校园手机一卡通系统安全性研究

岳志强[1,2] 沈记全[1]
(河南理工大学计算机科学与技术学院 焦作 454000)[1] (焦作师范高等专科学校 焦作 454000)[2]

摘 要 在校园引入手机"一卡通"业务时,需在数据安全等方面不断探索和改进方能全面提升管理效率和管理水平。对影响手机一卡通系统的不安全因素进行了分析,在系统采用的密钥系统、卡片加密机制、通讯安全性、数据存储安全性等方面进行了研究与设计。

关键词 大学校园,手机一卡通,安全

Analysis on System Safety of Campus Mobile Card

YUE Zhi-qiang[1,2] SHEN Ji-quan[1]
(School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)[1]
(Jiaozuo Teachers College, Jiaozuo 454000, China)[2]

Abstract Under introduction of mobile card business on campus, data security need to be explored and improved in order to promote management efficiency and enhance the management level. The impact of insecurity of mobile card system were analyzed, and key systems, card encryption, communication security, data storage security were researched and designed.

Keywords University Campus, Mobile card, Security

1 引言

随着2008年中国电信业的重组合并和3G牌照的发放,三大电信运营商正积极利用各自融合后的网络资源优势争夺电信市场,并不断地巩固已有的阵地和开发新的贴心增值服务,其中,在校园市场中占有重要地位的学生用户更是必争的群体。校园手机一卡通是近年来推出的一种新型的集手机卡与校园卡为一体的移动支付业务系统,以手机为纽带,促进了数字化校园的建设,丰富了数字化校园的内容,是"数字化校园"的重要组成部分和基础设施。

校园手机一卡通系统是将传统的学生卡/员工卡功能集成到具有RFID(射频识别)功能的SIM卡中。在获得了运营商的放号授权后,手机用户除了可享受通信服务以外,还可刷手机实现门禁考勤等身份认证类服务、食堂超市等小额消费类服务、信息获取发布服务以及其他手机支付消费服务。按照手机刷卡的应用划分,将其分为城际消费领域和固定消费领域(如校园、企业)。后者经常会拓展一些校园内的其他应用,例如考勤、门禁、车辆出入、图书借阅、机房上机等。

2 系统安全方案设计

"校园手机一卡通"系统是一个开放型系统,整个系统的安全保障是系统正常运行的关键因素。安全性是数字校园系统的核心部分[1-6]。无论是在设计的初期还是在建设的整个过程中,都应该把安全性放到首位。系统的安全性涉及网络的通信安全、数据库安全、个人信息、校园卡使用过程的安全等方面。

2.1 安全技术理论与算法

数据在传输时,可能会受到各种干扰或攻击。攻击者的类型可以分为两种:一种是被动的,其试图窃听传输线路获取秘密而达到非法目的;另一种是主动的,其操作传输数据并为个人利益而修改数据。对明文数据在传输前进行加密就可以有效防止主动攻击和被动攻击。加密的数据传输总是按相同的模式进行:通过使用密钥 K_1 和加密算法对传输数据(明文)进行处理,得到密文。任何对加密算法和加密密钥 K_1 不了解的攻击者无法破解密文而获得明文,即无法从密文中重现传输信息的真实内容。在接收端,使用解密密钥 K_2 和解密算法将密文恢复成明文[7,8]。

根据所使用的 K_1 和 K_2 是否相同,将密钥体制分为对称密钥体制和公钥密钥体制[9,10]。在校园一卡通系统中,最常用的是对称密钥体制。对称密钥算法又叫传统密钥算法,就是用加密数据使用的密钥可以计算出解密数据的密钥,反之亦然。在大多数对称算法中,加密解密密钥是相同的。这些算法要求发送者和接收者在安全通信之前,商定一个密钥。对称算法的安全性依赖于密钥[11-13],泄漏密钥就意味着任何人都能对消息进行加密解密。只要通信需要保密,密钥就必须保密。对称算法的加密和解密表示为:

本文受河南省基层与前沿研究项目(092300410216),河南省软科学研究项目(102400450064)资助。
岳志强(1978-),男,硕士,讲师,主要研究方向为计算机网络技术;沈记全(1969-),男,博士,教授,主要研究方向为智能网格与网格、智能信息系统、计算机控制技术、企业应用系统集成等。

$E_k(M)=C$

$D_k(C)=M$

对称算法中，使用最广泛的是 DES 算法。

(1)DES 算法

DES(Data Encryption Standard，数据加密标准)是一种单钥密码算法，又称对称密码算法。DES 算法是一个分组加密算法，以 64bit 位(8 byte)为一组对数据进行加密，其中有 8 bit 奇偶校验，有效密钥长度为 56 bit。64 位一组的明文从算法的一端输入，64 位的密文从另一端输出。

DES 算法的流程如图 1 所示。DES 算法的入口参数有 3 个：Key、Data、Mode。其中 Key 为 7 个字节共 56 位，是 DES 算法的工作密钥；Data 为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种：加密或解密，如果 Mode 为加密，则用 Key 对数据 Data 进行加密，生成 Data 的密码形式作为 DES 的输出结果；如 Mode 为解密，则用 Key 对密码形式的数据 Data 解密，还原为 Data 的明码形式作为 DES 的输出结果。在使用 DES 时，双方预先约定使用的“密码”即 Key，然后用 Key 加密数据；接收方得到密文后使用同样的 Key 解密得到原数据，这样便实现了安全性较高的数据传输。

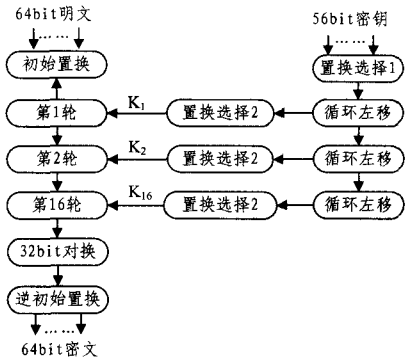

图 1　DES 加密算法流程

从图 1 的左边部分可以看出，明文的处理大致经历了 3 个阶段。第一阶段，64 比特的明文经过一个初始置换，比特重排后产生了经过置换后的输入。第二阶段是对同一个函数进行 16 次循环，这个函数本身既包含有置换又包含有替代函数。最后一个循环(第 16 个)的输出由 64 比特组成，它是输入明文和密钥的函数，这个输出的左边和右边两个部分经过交换后就得到预输出。最后一个阶段，预输出通过一个逆初始置换就形成了 64 比特的密文。

图 1 的右半部分给出了 56 比特密钥的使用方式。密钥首先通过一个置换函数，接着对于 16 个循环的每一个都通过一个循环左移操作和一个置换操作的组合产生出一个子密钥 K_i。对每一个循环来说，置换函数是相同的，但由于密钥比特的重复移位，产生的子密钥并不相同。

(2)MD3 加密算法

3DES 算法由单 DES 演化而来，3DES 算法用两个密钥对明文进行 3 次 DES 加密－解密－加密(EDE)。目前还没有针对三重 DES 的实用密码分析攻击方法。

3DES 是 DES 向 AES 过渡的加密算法，是 DES 的一个更安全的变形。它以 DES 为基本模块，通过组合分组方法设计出分组加密算法。比起最初的 DES，3DES 更为安全。

发送者先用第一个密钥对明文加密，然后用第二个密钥解密，最后用第一个密钥加密；接受者用第一个密钥解密，用第二个密钥加密，最后用第一个密钥解密。设 $E_k()$ 和 $D_k()$ 代表 DES 算法的加密和解密过程，K 代表 DES 算法使用的密钥，P 代表明文，C 代表密文，则

3DES 加密过程为：$C=E_{K_3}(D_{K_2}(E_{K_1}(P)))$

3DES 解密过程为：$P=D_{K_1}(E_{K_2}(D_{K_3}(C)))$

K_1，K_2，K_3 决定了算法的安全性，若 3 个密钥互不相同，本质上就相当于用一个长为 168 位的密钥进行加密。多年来，它在对付强力攻击时是比较安全的。

2.2　系统采用的密钥体系

在手机一卡通中，为不同的需要设计了两种不同的密钥体系：金融级(PSAM 卡加密)密钥系统、准金融级(用户自定义密码基础下的一卡一密等)密钥系统。

(1)准金融级密钥系统

准金融级加密方案中系统母卡、系统子卡、数据库存储密钥信息；在读写卡、设备通讯时验证密钥。该体系采用了“一卡一密”技术，如图 2 所示。

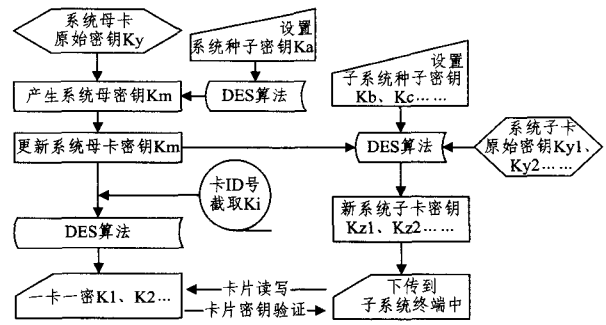

图 2　密钥系统

(2)金融级密钥系统

金融级加密方案中采用动态多级分散密钥，通过 PSAM 卡记录密钥；在读写卡、设备通讯时通过 PSAM 卡进行密钥验证。

2.3　卡片加密机制

一卡通系统采取“一卡一密，一扇区一密”的安全加密机制[14-16]。

(1)卡片密钥生成

一卡通系统采用“一卡一密”的方式对卡片中的各个扇区进行加密。所谓“一卡一密”，即由学校指派两位值得信任的人员背对背输入两个 16 位的字符串(字母或数字)作为种子 A 和种子 B，以保证种子的安全性和不可复制性，种子经过发散、3DES 加密后再经内部计算处理生成根密钥，根密钥被存放在密钥卡中，然后再载入读卡器。读卡器将用这些根密钥在访问卡片时，产生真正的各扇区应用子系统的访问密钥，即动态生成应用子系统的访问密钥。这些密钥是根据读卡器中的公式产生的，此公式利用了根密钥、扇区号和卡的唯一序列号，因此可以保证任意两张卡片的密钥都不相同，所以称为

“一卡一密”。这样，即使有一张卡片的密钥被破译，也无法得知其它卡片密钥和根密钥，系统的安全性得到了提高。

一张卡片中的16个扇区，每个扇区的密钥都是不同的，即“一扇区一密”。每一个应用系统都有一个不同的访问密钥，每张卡也有一个不同的访问密钥，这就是说，同样的应用系统的密钥，在不同卡上也是不一样的。

(2)密钥存储

根密钥存放在密钥卡中，同时还生成一张根密钥控制卡，各个扇区的应用系统所要用的根密钥可以从这些密钥卡中载入到读卡器中。读卡器对每一张卡自动给予不同密钥，以保证即使某张卡被解密，也不会影响到整个系统。

(3)卡片密钥写入

对于新购进的卡片，在发给用户使用前，必须在一卡通系统进行注册。卡片注册时，读卡器将读出卡片中的初始密钥，发卡程序将产生的根密钥、用户定义的数据、所需要的应用文件(如卡管理、钱包等)及生成的卡片访问密钥写入卡中。卡片上的数据区分为两类，即一卡通数据区和第三方子系统数据区。一卡通系统数据区采用卡片注册时生成的密钥进行读写控制；第三方子系统采用卡片的出厂密码，在建立该子系统时，更改该访问密码。

2.4 通讯安全性设计

一卡通系统中数据传输系统在进行数据传输时，为了防止数据被盗窃，保证数据传输的安全性，针对不同数据，采取对称密码算法或者非对称密码算法对数据进行加密传输。通过在校园一卡通应用系统应用服务器与数据库服务之间增加加密机或PCI加密卡等数据通讯设备，来实现身份认证、加密和报文认证，从而保障数据传输的真实性、完整性和保密性。

为保证读卡机具与中心数据库服务器和应用系统服务器之间的数据通信安全，读卡机具需在系统中进行注册，系统在发行PSAM卡时可将读卡机具名称或商户名称进行授权信息绑定，未注册的机具、商户、卡片无法使用。对于从POS机中采集的交易流水，为防止在传输过程中数据被篡改，应对所有交易流水加校验。如果系统发现交易流水被篡改，则可以重新采集所有数据，并从中过滤正常的数据。

每产生及上传一笔交易记录时，每笔记录中均采用16位CRC校验；在配置有PSAM卡的POS中，每产生及上传一笔交易记录时，每笔记录中均通过PSAM卡加密校验，然后上传至数据通讯网关，数据通讯网关上传各应用服务器时需要通过金融数据加密机TAC校验，以确保采集到的每条交易记录的完整性和合法性。

为应对数据传输过程中因网络故障而导致的数据丢失，在POS机的硬件设计中增加重复采集的功能。即在采集脱机交易流水时，指示电信指针，采集完毕后流水仍存在于POS机的数据存储器内，以便对全部或指定范围的流水记录重新采集。由于数据丢失往往是存储芯片中的数据指针丢失造成的，因此需要将数据指针保存在存储器中的多处不同位置。只要指针有一处存在，即可确保数据读取正确。

2.5 数据存储安全性设计

为了确保交易数据存储的安全，POS机内设置大容量的非易失性存储空间，以存储足够的脱机交易记录和黑名单。在内部的数据存储器空闲存储空间不多时，POS机可以自动产生提示信息。在内部的数据存储器已经存满时，POS机可以自动报警并拒绝消费，以保证已经存储的数据安全可靠。存储脱机交易流水信息时，在每条记录中增加通过加密算法生成的校验码，以识别对数据存储器的非法修改。

结束语 手机一卡通系统从分析、设计到实现都要充分体现安全理念。本文对影响手机一卡通系统的不安全因素进行了分析，详细分析了安全技术的理论基础与算法，对系统的一卡一密、通信加密、存储安全方面进行了研究与设计。

参 考 文 献

[1] 王玉. 校园一卡通系统中工作站数据安全策略的研究[D]. 沈阳：沈阳理工大学，2009

[2] 郭雷. 校园一卡通系统设计方案及安全策略[D]. 大连：大连理工大学，2009

[3] 汪汉. 校园一卡通系统的安全策略与实施[J]. 武汉理工大学学报：信息与管理工程版，2007(1)：75-78

[4] 赵建伟，刘顺波，关永魁. 校园一卡通系统的设计与安全性分析[J]. 金卡工程，2006，3(8)：27-31

[5] 张宁. 校园一卡通系统的设计和安全性研究[D]. 天津：天津大学，2007

[6] 贾晶，陈元，王丽娜. 信息系统的安全与保密[M]. 北京：清华大学出版社，2002：123-125

[7] 倪原，王丽娟，关立行. PKI公共密钥系统[J]. 微机发展，2003，(13)：72-73

[8] 卢开澄. 计算机密码学通信中的保密与安全[M]. 北京：清华大学出版社

[9] 赖溪松，韩亮，张真诚. 计算机密码学及其应用[M]. 北京：国防工业出版社，2001

[10] 张焕国，刘玉珍. 密码学引论[M]. 武汉：武汉大学出版社，2003

[11] 陈琳. DES算法的安全性及其应用[J]. 福建信息技术教育，2008，2：17-19

[12] William S. Cryptography and Network Security：Principles and Practice[M]. 北京：清华大学出版社，2002

[13] Stallings W. Cryptography and Network Security Principles and Practice[D]. Publishing House of Electronics

[14] 黄亮. 校园一卡通系统中非接触式IC卡读卡器的设计[D]. 北京：中国地质大学，2007

[15] 电感应的应答器和非接触IC卡的原理与应用[M]. 北京：电子工业出版社，2001

[16] 朱萍. 校园一卡通系统的设计与安全性研究[D]. 上海：同济大学，2009