第33卷 第19期 计 算 机 工 程 2007年10月
Vol.33 No.19 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)19—0168—02 文献标识码：A 中图分类号：TP309

基于CA认证的远程数据访问模型

谭云松
(武汉工程大学计算机科学与工程学院，武汉 430073)

摘 要：在介绍数据传输和数据库安全重要性的基础上，分析了基于CA认证的远程数据访问模型，该模型分为客户身份认证模块、SQL解析模块、数据安全传输模块等功能模块，介绍了各模块所实现的功能和实现的流程。该模型利用CA认证过程来为通信两端提供安全可靠的通信通道，具有信息保密性、信息完整性、身份认证等功能，同时，对企业重要数据字段进行加密，来保证数据库端的数据安全，在一定程度上能保证数据在远程访问过程中的安全，同时保证数据在数据库端对非相关人员的不可见性。

关键词：CA认证；远程访问；数据安全

Model of Teledata Access Based on CA Authentication

TAN Yun-song
(School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan 430073)

【Abstract】Besides importance of data transmittal and database security illustrated, the requisite analysis of the model of teledata access based on CA authentication are elaborated as well. The model is divided into client authentication modules, SQL resolution modules, and data transmittal modules and so on. The model functioned with confidentiality, integrity, identity authentication etc, provide secure and reliable channel for sensitive data between two communication terminals; On the other hand, sensitive data in server database is encoded by fields, which keep invisibility for non-correlation persons. The model, to some extent, can keep sensitive data safe in most enterprises.

【Key words】CA authentication; remote access; data security

随着 Internet 的快速发展，其开放性、国际性和自由性的特点也使得网络与信息安全成为人们高度关注的社会性问题。人们已逐渐认识到网络领土已成为国家领土和主权的重要组成部分，网络与信息安全直接关系到国家安全和人们的日常生活。信息安全的概念经历了一个漫长的历史阶段，从信息的保密性，拓展到信息的完整性、信息的可用性、信息的不可否认性，甚至到信息系统的保障。随着企业信息化水平的提高，企业员工流动和信息流通的速度加快，信息量的需求加大，从而引发了企业对内部数据信息安全提出新的需求。本文所论述的数据安全访问模型主要从两个方面来确保数据的安全，数据传输过程中的安全和数据访问过程中的安全。

1 数据安全访问模型分析

在网络环境下的数据安全应分为两个层面：数据的静态安全和数据的动态安全。静态安全是指防止存放在数据服务器存储设备内的数据被盗窃、修改、删除、破坏。动态安全是指防止在数据传输交易过程中被截取或篡改。所以保证数据安全至少要有两方面技术手段及工具：(1)系统防护技术，指从桌面系统到网络环境到数据服务器的防病毒、防黑客入侵技术能用现有的网络防病毒技术、防火墙技术、入侵检测技术来实现，防止数据被盗窃、修改、删除、破坏，可以用身份认证技术、数据加密技术。(2)系统保护技术，指数据备份、快速恢复、异地存放、远程控制、灾难备援等技术。数据安全存取模型在系统防护技术方面主要采用身份认证技术、数据加密技术来确保安全，在系统保护技术方面主要采用数据备份、快速恢复来确保[1]。

数据安全主要分为传输安全和存取安全两大部分，主要设备有：客户端(Client)，认证服务器(Authentication)，CA中心(CA Center)，事务服务器(MTS Server)，数据服务器(Data Server)和数据库(DB)组成。模型采用3层构架实现，其结构如图1所示。

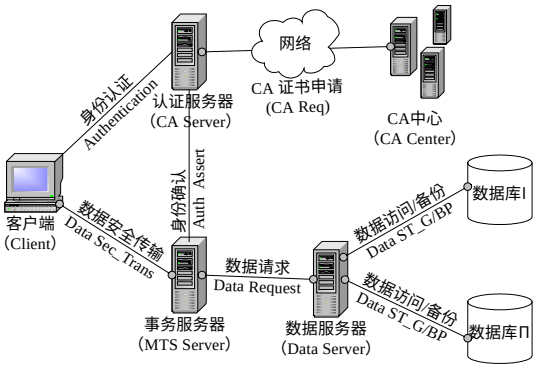

图1 数据安全访问模型

身份认证由客户端、认证服务器和事务服务器共同组成，客户端发起认证请求，认证服务器验证请求，如果通过验证，则向事务服务器发送身份确认，如果没有通过验证，则向客户端发送服务拒绝。

数据安全传输在客户端和事务服务器端使用一次一密方式加密传输交互的数据包，保证数据在网络传输中的安全。

事务服务器的处理模块是本模型中的核心，其中主要处理模块有：数据安全通信机制，SQL语句解析机制，库文数

作者简介：谭云松(1972－)，男，讲师、硕士，主研方向：信息系统安全

收稿日期：2006-10-15 **E-mail：**yunsongtan@yahoo.com.cn

据加解密等重要机制。

数据服务器的作用是管理和处理数据库，主要操作有数据库的备份、恢复和日志管理，同时提供给事务器的数据请求接口。

数据请求运行机制如下：

(1)客户端产生会话密钥 SessionKey；

(2)向认证服务器提交身份认证申请 AuthRequest，客户端将会话密钥与身份认证申请一起提交认证服务器；

(3)证服务器向客户端确认身份，同时向事务服务器报告有客户已经通过认证，并把会话密钥交给事务服务器；

(4)客户端用会话密钥加密数据请求语句发送至事务服务器；

(5)事务服务器用会话密钥解密数据请求语句，解析 SQL 语句，分析其中有无加密字段，重组 SQL 语句，向数据服务器请求数据；

(6)数据服务器从数据库中取出数据，返回给事务服务器；

(7)事务服务器根据加密字段的情况解密数据，还原成明文，用会话密钥加密数据，回传给客户端；

(8)客户端用会话密钥解密数据作数据分析处理。

数据请求操作流程如图 2 所示。

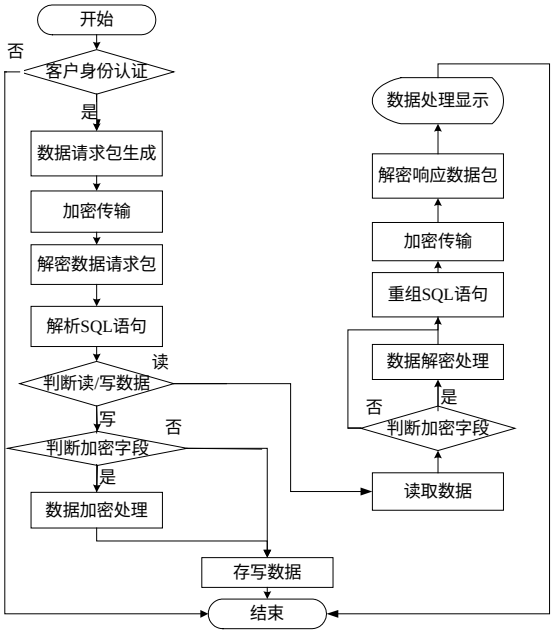

图 2　安全操作流程

2　模型中的 CA 认证体制

CA认证体制是基于X.509 认证协议的一个身份认证模型，包含了 3 种身份验证过程：单向身份认证，双向身份认证和三向身份认证，所有过程都采用了公钥签名技术，验证过程是假定双方都知道对方的公钥，或通过从目录中获得对方的证书，或证书包含在双方的初始消息中[2]。该机制现在已经比较完善，而且，在各大机构和部门都有应用，在开发成本上由于现在有公开源代码OPENSSLE可以参考，其中的代码可以移植到Windows平台上，从而可以极大地减少开发成本。一般对一个CA中心，证书的维护的主要内容有CA证书申请、CA证书注销、CA证书更换、CA证书恢复、身份认证等操作，在本文的CA认证机制中客户端的所有这些服务操作都只向认证服务器提出，由认证服务器通过CA中心完成。

(1)CA 证书申请由认证服务器统一从认证中心(CA Center)取得服务器 CA 证书和客户端 CA 证书、保存，当客户端需要证书时不用向认证中心申请，而向认证服务器申请，由认证服务器发给客户端 CA 证书。

(2)CA 证书注销由客户端向认证服务器提出 CA 证书注销申请，认证服务器在向 CA 中心提出注销该客户的 CA 证书，注销成功时，认证服务器删除在证书库中的该 CA 证书，并通知客户端。

(3)CA 证书更换由客户端向认证服务器提出 CA 证书更换申请，认证服务器在向 CA 中心提出更换该客户的 CA 证书，更换成功时，认证服务器更换在证书库中的该客户的 CA 证书信息，并把新的 CA 证书发给客户端。

(4)CA 证书恢复由客户端向认证服务器提出证书更换申请，认证服务器从证书库中取出该客户的 CA 证书，发给客户端。

(5)身份认证通过 CA 证书的交叉认证功能来实现。

这种身份认证模型可以使得 CA 中心相对独立，从而使其可以给其他应用系统提供证书分发、认证服务，认证服务器可以在 CA 证书中增加一个字段形成扩展，另一方 CA 证书(ExtCA)用来存储通信的会话密钥，以达到对本模型更优化的功能，能在认证过程同时完成交换客户端与事务服务器(MTS Server)之间的会话密钥。建立这种 CA 认证模型的先决条件：(1)事务服务器与认证服务器之间、客户端与认证服务器之间是信任的；(2)认证服务器与事务服务器之间的通信是安全的。

3　模型中的数据安全传输机制

数据安全传输是保证信息的机密性、完整性和不可否认性的必要手段，数据的不可否认性，可以通过上面的客户身份认证技术来保证；数据的完整性，主要通过消息认证技术，常用手段是在传输消息中加入传输消息的消息摘要，也即散列值(Hash 值)，在接收方再次产生消息摘要，检验这两则消息是否相同来保证。在这里不再实现专门的消息认证技术，而在应用中通过检验传输到来的数据是否符合要求来保证消息的完整性，因为消息在传输过程中是加密的，如果在传输过程中被修改，那么收到的数据一定是乱码或不符合模型数据格式，就可以要求发送方再次发送数据。保护数据在传输过程中保证不被不法分子非法窃取、篡改或泄漏，使数据具有极高的可信性，在数据传输中提倡一次一密的加/解密策略。数据安全传输的常用方式有两种：

(1)基于公钥体制的数据安全传输：这种方式下要求发送方知道接收方的公钥，接收方通过私钥解密接收到的数据。这种加密传输方式的缺点是加密速度较对称加密慢，在实际上常用公钥体制加密会话密钥，而用会话密钥加密数据进行数据传输以提高效率。

(2)基于对称密钥体制的数据安全传输: 基于对称密钥体制的数据加密传输需要发送方和接收方有一个交换会话密钥的过程，发送方用会话密钥加密数据，接收方用同样的密钥解密。这种加密传输方式比非对称加密/解密方式速度快得多，但此方式需要有一个会话密钥交换过程。

在本模型中采用对称密钥体制方式，同时会话密钥的交换可以在客户的身份认证过程中完成，也即客户产生会话密钥和身份认证消息一起发送给认证服务器，认证服务器在确认客户身份的同时，将会话密钥转交给事务服务器，这样客户和事务服务器都掌握了相同的会话密钥，发送方用此密钥加密数据，接收方用此解密获得数据。

4　SQL 语句解析

数据库系统一般可以理解成两部分：(1)数据库，按一定的方式存取数据；(2)数据库管理系统，为用户及应用程序提供数据访问，具有对数据库进行管理、维护等多种功能。在本模型中使用的SQL是嵌入到某种高级程序设计语言中使用的，且对加密字段要进行分解操作，分解成加密字段和非加密字段。主要涉及数据操作有数据查询和数据操纵语句[3]。

（下转第 172 页）