安全操作系统中基于可信度的认证和访问控制技术

汪伦伟 编著

国防科技大学出版社

安全操作系统中基于可信度的认证和访问控制技术

汪伦伟　编　著

国防科技大学出版社
·长沙·

图书在版编目(CIP)数据

安全操作系统中基于可信度的认证和访问控制技术/汪伦伟编著.—长沙:国防科技大学出版社,2005.6

ISBN 7-81099-191-4

Ⅰ.安… Ⅱ.汪… Ⅲ.操作系统-安全技术 Ⅳ.TP316

中国版本图书馆 CIP 数据核字(2005)第 060055 号

国防科技大学出版社出版发行

电话:(0731)4572640 邮政编码:410073

E-mail:gfkdcbs@public.cs.hn.cn

责任编辑:文 慧 责任校对:唐卫葳

新华书店总店北京发行所经销

国防科技大学印刷厂印装

*

开本:850×1168 1/32 印张:4.5 字数:117 千

2005 年 6 月第 1 版第 1 次印刷 印数:1-1500 册

ISBN 7-81099-191-4/TP·18

定价:10.00 元

前　言

安全操作系统在计算机系统的整体安全性中具有至关重要的作用。然而，当前安全操作系统还存在一些问题，需要进一步分析和研究，如：如何度量认证系统存在的不确定性；如何度量访问控制框架中策略对访问请求判定结果的影响程度；如何在认证和访问控制之间建立更紧密联系，使用户通过不同强度的认证机制对应具有不同的系统访问权限。

本书研究了安全操作系统中基于可信度的认证和访问控制技术，主要包括基于可信度的认证技术、基于可信度的访问控制技术，以及对象可信访问技术。

针对如何度量认证系统存在的不确定性问题，作者提出了认证可信度推理模型，对认证系统中存在的不确定性给出可信度度量；针对认证成功或失败的两种结果，给出了认证成功可信度因子和认证失败可信度因子的定义。由于安全操作系统要求提供多种认证机制进行身份认证，给出了用户通过多种认证机制后的可信度计算方法。作者还对认证可信度推理模型从阈值限度和加权两方面进行扩展，以满足多种应用环境的具体需要。通过在认证系统中引入可信度的思想，更好地描述了认证系统中的不确定性，增强了高安全级系统在多认证机制情

况下的安全性。在认证可信度推理模型的基础上，作者提出了一个基于认证规则的带有认证可信度计算的 PAM 认证框架 AT-PAM，它更能满足实际系统的需要。

针对访问控制框架中不同策略对访问判定的影响程度不同，作者提出了加权策略框架下访问请求可信度推理模型。在操作系统的访问控制框架中，对安全策略分配策略增强因子和策略削弱因子，用访问请求可信度变化的相对程度来体现策略对访问判定的影响；还给出了在加权策略框架中策略判定后的访问请求可信度计算方法，用求得的访问请求可信度与访问请求授权阈值进行比较，形成授权判定。模型根据访问请求的可信度判定是否授权，这比当前访问控制框架采用的授权方法粒度更细，更灵活，且更能满足实际系统的需要。

针对安全操作系统中认证和访问控制两个重要安全机制相互脱节，作者利用用户的认证可信度，给出了对象可信访问条件，在认证和访问控制之间建立桥梁。作者已将该条件应用于RBAC访问控制模型和 ISO 通用访问控制框架，并分别提出了基于认证可信度的RBAC模型(AT-RBAC)和基于对象可信访问的访问控制框架(TC-ACF)。AT-RBAC 模型是一个通过对象可信访问条件，将认证和访问控制两种安全机制关联而成的角色访问控制模型，它通过二重对象可信访问约束扩展了原来的 RBAC96 模型。TC-ACF 是基于 ISO 通用访问控制框架的，满足对象可信访问条件、需要进行访问请求可信度计算的关联认证和访问控制安全机制的访问控制框架。

总之，本书的研究成果推进了安全操作系统中基于可信度的认证和访问控制技术研究，并为安全操作系统的实际开发提供有益的借鉴。

本书的出版得到国家863重大软件专项服务器操作系统内核项目(2002AA1Z2101)资助。

目　录

第1章 绪 论

1.1 背景

1.1.1 安全操作系统的重要性

在信息系统安全涉及的众多内容中,操作系统、网络系统与数据库管理系统的安全问题是核心。没有系统的安全就没有信息的安全。操作系统作为系统软件的最基础部分,其安全问题的解决又是关键之关键。近年来,随着互连网的高速发展,安全问题日益复杂、严重。各种信息安全系统的核心,例如:密码认证系统(如Kerberos)的密钥分配服务器;虚拟专用网(VPN:Virtual Private Network)的网络密码机、安全策略服务器和客户端;网络入侵检测系统的主机;防火墙系统的堡垒主机、管理中心;网络杀毒的系统中心;公开密钥基础设施(PKI:Public Key Infrastructure)的认证中心(CA:Certificate Authority)、注册机构(RA:Registration Authority)、证书库(CR:Certificate Repository)等等,都需要首先保护自身不被攻破。所以,仅有应用层的安全措施绝对是不够的,需要安全操作系统作为安全信息系统的基石。

操作系统的安全性在计算机系统的整体安全性中具有至关重

要的作用，没有操作系统提供的安全性，计算机系统的安全性是没有基础的[1,2,3,120]。AT&T 实验室的 S.Bellovin 博士曾经对美国 CERT(Computer Emergency Response Team)提供的安全报告进行过分析，分析结果表明，很多安全问题的根源都在操作系统的安全脆弱性之中[4]。

操作系统的安全机制在支持高层应用程序的安全性上有着重要的作用，它对于整个系统安全的重要性是无可替代的。上层的应用软件要想获得运行的高可靠性和信息的完整性、保密性，必须依赖于操作系统提供的安全机制作为基础，任何想像中的、脱离操作系统的应用软件的高安全性，就如同幻想在沙滩上建立坚不可摧的堡垒一样，毫无根基可言。

1.1.2　安全操作系统研究的新问题

当前安全操作系统的研究主要有安全模型的研究、安全策略和安全机制的研究、检验和评估系统安全性的科学方法和准则的研究，以及符合这些模型、策略和准则的系统的研制等。由于 Linux 的出现，基于该原型的安全操作系统的研究得到进一步的发展，主要的技术途径是利用现有的安全技术和安全标准(如 ISO/IEC 15408 标准[66])对其进行充实和增强。尽管安全操作系统的研究取得了很大的进展，但是我们发现安全操作系统还存在下面一些需要讨论的问题。

1.1.2.1　如何度量认证系统存在的不确定性

在当前的安全操作系统中，用户成功地通过系统的某种认证机制，便认为该用户为“可信”用户。然而，黑客可以通过多种途径成功骗取用户的认证凭证而通过系统对其的认证，但黑客明显不是“可信”用户。而且可信是非理性的[5,6,7,8]，是一种经验的体现，

不仅仅有具体的内容，还应有程度的划分。通过系统认证的用户其可信的程度如何？他通过本地登录认证和通过网络认证后的可信程度相同吗？如果不同，应该如何区分不同的可信程度？

因此可以说认证系统存在一些不确定性，具体表现为：认证机制是否可信、认证规则是否可信，以及认证结论是否可信。

认证机制是否可信的不确定性指安全管理员主观上对认证机制的可靠性和安全性不能完全确定。认证机制是否安全？是否正确？机制中是否有可信路径保证在认证过程中将认证信息传输到正确的验证方？是否含有特洛伊木马程序以骗取用户的认证凭证？所有这些问题均会导致认证机制是否可信的不确定性。因此，在进行认证判定时，需要考虑认证机制的可信性。认证规则是否可信的不确定性指用户通过某种认证机制的认证即为合法用户，这仅仅是一种“可能”，也就是说，安全管理员需要对认证规则持有某种信任度。这种未必都有100%把握的认证规则的信任度也叫做认证规则强度。

认证结论是否可信的不确定性指在包含各种不确定性的前提条件下，运用具有不确定性的认证规则，引出的结论是否可信不可避免地具有不确定性，它反映了认证机制是否可信和认证规则是否可信不确定性的动态积累和传播过程。在推理的每一步都需要综合考虑认证机制是否可信和认证规则是否可信的不确定性，为此，需要对不确定进行度量，寻找尽可能符合客观实际的计算模式，随着推理步骤的展开和不确定性度量的传递计算，最终得到认证结论是否可信的不确定性度量。

此外，不同的认证机制对于整个系统的安全性影响是不同的，高安全级系统采用的认证机制必然要求具有较高的安全强度，如何体现这些认证机制的安全强度？而且，随着认证技术及认证框架[9-13]的发展，一些高安全级系统不仅要求有很强的安全认证机制，而且要求有多种认证机制共同增强系统的安全性，那么，如何

有效地组织多种认证机制形成的认证判定，并给出最终的判定结果？

1.1.2.2　如何表示访问控制框架中策略对访问决定的影响程度

当前，安全操作系统发展到动态策略时期[103]，要求操作系统支持多种安全策略的动态变化，实现安全策略的多样性，为安全策略提供灵活性支持，没有一种策略模型可以满足各种环境的安全需要，系统必须支持多个安全策略模型，如 RSBAC(Rule Sets Based Access Control)[14]、SELinux(Security Enhanced Linux)[16,17]就支持多个安全策略模型。

由于访问控制框架[86,88]可以对多个安全策略提供支持，因此，许多安全操作系统都采用访问控制框架来支持多个安全策略，如 RSBAC 系统中采用的 GFAC(Generalized Framework for Access Control)框架[15]、SELinux 系统中采用的 Flask[18,19,43]结构、TrustBSD 中采用的 MAC 框架[20-23]等，包括 Linux 也采用了 LSM(Linux Security Modules)框架[24,25]。国内也有一些科研机构对安全操作系统访问控制框架进行了研究，包括红旗安全操作系统(RFSOS)采用二项缓冲机制的 GFAC，称之为 DGFAC(Double-levels-cache GFAC)[111]；国家 863 重大软件专项服务器操作系统 Kylin 采用的 KACF(Kylin Access Control Framework)，等等。

一些多安全策略系统，如文献[26,27]所描述，它将策略授权分为强授权和弱授权，其基本思想是：强授权的优先级高于弱授权，强授权不能被覆盖，而弱授权根据具体的规则，可以被其他强授权或弱授权所覆盖。

然而，在当前的访问控制框架研究中，所有的安全策略都具有相同的重要性，它们在访问控制框架中都是并列关系。在实际应用中，由于具体应用环境的不同，对具体安全策略的需要也不同，有些系统要求强调数据机密性，而有些系统要求强调数据完整性，

等等,不同的安全策略在访问控制框架中应该具有不同的重要性,如何区分访问框架中这些策略的重要性?而且,不同策略对访问请求的判定有可能成功,也有可能失败,判定成功情况下还有强授权和弱授权之分,如何体现访问控制框架中不同策略对访问请求最终判定结果的影响程度?如何根据多安全策略框架下不同策略针对访问请求形成的访问判定,组织形成最终的访问判定结果?

1.1.2.3 认证与访问控制相互脱节

安全操作系统要求提供包括身份标识和鉴别(认证)、访问控制、审计等多种安全功能,而且安全操作系统的各种评估标准都对用户鉴别给出了相应的说明及要求,用户鉴别作为其他安全功能(如访问控制、安全审计)的前提,其他安全功能的有效性都建立在对用户的正确标识和鉴别基础上。因此,认证在安全操作系统中具有很重要的作用。

当前很多安全操作系统都基于 PAM(Pluggable Authentication Modules),即可插拔认证模块提供系统认证服务。PAM 框架为实现和应用最新的认证技术提供了灵活的途径,它可以提供多种认证机制来增强系统的安全性。根据系统的认证规则,用户通过系统认证机制的认证,则认为其身份合法,但在一些带有多认证机制的高安全级系统中,要求用户通过不同强度的认证机制后,所具有的访问权限也不相同。相对于认证强度较弱的机制,如口令机制,系统将授予通过此类机制认证的用户较少的访问权限,而对于较强的认证机制,如指纹仪认证机制等,系统将授予通过此类机制认证的用户更多的访问权限。

当前的安全操作系统中,用户通过系统认证,则确定其安全标识,系统的其他安全机制,如访问控制则根据用户的标识进行判定,用户具体通过哪种认证、认证机制的强度如何、认证策略的配置是否存在问题等等,这些都与访问控制无关。认证与访问控制

作为安全操作系统的两个重要安全机制，互相脱节，这不满足安全系统的需要。

1.2　相关的研究工作

本书主要针对安全操作系统中认证系统存在不确定性、访问控制框架中策略对访问决定的影响程度，以及认证和访问控制之间如何紧密关联进行的研究，涉及到对不确定性进行度量的可信度的一些概念和安全操作系统中认证和访问控制框架技术等内容。因此，我们进行了大量的调研工作，在本节里把国内外一些相关的研究工作总结如下。

1.2.1　可信的概念及定义

目前，对于可信还没有一个精确的、广泛可接受的定义。《美国传统辞典》对名词词性的“可信”的解释是：Trust denotes a feeling of certainty that a person or thing will not fail. Trust implies depth and assurance of feeling that is often based on inconclusive evidence.（可信代表着一种对某个人或某件事不会失败的必然性的感觉。可信暗示着这种基于不确定证据之上的感觉的程度和确定性）。

心理学家 Golembiewski 和 McConkie 专门从心理学的角度对可信进行研究，并认为：“可信暗示着对结果的不确定性程度，可信暗示着对结果的希望和乐观”[28]。在计算机人工智能研究领域，多数学者[29-32]接受了从心理学角度对可信的理解，普遍认为可信是一种主观信念。其中，D.Gambetta 给出了一个比较完整的可信定义，“可信（或不可信）是一个 agent 评价其他 agent 或 agent 团体实际行为的主观可能性程度，评价在对该行为进行监控（或根本不可

能监控该行为)之前和与该行为对其自身行为产生影响的情况下进行"[32]。该定义给出了可信的几个重要特征:

(1) 主观性,不同的个体对同一事物的看法会受个体喜好等因素影响而不同;

(2) 可能性预期,可信的程度可表示为对事件发生概率的估计;

(3) 内容相关,可信是对事物的某个方面(如完成某项任务的能力)而言的。

可信计算组(TCG:Trusted Computing Group)从行为角度来定义可信性[33]:一个实体是可信的,如果它的行为总是以期望的方式,趋向预期的目标。围绕此定义,TCG 给出了可信计算的相关概念以及一些可信计算规范[34-36]。

所谓的可信计算,是以行为作为判别依据的,区别于 TCSEC[37]中的权限判别。其基本思路是从一个初始的"信任根"(基于物理安全保证的,具有良好的管理安全性)出发,在平台计算环境的每一次转换时,这种信任状态可以通过传递的方式保持下去并不会被破坏,那么平台上的计算环境始终是可信的,在可信环境下的各种操作也不会破坏平台的可信,平台本身的完整性得到保证,终端安全也自然得到了保证,这也就是信任链的传统机制。

作者认为,在计算机安全操作系统中,可信是指一个实体对其他实体是否能够正确地、非破坏性地进行某项(类)活动的主观可能性预期,预测的依据来源于此前该实体所观察到(包括其他可信任第三方提供)的目标实体的行为,预测结果受该实体对此项活动的重要程度评价的影响。

依据可信的定义,一个完整的可信度推理模型应包含如下主要内容:

• 可信度推理实体。可信度推理过程中的参与者,包括可信度推理主体、可信度推理客体以及可信度信息推荐者。

• 可信关系的度量。如何解释和量化可信关系，亦即选择何种实体间传递的信息来解释和量化可信关系。

• 可信度相关信息的推导和综合。可信度信息可能通过多个实体组成的路径最终传递到可信关系的推理主体，模型应该给出如何推导和综合这些可信度相关信息的方法。

• 可信度判断。可信关系的度量目的是进行可信度判定，可信度推理模型还应包括如何依据可信度进行可信度判断。

1.2.2　安全操作系统身份认证技术

身份认证是安全操作系统的重要机制之一，是安全操作系统的首要屏障，目的是验证通信双方的真实身份，防止非法用户假冒合法用户进入系统，窃取敏感数据。

身份认证的本质是被认证方有一些信息（无论是一些秘密的信息，还是一些个人持有的特殊硬件或个人特有的生物学信息），除被认证方外，任何第三方都不能伪造，被认证方能够使认证方相信他确实拥有那些秘密（无论是将那些信息出示给认证方或者采用零知识证明的方法），则他的身份就得到了证实。

安全操作系统要求提供包括身份标识和鉴别（认证）、访问控制、审计等各种安全功能，而且安全操作系统的各种评估标准都对用户鉴别给出相应的说明及要求，用户鉴别作为其他安全功能（如访问控制、安全审计）的前提，安全功能的有效性都建立在对用户的正确标识和鉴别基础上。因此，认证在安全操作系统中具有很重要的作用。

近年来认证理论和技术得到了迅速发展，产生了各种认证机制，如口令机制，RSA、DCE、kerberos[38]认证体制，S/Key[39]和基于智能卡的身份认证等。这些认证机制可以分成三种身份认证类型（按最弱到最强的顺序排列），它们的依据分别是：