文章编号:1000 - 582X(2003)07 - 0124 - 04

基于 MIDAS 技术的数据库安全代理的设计与实现*

蒋华林[1], 李志敏[1], 李立新[1], 杨 忠[2], 王洪建[1]
(1. 重庆大学 光电技术及系统教育部重点实验室,重庆 400044;2. 重庆大学 图书馆,重庆 400044)

摘 要:目前国内的数据库应用系统,多数是在 Client/Server 模式主流商用数据库产品环境下进行开发和运行,其安全级别较低。由于不可能对商用数据库产品进行修改,从应用实际出发,提出由数据库安全代理增强数据库应用系统的安全性。在分析数据库应用系统特点和安全需求基础上,结合实际系统研究了数据库安全代理的功能和在 MIDAS 技术基础上的设计和实现,并对其抵御常见数据库攻击手段的能力进行了分析和实验。

关键词:MIDAS; 数据库安全代理; 设计
中图分类号:TP391 **文献标识码**:A

1 数据库应用系统的特点与安全需求分析

随着数据库技术和网络技术的不断发展,基于网络和数据库的数据库应用系统得到越来越广泛的应用,其特点主要包括:1)以数据库为核心,所有的信息存储都是由数据库来完成的;2)以网络为载体,所有的数据传送均由网络来完成;3)要求较高的安全性;4)以为合法用户提供信息为目的。

一般来讲,数据库应用系统在以下几个方面容易受到攻击:

1)基于网络的攻击

目前绝大多数系统均在 Client/Server 模式下构建,信息在公用网络(如 Internet)上传输,非法用户就可通过网络监听等非法手段获得信息;即使在内部网络传输时低安全级别用户也可通过网络监听等非法手段获取高安全级别的数据。

2)基于数据库的攻击

数据库中的数据具有不同的敏感程度,具有相应权限的用户才能对其操作,而非法用户可能通过系统的漏洞访问到其不具备访问权限的数据。

3)基于应用系统的攻击

数据库应用系统对于所面对的用户按照可以完成的功能不同授予不同的权限,而不具有某项权限的用户可能通过某些非法操作以获得此权限而获得非法信息。

针对数据库应用系统所面临的安全风险,其安全需求主要包括:

1)客户机和服务器之间的严格的身份认证。

2)数据在网络上以加密形式传输。用户向数据库服务器发送的查询请求和数据库服务器返回的查询结果都应该以高强度的加密算法加密以防被窃取。

3)数据能以密文形式存放在数据库中。对一个数据库系统来讲,只要数据以可读的形式存储在数据库中,就可能存在潜在的危险,为此必须采用数据库加密的方法。加密后的数据库称为密文数据库。

4)完善的用户授权机制。数据库应用系统应该实现授权用户的授权管理,实现授权用户对授权对象的访问权限的分配、回收、定义和控制。

以上简要分析了数据库应用系统的安全需求,在数据库应用系统的实际开发中,可以根据实际需求选择相应的技术加以满足。

2 基于 MIDAS 技术的多级安全数据库应用系统的设计

2.1 数据库安全代理的概念和体系结构

数据库应用系统的安全需求,在 C/S 模式下难以直接满足。一种解决方案是对数据库和网络系统重新进行整体设计,将密钥管理、加解密、多级安全数据库系统、VPN、CA 等集成到系统中,这样使安全特性和数据库系统紧密结合,有利于提高效率,但设计开发复杂,代价很高。为了以较低的代价增强在现有的成熟的 DBMS 系统上开发的数据库应用系统的安全性,满足其安全需求,现引入数据库安全代理。由数据库安全代理综合完成与安全相关的功能,包括用户认证、网

* 收稿日期:2003 - 03 - 04
作者简介:蒋华林(1972 -),男,四川广安人,重庆大学硕士研究生,讲师,主要从事数据库和 MIS 系统研究。

络加密传输、授权管理、多级安全等。其结构如图 1 所示。

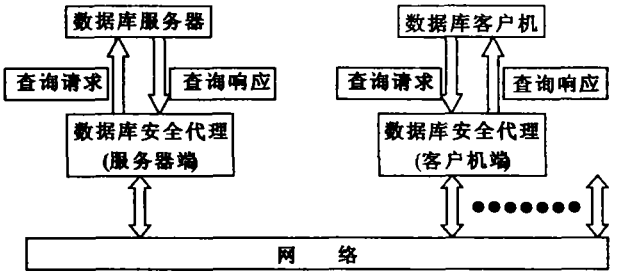

图 1　数据库安全代理结构

数据库安全代理的设计中，安全代理分为客户机代理和服务器代理，分别如图 2 所示。客户机代理包括通信模块、认证模块、加解密模块、数据访问模块 4 个部分，服务器代理还包含了用户授权管理模块。

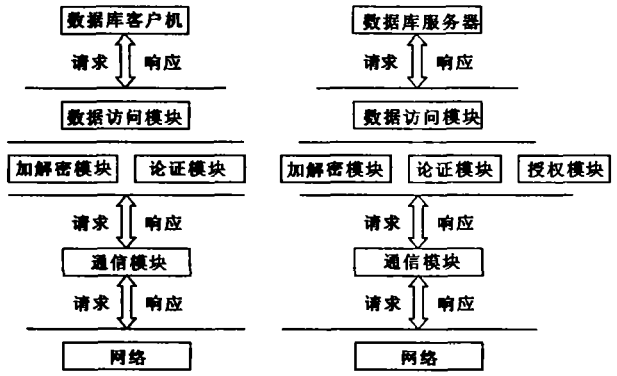

图 2　数据库安全代理的模块

在客户机一端数据访问模块负责接收数据查询和将解密后的查询结果返回给数据库客户机，在服务器一端数据访问模块将经过解密处理、安全检查之后的数据查询请求发送给数据库服务器，并接收数据库服务器对查询请求的响应，然后根据认证信息和授权模块的处理规则对响应的数据进行过滤，去掉根据访问规则不应该被该用户浏览的数据，然后将数据包交加解密模块进行处理。

加解密模块主要完成的功能包括：在客户机一端，负责将数据访问模块传来的数据查询请求加密后交通信模块发送，还需要将通信模块上传的查询响应数据包进行解密处理；在服务器一端，则包括将通信模块上传来的客户机查询请求解密并转交数据访问模块，以及对数据访问模块处理后的查询结果进行加密处理。

服务器端授权模块主要根据经过认证的用户信息确定用户的权限供数据访问模块使用。

服务器端和客户机端的认证模块共同完成用户的身份认证。认证技术可以采用基于对称密码体制的，也可以采用基于公钥密码体制的。

2.2　利用 MIDAS 技术实现数据库安全代理

与传统的 Client/Server 模式相比，三层应用体系结构使应用系统的性能、安全性、扩展性有了很大的提高，也方便了系统的维护和管理。数据库安全代理的功能，实际上属于三层应用体系结构中的应用服务层的功能。因此，基于中间件技术开发数据库安全代理是一个自然的选择，有助于提高安全代理的性能、安全性，尽量避免系统性能的下降。

MIDAS(Multi - Tier Distributed Application Services Suite)是 Insprise 公司开发的用来实现多层分布式数据库应用的通用中间件，它为开发多层应用提供了一套高级组件、服务器及核心技术，其特点是针对多层结构有多种代理和新一代的数据库引擎来适应它。

MIDAS 中为使用 SOCKET 通信协议的多层应用系统加入了一个称为“Interceptor”的技术，利用该技术可以拦截多层应用系统中客户端和应用服务器端流动的数据，以进行特殊处理。在多层应用系统中，数据在客户端和应用服务器之间有两个流动方向，每一个方向都有数据流出和流入两个点，则在两个方向存在。

如图 3 所示，利用“Interceptor”技术，可以在这 4 个拦截点实现对数据的拦截和加密。

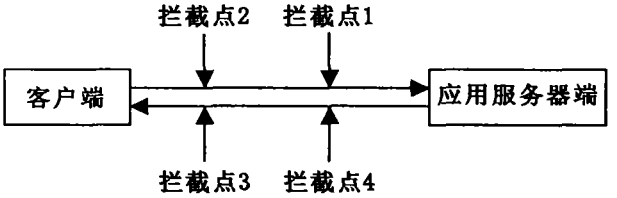

图 3　Intercept 技术

在检索密文数据库时，数据库安全代理的数据访问模块需要对密文字段进行解密处理并重新加密后交数据通信模块传送给客户端代理。Delphi 的 MIDAS 机制提供了数据加密的途径，可以在数据传往客户端之前对一些字段进行加密，也可以在接收到客户端的更新数据请求后对来自客户端的数据的相应字段进行解密后才向数据库进行更新。为此在服务器程序的远程数据模块中加入一个 Tprovider 或是 TdataSetProvider 对象，并将此对象的 DataSet 属性置为要处理的数据集。在 Tprovider 的 OnGetData 事件中加入相关代码对敏感字段进行处理即可；同样，在 Tprovider 的 OnUpdateData 事件中加入一些处理代码便可对客户端送来的数据进行解密。而在客户端的数据库安全代理中，则可以利用敏感字段的 OnGetText 事件对敏感数据进行处理。

2.3　用户认证和加密方案

在综合考虑强度、用户的可接受度、成本的基础上采用了一种基于对称密钥体制的通行字/口令用户认证方案。该方案的基本思想是采用对称密码技术与认证服务器(即服务器端数据库安全代理的认证模块)进行用户认证工作。具体作法如下：

服务器端安全代理保存有关用户的 ID、口令等身份信息，系统在添加新用户的时就为该用户生成一个用于对称密码算法 IDEA(128 位)的密钥，该密钥利用用户口令加密后形成一个密文文件，该密文文件通过可靠

渠道如密钥盘的形式传递到用户手中。避免用户口令在网上的传输。客户端数据库安全代理通过用户口令解开密文得到对称密钥,并利用此对称密钥加密用户ID和时间戳(timestamp)认证信息,该对称密钥同时还保存在服务器端的数据库中。认证服务器根据用户ID找到相应的对称密钥,此对称密钥解开客户端传来的认证信息,通过比较认证信息,认证服务器可以确信对方拥有正确的密钥,也就是客户知道正确的口令。

认证成功之后,使用Hash函数(选用MD5)作用于用户的对称密钥和一个随机数形成会话密钥;认证服务器保存用户ID、会话密钥、用对称密钥加密的会话密钥、时间戳(timestamp);认证服务器将成功的消息(包括加密的会话密钥)返回到客户端代理;客户端代理收到后用用户的对称密钥解密得到会话密钥。

该认证方案具有实现简单高效的特点,但不能实现双向认证,适合于对认证要求较低的封闭区域认证,在系统的初步实现中采用该认证方案。

为了在开放性的网络上对远程的使用者进行认证,应采用基于X.509、认证中心CA的认证方案。

2.4 密文数据库加解密的处理

数据库系统的加密需要满足的要求是:数据的生存周期长,密钥的保存时间也相应较长,加密算法的密码强度足够高,以保证加密后的数据是安全的;加/解密的额外开销足够小,以避免系统效率,特别是查询效率的降低;密钥管理方案方便灵活。

主要将数据库中的表分为两类:一种是含有加密字段的表;一种是不含加密字段的表。不含加密字段的表只进行校验,在对数据表进行插入和修改时采用MD5算法计算记录的校验和,该和再用表密钥加密;含有加密字段的表的数据加密采用字段一级的加密和数据项一级的加密。字段一级的加密是每个字段共用一个密钥,适用于对加密强度要求较低的数据,数据项一级的加密则适合对加密强度要求较高的情况。一个表中所有的校验和共用一个表密钥,字段密钥也保存在相应的密钥表中。整个密钥表用系统主密钥加密后保存在系统中,每次运行时读入主密钥将其解密,由主密钥的安全来保证系统的安全。

下面以对数据项的加密方法进行说明:

设有一个具有 m 条记录,n 个属性的数据库,每个数据项表示为 $x_{i,j}$,其中 $1\leqslant i\leqslant m, 1\leqslant j\leqslant n$.

数据项加密是对 $x_{i,j}$ 进行密钥变换:$y_{ij}=E(x_{ij},k_{ij})$,其中 E 为加密算法;k_{ij} 是数据项 $x_{i,j}$ 的密钥,y_{ij} 是加密后得到的密文,存放在数据库中。D 是解密算法,是 E 的逆运算。

数据库中每一个数据项 $x_{i,j}$ 都应该有自己的密钥 k_{ij}。一般情况下,不同的2个数据项 $x_{i,j}$ 和 x_{pq},其密钥应该是不同的,以避免通过统计分析、明密文对照等攻击。因此数据项密钥的个数与数据项的个数一样多,如果采用随机数的方法生成,则必须将其全部保存,其安全性和空间开销都难以解决。而采用函数生成的方法,则避免了这些问题。具体说明如下:

数据项 x_{ij} 的密钥 $k_{ij}=F(TK,R_i,C_j)$,其中 F 为密钥生成函数,R_i,C_j 是记录及属性的参数,在表中以明文的形式出现。将 R_i 设为记录的ID域,C_j 取为属性名的MD5值,需要保密的就是表密钥TK,而对函数 F 必须满足以下条件:

1)不同数据项的密钥相同的概率极小,特别是对同一属性中数据项;

2)即使数据项的明文或其概率分布已知,也难以根据密文求得有关数据项的其它信息;

3)从一个数据项密钥求得其它数据项密钥非常困难。下面给出这样一个函数:

$$K_{ij}=E(TK,R_i)\oplus E(TK,C_j) \tag{1}$$

其中 E 是一种块加密算法,如IDEA、DES等。

对于同一记录 i 中的2个不同数据项 x_{ij} 和 x_{iq},由 C_j 和 C_k 的产生方式知 $C_j\neq C_q$,所以 $E(TK,C_j)\neq E(TK,C_k)$,所以 $K_{ij}\neq K_{iq}$;同理,对于同一属性 j 的不同数据项 x_{ij} 和 x_{pj},也有 $K_{ij}\neq K_{pj}$。

对于任意2个数据项 x_{ij} 和 x_{pq},其中 $i\neq p, j\neq q$,若要 $K_{ij}=K_{pq}$

就是要

$$E(TK,R_i)\oplus E(TK,C_j)=E(TK,R_p)\oplus E(TK,C_q) \tag{2}$$

其中 $R_i\neq R_p$,$C_j\neq C_q$,而寻求使得上式成立的 K_{ij} 和 K_{pq} 是相当困难的,所以函数满足安全条件1;

而安全条件2只要采用采用高强度的块加密算法即可以满足;

由于 $E(TK,R_i)$ 和 $E(TK,C_j)$ 的不可知性,攻击者不可能求得另外的密钥 K_{pq} 或者 TK,所以安全条件3也满足。

总之,该密钥生成函数满足安全条件。

3 防御常用数据库攻击手段的能力分析及实验

由于数据库系统的重要性,数据库系统也成为"黑客"在对计算机系统进行攻击时的一个重要目标。其常用攻击手段主要包括:

1)利用SA漏洞

数据库服务器软件安装后都建有内置的管理员帐号和密码,其服务端口也是公开的,攻击者就可以在与服务器相连的任何一台计算机上利用相应工具直接连接数据库系统。

2)字典攻击

通过"黑客字典"将数据库用户可能的口令进行穷举实验,一旦实验成功,就可以联结到数据库服务器上的某个数据库中并进一步执行数据库中的相关存储过程或者对预定义的存储过程进行修改。

3)在客户机端窃取密码

在C/S模式下，通常在客户端设置有连接服务器所需要的帐号和密码，使用一些工具非常容易窃取密码。

4）嗅探器软件"Sniffer"的使用

在网络环境下攻击者常用的Sniffer软件，可以探测到同一网段的传输信息，进而获取相关信息。对于网络上未经过加密的信息，使用Sniffer软件特别有效。

这些攻击手段在应用于基于安全代理的数据库应用系统时却基本失去了作用。从实验结果来看，配合IP端口控制，在客户机一端无法直接连接到数据库服务器上，只能连接到服务器端安全代理，攻击手段无效。

对于攻击手段2，在采用前文中的认证方案时，攻击者由于无法得到用户的密钥盘，即使知道用户的ID，通过穷举口令，也无法通过认证，因为攻击者还必须穷举对称密钥。假设口令为5位数字，对称密钥为128位，则必须试验$10^5 * 2^{128} \approx 3.4e+43$次，这在实际上是不可能的。而且，还可以进一步采用认证强度更高的认证方案或者定期更换密钥盘的方式增强抗攻击能力。

对于攻击手段3，由于用户ID和密码并不保存在客户机上，也就大大减少了被窃取的机会。

对于攻击手段4，在运用Sniffer软件进行嗅探攻击时，由于信息均以加密形式在网上传输，故成功的可能性很小。

在各种攻击数据库系统的方法中，对数据库服务器的攻击最为直接，一旦攻击者获取对数据库服务器的控制，就可以对数据进行任意的窃取和破坏。数据库安全代理的设计思想就是在数据库服务器与客户机之间充当安全屏障，避免对数据库服务器的直接攻击。在网络结构中，服务器端数据库安全代理可以看成一个应用网关。

4 结 论

在现有的Client/Server模式主流商用数据库产品应用环境下，通过由数据库安全代理增强数据库应用系统的安全性，是一种比较切实可行的方法。特别是多层数据库应用技术的出现，极大地方便了数据库安全代理的实现。开发专用的安全中间件，是国内研究与开发的一个重点，也是进一步研究的方向。文中给出了在Insprise公司的MIDAS技术的基础的数据库安全代理设计和实现，并已经应用于实际系统。数据库加密方法从目前的研究进展看，尚需进一步研究。考虑到对安全认证要求的提高，身份认证在进一步的开发中应该采用安全强度更高的方案，如基于Kerberos、X.509的PKI的认证方案。

参考文献：

[1] DEPARTMENT OF DEFENSE. United States. Trusted Computer System Evaluation Criteria[Z]. DoD 5200.28 - STD, Washington, DC. December 1985.

[2] NATIONAL COMPUTER SECURITY CENTER. United States. Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria[Z]. NCSC - TG - 021, April 1991.

[3] BRUCE SCHNEIER. Applied Cryptography, Protocols, algorithms and source code in C[M]. HOBOKEN, New Jersey; USA: Wiley Press, 2000.

[4] 陈庆章. 基于用户角色和阶段性控制的网上公文传送的安全机制[A]. 第一届中国信息和通信安全会议学术会议论文集(CCICS99)[C]. 北京:科学出版社, 2000.

[5] 蒋继洪. 计算机系统、数据库系统和通信网络的安全与保密[M]. 成都:电子科技大学出版社,1995.

[6] 王涛. 多层分布式数据库实战[M]. 北京:清华大学出版社,2000.

Design and Realization of Database Security Proxy Based on MIDAS

JIANG Hua-lin[1], *LI Zhi-min*[1], *LI Li-xin*[1], *YANG Zhong*[2], *WANG Hong-jian*[1]

(1. Key Laboratory of Opto-electronic Technology and System under the State Ministry of Education, Chongqing University, Chongqing 400044, China; 2. Library of Chongqing University, Chongqing 400044, China)

Abstract: Most database application systems are developed and operated under the environment of current C/S business database products, therefore the security is low. It is impossible to modify the business database products, according to the realization, database security proxy is put forward to enhance the security of database application system. Based on the characteristics and security requirement of database application system, the authors study the function of database security proxy and its design and realization based on Borland's MIDAS (Multi - Tier Distributed Application Services Suite), and analysis and experiments are done on the ability of preventing main attack methods to database.

Key words: MIDAS; database security proxy; design

（编辑　张小强）