多权限信息系统授权机制的研究与实践

龚洪泉　姚　丹　钱乐秋
(复旦大学计算机与信息技术系软件工程实验室　上海 200433)

摘　要　本文针对信息系统中出现的权限管理问题,结合信息系统开发的实践经验,对多权限信息系统中的授权机制问题进行了深入浅出的研究。针对传统授权机制的缺陷,提出了动态授权机制和增强的授权机制,最后遵循软件复用的思想,利用软件构件技术开发了权限管理构件,并在实际的信息系统开发中成功地应用了该技术。

关键词　多权限信息系统　授权机制　软件复用　软件构件技术

RESEARCH AND PRACTICE ON AUTHORIZATION MECHANISM OF MULTI-PRIVILEGE INFORMATION SYSTEM

Gong Hongquan　Yao Dan　Qian Leqiu
(Software Engineering Laboratory, Department of Computer and Information Technology, Fudan University, Shanghai 200433)

Abstract　In this paper, some problems about privilege management in information system are addressed. Based on the experiences acquired in the process of information system development, the authorization mechanism of multi-privilege information system is studied exhaustively. To overcome the limitations of traditional authorization mechanism, dynamic authorization mechanism and enhanced authorization mechanism are proposed. Follow the software reuse idea, based on the software component technology, privilege management component is developed and successfully used in a real information system.

Keywords　Multi-privilege information system　Authorization mechanism　Software reuse　Software component technology

1　引　言

随着计算机和网络技术的发展,信息系统在网络环境下得到了广泛的应用,所有的操作人员通过网络在自己的计算机终端上使用信息系统。由于信息系统通常都涉及到企业的核心数据,信息安全成了计算机领域的一个研究重点。在各种网络安全技术的保护下,信息系统可以抵御来自外界的大多数威胁。然而,俗话说"家贼难防",每年全球各大企业因为内部员工泄密而遭受的损失数目惊人。

从这些事件中我们感到,除了保护信息系统免受外部的攻击外,我们还必须加强信息系统的内部防护能力,也就是必须在信息系统内部为不同操作人员设置不同级别的信息读写权限。然而,这种权限级别的设置,通常是依靠用户名和口令来确定的,一旦口令泄密,整个权限管理形同虚设,所以应当为信息系统考虑更加完善的权限控制机制。

在早期的信息系统中,系统的规模和结构比较简单,功能比较单一,所有的操作人员拥有相同的系统使用权限,只要有登录口令就可以进入系统,执行所有的操作。在这种系统中,由于所有操作人员的权限都是一样的,彼此没有差别,我们称这种系统为单一权限信息系统。在设计这种系统的过程中,往往只需要在用户登录时检查他们的口令,而不需要对其它任何操作考虑用户的权限问题,这样存在很大的安全隐患,如果一个操作员对他人心存怨恨,他就可以向系统中输入对自己有利或对他人不利的信息,比如工资数据。一时信息系统的口令泄密,别人就可以轻易地窃取或恶意篡改系统的机要数据。由于系统的权限单一,所以不能在权限机制上很好地保护信息系统的核心数据。

在随后的信息系统中,系统规模和结构变得越来越复杂,系统功能也越来越多,而且系统往往涉及到企业的所有业务操作数据。为了达到既能完成系统业务操作,又能保护系统信息的目的,对信息系统的操作人员划分权限级别的机制被提了出来。不同级别的操作人员拥有不同级别的操作权限,每个操作人员只能对自己权限允许的数据进行操作,而不能跨越级别去操作另一级别权限所保护的数据。比如在人事管理系统中,经理可以决定每一个员工的工资级别,而一般的操作人员只能处理员工工作业绩信息。

在这种系统中,对不同的操作人员有不同的权限要求,我们称这种系统为多权限信息系统。在设计这种系统的过程中,必须考虑操作人员的权限问题。如何对操作人员授权,什么时候授权,授权后如果发生口令泄密问题如何应付,所有这些问题引出了我们对多权限信息系统授权机制的研究。

2　传统授权机制

对于多权限信息系统,为了控制拥有不同权限级别的操作人员在信息系统中的操作,我们必须对所有的操作进行权限划

收稿日期:2003 - 01 - 10。龚洪泉,博士生,主研领域:软件工程,软件复用,构件库管理系统,基于构件,构架的软件开发方法,系统开发模式。

分,然后根据操作人员的业务范围决定他可以执行哪些操作,最后把可以执行这些操作的权限赋给该操作员就算完成了系统权限的授权过程。

一种看似简便的授权机制是在信息系统集成时,为不同级别权限的操作人员集成与之权限级别相对应的系统功能,每个级别的操作人员对应一个单一的小系统,有不同级别权限的操作人员使用与自己权限相对应的系统。这种机制在只有两三种权限级别的情况下比较容易实现,如果系统的权限级别比较多,而且经常变动,这种方法实现起来就比较浪费时间。原因是它必须为每种权限作一次系统集成,在权限调整后又要重新集成,这种时间上的浪费是显而易见的。

更进一步来说,在信息系统交付用户以后,脱离了集成环境,就不可能再随时变动权限设置,这就使得它缺乏灵活性,无法为用户的管理带来更多的方便。另外,这种机制所带来的直接后果就是信息系统被分裂成多个功能重叠的小系统,使系统维护和升级工作显得十分烦杂,给用户和系统维护人员增加了不必要的负担。

如何在保证系统完整性的情况下,在系统运行过程中,动态地调整操作人员的权限而不需要重新集成系统,这就是动态授权机制所要考虑的问题。

3　动态授权机制

所谓动态授权机制,就是信息系统只需要一次系统集成工作,在系统运行过程中,系统管理人员可以随时赋予操作人员新的权限,也可以随时从操作人员那里收回权限,所有这些赋予和收回权限的操作都不会影响整个信息系统的运行。这种机制可以保证信息系统的完整性,既节省了系统集成时间,又减轻了系统维护负担,也为信息系统的管理工作带来了极大的方便。

在多权限信息系统设计过程中,我们不但要完成信息系统功能方面的设计,同时还必须考虑操作人员的权限如何动态赋予和收回的问题。一种方法是在执行每个操作之前实时查询操作人员是否有权执行这个操作,这种机制能够实现授权机制的完全动态性。只要系统的权限设置发生了变动,在操作人员执行下一个操作时就可以反映出来,这样能保证动态授权的及时有效性。

但是为了实现这种机制,在每个系统功能的实现代码前都必须嵌入一段判断当前操作人员权限的代码。一方面它会使得信息系统的代码变得十分臃肿,另一方面也使得信息系统的功能实现和权限管理交织在一起,给系统维护增加额外的负担。如果某个操作代码前遗漏了关于权限判断的语句,那么所有的权限设置都成了一纸空文。所以我们必须考虑一种与系统功能实现完全独立的动态授权机制实现方案。

动态授权机制的第二种实现方法就是,在完成信息系统功能设计与开发后,得到该信息系统的功能清单,然后由系统管理员对信息系统不同权限级别的操作人员分配执行这些功能的权限。当操作人员登录信息系统时,信息系统根据该操作人员分配到的权限动态生成相应的操作界面,从而达到根据信息系统功能分配来控制操作人员权限的目的。当系统权限发生变更后,未受权限调整影响的操作人员仍然可以继续使用系统,受影响的操作人员在重新登录系统后就能得到新的界面,执行新权限所赋予的功能。这种"分而治之"的方法使得信息系统的功能实现与权限控制完全独立开来,系统设计人员就不会在进行功能设计的时候被系统的权限管理问题分散注意力,而且系统维护工作也变得比较简单,只需要按照常规的维护程序进行就可以了。

正因为信息系统的功能实现与权限管理之间的关系是完全独立的,按照软件复用的思想,利用构件技术,我们可以开发一个在每个信息系统中都能应用的权限管理构件,在信息系统集成时将它集成进去,然后在信息系统中用管理人员的身份进入系统就可以执行系统的动态授权操作。

4　新的问题

上面的动态授权机制解决了不同级别操作人员有不同系统使用权限的分配问题。操作人员以自己级别的身份进入信息系统只可能做他(她)这个级别所允许的操作。但在信息系统的实际使用过程中,上面的技术方法无法克服管理方面的漏洞。比如说,某个职员无意中得到了部门经理使用信息系统的相关认证介质,则他(她)有可能通过自己的计算机使用部门经理的身份进入信息系统查看某些机要数据或恶意破坏系统的重要数据,这将对信息系统的安全造成极大危害。

5　增强的授权机制

在信息系统安全性方面有这样一句话:"三分技术,七分管理",它指出在系统权限控制方面,管理起着十分重要的作用。上面提到的新问题显然是由于管理不慎造成的,然而我们作为信息系统的设计与开发人员,应尽量在技术上使信息系统的权限控制更易于管理,使系统的安全性漏洞尽量减少。

新问题的关键在于操作人员获取了他人进入信息系统的相关认证介质后,可以在能访问信息系统的任意一台计算机上以他人的身份进入信息系统,从而造成系统安全性方面的隐患。针对这个问题,我们对动态授权机制进行了扩展,提出了下面增强的授权机制。

增强的授权机制在动态授权的过程中除了考虑信息系统功能和操作人员权限的对应关系外,还通过对使用信息系统的每一台计算机设定唯一的访问标志号来指定权限与计算机的对应关系。从表面上看,系统功能和权限是多对多的关系,权限与计算机的关系也是多对多的关系,但是,增强的授权机制在运行过程中实际上是通过权限对计算机进行了分组,每组计算机上只能由某种权限的操作人员使用。所以从本质上来说,除了系统管理员这个权限所对应的计算机可以执行所有的操作以外,其它的计算机上赋予的权限都是有限的。通过将计算机物理设备的管理融入到信息系统的权限管理过程中,在权限密码泄漏的情况下仍然可以确保系统拒绝他人在未被授权的计算机上登录。

在没有采用增强授权机制前,如果一个员工获得了部门经理的登录密码,他可以很方便地在能连上信息系统的任意一台计算机上用部门经理的身份进入系统,而且不易被别人发现。有了增强的授权机制,按照该机制的规则,部门经理这个权限只允许在部门经理办公室的计算机上登录,即使某个员工通过不正当渠道取得了部门经理的登录密码,他仍然不可能在其它的计算机上以部门经理的身份进入系统。而且由于有部门经理管理自己的计算机,员工不可能公然到部门经理的办公室去使用

(下转第 112 页)

5 结束语

本文介绍了在 Visual Studio.NET 环境下,利用 ASP.NET 实现动态 Web 报表一种方法,利用 Crytal Report 的"数据库专家"还可以轻松地在 Web 环境下实现各种统计图表,限于篇幅,不能详细介绍,有兴趣的读者,可以与作者联系交流。

参 考 文 献

[1] David Richard Kalksteim DeLoveh、William Sempf,Visual Studio.NET 高效编程,清华大学出版社,2002.

[2] 李劲,动态电子商务的 Web 服务,清华大学出版社,2002.

[3] Jason Bentrum、James Whatley,.MET 框架下电子商务站点建设指南,机械工业出版社,2002.

[4] http://msdn.microsoft.com.

(上接第 17 页)

部门经理的计算机。这样通过授权机制对计算机进行分组,同时加入人的管理因素,就能防止绝大部分内部员工泄密事件的发生。

增强授权机制的关键在于如何确定使用信息系统的每台计算机的唯一标识号,这可以根据计算机 CPU 编号或网卡的全球唯一编号来确定。同样遵循软件复用的思想,可以采用软件构件技术开发计算机标识号登记构件和标识号认证构件,然后把它们与动态授权构件结合在一起,形成增强的授权机制套件。在实际应用中只需要把增强的授权机制套件集成到信息系统中,由信息系统管理员采集整个系统的计算机标识号后对操作人员分配权限,整个系统就可以使用了。操作人员登录系统时,标识号认证构件将对操作人员使用的计算机进行认证,判定该操作员是否有权限使用该计算机。这种授权机制使得系统权限与操作人员权限级别和计算机进行双重关联,从而达到较高的信息系统权限控制水平,增强了信息系统的安全性。

6 授权机制的应用

上海市教育考试院的网上招生管理系统,是对上海市每年高考的考生档案进行电子化管理的多权限信息系统。它负责将考生档案投递到各个高校,同时完成对高校退档上报、录取上报的信息进行审核工作。该系统中涉及的用户有投档组、材料审核组、领导组、院校计划控制组、对外联络组等,每个组有不同的系统使用权限。比如说,投档组是控制每一批投档分数线的关键管理者,分数线是由系统根据当前院校的招生计划和考生的成绩排名来自动计算的,其他人员不得随意更改,所以投档组的口令是必须保密的。为了防止口令泄漏而被他人用投档组的身份进入系统的情况发生,我们采用增强的授权机制,将投档组的权限限制在由专门管理人员负责的某几台计算机上,很好地保护了招生工作的机要信息,杜绝了以往一般工作人员泄漏招生信息的现象。在该系统开发过程中,我们采用了上面提出的多权限信息系统授权机制,开发了增强的授权机制权限管理套件,并在该系统中应用,取得了良好的效果,减轻了招生过程中权限管理的负担,增强了该系统的安全性。

7 结束语

在信息系统开发过程中,我们越来越多的遇到多权限信息系统的授权机制问题。值得注意的是,信息系统的授权机制问题与信息系统的安全问题侧重点不同,信息系统授权机制问题主要研究如何控制信息系统内部操作人员使用信息系统的权限,它是确保信息系统安全的一种手段。本文根据信息系统开发的实践经验,深入浅出地对该问题进行了详细的研究,提出了可行的多权限信息系统授权机制,同时遵循软件复用的思想,利用软件构件技术开发了权限管理套件,并在实际的信息系统开发中成功应用了该技术。

参 考 文 献

[1] 朱三元、钱乐秋、宿为民,软件工程技术概论,科学出版社,2002 年.

[2] 徐正权,软件复用方法与技术,华中理工大学出版社,1998 年.

[3] 冯玉琳等,对象技术导论,科学出版社,1998 年.

[4] 周之英,现代软件工程,科学出版社,2001 年.

[5] Roger S. Pressman,Software Engineering,A Practioner's Approach,(4th Edition),McGraw-Hill,1997.

[6] Ivar Jacobson,Martin Griss,Patrik Jonsson,Software Reuse,1997.

[7] Andrew S. Tanenbaum,Computer Networks,(3rd Edition),Printice Hall,1996.

(上接第 73 页)

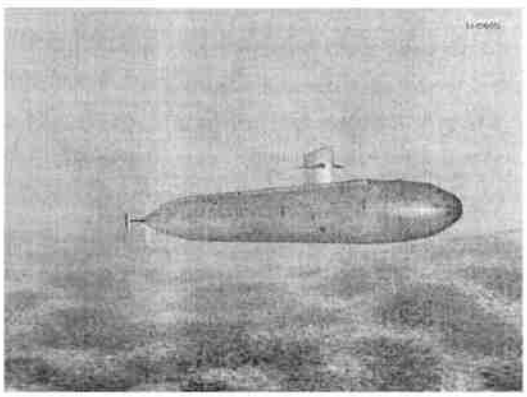

图 2 显示水下透明度的效果图

的研究设计等关键技术。本项研究也为其它专业领域的 Vega 用户开发自主知识产权的扩展模块进行了有益的探索。

参 考 文 献

[1] MultiGen-Paradigm Inc.,Sensor Products Guide (Version 3.7).[Z].U.S.A:MultiGen-Paradigm Inc.2001.

[2] 宋志明、康凤举等,"水下航行器视景仿真系统的研究[J]",《系统仿真学报》,2002,14(6):761～764.

[3] 军事海洋学[EB/OL],http://www,ikepu.com.cn/geography/ocean/branch/military_oceanography_total.htm,2002.9

[4] MultiGen-Paradigm Inc.,Vega Programmer's Guide (Version 3.7).[Z].U.S.A:MultiGen-Paradigm Inc.,2001.

[5] MultiGen-Paradigm Inc.,Vega Options Guide (Version 3.7).[Z].U.S.A.:MultiGen-Paradigm Inc.,2001.

[6] MultiGen-Paradigm Inc.,Lynx User's Guide (Version 3.7).[Z].U.S.A.:MultiGen-Paradigm Inc.,2001.

[7] MultiGen-Paradigm Inc.,Vega Man Pages (Version 3.7).[Z].U.S.A.:MultiGen-Paradigm Inc.,2001.

[8] David J. Kruglinski,Inside Visual C++,4th Edition [M].Microsoft Press,1997.

[9] Open GL,三维图形设计与制作[M],北京:人民邮电出版社,1999.

[10] 宁波海洋学校,海洋学[M],北京:海洋出版社,1986.