两者进行了讨论,本质上这两种撤销方式与 RDM2000 和 RBDM 中的撤销操作相同。

ABDM^[8]就基于属性的委托进行了讨论。在 ABDM 中,用户的属性用来表明用户所处的状态、所具有的资格和能力。而角色和权限的属性则表明其对用户状态资格和能力的要求。在该模型中,属性作为用户授予角色的委托约束条件。因而当用户或角色权限的属性发生改变后,其约束条件将发生变化,使得用户可能不再满足该约束条件,会引起相应的委托撤销操作。该文并没有研究委托撤销所引起的相关问题,特别是多步委托和撤销之间的关系。而文献[9]主要讨论了利用 XML 来表达委托和撤销过程所需的相关信息。现有文献中很少对多步委托中撤销与委托的关系进行详细分析,本文则主要考虑了基于属性的多步委托与撤销的关系。本文第

到稿日期:2009-07-28 返修日期:2009-10-15 本文受国家自然科学基金(No. 60803027)资助。

叶春晓(1973—),男,副教授,CCF 高级会员,主要研究方向为访问控制、数据库和软件工程,E-mail: yecx@cqu.edu.cn;符云清(1969—),男,教授,主要研究方向为分布协调作业、远程教育。

2 节简要回顾了 ABDM 模型;第 3 节讨论了多步委托与撤销之间的关系;最后是总结和进一步的工作。

2 ABDM 模型简介

在 ABDM 中,委托约束条件既包含委托先决角色(CR),也包括委托属性表达式(DAE)。只有同时满足 CR 和 DAE 的受托者才能获得委托角色或权限。ABDM_A 考虑了永久委托和临时委托对受托者在资格和能力上的不同要求。

ABDM 中出现两种新委托类型:确定受托者委托(DDD)适用于委托者在委托之前就指定了受托者的场合,现有委托模型中的委托操作与之类似;不确定受托者委托(UDD)适用于委托者不知道受托者确切范围或委托者无法在委托前指定受托者的场合中。无论哪种类型的委托,受托者不但要满足委托先决条件,而且其委托属性表达式还要满足委托权限的委托属性表达式。

ABDM 还支持两种不同类型的委托:临时委托和永久委托。临时委托主要适用于即使受托者不能完全满足委托属性表达式,但也需要进行委托操作的情形。相对于永久委托来说,临时委托中对受托者的限制较弱。永久委托要求受托者必须满足委托属性表达式的要求,限制较强。相应地,ABDM 中将这两种不同类型的委托属性表达式分为临时委托属性表达式(TDAE)和永久委托属性表达式(PDAE)。TDAE 只用于临时委托,而 PDAE 可用于两种类型的委托中。每个权限都同时拥有 PDAE 和 TDAE,其 PDAE 和 TDAE 可能相同,也可能不同。

ABDM 模型的主要组件在文献[8]中详述。在 ABDM 中,临时和永久委托是通过 3 个关系实现的: $can-delegateDP \subseteq R \times CR \times PDAE \times TDR_M$, $can-delegateDT \subseteq R \times CR \times TDAE \times TDR_N$ 和 $can-revokeU \subseteq U \times Uee \times TDR$ 。相应地,ABDM 中委托撤销可通过关系: $can-revoke \subseteq U \times TDR$ 实现,此处不详细说明,主要讨论委托与撤销之间的关系。

ABDM 模型中用户、权限的属性表达式会发生变化,因而会引起受托者的属性表达式不再满足委托角色的属性表达式。当用户的属性表达式不满足临时委托角色的属性表达式后,该用户不应当继续拥有该临时委托角色。这种委托撤销建立在属性表达式的基础上,由属性表达式的变化引起,这种变化应当作为委托撤销的触发机制。本文不详细说明具体过程,将主要讨论委托与撤销之间的关系。

3 委托与撤销优先级

ABDM 模型中的委托与撤销均发生在临时委托角色失活的状态下,即延迟委托和延迟撤销。前者主要是为了防止用户可能将不能继续拥有的角色再次委托出去;后者是为了避免在临时委托角色激活期间撤销权限而引起的用户不能正常行使委托权限的问题。因此,当系统撤销触发条件出现在临时委托角色活动期间时,引起的撤销和用户发出的委托均在委托角色处于失活状态后得到响应。这就存在一个系统优先响应哪一种请求的问题,即委托和撤销请求的优先级问题。

图 1 中给出了委托和撤销两种不同操作的时间顺序关系。临时委托角色 tdr 在 t_0 到 t_4 阶段处于活动状态,而拥有 tdr 的受托者 u 在 t_1 阶段发出委托请求,将 tdr 再次委托出去。由于 tdr 还处于活动状态,因此该请求一直持续到 t_4 时刻。而 u 的 uae 在 t_2 时刻不再满足 tdr 的 rae ,应当将 tdr 从 u 中撤销。由于 tdr 仍然处于活动状态,使得撤销操作只能从 t_4

时刻开始,而由系统发出的撤销请求在 t_3 时刻产生。这样,在 t_4 时刻系统中会同时存在着将 tdr 再次委托出去和将 tdr 从 u 中撤销两种操作请求。系统需要在 t_4 时刻作出判断。

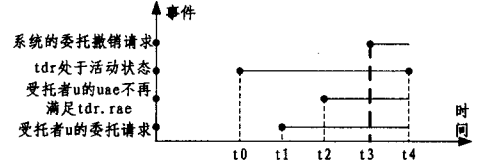


图1 委托与撤销之间的时间关系

3.1 先来自响应

显然,如果系统按照请求的“先来自响应”原则来处理这两类操作请求,则由于用户的委托申请先于系统的委托撤销请求,使得 t_4 时刻系统响应用户的委托请求。这样处理显然违反了前面的限制,使得用户将不再属于他的权限再次委托出去。同时,这样处理还会带来一个严重的后果:当系统先响应用户的委托请求后,设用户 u 将 tdr 委托给用户 u' ,然后系统响应委托撤销请求,将 tdr 从用户 u 中撤销。这两种操作的先后顺序如下:

系统在 t_4 时刻先响应委托请求,委托操作在 t_5 时刻结束后,系统紧接着响应委托撤销请求。

按“先来自响应”策略操作的结果如图 2 所示,委托和撤销时间关系如图 3 所示。图 2(a)表示由于 u 将 tdr 委托给 u' ,因此产生了从委托者 u_d 开始到 u' 的一棵有向树。该树表明了,在多步委托中各个用户之间的关系。图 2(b)表示当 u 将 tdr 委托给 u' 后, tdr 再从 u 中撤销,则委托树中 u_d 到 u 之间没有有向边,不再构成一棵有向树。由于级联撤销中撤销路径是与委托树的有向边相反,使得从 u' 到 u_d 之间不再形成撤销路径,从而造成 u_d 无法将 tdr 从 u' 中撤销。

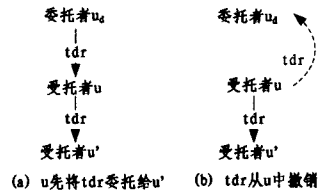


图2 “先来自响应”中委托和撤销的结果

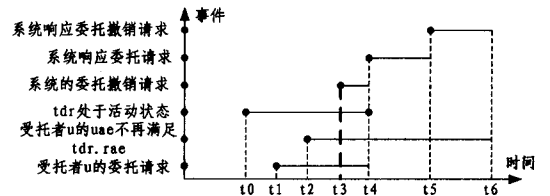


图3 “先来自响应”中的委托和撤销时间关系

这一问题虽然可通过级联撤销来解决,但会造成短时间内多次撤销操作,增加系统负担,特别是当用户进行多重委托时,或者当临时委托角色的活动周期很长,而多步委托层次较深时。最好的办法是限制系统在同时存在对同一个临时委托角色的既委托又撤销操作,防止系统在撤销前执行委托操作。

3.2 先撤销后委托

若先响应撤销请求,再响应委托请求,其操作的先后顺序如图 4 所示。

由于委托撤销执行后, u 不再具有临时委托角色 tdr ,因此系统不再响应委托请求。其结果如图 5 所示。

图 5 中,先响应撤销请求后,即使 u 想将 tdr 委托给 u' ,也会因为 u 不再具有 tdr 而不能成功实施该委托。这就避免

了上面出现的无法撤销的问题。

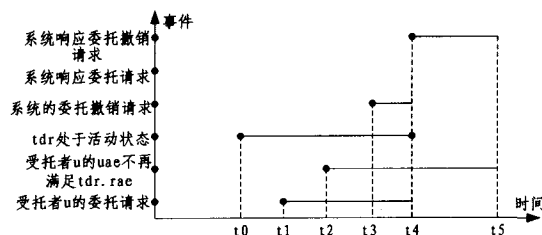


图4 “先撤销后委托”中的委托和撤销时间关系

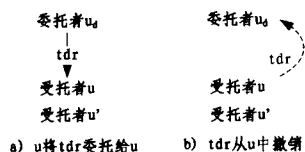


图5 “先撤销后委托”中委托和撤销的结果

因此,当同时存在针对同一个临时委托角色的委托和委托撤销请求时,要求系统优先响应委托撤销请求。此处用临时委托角色 tdr 的当前状态来表示在其上的两种操作和所处的状态。

定义1 记用户 u 的临时委托角色 tdr 的当前状态为 $\lambda(u, tdr)$, 其取值定义为:

$$\lambda(u, tdr) = \begin{cases} 1 & \text{当在 } u \text{ 中的 } tdr \text{ 上只存在委托请求} \\ 2 & \text{当在 } u \text{ 中的 } tdr \text{ 上存在委托撤销请求} \\ 0 & u \text{ 中的 } tdr \text{ 两种请求均不存在} \end{cases}$$

式中,只有当 $\lambda(u, tdr) = 1$ 时,才能够委托成功。

前面例子在引入了临时委托角色状态后,系统的操作时间顺序以及临时委托角色的 λ 值的变化如图6所示。

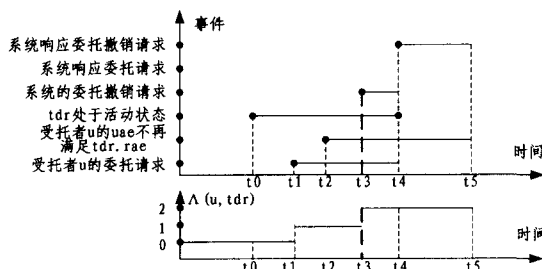


图6 引入 $\lambda(u, tdr)$ 后的委托和撤销时间关系及 $\lambda(u, tdr)$ 变化过程

引入状态函数后,委托系统在处理受托者将临时委托角色再次委托出去时必须保证该状态函数取值为1。因此,撤

销对多步委托就产生了影响。本文并不在此深入探讨,可作为进一步的研究之用。

结束语 撤销是委托模型必不可少的功能,作为 ABDM 模型的重要组成部分,本文和文献[8]分别从撤销和委托两个方面说明了基于属性的委托模型中撤销与委托操作。本文认为为保证委托和撤销操作的正确性,在对某个临时委托角色同时存在委托和撤销操作时,需优先执行撤销操作。本文只给出了最基本的撤销操作,进一步的工作将包括如何进行基于属性的多步和多重撤销。

参考文献

- [1] Sandhu R, Coyne E, Feinstein H, et al. Role-Based Access Control Models[J]. IEEE Computer, 29(2): 38-47
- [2] Barka E, Sandhu R. Framework for Role-Based Delegation Models[C]//Proc. of 16th Annual Computer Security Application Conference (ACSAC2000). New Orleans, USA: IEEE Computer Society Press, 2000
- [3] Barka E, Sandhu R. A role-based delegation model and some extensions[C]//Proc. of 23rd National Information Systems Security Conference (NISSC 2000). Baltimore, USA, 2000
- [4] Zhang Longhua, Ahn Gail-Joon, Chu Bei-Tseng. A rule-based framework for role-based delegation[C]//Proc. of SACMAT '01. Chantilly, VA, USA: ACM press, 2001
- [5] Tamassia R, Yao Danfeng, Winsborough W H. Role-based cascaded delegation[C]//Proc. of the SACMAT '04. Yorktown Heights, New York, USA: ACM press, 2004
- [6] Zhang Xinwen, Oh S, Sandhu R. PBDM: A Flexible Delegation Model in RBAC[C]//Proc. of the SACMAT '03. Como, Italy: ACM press, 2003
- [7] 赵青松, 孙玉芳, 孙波. RPRDM: 基于重复和部分角色的转授权模型[J]. 计算机研究与发展, 2003, 40(2): 221-227
- [8] 叶春晓, 吴中福, 符云清, 等. 基于属性的扩展委托模型[J]. 计算机研究与发展, 2006, 43(6): 1050-1057
- [9] Stoupa K, Vakali A, Li Fang, et al. XML-based revocation and delegation in a distributed environment[C]//Proceedings of the EDBT International Workshop on Database Technologies for Handling XML information on the Web. Heraklion, Greece, 2004: 299-308
- [10] 孙波, 赵庆松, 孙玉芳. TRDM-具有时限的基于角色的转授权模型[J]. 计算机研究与发展, 2004, 41(7): 1104-1109

(上接第141页)

关键问题得以解决。实践证明,该嵌入式系统功能完整、集成度高、稳定可靠、简洁实用,具有可编程性、可裁减性、易操作性、灵活性以及低成本等特点,具有广泛的应用价值。

参考文献

- [1] Pottie G J, Kaiser W J. Embedding the Internet: Wireless Integrated Network Sensors[J]. Communications of the ACM, 2003, 43(5): 51-58
- [2] Cerpa A, Elson J, Estrin D, et al. Habitat Monitoring: Application Driver for Wireless Communications Technology[C]//Proceedings of the ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean. San Jose, Costa Rica, 2001
- [3] 孙利民, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005(4)

- [4] Raghunathan V, Schurgers C, Park S, et al. Energy-Aware Wireless Microsensor Networks[J]. IEEE Signal Processing Magazine, March 2002: 40-41
- [5] Barnett R, Larry O'cull, Cox S. 嵌入式 C 编程与 Atmel AVR [M]. 周俊杰, 译. 北京: 清华大学出版社, 2003: 75-76, 52-53
- [6] Altera Corporation, Nios3. 0CPU Datasheet[Z]. Version 2. 2, 2004. 10
- [7] Semiconductors P. The I2C Bus Specification, 2003: 11-12
- [8] 何立民. I2C 总线应用系统设计[M]. 北京: 北京航空航天大学出版社, 1995: 178-180
- [9] Labrosse Jean J. uC/OS-II 一源码公开的实时嵌入式操作系统 [M]. 北京: 中国电力出版社, 2006
- [10] Dunkels A. LwIP. A free small TCP/IP implementation for 8 and 16-bit microcontroller[Z]. 2006
- [11] 高雷, 郑相全, 张鸿. 无线传感器网络中一种基于三边测量法和质心算法的节点定位算法[J]. 2009, 23(7): 138-141