第 32 卷 第 18 期 计 算 机 工 程 2006 年 9 月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0169—03 文献标识码：A 中图分类号：TP309

入侵检测中的审计追踪技术

蒋卫华[1]，种 亮[2]，杜 君[3]
(1. 第二炮兵工程学院控制科学与工程博士后流动站，西安 710025；2. 西北工业大学软件学院，西安 710065；
3. 西北工业大学计算机学院，西安 710072)

摘 要：审计追踪技术是计算机网络安全领域中一个十分重要的研究课题，它是对有关操作系统、系统应用或用户活动所产生的一系列的计算机安全事件进行记录和分析的过程。该文从审计追踪的基本概念入手，对所涉及的一些关键技术和标准进行了总结和归纳。通过分析和研究，最后提出了详细的安全审计方法和具体实施步骤。实践证明，该方法是一种有效而易于实现的安全审计方法。
关键词：网络安全；入侵检测；审计追踪

Technology of Audit Tracing for Intrusion Detection

JIANG Weihua[1], CHONG Liang[2], DU Jun[3]
(1. Postdoctoral Research Fellow Control Science and Engineering, Second Artillerist Engineering Institute, Xi'an 710025;
2. College of Software Engineering, Northwestern Polytechnical University, Xi'an 710065;
3. College of Computer Science, Northwestern Polytechnical University, Xi'an 710072)

【Abstract】 The technology of audit tracing is a very important aspect in network security. It is the process of memorizing and analyzing a series of computer security events produced by operating system, system application or user activity. This thesis introduces the basic conception , and the key technology and standard have been summarized. The detailed method and basic process of security audit have been proposed. This method has been proved to be effective and prone to be carried out.
【Key words】 Network security; Intrusion detection; Audit tracing

1 概述

审计追踪就是对有关操作系统、系统应用或用户活动所产生的一系列的计算机安全事件进行记录和分析的过程。在计算机网络中，网络安全管理员采用审计系统来监视系统的状态和用户的活动，并对日志文件进行分析，及时发现系统中存在的安全问题。

审计追踪可以自动记录一些重要安全事件，如入侵者持续试验不同的通行字企图接入，所记录的事件应包括试图联机的每个用户所在工作站的网络地址和时间，同时也要对管理员的活动进行记录，以便研究入侵事件，因为有些入侵成功可能是由管理员的错误所造成的。审计追踪是检测入侵的一个基本工具。一般来说，对审计追踪的技术要求有 5 个方面：

(1)自动采集跟所有安全性有关的活动信息，这些活动是由管理员在安装时所预先选定的一些事件；

(2)采用标准格式记录信息；

(3)建立和存储审计信息是自动的，不要求管理员参与；

(4)在一定安全体制下保护审计记录；

(5)对计算机系统的运行和性能影响尽可能小。

审计追踪提供了实现多种安全相关目标的一种方法，这些目标包括个人职能、事件重建、入侵探测和故障分析。

1.1 个人职能(individual accountability)

审计追踪是管理人员用来维护个人职能的技术手段。通过告知用户应该为自己的行为负责，通过审计追踪记录用户的活动，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，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，审计追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。审计追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。

逻辑访问控制是用于限制对系统资源的访问，允许用户访问特定资源意味着用户通常要通过这种访问完成他们的工作。当然，被授权的访问也会被滥用，这种情况下审计追踪就能发挥作用。当无法阻止用户通过其合法身份访问资源时，审计追踪就可以用于检查他们的活动。

1.2 事件重建(reconstruction of events)

在故障发生后，审计追踪可以用于重建事件。通过审查系统活动的审计追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。通过对审计追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，通过对审计追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。而且，在发生技术故障时(如数据文件损坏)，审计追踪可以协助进行恢复(通过更

作者简介：蒋卫华(1973—)，男，博士后，主研方向：网络安全；种 亮，博士；杜 君，硕士
收稿日期：2005-12-23 **E-mail：**chongliang@vip.sina.com

改记录可以重建文件)。

1.3 入侵检测(intrusion detection)

如果用审计追踪记录适当的信息，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，不过事后检查(定时检查审计记录)也是可行的。

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。但是实时审计可能会降低系统性能。

事后鉴别可以标示出非法访问的企图(或事实)。这样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。

1.4 故障分析(problem analysis)

在线的审计追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。

2 审计系统模型与记录标准

一个审计系统的简单模型包括两个部分：审计数据采集器，它用于采集审计数据；审计数据分析器，它负责对审计数据采集器发送给它的数据进行分析。

通常，从数据采集器向数据分析器传送审计数据，是由一个文件来完成的。当从不同的系统采集审计数据时，就会产生问题，这是因为对审计追踪来说，缺少一个标准的接口。为审计追踪的数据格式和内容开发相关的标准，此时就显得非常重要。

另外为审计格式和内容开发获得广泛认同的审计追踪标准用以支持安全目标，是克服非兼容性的重要一步。

2.1 格式标准

广泛认同的标准格式将有利于克服非兼容性和互操作性，是审计数据分析系统的开发者所面临的重要问题。采用标准的格式也有利于来自不同的审计系统的审计数据的交换，并促进网络环境下对数据的协同分析。

关于审计追踪的格式，有以下几个标准：

(1)Bishop 的标准审计追踪格式。Bishop 提出，一个标准的格式必须是既可扩充又可移植的，以满足多种不同系统的需求，以及跨越各种系统和网络协议的可移植性。Bishop 定义了标准的日志记录格式，它既可移植，又可扩展。在此标准格式中,每个日志记录包含一些域,域之间由域分割符“ # ”分开，由启动和终止符号“ S ”和“ E ”来定界。域的数目是不固定的，以满足扩展性的需要。全部的数值都是 ASIC II 代码串，这就避免了字节排序和浮点格式的问题。然而，这一格式没有对审计追踪记录的域进行标准化。

(2)归一化的审计数据格式。归一化的审计数据格式(NADF)是由 ASAX 误用检测系统的开发者所定义的,旨在提供一定程度的操作系统独立性。NADF 审计追踪是有序的 NADF 记录文件，任何审计追踪都能转化成 NADF 格式。在转换时，对本地审计追踪的审计记录被抽象成为一系列审计数据值。每个审计数据值存放在一个独立的 NADF 记录中。每条记录包括 3 个域：识别符——审计数据值的类型；长度——审计数据值的长度；值——审计数据值。

(3)SVR4＋＋通用审计追踪互交换格式。这是一个专为 Unix 系统设计的标准。一条审计记录中所输入的属性组包括时间、事件类型、进程识别符、结果、用户和用户组信息、会话识别符、进程的标号信息，以及有关目标和各种数据的其他一些信息。这些属性组均以 ASCII 代码的形式表示。这一标准的优点是更接近可移植性，缺点是缺少了可扩展性的某些特征。

2.2 内容标准

审计追踪的内容也需要标准化，这将有利于对来自不同审计源的审计数据进行分析，并且可以提高网络环境下的互操作性。已提出的标准有如下几种：

(1)DoD 的可信计算机系统评估规范：是由美国国家计算机安全中心创立的，旨在对计算机系统的安全性进行评估。这一标准有 4 类规范，分别称为 A，B，C 和 D。满足最高划分规范 A 的系统能够提供最高等级的安全保证。在 B 和 C 类中，又包含一些子类。C2 到 A1 等级要求在系统中具有审计安全相关活动的能力。这一标准阐述了何种事件需要审计，每一审计事件要含有哪些内容。此外，每一审计事件的内容应当包括下面的信息：事件的日期和时间；用户识别符；事件的类型；事件的成功和失败；发出鉴别和认证事件请求的源点；导入/删除事件的对象名称。

(2)分布系统的安全规范：是由美国防护分析协会在 1995 年制定的。这一标准规定了各种需要审计的事件。这些事件可以划分为 6 类：访问控制和管理策略事件；数据机密性和完整性策略事件；非自主的策略事件；可用性策略事件；密码策略事件；缺省和从属性事件。它规定了对每一事件要记录的信息；它们分别是：日期和时间；主体的属性信息；对生成审计记录的主机的识别；事件的种类；此类事件的识别符；事件的结果。

3 审计追踪的实施

为了确保审计追踪数据的可用性和正确性，首先需要对审计追踪数据进行保护；其次对日志数据进行及时审查。审计追踪应该根据需要(经常由安全事件触发)定期审查、自动实时审查、或二者兼而有之。系统管理员应该根据计算机安全管理的要求确定对审计追踪数据的维护时间，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)保护审计追踪数据；

(2)审查审计追踪数据；

(3)用于审计追踪分析的工具。

3.1 保护审计追踪数据

访问在线审计日志必须受到严格限制。计算机安全管理人员和系统管理员或职能部门经理出于检查的目的可以访问，但是维护逻辑访问功能的安全和管理人员没有必要访问审计日志。

防止非法修改以确保审计追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追踪记录以掩盖自己的踪迹是审计追踪文件需要保护的原因之一。使用强访问控制是保护审计追踪记录免受非法访问的有效措施。当牵涉到法律问题时，审计追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)。此类法律问题应该直接咨询相关法律顾问。

审计追踪信息的机密性也需要受到保护，例如审计追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。

3.2 审查审计追踪数据

审计追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判断和发现异常活动。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追踪记录并生成所需的报告，使得审计追踪检查容易些。

(1)事后检查

当系统或应用软件发生了故障、用户违反了操作规范、发现了系统或用户的异常问题时，系统级或应用级的管理员就会检查审计追踪。应用或数据的拥有者在检查审计追踪数据后会生成一个独立的报告以评估他们的资源是否遭受损失。

(2)定期检查

应用的拥有者、数据的拥有者、系统管理员、数据处理管理员和计算机安全管理员应该根据非法活动的严重程度确定检查审计追踪的频率。

(3)实时检查

通常，审计追踪分析是在批处理模式下定时执行的。审计记录会定时归档用于以后的分析。审计分析工具可用于实时和准实时模式下。此类入侵探测工具基于审计数据精选、攻击特征识别和差异分析技术。由于数据量过大，在大型多用户系统中使用人工方式对审计数据进行实时检查是不切实际的。但是，对于特定用户和应用的审计记录进行实时检查还是可能的。这类似于击键监控，不过这可能会涉及到法律是否允许的问题。

3.3 审计追踪工具

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，审计追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。

3.3.1 审计精选工具(audit reduction tools)

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。

3.3.2 趋势/差别探测工具(trends/variance-detection tools)

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。

3.3.3 攻击特征探测工具(attack signature-detection tools)

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。

4 审计追踪的分析方法

审计追踪需要进行分析以确定脆弱性，建立可计算性的评估损失和恢复系统运行。对审计追踪的人工分析虽然十分麻烦，但经常使用，因为要从审计记录中提取综合的信息来形成查询是非常困难的一件事。在浏览审计时，可以借助于许多工具。在开发有效的审计分析工具时，所遇到的主要障碍是需要处理日志机制产生的大量数据。

目前，人们已经在自动审计分析领域中做了大量工作，主要是以检测入侵为目的。这些工具将审计数据作为输入，而把审计分析后所产生的结果作为输出。

这些工具主要基于 3 种分析方法：

(1)统计分析。这种分析方法定期收集与合法用户行为有关的数据，而后用于对观察的行为进行统计检验，以高可信度决定是否与合法用户行为相符；

(2)基于规则的专家系统。自动专家系统采用了不同的方法，这些系统与“异态检测”的区别是，通过采用预先设定的规则来进行“误用检测”，而这些规则都是由入侵检测专家们预先设计好的；

(3)机器自动学习。采用会自动学习入侵检测的机器进行自动审计分析，是一种相对来说较新的方法，能学会监视和学习用户的正常活动。

另外，分布式审计分析对网络安全来说是必需的。如前所述，发生在不同主机上的用户活动的相关性能够导致某个恶意的行为，而这些活动在单个主机层面上来看可能是合法的。它比集中式的审计追踪分析有以下优点：大量地降低了网络数据的流量，因为在集中式分析中，所有的审计数据都要发放到中心主机进行处理；它能够使多个分析主机的 CPU 负荷得到均衡。它不像集中式审计分析那样，所有的负荷全部由中心主机进行处理，而是由多个主机分担。

5 结语

安全审计追踪是网络安全中一个十分重要的内容。要做好安全审计工作，归纳起来有以下几个关键步骤：

(1)确定审计的类型。包括对主机、防火墙和网络的审计；

(2)预审计。预审计就是要对所采用的审计工具和环境的检查；

(3)审计/反复检查安全策略；

(4)收集审计信息；

(5)生成审计报告；

(6)基于报告的发现采取相应的行动；

(7)对审计数据和报告进行安全保护。

综上所述，安全审计追踪是一项繁琐和需要耐心的工作，无论在技术上还是在管理上对人员的素质要求都很高。它不是一项单纯依靠安全审计工具就能够完成的工作，还需要网络安全管理员和技术人员的参与和支持，以及必要时采取人工操作的方式来实现。

参考文献

1 Harold F, Krause T M. 王卫卫, 杨　波译. Information Security Management Handbook: Volume I(Fourth Edition)[M]. 北京: 电子工业出版社, 2004.

2 王位钊, 李　承, 李家滨. 网络安全审计系统的实现[J]. 计算机应用与软件, 2002, 19(11): 24-26.

3 Proctor P E. 邓琦皓, 许鸿飞译. 入侵检测实用手册[M]. 北京: 中国电力出版社, 2002.

4 Ning P, Wang X S, Jajodia S. Modeling Requests Among Cooperating Instrusion Detection Systems[J]. Computer Communications, 2000, 23(17).

5 Diparti G V. Inspect: A Light Weight Distributed to Automated Audit Trail Analysis[Z]. http://www.sureserv.com/technic/IDS.html.

6 Sobirey M, Richter B, Konig H. The Intrusion Detection System AID ——Architecture, and Experiences in Automated Audit Analysis[Z]. http://www-900.ibm.com/.