维普资讯 http://www.cqvip.com

数据库安全评测系统研究*)

王艺超 冯 玉 王 珊
(中国人民大学数据与知识工程研究所 北京 100872)

摘 要 多年来,如何增强和评测DBMS安全已成为一个研究热点。本文首先概述了DBMS安全的当前研究工作,并介绍了一些数据库安全评测系统。最后以Kingbase ES为例,介绍了一个实际的数据库安全评测系统。

关键词 信息安全,DBMS安全评测,脆弱性

On Evaluating System of DBMS Security

WANG Yi-Chao FENG Yu WANG Shan
(Institute of Data and Knowledge Engineering, Renmin University of China, Beijing 100872)

Abstract The problem of enhancing and evaluating DBMS security has been an interesting research topic for many years. This paper reviewed the current research work on DBMS security and introduced some database security evaluation systems. Moreover, the paper described the design and architecture of a Kingbase ES security evaluation software.

Keywords Information security, DBMS security evaluation, Vulnerability

1 引言

数据通常是一个组织最敏感、最有价值的资源,数据库管理系统作为数据管理的核心软件,在重大的商业、金融、国防应用中,其安全性甚至比数据库的性能更为重要。

面向数据的安全指的是数据的保密性、完整性和可用性。数据的保密性指对数据访问权限的限制,禁止未经授权的用户进行数据访问。数据的完整性指禁止数据被未经授权的篡改,要求保持数据原样,正确地生成、存储和传输数据。数据的可用性指的是保证被授权用户对数据的使用,防止由于计算机病毒或其它因素造成的系统拒绝服务。

数据库管理系统(DBMS)是一个非常复杂的系统,检测和评估数据库的安全性,涉及到众多的参数、设置、选项和数据库本身的方方面面。安全评测可以采用专家评测或运行评测系统两种方式,二者各有所长。一方面,专家评测比评测系统具有更强的灵活性,可以充分发挥专家的智能和经验。另一方面,评测系统更适用于数据库系统定期的安全评测。专家评估只是针对被评估时的状态,但是系统是在不断变化的,如果系统状态发生了变化(比如添加了一些新用户,修改了某些用户的权限),也许会出现新的安全漏洞。定期聘请专家评估的成本比较高,安全评测系统则可以在系统状态发生变化后重新进行评测。

随着信息科技的日益发展,信息安全越来越受到各界的重视,各种防火墙、防病毒系统以及入侵检测产品不断涌现。但是目前对安全性的研究多集中在网络安全和操作系统安全方面,数据库作为信息系统的核心、组织的重要资产,其安全性却没有受到足够的重视。数据库安全评测系统可以简便而经济地协助人们评估系统安全等级,发现安全隐患和漏洞,加强系统的安全防御。研究标准、高效的数据库评测系统对于提高数据库安全性,促进数据库安全性研究有非常重要的意义。

本文介绍了国内外数据库安全评测研究以及数据库评测系统发展的情况,总结了优秀数据库评测系统的基本要求,着重描述了北京人大金仓公司的金鼎数据库服务器Kingbase ES安全评测系统的特点和体系结构。

2 数据库安全性评测系统的定义、用途和分类

计算机系统的安全性问题可分为技术安全类、管理安全类和政策法律类[1]。一般讨论的存取控制、审计以及数据加密技术都属于数据库的技术安全范畴。政策法规类指政府部门建立的有关计算机犯罪、数据安全保密的法律道德准则和政策法规、法令。技术安全之外的,诸如软硬件和场地管理相关的安全问题,视为管理安全。数据库安全评测系统同时涉及到这3类问题。

数据库安全评测系统指的是检测数据库的安全隐患和漏洞,评估数据库安全保护能力和级别的系统,包括软件和硬件。完备的数据库安全评测系统应能够从数据库安全策略、漏洞评估、漏洞修补、风险评估和安全体系等多个方面综合对数据库系统进行安全评测。当然目前有的系统侧重于寻找安全漏洞,有的侧重于评估。

不同的人对数据库安全评测系统有不同的需求,数据库安全性评测系统的用途非常广泛。首先,数据库管理人员可以定期运行数据库安全评测系统,在数据库的安全性受到侵害的事前、事中、事后为数据库提供安全帮助和保护。比如,在发生入侵前,管理员可以利用数据库安全评测系统尽可能早地找出数据库中存在的隐患和漏洞,及时弥补漏洞;在入侵发生时,数据库安全评测系统可以帮助管理员及时反应,尽量减少

*)本文研究得到国家"863计划"数据库管理系统及其应用重大专项课题"通用数据库管理系统Kingbase ES V4.0研发及其应用"项目资助。
王艺超 硕士研究生,主要研究方向为数据库与知识工程。冯 玉 博士,主要研究领域为高性能数据库管理系统,数据仓库与数据挖掘。王 珊 博士生导师,主要研究领域为数据库与知识工程。

维普资讯 http://www.cqvip.com

损失；在入侵发生后，数据库安全评测系统可以协助分析确定数据库被攻击的漏洞所在，提供调查攻击来源的资料。其次，系统开发人员和系统集成人员可以利用安全性评测系统，进行数据库建库和数据库改造前后的安全规划评估和成效检验。再次，第三方评测机构可以利用数据库安全性评测系统评估数据库的安全保护能力和级别。

数据库安全评测系统大致可以分为两类：第一，侧重于寻找安全漏洞的安全扫描工具；第二，侧重于评估安全级别的等级划分工具。目前安全扫描工具明显多于等级划分工具。

目前的数据库安全评测系统具有以下共同点：

· 针对性强。各种软件的设计、实现、接口不同。目前的绝大多数数据库安全评测系统只能支持某一种或某几种具体的DBMS。

· 等级划分工具进行评测的标准通常是国家或行业颁布的安全等级划分标准，安全扫描工具进行评测的标准通常是实践经验和国际漏洞标准CVE。

评测必须依据标准，安全标准是数据库安全评测的基础，下一节介绍了国内外信息安全尤其是数据库安全标准的研究情况。

3 信息安全标准及数据库安全标准研究现状

从1984年美国首次进行安全产品评估以来，评估认证标准大致可分为三个阶段：一是20世纪80年代，美国国防部发布橘皮书《可信计算机系统评估标准(TCSEC)》，二是90年代开始，美国推出《联邦评估标准(FC)》，加拿大颁布《可信计算系统评估标准(CTCSEC)》，欧洲各国联合研制出欧洲《信息技术安全评估标准(ITSEC)》，三是90年代末期，在上述标准的基础上，美国、加拿大和欧洲联合研制《信息技术安全评估通用标准(Common Criteria for Information Technology Security Evaluation)》[2]。1999年12月，ISO接受CC为国际标准，编号ISO/IEC 15408，并正式颁布发行。

3.1 信息技术安全评估通用标准

国际标准ISO/IEC15408-1999《信息技术安全评估通用标准(CC)》源于TCSEC，但完全改进了TCSEC[3]。TCSEC主要面向操作系统的评估，提出安全功能要求。CC全面地考虑了与信息技术安全性有关的所有因素，是安全准则的集合，也是构建安全要求的工具。但是CC并不涉及管理细节和信息安全的具体实现、算法、评估方法，也不作为安全协议、安全鉴定等。2001年3月我国正式接受CC作为国家标准，编号GB/T 18336-2001。

CC分3个部分。第1部分"简介和一般模型"，介绍CC的基本概念和基本原理；第2部分"安全功能要求"，提出了技术要求；第3部分"安全保证要求"，提出了非技术要求和对开发过程、工程过程的要求。保护轮廓(Protection Profile)和安全目标(Security Target)是CC中的重要概念[4]。简单说来，保护轮廓表述的是"有什么样的安全需求"，与实现无关；而安全目标表述的是"安全解决方案可以提供什么"，依赖于具体实现。CC将评估等级分为从EAL1到EAL7共7级。每一级均需评估7个功能类，即配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试、脆弱性评估。

使用CC的人包括产品的用户、开发者、评估者、审计人员、认证人员等等。用户用CC描述对信息产品的安全要求；产品开发人员和系统集成人员用CC来说明其产品的安全特性；评估人员用CC来评估信息产品的安全等级。

3.2 中国信息安全标准体系

中国信息安全标准的制定始于1997年，1999年9月发布的GB 17859-1999《计算机信息系统安全保护等级划分准则》，是我国计算机信息系统安全等级管理的重要标准[5]。GB 17859-1999规定了计算机系统安全保护的五个等级。安全保护能力随级别提高而加强。安全级别主要考核标准如下：身份认证、自主访问控制、数据完整性、审计隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径、可信恢复等。

2002年7月18日，我国公安部正式发布实施了《计算机信息系统安全等级保护数据库管理系统技术要求》等五个公共安全行业标准。这些标准是我国计算机信息系统安全保护等级系列标准的一部分。其中GA/T 389-2002《计算机信息系统安全等级保护数据库管理技术要求》详细说明了为了实现GB17859-1999所提出的安全等级保护要求对数据库管理系统的安全技术要求，以及为确保这些安全技术所实现的安全功能达到其应具有的安全性而采取的保证措施，并将GB17859-1999对计算机信息系统5个安全保护等级每一级的要求，从技术方面进行详细描述[6]。

3.3 国际漏洞标准CVE

CVE(Common Vulnerabilities and Exposures)的目标是将众所周知的安全漏洞和信息泄漏的名称标准化。CVE类似于一个字典表，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称，为每个漏洞和安全薄弱点确定惟一的名称和标准化的描述，可以成为评价入侵检测和漏洞扫描等安全产品的参考标准。CVE的编委包括多个安全信息相关组织，由商业安全工具供应商、学术界成员、研究机构、政府机构和安全专家组成。目前CVE的版本号是20030402，共包含2572个正式漏洞，其中有39个是关于数据库服务器的[7]。

4 数据库安全评测系统的研究现状

本节简要介绍了一些现有的数据库安全评测系统。因为数据库安全等级评测工具的用户通常限于第三方认证机构，而安全扫描工具有更为广阔的用户群体，所以市面上的数据库安全评测系统基本上都是数据库安全漏洞扫描工具。

4.1 数据库安全保护等级评测工具

根据2002年7月，国家计委项目"1110工程"进展情况报告，我国针对按照等级保护要求开展评估和检测的需求，专门定制了信息产品安全等级评测工具，其中包括数据库安全保护等级评测工具。

4.2 Database Scanner

著名的网络安全公司(Internet Security Scanner，ISS)公司开发了Internet Security Scanner系列安全扫描工具，其中Database Scanner专门扫描数据库安全漏洞。它的研发小组X-Force成立了世界上第一个网上数据保护中心。

Database Scanner对关系数据库进行详细的安全性分析，扫描的内容覆盖3个方面：身份鉴别、授权和系统完整性，包括账户管理、密码管理、登陆管理、审计、存储过程、文件访问权限等内容。评测工作分为扫描系统当前状态和分析审计数据，使用系统内置的专业安全策略衡量DBMS的安全保护能力和薄弱点。根据薄弱点影响安全性的风险把它们分为高、中、低三级，并对薄弱点提出解决方案或建议。

Database Scanner支持3种流行的商用DBMS：Microsoft SQL Server，Sybase和Oracle。

维普资讯 http://www.cqvip.com

4.3 Oracle 安全基准及计分工具

互联网安全中心(Center of Internet Security,CIS)是一个非盈利性组织,他们提出的安全性基准称为用户模式的基准,他们的安全性建议通常来自用户的实践经验。CIS 不断推出针对操作系统,数据库管理系统和网络设备的安全基准以及对安全性记分的工具,帮助衡量和增强系统安全性。

在 DBMS 方面,CIS 只发布了 Oracle 安全基准及计分工具,目的是评价和提高 Oracle 数据库的安全性[8]。这个基准不是满足所有系统安全要求的万灵丹,用户必须分析实际需求,慎重选择适当的参数和配置方案。CIS 的 Oracle 安全基准的主要内容是一些推荐表,推荐表包括了:参数、选项名称,推荐的参数和选项,适用的版本号和操作系统,测试点级别等内容。记分工具的功能是根据基准对 Oracle 的安全性评分。

4.4 微软基线安全分析器

微软根据当前的安全威胁情况推出了安全基线分析器(Microsoft Security Baseline Analyzer,MSBA),目的是诊断企业内部安全性。2004 年 1 月 19 日推出 1.2 版本。这个工具可以评价 Windows 操作系统系列以及 IIS 网络服务器、SQL Server 数据库管理系统、Office 办公软件、IE 浏览器的安全性。评价系统的安全性,并且列出安全薄弱项。但是与其他产品相比,MSBA 的数据库扫描项目少得多,主要集中在账号管理、组管理和权限管理方面。

5 我国数据库安全评测发展现状

数据库安全评测产品研究力度不足。根据公安部计算机信息系统安全产品质量监督检验中心网站公布的数据,从 2000 年 1 月到 2004 年 3 月下旬,送检的安全性产品共 1111 个,和数据库安全相关的产品仅 7 个,其中只有 1 个数据库安全性分析系统(北方计算中心开发的 DBSExplorerVer1.0),剩下主要是针对网络安全的产品,比如防火墙,网络监控系统,身份认证安全部件等。

数据库安全评测标准与国外差距较大。公安部的《计算机信息系统安全等级保护数据库管理系统技术要求》大量参考了美国国家计算机安全中心颁布的《可信计算机系统评估标准关于可信数据库系统的解释(TDI)》,规定的五个安全等级基本上与 TDI 的从 C1 级到 B3 级要求相对应。借鉴国际研究成果,立足我国国情,研究和建立创新性安全理论和标准仍是一项艰巨的任务。

数据库安全意识淡薄,缺少必要的数据库安全评测和监控系统。

6 优秀数据库安全评测系统的要求

评价一个数据库安全评测系统,主要需关注以下几个方面[9]:

1) 依据公认的标准评价数据库安全性,评测依据全面、权威,支持国际 CVE 标准。

2) 检测项目全面,更新速度快,能对评测标准的修改以及新出现的安全漏洞做出迅速的反应。

3) 功能强大,能够从安全策略、风险评估、漏洞评估、漏洞修补和安全体系等多个方面综合对数据库进行安全评估和支持。安全性评估分析应包括目标的风险等级评估、同一目标多次扫描形成的趋势分析、多个目标扫描后结果的总体分析、关键漏洞扫描信息的摘要等等,而不能仅仅将扫描结果进行简单罗列。

4) 产品本身安全性高。由于安全评测系统管理的对象是系统安全性,尤其是漏洞扫描产品往往有模拟攻击的举动,这就要求该类产品具备抗攻击能力,如果安全评测系统感染有害程序,或被人恶意利用,那么后果不堪设想。由于软件产品无法杜绝被感染的可能,漏洞扫描器正在向硬件化的方向发展,高档产品还在文件系统、通信接口等方面采用非通用程序,以彻底杜绝被恶意程序攻击和感染的可能。

5) 通过正规的产品认证。目前我国对安全产品进行认证工作的权威部门包括:中国信息安全产品测评认证中心、公安部计算机信息系统安全产品质量监督检验中心、国家保密局测评认证中心、解放军信息安全产品测评中心。

6) 良好的可扩充性,产品升级简便。

7) 用户界面友好,安全分析报告清晰、有条理。

8) 适用广泛。可以评测各种 DBMS,尤其是流行 DBMS 的安全性。

当然,完全满足上述要求的数据库安全评测系统目前可以说只是一个理想。

7 Kingbase ES 安全评测系统的设计

企业级数据库服务器 Kingbase Enterprise Server 是北京人大金仓公司和中国人民大学数据与知识工程研究所联合开发的通用数据库管理系统。针对这个具体的 DBMS,我们设计了一个 Kingbase ES 安全评测系统,帮助用户提高和评测 DBMS 的安全性。

数据库的安全性离不开操作系统的安全性。评测系统需要检测的内容不但涉及到数据库本身,还有很多涉及到操作系统。所以对 Kingbase ES 数据库管理系统来说,需要分别开发针对 Windows 和 Unix 平台的安全评测工具。基本思路是根据 GA/T 389-2002、GB/T 18336-2001 和 7.1 小节的安全管理规则,制定测试项目,检查测试点的测试情况,对整体安全性打分,评定安全级别,并列出安全薄弱点,对安全薄弱点提出弥补建议。

7.1 安全管理规则

为了保证数据库的安全性,有一些实践性安全管理规则。这些规则往往并不复杂,但是把这些规律落实到具体的 DBMS 的参数设置和其他管理方面就是一项繁重的工程了。我们参照 Oracle、SQL Server、Mysql 的安全管理策略,以及第 4 节提到的安全评测系统的评测项目,基本依据以下规则设计了 Kingbase ES 安全评测系统:

1) 避免默认规则。应该修改和身份鉴别相关的默认设置。很多用户习惯使用默认的参数,但是默认的参数往往是严重的安全隐患。举一个简单的例子,如果在安装了数据库之后,仍然让默认超级用户使用原先的默认口令,那么很可能有人会利用这个超级用户在数据库中为所欲为。

2) 密码管理规则。尽量严格管理密码。比如,要求密码必须有足够的长度,让密码容错次数尽量少。

3) 资源管理规则。尽量防止某个用户无限申请某项资源,尤其是比较稀缺的资源,这样可以在一定程度上对付拒绝服务(denial-of-service)攻击。例如:禁止表空间自动增长,可以避免恶意用户用无用的数据占用硬盘空间。

4) 授权管理规则。在管理权限的时候采用吝啬的态度,只赋予用户能够完成合法操作的最小权限。

5) 可能带来安全隐患的东西如果不必要就应该删除或禁止。比如,在 linux 平台上,.bash_history 文件中可能会记

维普资讯 http://www.cqvip.com

载带有用户和密码的命令行，若存在则有安全隐患，如果不用的话最好删除这个文件。

6）审计管理规则。要求启动与安全策略相应的审计。比如：身份鉴别审计，对客体引入用户地址空间的审计，删除客体审计，对操作员、系统管理员和系统安全管理员实施的动作，以及其他与系统安全有关的事件的审计。

7）连接管理规则。严格管理数据库连接。比如，禁止没有密码的连接；对数据库连接进行 IP 限制；把一个用户的最长有效连接时间尽可能设的短一些；对网络传输的内容进行加密。

8）存储管理规则。功能不同的数据应该存放在不同的地方。比如：存档文件应该保存在磁带或另一块硬盘上；数据文件、索引文件、日志分到不同磁盘上；与数据库相关的文件和与数据库无关的文件保存在不同的分区上。

在实际工作中，如果有些配置方法与应用逻辑冲突，那么应该保证遵守应用逻辑，然后考虑如何解决存在的安全问题。

7.2 Kingbase ES 安全评测系统的体系结构

如图 1 所示，虚线包围的就是 Kingbase ES 评测系统的体系结构，主要包括 3 个部分。第一部分是脚本信息，把需要检测的项目用脚本的方式记录下来，可以根据需要修改。当然这些脚本必须加密存储；否则，如果被人恶意修改之后，可能会严重危害安全性。为了减少冗余，把评测信息划分到 3 个脚本中。第一个脚本 KB_Item 保存评测项目，也就是记录有多少个评测点。第二个脚本 KB_Method 保存测试方法，也就是调用什么方法获得每个测试点的实际配置。第三个脚本 KB_Evaluation 保存测试点评分标准，也就是如何根据每个测试点的实际配置情况对该评测点进行评分。

第二部分包括评测引擎和记分引擎。评测引擎的功能是根据脚本中记录的信息，访问数据库和操作系统。记分引擎根据获得的信息对所有评测点进行评价，粗略划分 DBMS 当前的安全级别，选出可能成为安全薄弱点的项目，并把结果记录到结果文件中。

第三部分是结果文件和结果展示程序。用 xml 格式保存评测结果，每次的评测结果都独立保存在一个文件中。结果展示程序的功能就是展示评测结果。结果展示程序输出 DBMS 当前的安全级别，列出安全薄弱点，并显示针对安全薄弱点的弥补建议。

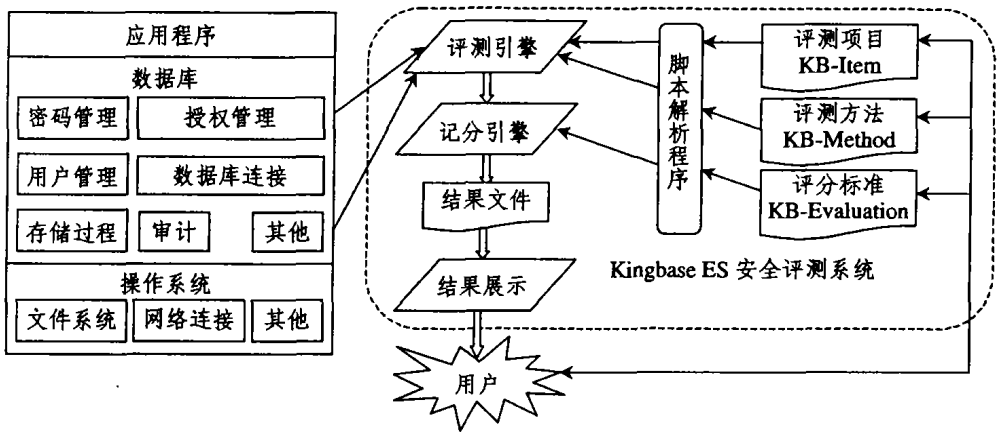

图 1 Kingbase ES 安全评测系统体系结构

7.3 Kingbase ES 安全评测系统的特点

Kingbase ES 安全评测系统有如下特点：

- 安全检查列表内容丰富。依据公安部标准 GA/T 389-2002 和国标 GB/T 18336-2001，借鉴国际 CVE 标准、一些流行数据库管理系统的安全管理策略以及一些知名数据库安全分析系统的经验，设计了丰富的安全检测项目。
- 不仅仅罗列安全隐患和漏洞，还侧重于分析，提供漏洞修补的解释。
- 易扩展，增加检测点简便。
- 设计了通过互联网直接升级的接口。
- 严格限制运行安全评测系统的用户权限，加密存储安全检查列表，保证了评测系统自身的安全性。
- 能够对比数据库当前状态与上次扫描后状态的改变，分析数据库中重要对象、权限的变化情况。
- 应用广泛。Kingbase 安全评测系统是针对各种用户的需要设计的。数据库管理人员可以利用它定期地进行数据库安全检测服务，消除安全隐患；系统开发和系统集成人员可以利用它在数据库建库和数据库改造前后进行安全系统建设方案和建设成效评估；它还可以协助安全管理员在安全事故后进行分析调查，帮助第三方评估机构进行安全性测评。

结束语 开发数据库安全评测系统是非常有意义的，既可以帮助用户检查和提高系统安全性，也可以协助第三方评估人员进行安全性评估，推进信息安全的发展进程。本文首先讨论了数据库安全评测系统的整体概念，然后介绍了国内外数据库安全评测标准和工具的发展情况，接下来总结了优秀的数据库安全评测系统应该满足的基本要求，最后以 Kingbase ES 为例，介绍了一个实际的数据库安全评测系统。

参 考 文 献

1 萨师煊，王珊．数据库系统概论．高等教育出版社，2000
2 段云所．网络与信息安全教程，2001
3 中国信息安全产品测评认证中心．GB 18336 介绍，2002
4 National Institute of Standards and Technology. Common Criteria Familiarization，1998
5 国家质量技术监督局．GB 17859-1999，计算机信息系统安全保护等级划分准则，1999
6 中华人民共和国公安部．GA/T 389-2002，计算机信息系统安全等级保护数据库管理系统技术要求，2002
7 The MITRE Corporation. Common Vulnerabilities and Exposures version 20030402，2003
8 The Center for Internet Security. Oracle Database Security Benchmark v1.0，2003
9 钟力，万孝雄．明查秋毫-漏洞扫描产品购买指南．网络世界，2003-3-31，第 10 期