涉密应用系统安全审计解决方案

杨光宏，朱行林，黄聪敏
（中国工程物理研究院 计算机应用研究所，四川 绵阳 621900）

摘 要：安全审计已经成为了涉密应用系统的重要环节，近年来国家对涉密应用系统的审计提出了明确要求；为了提高涉密应用系统的可靠性和安全性，安全审计满足国家相关要求，通过建立涉密应用系统安全审计模型、整体框架、安全审计策略和审计实现的可配置审计技术和审计保护技术，提出了涉密应用系统的安全审计解决方案；并基于轻量级的J2EE框架（spring+hibernate+dorado）实现了可配置的审计组件，涉密信息系统集成审计组件，可以提高涉密系统的可靠性、安全性，提升审计工作的效率，降低审计成本。

关键词：安全审计；AOP；数字签名
中图分类号：TP399 **文献标识码**：A **文章编号**：1673-629X(2011)03-0178-03

A Security Audit Solution to Classified Applications

YANG Guang-hong, ZHU Xing-lin, HUANG Cong-min
(Institute of Computer Application, China Academy of Engineering Physics, Mianyang 621900, China)

Abstract: Security audit has become an important dimension for classified applications. In recent years, China has released relevant laws and regulations regarding security auditing for classified applications. To enhance reliability and security so that application systems meet security audit needs, have worked on security model, overall framework, and security auditing policies that enable configurable auditing and auditing protection. A security auditing solution for classified applications is proposed; and based on a lightweight J2EE framework (spring+hibernate+dorado) can be configured to achieve the audit component of the audit classified information system integration components, can improve the secret system reliability, security, enhance audit efficiency and reduce audit costs.

Key words: security audit; AOP; digital signature

0 引 言

涉密应用系统安全管理可以通过安全评估[1]、安全策略[2]、安全标准、安全审计等环节来加以规范并实现有效的管理，安全审计已经成为涉密应用系统重要的环节，BMB17-2006《涉及国家秘密的信息系统分级保护技术要求》对涉密应用系统审计提出了明确的要求：1）审计范围；2）审计记录类容；3）审计记录保护；4）审计记录时间。随着信息系统向大型分布式系统发展，审计事件类型大量增加，传统的对单一层面上的事件进行审计已经不能满足涉密应用系统的安全需求。同时审计记录量急剧增涨，各种形式不一、内容各异的审计记录和审计系统分析的智能性不高给管理员带来了繁重的工作量。信息系统业务的动态扩展，使传统紧耦合的审计系统结构很难适应其业务扩展的需要。当前，灵活的组织结构、多层次的数据采集、分布式的数据处理和智能化分析逐步成为信息系统审计研究的热点。一个设计良好的安全审计可以提高涉密应用系统的可靠性、安全性；提高审计工作的效率，提高审计的正确性与准确性，降低审计成本。

收稿日期：2010-09-07；**修回日期**：2010-12-04
基金项目：中国工程物理研究院科学技术发展基金(09-0541)
作者简介：杨光宏（1975-），男，四川西充人，工程师，研究方向为计算机应用与软件。

1 涉密应用系统安全审计模型和框架

安全审计主要是指对与安全有关的活动的相关信息进行识别、记录、存储和分析，审计记录用于检查分析那些与安全有关的活动，谁对这个活动负责。审计记录[3]应包含事件、时间、地点、类型、主体、客体和结果等，以确定发生的事件及其来源和结果；且审计事件应与唯一的用户标识符关联。审计整体框架是把来自各个（审计）数据源[4]，通过审计的数据采集模块，采集审计数据后，通过格式化处理模块把审计信息转化为统一格式，并存储在服务器上，存储审计信息的同时根据审计策略库分析此审计信息是否有异常，如果有异常，存储审计异常信息到异常库，方便审计信息审计和提高审计效率。安全审计实体模型和整体框架如图1、2所示。

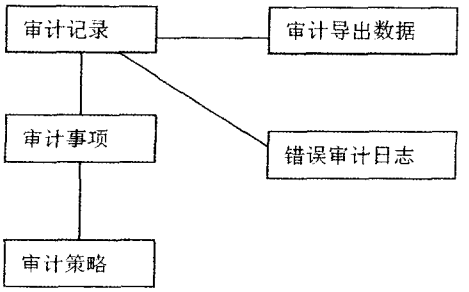

图 1　审计实体模型图

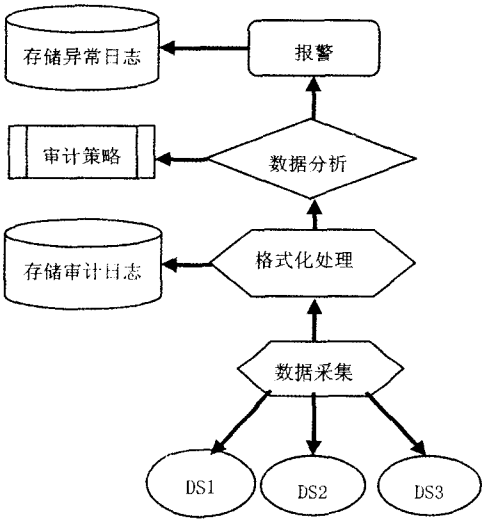

图 2　审计整体框架

2　涉密应用系统安全审计策略

审计功能主要记录系统用户业务操作的过程,为审计员判断用户操作的合法性提供依据[5]。它同日志之间的区别在于,日志关注函数请求的概念,而审计关注业务操作的概念,一次业务操作可能包含多个函数操作;日志记录请求的发生与否,以及发生序列,而审计还要记录请求执行成功与否。通过对涉密 OA 办公自动化,质量信息管理系统,科研信息管理系统和设备管理系统它们对审计信息的需求如以下三方面。

2.1　审计信息记录

审计信息记录是指根据审计策略产生的审计记录的管理,包括记录的备份、恢复、导入、导出,以及报表的生成。审计信息关注的焦点应该包括:事件、时间、操作人员、操作对象、执行要素、行为状态等因素。其中使用方法名可以表示事件的发生,时间需要反应操作发生的真实时间,操作人员表明操作执行的主体,操作对象记录操作中被执行对象,执行要素标示操作发生的关键要素或者第三方对象,行为状态标示事件开始、结束、失败、成功等执行情况。

2.2　审计事项管理

审计事项管理是指对核心业务操作、需要进行审计的事件的定义和管理[6],配置和定义所有可能需要审计的事项或操作。

2.3　审计策略配置

审计策略配置是指审计事项和审计人员之间的关联、设置关系,也就是设置哪些关键人员的哪些关键操作(事项)需要审计;而且根据 BMB17-2006《涉及国家秘密的信息系统分级保护技术要求》要求,系统管理员、审计管理员和安全管理员的所有操作和用户登陆系统,退出系统必须审计,因此根据审计内容审计分为两类强制审计和可配置审计,如图 3 所示。

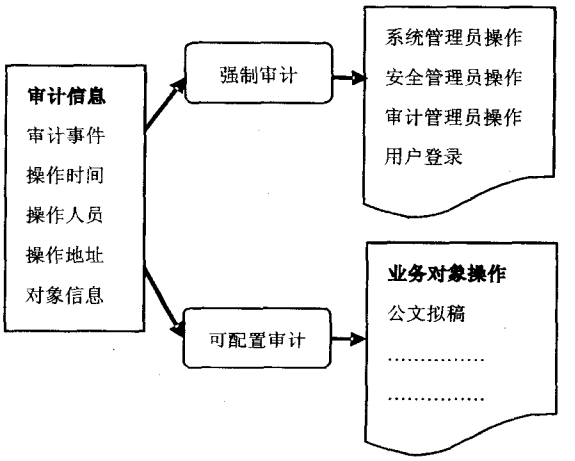

图 3　审计信息类型

3　涉密应用系统可配置审计技术

在应用程序开发时,都主要关注业务实现,往往忽略审计信息开发,如果能够开发一个审计信息独立于业务实现,使程序员只关注于业务实现,将大大提高开发效率[7]。因此灵活可配置审计技术非常关键。在设计可配置审计审计中 AOP 是其中最关键的技术。

AOP 是 Aspect Oriented Programming 的缩写,意为面向方面编程,是 OOP(Object-Oriented Programming,面向对象编程)的进一步发展的结果,也是 GoF 设计模式的实践结果[8]。设计模式从理论上孜孜不倦地追求调用者和被调用者之间的解耦,AOP 正是实现了这一点。

在 AOP 中,有三个概念需要关注:advice、pointcut 和 advisor。其中,advice 是需要在程序内部、不同地方注入的代码;pointcut 用来定义需要注入 advice 的位置,通常是某个特定的类的一个 public 方法;advisor 是 advice 和 pointcut 的装配器,是将 advice 注入主程序中预定义位置的代码[9]。

采用 AOP 技术,建立操作函数和业务事件之间的映射,可以解决"事件"因素;同时,可以监控事件的行为状态[10];通过上下文环境,可以获得时间、操作人员信息;而操作对象、执行要素的信息,可以通过函数中参数(包括传入参数、返回参数)的性质来决定。

4 涉密应用系统审计保护技术

审计信息在审计操作的合法性的同时也必须保证自身审计信息的合法性，因此必须对审计信息进行保护[11]。目前数字签名技术应用比较广泛，采用数字签名来对审计信息进行保护能够保证审计信息的合法性。审计信息的保护包括两方面，审计信息的安全导出和审计信息导入的合法性验证[12]，如图 4、5 所示。

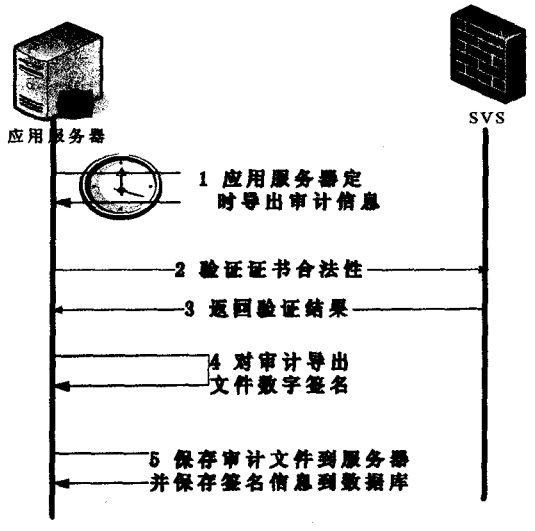

图 4 审计信息导出

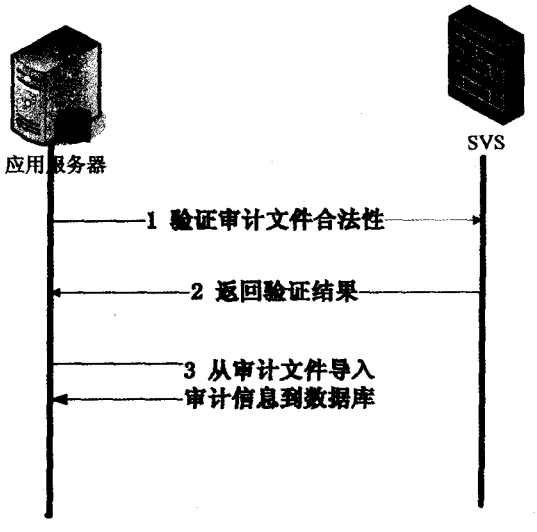

图 5 审计信息导入

5 可配置审计组件实现

根据以上的解决方案，采用轻量级的 J2EE 框架（spring+hibernate+dorado）实现了可配置的审计组件，该组件既可以独立部署为各个应用系统提供服务，也可以插入基于 J2EE 架构开发的应用系统中，审计组件部署结构图如图 6 所示。

如图 6 所示应用系统通过两种方式接入审计组件，对不能嵌入审计组件的应用系统，通过调用审计服务器的审计服务把审计信息写入审计数据库，应用系统 2 直接嵌入审计组件，由于审计组件是基于 AOP 设计的，因此嵌入审计组件的应用系统不用修改程序，审计组件提供拦截器拦截应用系统所有操作，并把操作审计信息写入审计数据库，做到审计信息统一存储。

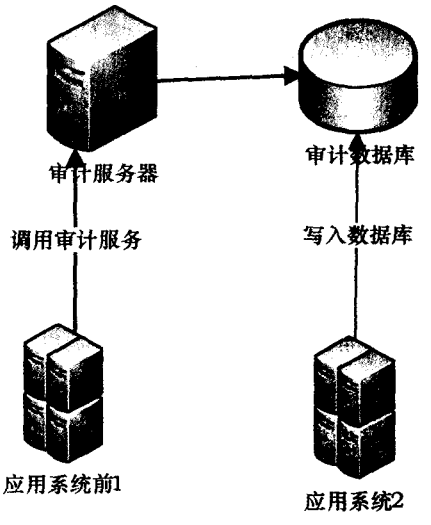

图 6 审计组件部署结构

审计服务器提供的 webservice 审计服务接口如下：

```
sendAuditMessage ( StringopeUser, String remoteAddr,String thingName,String objectInfo)
```

审计组件提供的审计拦截器示例代码如下：

```
<aop:config>
<aop:aspect id="audit" ref="returnAdvice">
<aop:pointcutid = " methodlog" expression = " execution( * com. swcc. . service. impl. * Impl. * (. . ))"/>
</aop:aspect>
</aop:config>
```

审计组件的功能如下：

审计组件功能包括：

审计查询：查询所有所有审计记录，可以按照人员、时间、时间和要素查询；

审计分析：生成用户按年或月审计信息报表，所有用户审计信息报表，按照审计事件审计信息报表；

审计导出：按月导出审计信息；

审计服务：提供 webservice 审计信息服务。

6 结束语

通过研究涉密应用系统通用审计功能，使审计功能与业务分离开来，使涉密信息系统业务可以动态扩展，提高涉密应用系统的可靠性、安全性；提高审计工作的效率，提高审计的正确性与准确性，降低审计成本。

（下转第 184 页）

表1说明了在对Web数据库正常访问,本系统对其响应结果影响不大,仅比普通的情形稍好;表2说明了在对Web数据库非法、越权访问时,应用本系统的基于GEP-UCON的安全访问控制技术准确率、安全性比普通的情形高很多,而主、客体属性库的规模直接影响分析结果,主、客体属性库随着访问次数的增多而增多,准确率越来越高。文中的GEP-UCON算法方法的优势在于无须手工添加主、客体属性参数,所以易于扩展,有利于软件的升级,更适合实际软件设计需要。同时保证了过滤结果基本达到了无知道学习的一般水平。

5 结束语

在计算机安全性体系中,任何优秀的加密技术和密钥管理都可能存在意外的时候,换句话说,访问控制技术是用来抵御攻击的最后屏障,这对于Web数据库而言也不例外。基于GEP-UCON模型的安全访问控制是一种先进的访问控制技术,它在保证安全的同时把访问控制的复杂性以智能化、自学习的方式解决,使访问决策变得更容易。我们利用基于GEP-UCON模型的访问控制技术为Web数据库建立了一个多层次安全防御模型,其原型系统已在实际应用,对解决Web数据库及服务器的安全问题具有十分现实的意义。

参考文献:

[1] Ferreira C. Gene expression programming: a new adaptive algorithm for solving problems[J]. Complex Systems,2001,13(2):87-129.

[2] Ferreira C. Gene expression programming: mathematical modeling by an artificial intelligence[M]. New York: Springer-Verlag, 2002.

[3] Ferreira C. Function finding and the creation of numerica constants in gene expression programming[C]//The 7th Online World Conference on Soft Computing in Industrial Applications. England:[s. n.], 2002.

[4] Yuan Chang-an, Tang Chang-jie, Wen Yuan-guang, et al. Intelligent Function Model Discovery System Based upon Gene Expression Programming[J]. Journal of Computational Information Systems,2006,2(4):1299-1304.

[5] Yuan C, Tang C, Wen Y, et al. Convergency of Genetic Regression in Data Mining Based in Gene Expression Programming and Optimized Solution[J]. International Journal of Computers and Applications, 2006,28(4):359-366.

[6] Lopesh S, Weinertw R. Egipsys: an enhanced gene expression programming approach for symbolic regression problems [J]. International Journal of Applied Mathematics and Computer Science, 2004,14(3): 375 -384.

[7] 邓集波,洪 帆. 基于任务的访问控制模型[J]. 软件学报,2003,14(1):76-81.

[8] 徐 锋,吕 建. Web安全中的信任管理研究与进展[J]. 软件学报,2002,13 (11): 57-64.

[9] 张 欢. 基因表达式编程中的转基因关键技术研究[D]. 成都: 四川大学, 2006.

[10] 彭 京,唐常杰,元昌安,等. 基于重叠表达的多基因进化算法[J]. 计算机学报, 2007(5):1778-1781.

[11] 谢方军,唐常杰,元昌安,等. 基于基因表达式的演化硬件进化和优化算法[J]. 计算机辅助设计与图形学学报,2005,17(7):1415-1420.

[12] 王 东,吴湘滨. 遗传编程运行期个体多样性分析方法及应用[J]. 计算机技术与发展,2006,16(9):59-61.

(上接第185页)

参考文献:

[1] 彭 友,王延章. 信息系统内部安全审计机制[J]. 北京交通大学学报,2009(2):112-116.

[2] 王希忠. 安全审计在信息安全策略中的作用[J]. 信息技术,2010(3):171-172.

[3] 周洪昊. 安全审计系统的设计与实现[J]. 计算机应用,2004(7):105-107.

[4] 黄 晨. 分布式安全审计系统设计与实现[J]. 计算机工程与设计,2007(4):811-813.

[5] 郭建东,秦志光,郑 敏. 信息系统的安全模型[J]. 电子科技大学学报,2008(2):285-288.

[6] 邓小榕,陈 龙,王国胤. 安全审计数据的综合审计分析方法[J]. 重庆邮电学院学报(自然科学版),2005(5):604-607.

[7] 毕晓冬. 电子商务安全审计系统的研究与设计[J]. 工会论坛,2007(2):94-96.

[8] Agrawal R,Strikard R. Fast Algorithms for Mining Association Rules[C]//Proceedings of the 20th ULDB Conference. Santiago, Chile:[s. n.],1994.

[9] Klemettinen M, Mannila H, Ronkainen P, et al. Finding Interesting Rules from Large Sets of Discovered Association Rules[C]//Proceedings of the 3rd International Conference on Information and Knowledge Management (CIKM'94). Gainthersburg, MD:[s. n.],1994:401-407.

[10] Stolfo S L, Promidis A L, Tselepis S, et al. JAM: Java Agents for Meta - Learning Overdistributed Databases[C]//Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining. Newport Beach, CA: AAAI Press, 1997:74-81.

[11] 张世永. 信息安全审计技术的发展与应用[J]. 网络与信息安全,2003(2):29-33.

[12] 周琪锋. 基于网络日志的安全审计系统的研究与设计[J]. 计算机技术与发展,2009,19(11):139-142.