浅析访问控制的审计跟踪

Brief Analysis of Access Control Audit Trail

杨志彬 （安徽财经大学 实验室管理处 安徽 蚌埠 233030）

摘 要： 随着网络的日益普及,网上办公及网络资源访问成为我们工作的一项重要内容。网上资源及信息的安全则关系到相关网络信息系统软件的正常使用。除了对网络及相关资源的正常安全维护措施以外,访问控制从权限方面对信息的使用者进行了一定的分类约束,审计跟踪为访问控制的实施提供了坚实的保障。

关键词： 访问控制 审计跟踪 攻击检测方法

随着互联网络技术的蓬勃发展,企业在信息资源的使用上日新月异,在企业提供越来越多的共享资源的同时,同样要求企业完善相应手段,阻止非授权用户对企业敏感信息资源的访问。访问控制就是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权访问,其目的就是为了保护企业在信息系统中存储和处理的信息的安全。

访问控制的实现首先要考虑对合法用户进行验证,然后是对控制策略的选用与管理,最后要对非法用户或是越权操作进行管理。所以,访问控制包括认证、控制策略实现和审计三方面的内容。本文从访问控制审计跟踪、审计跟踪目的、跟踪日志类型、审计跟踪实施以及审计信息跟踪攻击检测技术等方面对审计跟踪在企业信息资源的访问控制方面的作用进行简要分析。

1 访问控制审计和审计跟踪

1.1 访问控制审计

审计是访问控制的重要内容和必要补充。审计会对用户使用何种信息资源、使用的时间、以及如何使用(执行何种操作)进行记录与监控。审计是实现系统安全的一道防线,处于系统的最高层。审计能够再现原有的进程和问题,这对于责任追查和数据恢复非常有必要。

1.2 审计跟踪概述

审计跟踪是对系统活动的流水记录,记录着每个事件的环境及活动,审计跟踪通过书面方式提供责任人员的活动证据以支持访问控制职能的实现。审计跟踪记录系统活动和用户活动:系统活动包括操作系统和应用程序进程的活动;用户活动包括用户在操作系统中和应用程序中的活动。通过借助适当的工具和规程,审计跟踪可以发现违反安全策略的活动、影响运行效率的问题以及程序中的错误。审计跟踪不但有助于帮助系统管理员确保系统及其资源免遭非法授权用户的侵害,同时还能提供对数据恢复的帮助。

审计跟踪可以作为对正常系统操作的一种支持,也可以作为一种保证策略或前两者兼而有之。作为保证策略,所维护的审计跟踪只在需要时使用,比如系统中断。作为对操作的支持,审计跟踪用于帮助系统管理员确保系统及其资源免遭黑客、内部使用者或技术故障的伤害。

2 审计跟踪的目的

审计跟踪提供了实现安全的多种相关目标,这些目标包括个人职能、事件重建、入侵探测、系统负载的监控和故障分析。

2.1 个人职能

审计跟踪是管理人员用来维护个人职能的技术手段。通过告知用户为自己的行为负责,通过审计跟踪记录用户的活动,管理人员可以改善用户的行为方式,如果用户知道他们的行为被记录在审计日

志中,他们就不太会违反安全策略和绕过安全控制措施。

例如在访问控制中,审计跟踪可以用于鉴别对数据的不恰当修改(如在数据库中引入一条错误记录)和提供与之相关的信息。审计跟踪可以记录改动前和改动后的记录,以确定所作的实际改动。这可以帮助管理层确定错误到底是由用户、操作系统、应用软件还是由其它因素造成的。

访问控制用于限制用户对系统资源的访问,允许相应用户访问相应资源以完成他们的工作。当然,被授权的访问也会被滥用,在这种情况下审计跟踪就能发挥作用。当无法阻止用户通过其合法身份访问资源时,审计跟踪就可以用于检查他们的活动。比方说人事部的某员工需要访问他们所负责的员工的人事记录,通过审计跟踪发现该员工对人事记录的超常打印,这也许意味着盗卖人事数据。再比方说某工程师需要通过使用计算机来设计新产品,通过审计跟踪发现在该工程师在设计结束前通过调制解调器进行了可疑的对外通信,这可以用来协助调查公司的专利数据被非法泄漏给其它公司的事件。

2.2 事件重建

在故障发生后,审计跟踪可以用于重建事件。通过审查系统活动的审计跟踪可以比较容易地评估故障损失,确定故障发生的时间、原因和过程。通过对审计跟踪的分析通常可以辨别故障是操作引起的还是系统引起的。例如,当系统失败或文件的完整性受到质疑时,通过对审计跟踪的分析就可以重建系统、用户或应用程序的完整的操作步骤。在对诸如系统崩溃这样的故障的发生条件有清晰认识的前提下,就能够避免未来发生此类系统中断的情况。

2.3 入侵探测

审计跟踪记录的相关信息,也可以用来协助入侵探测工作。如果在审计记录产生时就进行检查(通过使用某种警告标志或提示),就可以进行实时的入侵探测。实时入侵探测主要用于探测外部对系统的非法访问,也可以用于探测系统性能指标的变化以发现病毒或蠕虫攻击,这样就可以提醒人们对损失进行评估或重新检查受攻击的控制方式。

2.4 系统负载的监控

在对系统数据访问时,除了要应对各种外界对数据资源的干扰以外,正常数据访问过程中因数据访问量过大,造成系统超负荷运行以致系统崩溃的事情经常发生,通过审计跟踪各用户对系统数据访问的不同时段的数据访问量的情况,产生各用户对系统负载的压力大小的报告,以此制定用户访问策略,分散数据访问压力。通过对长时间的系统数据访问的监控和审计还能对系统日后升级制定方案提供数据支持。

2.5 故障分析

在线的审计跟踪还可以用于鉴别入侵以外的故障。这常被称为实时审计或监控。如果操作系统或应用系统对公司的业务非常重要,可以使用实时审计对这些进程进行监控。

3 审计跟踪记录日志的类型

3.1 击键监控

击键监控用于对计算机交互过程中的用户键盘输入和计算机的反应数据进行检查或记录,通常被认为是审计跟踪的一种特殊应用。击键监控的例子包括检查用户敲入的字符,阅读用户的电子邮件以及检查用户敲入的其它信息。如果保存这些记录与之相关的用户鉴别码就可以协助管理员对击键人击键的目的进行监控。击键监控致力于保护系统和数据免遭非法入侵和合法用户的滥用,可以协助管理员评估和修复入侵造成的损失。

3.2 面向事件的审计日志

系统审计日志一般用于监控和微调系统性能。应用审计跟踪可以用于辨别应用程序中的错误和对安全策略的违背,分析用户审计记录可以发现各种不安全的事件,如安装木马或获取非法权限。

有时比系统审计跟踪更详细的记录也是需要的。应用审计跟踪就可以提供更详细的记录。如果应用是非常关键的,那么就不但要记录应用的发起者,还要记录每一个用户的具体细节。例如电子邮件应用,可能要记录发件人、收件人和信息长度。再比如数据库应用,应该记录数据库的访问者以及其具体读取(或更改、删除)哪个表的哪个行或列,而不是仅仅记录数据库程序的执行。

从安全角度看,系统管理员应该能够监控所有的

系统和用户活动,又能有选择地记录系统和应用的特定功能。至于日志记录的数量和需要审查的数量取决于相关应用或数据敏感性,应该由职能部门经理或应用所有者在系统管理员和计算机安全管理人的指导下根据日志的性价比确定。通常审计日志包含隐私内容,用户应该熟悉使用环境下和隐私相关的现行法律、法规和政策。

4 审计跟踪的实施

为了确保审计跟踪数据的可用性和正确性,审计跟踪数据需要受到保护。审计跟踪应该根据需要(经常由安全事件触发)定期审查、自动实时审查、或两者兼而有之。系统管理人和系统管理员应该根据计算机安全管理的要求确定维护审计跟踪数据时间长度,其中包括系统内保存的和归档保存的数据。与实施有关的问题包括:(1)保护审计跟踪数据,(2)审查审计跟踪数据,(3)审计跟踪分析工具。

4.1 保护审计跟踪数据

防止非法修改以确保审计跟踪数据的完整性尤其重要。使用数字签名是实现这一目标的一种途径。另一类方法是使用只读设备。入侵者会试图修改审计跟踪记录以掩盖自己的踪迹是审计跟踪文件需要保护的原因之一。使用强访问控制是保护审计跟踪记录免受非法访问的有效措施。当牵涉到法律问题时,审计跟踪信息的完整性尤为重要(这可能需要每天打印和签署日志)。审计跟踪信息的机密性也需要受到保护,例如审计跟踪所记录的用户信息可能包含诸如交易记录等不宜披露的个人信息。强访问控制和加密在保护机密性方面非常有效。

4.2 审查审计跟踪数据

审计跟踪的审查和分析可以分为事后检查、定期检查或实时检查。审查人员应该知道如何发现异常活动,他们应该知道怎么算是正常活动。如果可以通过用户识别码、终端识别码、应用程序名、日期时间或其它参数组来检索审计跟踪记录并生成所需的报告,那么审计跟踪检查就会比较容易。

4.3 审计跟踪工具

许多工具是用于从大量粗糙原始的审计数据中精选出有用信息。尤其是在大系统中,审计跟踪软件产生的数据文件非常庞大,用人工方式分析非常困难。使用自动化工具就是从审计信息中将无用的信息剔除。其它工具还有差异探测工具和攻击特征探测工具。

4.3.1 审计精选工具

此类工具用于从大量的数据中精选出有用的信息以协助人工检查。在安全检查前,此类工具可以剔除大量对安全影响不大的信息。这类工具通常可以剔除由特定类型事件产生的记录,例如由夜间备份产生的记录将被剔除。

4.3.2 趋势/差别探测工具

此类工具用于发现系统或用户的异常活动。可以建立较复杂的处理机制以监控系统使用趋势和探测各种异常活动。例如,如果用户通常在上午 9 点登录,但却有一天在凌晨 4 点半登录,这可能是一件值得调查的安全事件。

4.3.3 攻击特征探测工具

此类工具用于查找攻击特征,通常一系列特定的事件表明有可能发生了非法访问尝试。一个简单的例子是反复进行失败的登录尝试。

5 基于审计信息跟踪的攻击检测技术

5.1 检测技术分类

为了从大量的、有时是冗余的审计跟踪数据中提取出对安全功能有用的信息,基于计算机系统审计跟踪信息设计和实现的系统安全自动分析或检测工具是很必要的,可以用以从中筛选出涉及安全的信息。其思路与流行的数据挖掘技术是极其类似的。

基于审计跟踪的自动分析检测工具可以是脱机的,非实时地对审计跟踪文件提供的信息进行处理,从而得到计算机系统是否受到过攻击的结论,并且提供尽可能多的攻击者的信息;同时也可以是联机的,实时对审计跟踪文件提供的信息进行同步处理,当有可疑的攻击行为时,系统提供实时的警报,在攻击发生时就能提供攻击者的有关信息,其中可以包括攻击企图指向的信息。

5.2 攻击检测方法

5.2.1 检测隐藏的非法行为

对攻击的实时检测系统的工作原理是基于对用户

历史行为的建模以及在早期的证据或模型的基础。审计系统实时地检测用户对系统的使用情况,根据系统内部保持的用户行为的概率统计模型进行监测,当发现有可疑的用户行为发生时,保持跟踪并监测、记录该用户的行为。目前较为实用的实时检测系统能根据用户以前的历史行为决定用户当前的行为是否合法。并将用户的访问记录加放到用户的历史行为记录库。系统能够自适应地学习被检测系统中每个用户的行为习惯,当某个用户改变他的行为习惯时,这种异常就会被检测出来。

5.2.2 基于神经网络的攻击检测技术

在审计跟踪实践中,基于审计统计数据的攻击检测系统,具有一些天生的弱点,因为用户的行为可以是非常复杂的,所以想要准确匹配一个用户的历史行为和当前的行为相当困难。错发的警报往往来自对审计数据的统计算法所基于的不准确或不贴切的假设。作为改进的策略之一,神经网络可能用于解决传统的统计分析技术所面临的以下几个问题:

(1) 难于建立确切的统计分布:统计方法基本上是依赖于用户行为的主观假设,如偏差高斯分布;错发警报常由这种假设所导致。

(2) 难于实现方法的普适性:适用于某类用户行为的检测措施一般无法适用于另一类用户。

(3) 算法实现比较昂贵:由于上面一条原因,基于统计的算法对不同类型的用户行为不具有自适应性,因此算法比较复杂而且庞大,导致算法实现上的昂贵。而神经网络技术不存在这个问题,实现的代价较低

(4) 系统臃肿难于剪裁:由于采用统计方法检测具有大量用户的计算机系统,将不得不保留大量的用户行为信息,导致系统的臃肿和难于剪裁。而基于神经网络的技术能够回避这一缺点,根据实时检测到的信息有效地加以处理做出攻击可能性的判断。目前,神经网络技术提出了基于传统统计技术的攻击检测方法的改进方向,但尚不十分成熟,所以传统的统计方法仍将继续发挥作用,也仍然能为发现用户的异常行为提供相当有参考价值的信息。

5.2.3 基于专家系统的攻击检测技术

进行安全检测工作自动化的另外一个值得重视的研究方向就是基于专家系统的攻击检测技术,即根据安全专家对可疑行为的分析经验形成一套推理规则,然后在此基础之上构成相应的专家系统,对所涉及的攻击操作进行分析。

所谓专家系统是基于一套由专家经验事先定义的规则的推理系统。例如,在数分钟之内某个用户连续进行登录,且失败超过三次就可以被认为是一种攻击行为。类似的规则在统计系统似乎也有,同时应当说明的是基于规则的专家系统或推进系统也有其局限性,因为作为这类系统的基础推理规则一般都是根据已知的安全漏洞进行安排和策划的,而对系统的最危险的威胁则主要是来自未知的安全漏洞。实现一个基于规则的专家系统是一个知识工程问题,其功能应当能够随着经验的积累而利用其自学习能力进行规则的扩充和修正。当然这样的能力需要在专家的指导和参与下才能实现,否则可能同样会导致较多的错报现象。

5.2.4 基于模型推理的攻击检测技术

攻击者在攻击一个系统时往往采用一定的行为程序,如猜测口令,这种行为构成了具有一定行为特征的模型,根据这种模型所代表的攻击意图的行为特征,可以实时地检测出恶意的攻击企图。虽然攻击者并不一定都是恶意的。用模型的推理方法人们能够为某些行为建立特定的模型,从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本,这种系统就能检测出非法的用户行为。

当有证据表明某种特定的攻击模型发生时,系统应当收集其他证据来证实或者否定攻击的真实,既要不能漏报攻击,对信息系统造成实际的损害,又要尽可能的避免错报。

当然,上述的几种方法都不能彻底地解决攻击检测问题,所以最好是综合地利用各种手段强化计算机信息系统的安全程序以增加攻击成功的难度,同时根据系统本身特点辅助以较适合的攻击检测手段。

参考文献

1 赵玲涛.基于内容的安全审计跟踪算法及其应用研究[硕士学位论文].上海:上海交通大学,2007:12-13.