VDSI 系统的数据库安全性研究与实现

葛志赟 赵正德 孙培君
(上海大学计算机工程与科学学院,上海 200072)

摘 要 信源问题一直是汽车数字化过程中的一个瓶颈问题。射频识别(radio frequency identification,RFID)技术的日趋成熟为解决这个问题提供了新的方向。然而,作为 RFID 系统的一种应用,其安全问题必须得到很好的解决。本文就汽车数字化标准信源(vehicle digital standard info-source,VDSI)和 RFID 的特点以及当前信息安全现状提出了一种 VDSI 数据库加密引擎。

关键词 RFID VDSI 系统 信息安全 数据库加密引擎
中图法分类号: TP301.6 **文献标识码**: A **文章编号**: 1006-8961(2009)12-2623-04

The Research and Realization of Database Security in Vehicle Digital Standard Info-source System

GE Zhi-yun, ZHAO Zheng-de, SUN Pei-jun
(*School of Computer Engineering and Science, Shanghai University, Shanghai* 200072)

Abstract The information source has been a bottleneck problem which troubles the vehicle digitalization process for a long time. With the rapid growth and wide range of adoption of Radio Frequency Identification (RFID for short) technology, a new viable solution is provided to solve the problem. With the adoption of RFID technology, the information security problems can be solved. This paper discussed the characteristics and peculiarity of RFID technology as vehicle digital standard info-source (VDSI for short), and proposed a VDSI database encrypting engine.

Keywords RFID, VDSI system, information security, database encrypting engine

1 引 言

射频识别(RFID)技术从 1948 年奠定其理论基础至今,其基础理论与技术已十分成熟[1]。在制造技术方面,RFID 标签从有源到无源、小型化、低功耗、作用距离的增长等方面均取得了长足的进步,特别是工作于 UHF 频段的无源标签的研制、生产,已逐步确立领先地位并成为新的发展方向。这为 RFID 技术应用于汽车数字化标准信源(VDSI)提供了有利条件。

本项目提出将汽车和司机信息数字化和标准化的信息源称为 VDSI。VDSI 系统将有效解决汽车车辆自动识别和管控等问题。将 RFID 应用于 VDSI 系统工作原理图[2]如图 1 所示。

系统将 RFID 标签作为汽车身份特征信息和管理基础信息的信源载体,将 RFID 的读写设备与各种中间件配置并二次开发成依托“信源”进行信息资源开发的专门装置,再将它们集成在一个应用大系统中,为多个领域的用户提供社会化服务。这有效地克服了目前 AVI 系统的低效率等问题。但 RFID 应用于交通领域有其固有的问题。由于其存储的数据是海量的,信息安全问题就是比较突出的一个[3]。

基金项目:国家科技支撑项目(2007BA00083);上海市重点学科建设项目(J50103)
收稿日期:2009-06-14;**改回日期**:2009-09-18

第一作者简介:葛志赟(1985~),男。上海大学计算机工程与科学学院计算机科学与技术专业在读硕士研究生。主要研究方向为 RFID 应用及 VDSI 系统的信息安全等。E-mail:gzy0511@126.com

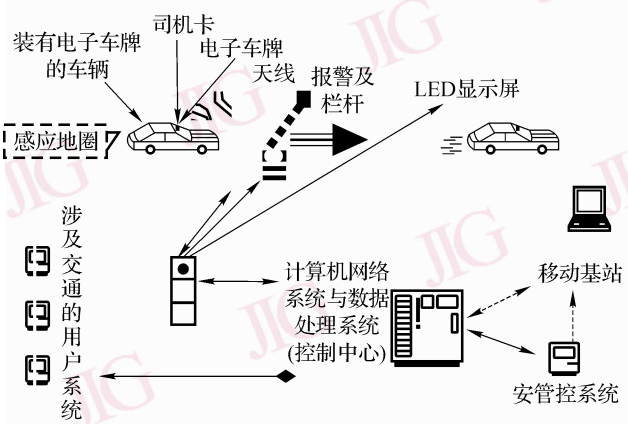


图 1 RFID 应用于 VDSI 系统原理图

Fig. 1 The principle picture of the application of RFID to vehicle digital system

本文在针对汽车数字化标准信源的需求和 RFID 的固有安全漏洞提出了 VDSI 数据库加密引擎。

2 VDSI 安全需求分析

2.1 RFID 在汽车数字化系统中的应用

将 RFID 作为汽车数字化系统中采集对象的唯一身份标识,需要突破 RFID 目前“工具型”应用的低级模式,充分开发其“资源型”应用的深层次潜质,以便为交通管理、人类社会等提供更合理、更全面的综合服务。然而这样的应用也必须面对当前 IT 时代无处不在的信息安全问题。

2.2 VDSI 的安全问题

众所周知,随着生产力的长足发展,人类已经步入了汽车社会。汽车和公路交通的管理是社会化的。这样的情况下,将 RFID 在汽车数字化系统中作“资源型”应用就需要将一些很多带有隐私或机密性质的信息作为资源存入信源内存中。这无疑增大了 VDSI 的安全需求。主要涉及以下几个方面:

(1)保密性:作为汽车数字化信源的 RFID 标签不应当向未授权的阅读器泄漏任何敏感的数据。

(2)完整性:保存在标签中的信息在被读卡器读出后未被修改和替换过。

(3)可用性:信源信息能够被系统中的授权基站读卡器使用,并且能够有效地抵制拒绝服务的攻击。

(4)真实性:信源标签和授权基站读卡器之间应该能够互相认证对方的真实身份。

而 VDSI 系统的数据库是海量信息的集聚之所,在运行时处于核心的位置,数据库的丢失将有可能使所有信息泄露,而数据库的损害则可能导致 VDSI 系统瘫痪。针对该问题本文通过分析 VDSI 系统特点提出了 VDSI 数据库加密引擎。

3 VDSI 数据库加密引擎

根据加密部件和数据库管理系统(database management system,DBMS)的位置关系可以将数据库加密分为库内加密和库外加密两种。由于 DBMS 库内加密对于 VDSI 系统数据库来说对性能影响太大,比如加重数据库服务器的负担;增大了加、解密协调的难度。而库外加密方式减少了 DBMS 的设计复杂度和运行负担,提高 VDSI 系统的灵活性。可见,对 VDSI 系统来说库外加密明显具有更好的效果。所以,选择设计 VDSI 数据库加密引擎的方式来实现 VDSI 数据库加密的安全保护。

3.1 VDSI 数据库加密引擎加密算法的选取

在 VDSI 系统中,信息主要存放于数据库中,其数据量巨大,但大部分都是车辆信息、号牌信息等普通数据,根据这一情况,在 VDSI 系统中,应该选用对称加密算法作为其主要加密算法。

DES 算法[4]历史悠久,性能可靠,实现方法清楚明确;Rijndael 算法[5]性能卓越,抗攻击能力强,是新一代加密标准。相对于这两种对称加密算法,IDEA[6],RC5 算法[7]历史不如 DES 算法,实现起来也较 DES 复杂,而其性能又比不上 Rijndael 算法。所以,将主要通过对 DES 以及 Rijndael 这两种对称加密算法的比较,从而完成对 VDSI 数据加密技术的研究。

3.2 两种对称加密算法的比较

(1)安全性比较

Rijndael 算法与 DES 算法最大的不同是不使用 Feistel 结构。在大多数加密算法中,轮回变换都使用著名的 Feistel 结构。在这个结构中,中间状态位部分通常不做更改地调换到另一个位置。Rijndael 的轮回变换不使用这个古老的 Feistel 结构。轮回变换由 3 个不同的可逆一致变换组成,叫做层。

线性混合层保证了在多个轮回后的高度扩散。而非线性层使用 S 盒的并行应用,该应用程序有期望的(因此是最佳的)最差非线性特性。S 盒是非线性的。这就是 DES 和 Rijndael 之间的密钥概念差异。因此,Rijndael 算法比 DES 有着更强的性能与

更强的安全性。

(2)速度比较

加密速度对于一个加密算法而言十分重要,而面对大量的待加密数据而言,这一点更是不言而喻的,为此,有必要通过加密时间的量化统计,对这两种对称加密算法的加密速度进行比较。软硬件测试环境如下:

硬件环境:

CPU:Intel Pentium processor 2.40 GHz

内存:2 GB DDR

软件环境:

Microsoft Windows XP Home Edition SP2

Visual Studio 2005

分别使用 64 位密钥 DES 算法与 128 位密钥 Rijndael 算法,测试其对于 1 byte,8 bytes,64 bytes,256 bytes 的数据进行加密所花费的时间。测试结果如图 2 所示。

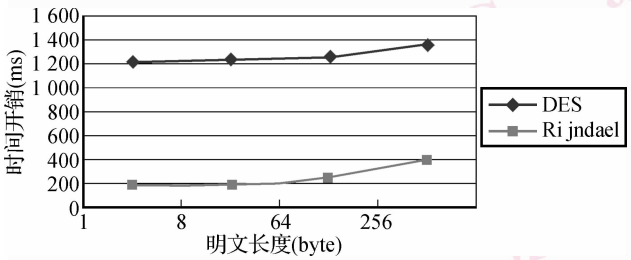


图 2　DES 算法与 Rijndael 算法加密时间开销比较

Fig. 2　The comparison of DEC algorithm and Rijndael algorithm in the encryption time overhead

通过比较可以发现,Rijndael 算法在时间花销上对比 DES 算法有着明显的优势,其速度要比 DES 算法快 10 倍以上,如果光考虑速度因素,Rijndael 算法无疑是进行加密时选用算法的最佳选择。

(3)密文长度比较

随着存储设备价格的不断下降,人们已经逐渐降低了对于减少数据存储长度的刻意追求,但是尽量减少数据存储的长度,有效利用存储设备,使用最少的存储媒介,储存最多的数据信息,以获得更高的性能价格比,仍然是应该追求的。因此,对所需储存的密文长度的研究也就显得相当重要。

依然分别使用 64 位密钥 DES 算法与 128 位密钥 Rijndael 算法,测试其对于 1 byte,8 bytes,64 bytes,256 bytes 的数据加密,所得到的密文长度。测试结果如表 1 所示。

表 1　DES 算法与 Rijndael 算法密文长度比较

Tab. 1　The comparison of DEC algorithm and Rijndael algorithm in ciphertext length

单位:byte

明文长度	Des 算法密文长度	Rijndael 算法密文长度
1	12	24
8	24	24
64	96	108
256	352	364

通过比较可以发现,当明文长度较短时,DES 算法与 Rijndael 算法所形成的密文长度相差较大,可以最高达到 2 倍的差距,而当明文长度达到 100 bytes 以上时,这种差距就并不明显了,为此,有必要对明文长度较短时的情况做进一步的研究。

通过对 1 byte 至 8 bytes 明文进行加密所做的测试,得到的结果如图 3 所示。当需加密的明文长度小于 8 bytes 时,DES 算法所取得的密文为 12 bytes,而 Rijndael 算法所取得的密文为 24 bytes,两者相差一倍。

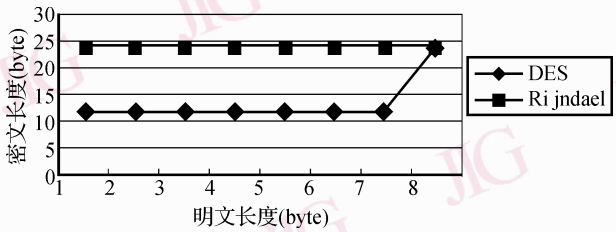


图 3　DES 算法与 Rijndael 算法密文长度比较

Fig. 3　The comparison of DEC algorithm and Rijndael algorithm in ciphertext length

为此,可以得出结论,当需加密的明文长度较小时,使用 DES 算法进行加密可以得到更小的密文长度,也就可以减少所占用的存储设备空间,从而降低对存储设备资金投入。

3.3　加密粒度选择

当加/解密粒度为每条记录的字段数据时,系统的安全性和灵活性都是最高的。当然,实现难度也最大。该加/解密粒度模式下,每个字段数据可以独立进行加解密操作,并使用互异的字段数据密钥。这样就可以只对需要操作的数据进行加解密,而不必每次将整张表或整条记录都加解密,所以,数据操作效率较高;并且由于不同的数据项使用不同的密钥,所以相同的明文会形成不同的密文,从而大大减少了同一密钥形成的明密文对。但问题是这种粒度

模式需要引入大量的密钥,这些密钥的设计和管理将直接关系整个加密方案的安全性和可行性。因此,只有以记录的字段数据即数据项为加/解密粒度,才能适应 VDSI 数据库加解密的操作。

3.4 VDSI 数据库加密引擎实现

VDSI 数据加密引擎的实现需使用 DES、Rijndael 等机密工具来对数据进行加密和解密处理。VDSI 数据库加密引擎实现的控制流程如图 4 所示。

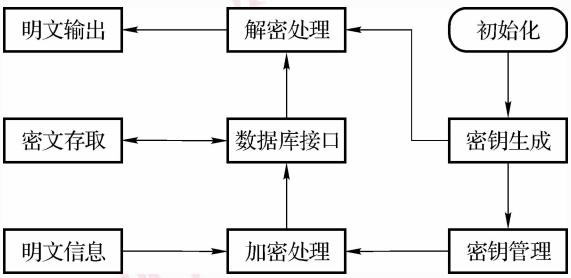
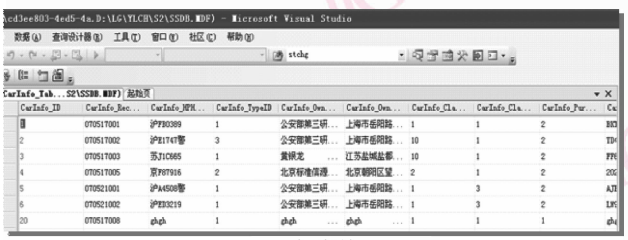


图 4 VDSI 数据库加密引擎控制流程

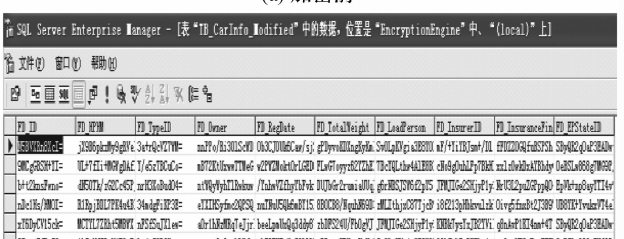
Fig. 4 The control flow of VDSI database encrypting engine

4 VDSI 数据库加密验证实例

采用 Rijndael 算法对那些安全性要求高或者加密速度要快的字段数据进行加密,比如车牌号(CarInfo_HPHM),车主(CarInfo_Owner),车所有人联系地址(CarInfo_OwnerAdress)等;而对那些安全性要求并不高且加密明文长度较小的字段数据则采用 DES 算法进行加密,比如车辆类型(CarInfo_TypeID)等。这样 VDSI 系统的安全性、数据操作效率就会有所提高,且从一定程度上减少了密文所占用的存储设备空间。通过数据库加密引擎加密前后的信息对比如图 5 所示。



(a) 加密前



(b) 加密后

图 5 VDSI 系统综合演示平台车辆信息表在数据库加密前后对照

Fig. 5 The comparison of the vehicle information table before encryption and after encryption in the comprehensive demonstration platform of VDSI system

从图 5(a)和图 5(b)中可以看出加密以前相同的数据在加密以后保持了密文无规律性。实现了前文中的信息加密的安全需求。

5 结 论

针对 RFID 作为在汽车数字化标准信源所面临的信息安全问题,根据汽车数字化系统的工作特征和现有的信息安全技术提出了一种数据库加密引擎,有效解决了在系统运行过程中必将面临的信息完整性、隐私保密性等问题。

参考文献(References)

1 Lang Wei-min, Lei Chen-da, Zhang Lei. RFID technology security research [J]. Micro Computer Information, 2006, **22**(17): 269-271. [朗为民,雷承达,张蕾. RFID 技术安全性研究[J]. 微计算机信息,2006,**22**(17):269-271.]

2 Huang Yan-bo. Radio frequency identification technology in the field of application of Intelligent Transportation Analysis [J]. International Intelligent Transportation, 2005, **1**(2): 39-42. [黄艳波. 射频识别技术在智能交通领域的应用浅析[J]. 国际智能交通,2005,**1**(2):39-42.]

3 Roberts C M. Radio Frequency identification (RFID) [J]. Computer & Security, 2006, **25**(1): 18-26.

4 Duan Gang. Encryption and Decryption (Second Edition) [M]. Beijing: Publishing House of Electronics Industry, 2003: 80-87. [段纲. 加密与解密(第二版)[M]. 北京:电子工业出版社,2003:80-87.]

5 Daemen J, Rijmen V. The Design of Rijndael: AES-The Advanced Encryption Standard[M]. Berlin: Springer, 2002: 5-10.

6 William S. Cryptography and Network Security and Principles and Practices(Fourth Edition) [M]. Translated by Meng Qing-shu, Wang Li-na, Fu Ji-ming, *et al*. Beijing: Publishing House of Electronics Industry, 2006: 47-54. [Willian S 著. 密码编码学与网络安全——原理与实践(第四版)[M]. 孟庆树,王丽娜,傅建明等(译). 北京:电子工业出版社,2006:47-54.]

7 Rivest R L. The RC5 Encryption Algorithm [A]. In: Proceedings of the Second International Workshop on Fast Software Encryption [C], Berlin, Germany: Springer, 1995: 86-96.