

基于角色信任度动态监控的访问控制研究

陈彦竹,郝天曙

(南京邮电大学 计算机学院,江苏 南京 210003)

摘要:安全访问控制是云计算安全领域中一个迫切需要解决的问题,其中在用户登入系统后,实施合理的动态监控用户行为以确保资源安全是当前研究的热点。传统的访问控制策略已经不能满足现在的安全需求,单一地将用户和角色进行关联,并不能全面地反映用户的安全属性,也无法实时获取用户的行为。因此,提出了一种基于信任度评估和行为级别评估的访问控制模型。该模型的信任管理考虑了用户的跨域操作,结合用户的初始信用度、历史信用度和域间参考信用度进行综合评价,在信用度累积过程中,系统会根据用户的当前信用度,动态赋予用户不同的信用度加成,同时监控用户行为,根据用户行为级别,更改监控时间片。通过实验分析证明,该模型在安全访问控制上,更加细粒度,更加安全可靠,实时性更好。

关键词:访问控制;综合信用度;行为级别;跨域;细粒度

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2017)10-0106-05

doi:10.3969/j.issn.1673-629X.2017.10.023

Research on Access Control of Dynamic Monitoring with Role Trustrank

CHEN Yan-zhu, HAO Tian-shu

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Security access control is an urgent issue to be solved in the field of cloud computing security, in which implementing reasonable dynamic monitoring users' activity to ensure the security of resources after logging in the system is the hot issue of current investigation. The traditional access control policy can't satisfy the current security requirements, just integrating roles with users can't fully reflect the users' security attributes, and can't obtain the users' behavior in real time. Therefore, a kind of access control model based on the evaluation of trust rank and assessment of behavior rating is put forward. Its trust management takes the cross-domain operation of the users into account, and combines the users' initial trust, historical trust and cross-domain reference trust for evaluation. During the process of accumulating trust, the system dynamically assigns different trust degrees to users according to their current trust. Meanwhile, the system monitors the users' behavior, and the monitoring time slice changes with user behavior level. The experimental analysis proves that it is more fine-grained, more reliable, safer and better real-time in security access control.

Key words: access control; comprehensive trust degree; behavior level; cross-domain; fine-grained

0 引言

云计算^[1]是基于并行计算、分布式计算和网格计算发展起来的,主要特点是超大规模,扩展性强,高可用性,虚拟化及按需服务,等等。云环境中,所有资源都整合到了云中,用户可以动态申请云中的资源和服务^[2]。云安全授权用户的非法行为和非法用户的恶意操作会威胁云中资源^[3]。所以,必须要对用户进行安全认证,行为监控并根据用户访问控制模型进行评估,从而确保资源的安全性。

访问控制一直是云计算领域中长期需要解决的难题^[4]。访问控制的实质就是对于所有资源设置一定策略的授权访问,使得资源在合法范围内被用户访问和操作。在传统的访问控制中,用户通过获得某种角色而获取相应权限进行访问,很好地解决了集中式环境下的访问控制。但是随着云计算的飞速发展和分布式场景的广泛引用,以前的相对静态的或者相对封闭的网络环境已经越来越少,逐步向开放式发展,用户频繁登入和退出,且用户身份不固定,因此对于访问控制策

收稿日期:2016-11-17

修回日期:2017-03-09

网络出版时间:2017-07-19

基金项目:教育部专项研究项目(20131116)

作者简介:陈彦竹(1988-),男,硕士研究生,研究方向为云计算、访问控制。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20170719.1112.066.html>

略的研究提出了更高要求。目前常见的控制策略有两种:基于角色的访问控制和基于属性的访问控制。当下绝大部分研究都是在这两种策略上进行提升和优化,其中一种比较热门的是在访问控制策略中引入“信任度”的概念。Blaze 等^[5]通过对主客体之间的信任度和安全策略之间的联系进行评定,阐述了“信任管理”的概念。

在研究分析现有访问控制策略的基础上,基于角色信任度的访问控制机制,提出了一种基于信任度动态监控的访问控制方法,并通过实验对其进行验证。

1 相关工作

1.1 传统访问控制

(1)自主访问控制(DAC)。

用户可以对自己创建的资源进行访问,也可以授权其他用户访问这些资源并撤销其授予其他用户的权限。优点是用户可以灵活地提供资源访问控制权限,便于实施有效的授权管理;缺点是由于系统管理员无法考虑到所有的用户和资源权限之间的关联关系,因此安全性较低。

(2)强制访问控制(MAC)。

将系统中的资源按级别或类型进行管理,资源会被标记上允许被哪些用户访问,也就是要求用户强制服从系统的访问控制策略。所有的主客体都由系统管理员来定义其安全属性,并且主体自身无法更改自身的安全属性。该策略无法适用于分布式系统环境,在灵活性和授权管理上也有些欠缺。

(3)基于角色的访问控制(RBAC)。

核心思想为将权限和角色进行关联,通过对用户的评估和分析,赋予用户不同的角色,从而使得用户拥有不同的资源操作权限。一个用户可以获得多个角色,用户和角色是多对多的关系。RBAC 主要解决了 who, what, how 的问题,权限授权的用户对于什么资源具有怎样的操作权限。MAC 和 DAC 主要存在的缺陷是将主客体绑定在了一起,当数量级很大时,授权工作会非常困难,而 RBAC 把资源的访问权交给了角色来做,简化了授权管理。

1.2 信任度

信任度^[6]用来表示服务提供方或资源拥有者对于申请访问控制的用户的综合评价,这种信任度值随着用户的操作时间、当前行为、历史行为以及上下文^[7]等因素的改变而改变。信任的评估一般有两种:身份认证和行为评估。身份认证一般用来验证用户的真实身份以及用户的安全级别,在传统的访问控制中一般只考虑身份认证。在认证通过后,用户就可以根据访问控制策略来对资源进行操作,系统会根据用户的行为

来判断其操作是否合法,以此来提高信任监控的实时性。

1.3 访问控制研究

Barker 等^[8]研究的基于身份认证的访问控制策略,是通过计算和评定用户当前行为和历史行为,来判断其是否满足请求访问的条件。虽然该方法有较好的行为分析,但是其动态监控能力一般,判决的实时性不强。赵明斌等^[9]提出了在传统 RBAC 上加入时态约束的基于角色的访问控制模型,通过加入主体这一角色,在主体和客体属性之间添加可变机制,增加灵活性,并在医疗系统中得到应用。但是该模型只是在传统的访问控制中进行了改进,忽略了信任对于访问控制的影响,并没有很好地解决云计算安全服务问题。吴慧等^[10]提出在云环境下的动态模型中加入信任元素,提高了节点之间交互的安全性,改进了恶意节点的惩罚策略,增大了惩罚力度,有效提高了访问资源的安全性。但该模型仅仅在关系信任模型上简单地引入了服务质量,单一地用信任度进行判别。吴明峰^[11]在其信任模型中,同样是使用信任度评估,不同的是将信任度作为模型的二级访问监控,通过信任度比较来决定是否可以被授权,实现了访问控制的统一管理。但该模型信任度评估的主观性太强,单纯用信任度作为判断访问控制的唯一条件,没有全面考虑资源访问的安全性。刘武等^[12]对于基于角色的访问控制模型进行了进一步提升,在 Blaze 的信任管理的思想上,提出了角色和信任相关联的访问控制策略。该策略从实际应用出发,综合考虑了结合多种信用属性,提升访问控制的灵活性,细化权限和信任度的关系,使得用户授权更加合理安全。宋国峰等^[13]提出一种基于信任动态监控的模型,主要是监控用户行为,通过 AHP 这种模糊矩阵来描述用户行为和信任度之间的关系,实现通过信用级别来授予不同级别的系统服务的访问策略。鹿晨等^[14]研究的基于信任度动态访问控制模型中,兼顾历史和当前信用度,将两者进行加权运算得到综合信用度,这种策略可能会受到用户通过信用度累加来进行欺骗行为的威胁。但上述策略没有考虑到跨域访问和域间信任度推荐的影响。谢四江等^[15]通过对现有的域间访问的安全性问题分析,提出了一种基于信任等级的域间访问策略,利用信任评级,平台信任度和域间信任度来制定域间访问控制策略,但是并未提出具体的实现过程。

为了进一步完善访问控制策略,文中提出了一种新的访问控制策略,实施双标准监控,在监控信用度的同时监控用户行为安全级别,对于信任度累积计算更加细化,在最终计算时,还考虑了域间访问的信用度参考价值,使得信用度计算更加精确。

2 访问控制策略研究

在云计算环境下,用户登录系统后,系统根据用户信用度确定是否有权限对资源进行操作,操作过程中,系统会动态监控用户行为并计算实时信用度,每次操作完成后,根据初始信用度、域间参考信任度和历史信任度计算用户的最终信用度。

2.1 域间访问控制

考虑到同一用户在不同的域之间的操作,有一定的关联性和参考价值,所以根据区域之间系统环境和访问策略的相似度分析,得出域间相关性,将其存放在数据库表单中,当进行跨域访问和域间推荐信任度计算时,查询数据库中域间关系进行计算。假设现有域 A,域 B,域 C,域 D,域 E,域 A 和域 B,C,D,E 之间的相似度值 $T_{reg}(n_i)$ 分别为 0.9,0.5,0.7 和 0。相似度值表明域 A 和域 B 之间的环境相似度很高,而域 A 和域 E 之间的相似度为 0,即用户在域 E 中的操作对用户 A 中的操作没有参考性。假设用户已经在域 A 以外的域进行过资源的访问控制,那么用户在该域中便有了历史信用度 $history_{T(u)}$,用户要在域 A 中进行信任度计算,除了在首次登入域 A 时获得的初始信用度 $init_{T(u)}$ 、历史信用度 $history_{T(u,reg)}$ 外,还有来自用户在其他域中的信用度通过域间信任度关系计算所得的参考信用度:

$$reference_{T(u)} = \sum_i^n (\theta init_{T(u,reg)} T_{reg}(n_i) + (1 - \theta) history_{T(u,reg)} T_{reg}(n_i)) / n,$$
$$\theta \in (0,1)$$

(1)

其中, $init_{T(u,reg)}$ 表示用户在其他域中的初始信任度; $history_{T(u,reg)}$ 表示用户在其他域中的历史信任度。通过加权和域间信任度关系计算出用户在域 A 中的参考信任度。

2.2 信任度计算及行为级别判定

每个首次登入云中的用户,系统会根据该用户的用户信息和系统安全的关联度 $R(i,s)$,用户权限和系统安全的关联度 $R(p,s)$ 以及用户环境和系统安全的关联度 $R(e,s)$ 进行加权计算,得出用户首次登入的初始信用度,即用户的默认初始信用度:

$$init_{T(u)} = \frac{\alpha R(i,s) + \beta R(p,s) + \gamma R(e,s)}{\alpha + \beta + \gamma}$$

(2)

用户第一次登入进行访问控制后会产生首个历史信用度:

$$history_{T(u)} = init_{T(u)} W_i^T$$

(3)

该参数计算用户从登入到结束退出系统的总时间片 T 内所有操作累计后的信用度,其中 T 为动态监控时间片, W_i^T 为行为信任度加权。用户行为对应的时间片以及用户行为对应的用于计算的加权重值见表 1。

表 1 监控时间片和行为信任度加权重值与用户行为关系表

用户行为级别	高危行为	低危行为	安全行为 (信任度<初始值)	安全行为 (信任度≥初始值)
监控时间片 T	T_3	T_2	T_1	T_0
行为信用度加权重值 W_i^T	0.5	0.7~0.85	1.05	1.1

系统动态监控用户的行为和用户信用度的实时数据,操作正常且当前信任度等于初始信用度时,监控频率为默认时间片 T_0 ;当信用度大于初始值时,监控时间片变为 T_1 ;发生低危操作和高危操作时,监控时间片分别为 T_2 和 T_3 ($T_0 > T_1 > T_2 > T_3$)。

用户在首次操作完成后进行用户最终信用度计算:

$$final_{T(u)} = W_{init} init_{T(u)} + W_{history} history_{T(u)} + W_{reference} reference_{T(u)}$$

(4)

其中, $W_{history}$, $W_{reference}$, W_{init} 分别表示历史信用度、推荐信用度、初始信用度在计算最终信用度中的权重,三者关系为 $W_{history} > W_{reference} > W_{init}$,首次计算最终信用度时,历史信用度为 0,即 $history_{T(u)} = 0$,若无其他域历史操作,参考信誉度 $reference_{T(u)} = 0$ 。

此后,每次用户登录都会验证上次用户操作完成的最终信用度 $final_{T(u)}$ 来判断用户是否有操作资源的权限或者是否能激活用户角色。最终历史信用度为:

$$history_{T(u)} = \frac{t_{current} history_{T(u)} + t_{history} final_{T(u)}}{t_{history} + t_{current}}$$

(5)

其中, $final_{T(u)}$ 表示前一次操作的最终信任度; $history_{T(u)}$ 表示此次操作的历史信用度; $t_{history}$ 表示访问操作的历史时间; $t_{current}$ 表示用户登入到退出操作的总时间。权重大小关系为 $W_{history} > W_{reference} > W_{init}$, $W_{history} + W_{reference} + W_{init} = 1$ 。一般用户登入的初始信用度 $init_{T(u)} \in (0.9,1.1)$,系统实时监控用户的行为同时计算更新 $history_{T(u)}$,判断其是否高于信用度阈值的最小值,一旦小于会强制用户退出,规定信用度阈值在区间 $[0.5,1.5]$ 内。

为了提高安全性,防止恶意用户做信用度累计的欺骗操作,模型设置了双标准监控,同时监控用户的当前信用度和实时判别用户的行为级别。正如表 1 所述,所有危险操作对于信用度衰减的力度都大于安全操作,这样可以有效防止恶意用户利用安全操作累计信用度,在信用度达到最高值后进行恶意操作。由此,系统设置了实时判别用户的行为级别来保证系统安全,即使之前所有的操作都是安全的,用户的信用度达到最高的 1.5,一旦当前的行为级别为高危级别,会立刻被强制退出系统,并且重新计算和保存最终历史信

用度。

2.3 基于信任度动态监测的策略流程

访问控制方法主要在三个方面进行改进：

(1)对于信用度进行动态监控和计算,并且在行为信用度加权值的设置上遵循信用度累计慢,威胁操作信用度损耗快的原则；

(2)考虑用户的域间操作,并记录多个域之间操作的信用度,为其他域的访问控制操作提供参考信用度；

(3)在模型中增加对用户行为进行实时判别,以防止恶意用户通过信用度累计来进行欺骗行为,对资源实施恶意操作。

具体的系统操作流程如图 1 所示。

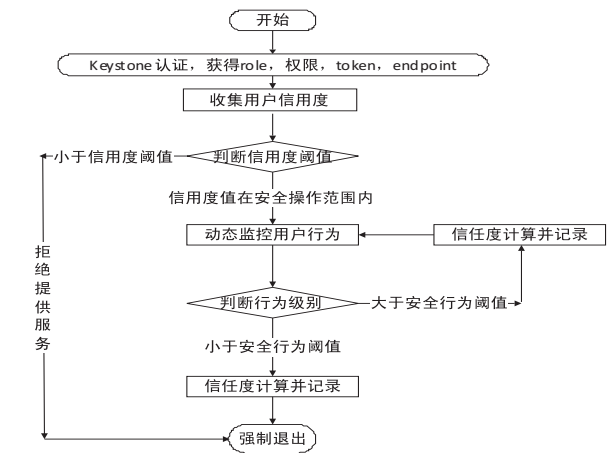


图 1 系统操作流程

(1)用户通过账户和密码登录系统,系统通过认证,赋予用户对应的角色、权限、token 令牌,以及资源的访问地址 endpoint。

(2)系统收集用户的信用度,即 $\text{final}_{T(u)}$,判断信用度是否满足安全的信用度阈值。若不满足,系统拒绝提供服务,强制用户退出;若满足,允许数据进行资源操作。

(3)系统动态监控用户行为:动态计算用户的信用度和实时监控用户的行为级别,如图 2 所示。

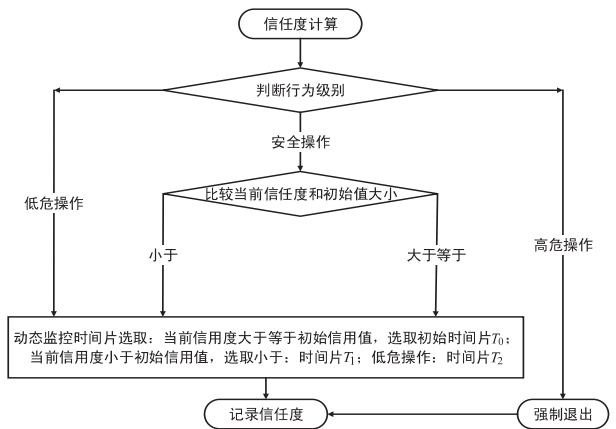


图 2 系统动态监控用户行为流程

实时信用度计算： $\text{history}_{T(u)} = \text{final}_{T(u)} W_t^T$,判断用户行为级别。

(4)用户当前信用度在有效阈值内且用户行为级别满足系统要求,回到第三步。

(5)用户当前信用度或用户行为级别任何一个不满足条件,记录信任度并强制退出系统。

3 实验与分析

服务器操作系统为 redhat7.0,搭载 OpenStack juno 版本,控制节点使用主备环境,使用 pacemaker/corosync 配置系统高可用集群环境,保证系统的高可靠性。系统存储使用网络文件系统 NFS。不同的存储表示不同的域。系统结构如图 3 所示,存储节点可根据需求不断扩展。

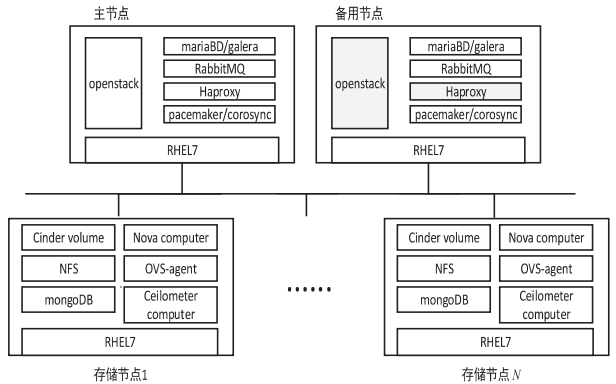


图 3 实验环境

用户登录系统时,利用 OpenStack 自身的 keystone 组件进行安全认证,以保证系统的安全性。假设用户 A 成功登陆后,系统会根据用户 A 的特性赋予其初始信用度 $\text{init}_{T(u)}$,此时用户 A 可以开始进行资源的访问操作。

实验 1 场景:用户 A 在成功登陆后获得初始信用度 $\text{init}_{T(u)} = 1$,此前用户 A 的信用度 $\text{final}_{T(u)} = 0.92$,略低于初始信用度,登入系统后先执行安全操作,做信用度累计,随后进行欺骗行为来执行低危操作,用户一直使用低危操作,并没有对资源造成直接威胁。

传统信用度计算方法:在安全操作的前提下,用户信任度小于初始值时,信任度计算加成取固定的 1.1,累计达到上限 1.5 便不再累计,危险操作的计算加成成为固定的 0.9,信任度小于阈值 0.5,强制用户退出系统。

计算方法:在安全操作的前提下,用户信任度小于初始值时,信任度计算加成取固定的 1.05,当信用度达到初始值后,加成提高到正常的 1.1,延缓信用度加成;相反对于危险操作也是一样,当行为定义在低危操作范畴内,危险性越高的操作,加权重越低。

图 4 是两种策略的信任度值的变化情况。文中方

法的特点是以更细粒度进行信用度计算,实现信用度累计慢、衰减快的特点,提高安全性。

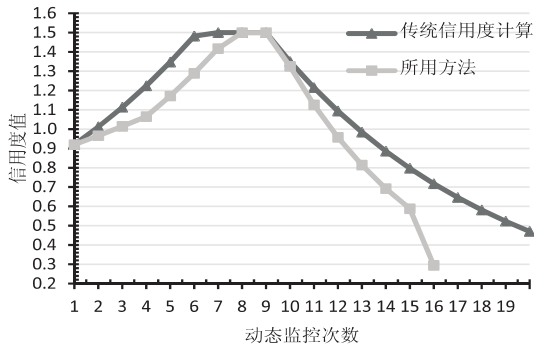


图 4 实验 1 对比

实验 2 场景:刚开始和实验 1 一样, $\text{init}_{T(u)} = 1$, $\text{final}_{T(u)} = 0.92$,略低于初始信用度,登入系统后先进行安全操作,做信用度累计,再进行欺骗行为来执行低危操作,用户刚开始进行了两次低危操作,随后是高危操作直接威胁资源的安全。

传统信用度计算方法如场景一所述。

文中方法:在动态监控用户行为级别时,低危行为依然可以做信任度计算和评价,但是一旦判别是高危行为,直接强制用户退出。

图 5 比较了是否有用户行为级别监控情况下的不同。在传统的策略上增加了用户行为级别监控,在发生高危操作时,传统方法仍然在进行信用度计算,等待低于信任度下限阈值才强制终止用户行为。而文中模型一旦评定行为是高危行为,直接强制用户退出,实时性和安全性都更高。

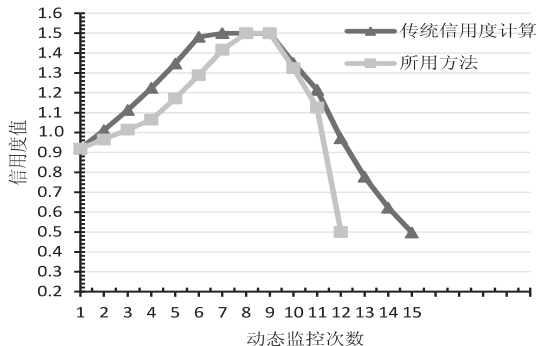


图 5 实验 2 对比

4 结束语

随着云计算的快速发展,传统的基于角色访问控制策略已经不能满足现在的安全需求。因此,文中提出一种基于角色信任度动态监控的访问控制模型。实

验结果表明,该模型在一定程度上提高了网络系统的安全性,可通过用户粒度细化解决基于角色的传统方法遇到的问题,有效提升了系统监控的实时性,并较好地解决了用户通过信任度累计进行欺骗行为的问题。

参考文献:

- [1] 李 乔,郑 啸. 云计算研究现状综述[J]. 计算机科学, 2011,38(4):32-37.
- [2] 陈 全,邓倩妮. 云计算及其关键技术[J]. 计算机应用, 2009,29(9):2562-2567.
- [3] 马 威,韩 臻,成 阳. 可信云计算中的多级管理机制研究[J]. 信息安全,2015(7):20-25.
- [4] Ren K, Wang C, Wang Q. Security challenges for the public cloud[J]. IEEE Internet Computing, 2012,16(1):69-73.
- [5] Blaze M, Feigenbaum J, Lacey J. Decentralized trust management[C]//Proceedings of 17th symposium on security and privacy. Washington, DC, USA: IEEE, 1996.
- [6] Li M, Wang H, Ross D. Trust-based access control for privacy protection in pervasion computing systems[C]//IEEE international conference on e-business engineering. [s. l.]: IEEE, 2009:425-430.
- [7] Kulkarni D, Tripathi A. Context-aware role-based access control in pervasive computing systems[C]//Proceedings of the 13th ACM symposium on access control models and technologies. [s. l.]: ACM, 2008:113-122.
- [8] Barker S, Sergot M J, Wijesekera D. Status-based access control[J]. ACM Transactions on Information and System Security, 2008,12(1):1-47.
- [9] 赵明斌,姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用, 2012,32:267-270.
- [10] 吴 慧,于 炯,于斐然. 云计算环境下基于信任模型的动态级访问控制[J]. 计算机工程与应用, 2012,48(23):102-106.
- [11] 吴明峰. 基于属性和信任评估的服务计算安全模型研究[D]. 济南:山东师范大学, 2013.
- [12] 刘 武,段海新,张 洪,等. TRBAC:基于信任的访问控制模型[J]. 计算机研究与发展, 2011,48(8):1414-1420.
- [13] 宋国峰,梁昌勇. 一种基于用户行为信任的云安全访问控制模型[C]//第十五届中国管理科学学术年会论文集(下). 北京:中国优选发统筹与经济数学研究会, 2013:669-676.
- [14] 鹿 晨,倪建成. 一种基于信任度的动态访问控制模型 T-DARBAC[J]. 电子技术, 2015(9):37-40.
- [15] 谢四江,查雅行,池亚平. 一种基于可信等级的安全互操作模型[J]. 计算机应用研究, 2012,29(5):1922-1925.