# AFC 系统中非接触式 IC 卡数据安全的研究与探讨

叶 飞,徐骏善
(南京理工大学 机械工程学院,江苏 南京 210094)

摘 要:针对 AFC 系统中非接触式 IC 卡存储数据和传输数据所受到的安全风险进行详细分析。从认证、加密、完整性三个方面对非接触式 IC 卡数据安全阐述了解决方案,并提出了部分实现。

关键词:非接触式 IC 卡;安全风险
中图分类号:TP315 文献标识码:A 文章编号:1674-7720(2011)15-0081-03

# Research and discussion of the data security in contactless IC card on AFC system

Ye Fei, Xu Junshan
(School of Mechnical Engineering, Nanjing University of Science & Technology, Nanjing 210094, China)

Abstract: The security risks to the storage and transmission of data in contactless IC card on AFC system was analyzed in detail. Expatiated solutions to the data security in contactless IC card from three aspects: authentication, encryption, integrality, and presented a part of realization.

Key words: contactless IC card; security risks

随着整个社会信息化进程的不断发展,尤其是国家“三金工程”的启动和发展,IC 卡在我国的应用范围正不断扩大。与此同时,针对 IC 卡及其系统的各种攻击性犯罪现象随时可能出现,这就使得 IC 卡数据加密的研究和实现处于十分重要的地位[1]。

IC 卡的安全级别分为:非加密存储卡、逻辑加密存储卡、CPU 卡。非加密存储卡不需要对其进行密码核对就可以进行读写操作,其安全性最差;逻辑加密存储卡需要先通过装置(一般为读卡器)将密码送入卡中,IC 卡核对密码正确后,输出正确的应答信号,才能进行下一步的操作,这样可以防止对卡中信息的随意阅读和改写,其安全性远远高于非加密存储卡;CPU 卡因其具有微处理器,具有更高的计算能力和和编程能力,故其安全级别比逻辑加密存储卡更高。

在地铁 AFC 系统中,国内大部分都采用了逻辑加密存储卡,如南京地铁目前单程票都采用了 MIFARE 的 Ultralight Token,而储值票(方卡)则采用了 Mifare Desfire 和 Mifare Standard,这几种卡都是逻辑加密存储卡。事实上,非加密存储卡因其较差的安全性已经在很大程度上退出了市场。

## 1 IC 卡面临的安全问题

### 1.1 安全类型缺陷

由于成本所限,IC 卡本身很难保证足够的安全,非法用户可以使用合法的读卡器或者自构一个读卡器,直接与 IC 卡进行通信,从而很容易地获取 IC 卡内的所存数据,使 IC 卡面临数据被改写的风险。而 IC 卡的数据通信链路是无线通信连接,与有线连接不一样,无线传输的信号本身是开放的,这就给非法用户的侦听带来了方便。

在读卡器中,除了中间件被用来完成数据的遴选、时间过滤和管理之外,读卡器只提供用户业务接口,但不提供能够让用户自行提升安全性能的接口。

### 1.2 AFC 系统中 IC 卡的安全问题

(1)车票安全:防止伪造、克隆、篡改、泄密、偷盗;

(2)设备安全:防止车票被偷盗后进行加值或复制,防止业务程序被攻击改变,防止重要参数及数据被改变;

(3)数据安全:防止篡改、窃取、丢失、抵赖;

(4)系统安全:防止攻击、破坏,泄露重要信息。

对于 IC 卡单程票,经过半自动售票机、自动售票机等环节发售到乘客手中,到出站闸机再进行回收。在整

个使用过程中,IC 卡处于两种状态:(1)在系统运营人员管理中,包括单程票的采购、初始化、发售、回收、循环运输等环节。(2)在乘客手中,从购买单程票到出站之间,对于 IC 卡储值票,经过半自动售票机、自动售票机等设备发售到乘客手中后,将一直在乘客手中重复使用,直至被收回。两种情况中,IC 卡在乘客手中时有更大的不安全风险。但是整体而言,单程票处在安全范围内比例要比储值票大,尤其是储值票,由于其储值金额可能较大,所以被攻击的可能性更大。

## 2 密码学概述

密码学通常被定义为在通信过程中进行解密和加密的过程和技巧。

密码技术可用于解决以下三大领域内的安全问题[2]:

(1)认证。用于可靠的确定某人或某物的身份,防止有人冒充合法用户或防止设备冒充合法资源。

(2)加密。对数据进行编码以防搭线窃听的过程。加密所提供的保护也称为机密性业务,提供该业务用以保护数据安全,不被非法者偷听。

(3)完整性。保证数据没有经过篡改,需要确认所收到的消息正是所发送的消息。

本文中涉及到传输数据的安全和存储数据的安全两个方面。其中传输数据的安全主要包括数据的机密性、完整性、可获取性和真实性。数据的机密性、完整性和可获取性是通过对数据的加解密来实现的。数据的真实性是通过相互认证技术实现的。存储数据的安全是指数据的持久性,是通过存储区域的访问条件控制和冗余存储实现的。

## 3 地铁非接触式 IC 卡的加密措施

### 3.1 认证

在对 IC 卡进行读写操作之前,必须对 IC 卡的密码进行认证。如果认证通过,才允许进行下一步操作。

非接触式 IC 卡的密码认证分为五个步骤,其过程如图 1 所示。

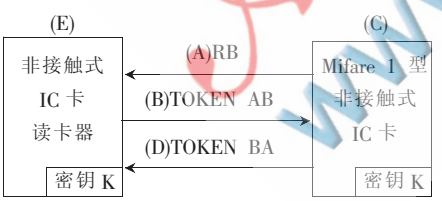


图 1 非接触式 IC 卡的密码认证

(A)由 IC 卡向读卡器发送一个随机数据 RB。

(B)读卡器收到 RB 后,向 IC 卡发送一个令牌数据 TOKEN AB=$E_K$(RB||RA||ID||T1),其中 RA 是读卡器发出的一个随机数,ID 是 IC 卡的物理唯一序列号,T1 是附加的时间戳数据。$E_K$ 表示一种加密算法,如 ASH-1 算法。

(C)IC 卡收到 TOKEN AB 后,对 TOKEN AB 的加密部分进行解密,并校验第一次由(A)中的 IC 卡发出的随机数 RB 是否与(B)中接收到的 TOKEN AB 中的 RB 相一致。

(D)如果(C)环节校验结果正确,则 IC 卡向读卡器发送令牌 TOKEN BA=$E_K$(RA||RB||T2)给读卡器。

(E)读卡器收到令牌 TOKEN BA 后,将对令牌 TOKEN BA 中的 RB(随机数)进行解密;并检验由(B)中读卡器发出的随机数 RA 是否与(D)中接收到的 TOKEN BA 中的 RA 一致。

地铁 IC 卡共有 16 个分区,每个分区都分别有自己的密码,互不干涉。因此即使通过了一个分区的的密码认证,也不能对其他的分区进行读写操作。如果想对其他分区进行操作,必须按照该分区密码重新完成上述的认证过程。每个分区都可独立地作为某一种应用,这也是 IC 卡一卡多用的原理。

如果上述的每一个环节都能正确通过验证,则整个认证过程将成功。认证过程中的任何一个环节出错,则整个认证过程终止,认证过程必须重新开始。如果事先不知道 IC 卡的密码,全部搜索需要很长时间,随机地给出一个密码而打开 IC 卡的一个分区的可能性几乎没有。

### 3.2 消息加密

目前使用较广泛的密码算法主要有对称密钥算法 DES (Data Encryption Standard)、IDEA (International Data Encryption Algorithm) 和公共密钥算法 RSA (由 Rivest, Shamir, Adleman 三人于 1978 年提出),DSA (Digital Signature Algorithm)等。

#### 3.2.1 南京地铁 2 号线采用了 3DES 算法

DES 算法产生于 20 世纪 70 年代,是传统的分组密码代码学的代表,其运算速度较快,但其密钥太短(56 bit),通过穷举法即可将其攻破。因此出现了改进的 DES 算法,即 3DES 算法[3]。3DES 算法加密时对原始明文进行三次 DES 处理,采用 K1、K2、K3 三个不同密钥(长度均为 8 B),如图 2 所示。解密时对密文按相反的顺序,还原成原始明文。为了减少系统在生产和管理密钥的开销,一般将 K1、K3 设为相同值,但 K1、K2 绝不能相同,否则三重 DES 就失去了意义。3DES 虽然降低了一定的运算速度,但是密钥长度是原来的两倍,安全性能得到了极大提高,迄今为止尚未被攻破,已成为一种国际公认的加密标准。

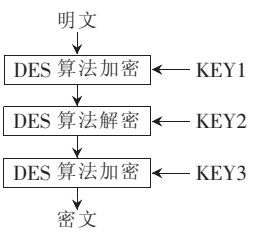


图 2 3DES 加密过程

其加密代码如图 3 所示。

#### 3.2.2 SHA-1 与 MD5 的性能比较

在南京地铁上,KEY 的产生采用了 SHA-1 安全算法,SHA-1 算法与 MD5 的算法类似,所以它们的性质极为相似。下面是 SHA-1 和 MD5 性能之间的比较。

(1)抗穷举攻击的能力:SHA1 抗穷举攻击的能力比

```
///   <summary>
///   使用给定密钥加密
///   </summary>
///   <param   name="original">明文</param>
///   <param   name="key">密钥</param>
///   <returns>密文</returns>
public static byte[] Encrypt(byte[] original, byte[] key)
{
    TripleDESCryptoServiceProvider des =
        new TripleDESCryptoServiceProvider();
    des.Key = MakeSHA1(key);
    des.Mode = CipherMode.ECB;

    return des.CreateEncryptor().TransformFinalBlock(
        original, 0, original.Length);
}
```

图 3 3DES 加密实现

MD5 强。

用穷举攻击方法产生具有给定散列值的消息:MD5 需要的代价为 2 128 数量级;SHA-1 需要的代价为 2 160 数量级。

用穷举攻击方法产生两个具有相同散列值的消息:MD5 需要的代价为 264 数量级;SHA-1 需要的代价为 280 数量级。

(2) 抗密码分析的能力:MD5 算法抗密码分析的能力较弱;SHA-1 算法抗密码分析的能力较 MD5 强。

(3)速度:SHA-1 执行的速度比 MD5 的速度慢得多。

(4) 简捷性:SHA-1 和 MD5 两种算法都易于描述和实现,不需要使用大的程序和置换表。

(5) 数据的存储方式:MD5 使用 little-endian 方式;SHA-1 使用 big-endian 方式,这两种方式没有本质的差异。

SHA-1 的实现代码如图 4 所示。

```
///   <summary>
///   生成SHA1摘要
///   </summary>
///   <param   name="original">数据源</param>
///   <returns>摘要</returns>
public static byte[] MakeSHA1(byte[] original)
{
    SHA1CryptoServiceProvider sha1 =
        new SHA1CryptoServiceProvider();
    byte[] keyhash = sha1.ComputeHash(original);
    sha1 = null;
    return keyhash;
}
```

图 4 SHA-1 实现代码

### 3.3 完整性

在通信过程中,由于受到人为或环境因素的影响,导致读写数据失败,数据不完整。

为了确保通信数据的完整性,可以采取数据校验措施,如奇偶校验和 CRC 校验等。特别是读写器与 PC 机之间的 RS-232 或 RS-485 串行通信,校验措施是十分必要的。通信的速度越高、距离越远,校验的必要性也就很高。

CRC(Cyclic Redundancy Check)码,即循环冗余校验码。由于其编码和解码方法简单,因而在 IC 卡的数据通信中广泛应用[4]。

在数据通信中应用 CRC 码的目的是校验数据传送是否正确。与奇偶校验方法相比,CRC 码校验的检错能力更强。因为奇偶校验仅采用了一位二进制作为校验码,如果传送的数据中恰好有两个位(或偶数个位)同时出错就不会被发现。CRC 码采用了 $r$ 位,可靠性大为提高。

利用 CRC 码进行数据传送校验的基本原理是:在发送端,根据要发送的 $k$ 位二进制码序列,以一定的规则产生一个用于校验的 $r$ 位校验码(即 CRC 码),使其附在原始数据后边,构成一个新的二进制序列(共 $k+r$ 位),然后一起发送出去。在接收端,根据数据码和 CRC 码之间所遵循的规则进行校验,以确定数据通信过程中是否出错。

其实现代码如图 5 所示。

```
public static int CalcCRC32(byte[] bytes)
{
    uint crc = 0xFFFFFFFF;
    for (int i = 0; i < bytes.Length; i++)
    {
        crc = (crcTable[(crc ^ bytes[i]) &
            0xff] ^ (crc >> 8));
    }
    crc = ~crc;
    return (int)(crc);
}
```

图 5 CRC 代码实现

CRC 校验的优点是识别错误可靠性高,只需要少量的操作就可以识别。但其缺点是其只能识别传输错误而不能校正错误。如果传输中校验到错误,只能让发送方重新发送。

本文通过对非接触 IC 卡数据安全所受到的威胁及其防护措施的分析,使 AFC 系统能够最大程度地保障非接触式 IC 卡的数据安全,并实现了部分必要的安全算法,将可能发生的风险控制在可接受的范围之内。

参考文献

[1] 贺金鑫,李文印.IC 卡数据加密的研究和实现[J].吉林大学学报,2003(11):1-2.

[2] 赵军辉.射频识别技术与应用[M].北京:机械工业出版社,2008.

[3] 赵时旻.轨道交通自动售检票系统[M].上海:同济大学出版社,2007.

[4] 杨振野.IC 卡技术及其应用 [M]. 北京: 科学出版社, 2006.

(收稿日期:2011-03-11)

作者简介:

叶飞,男,1986 年生,硕士研究生,主要研究方向:地铁 AFC 系统的研究与开发。

徐骏善,男,1964 年生,硕士研究生,副教授,主要研究方向:计算机集成制造,企业信息化等。