POS 机的安全调研报告

SA20225172 郭俊勇

一、需求分析

随着科学技术的逐渐升温,人们使用的物品也越来越方便,电子银行的使用已经较为广泛,而 POS 机这种设备在生活中的应用同样重要。该设备在购物或者是出行上面为人们提供了很大的便捷。

电子支付正日益成为人们日常生活中不可或缺的组成部分。目前, POS 行业已进入稳定增长期。从POS 终端的覆盖率来看,我国人均拥有POS机数量远低于国外,市场空间广阔。中国金融POS机行业发展现状及投资前景预测分析报告数据显示,中国每万人所拥有的POS 机是13.7 台,在美国这一数字跃升至179 台,而在韩国则高达 625 台。随着电子商务的发展、的普及和人们日常的消费行为习惯,刷卡已成为不可抵挡的趋势。

伴随着POS 行业的迅猛发展， POS 安全的问题也越来越备受人们关注。如何保证系统安全问题是GPRS 无线POS机系统应用的关键。采用GPRS 无线移动数据传输方式必须有效阻止黑客入侵、防止信息安全事故、简化网络应用。安全保障主要是防止来自系统内外的有意无意的破坏。

二、POS 机工作原理

操作员通过签到，获取工作密钥(WK)，用于交易类报文的计算 MAC 和用户密码的加密。

1) 用户通过在 POS 上刷卡或者插入 IC 卡操作，同时输入交易金额和用户密码(可输可不输)。

2) POS 机通过拨号或者网络或者无线方式将相关数据组织成银行或银联标准的 8583 报文，发送给相应的后台。

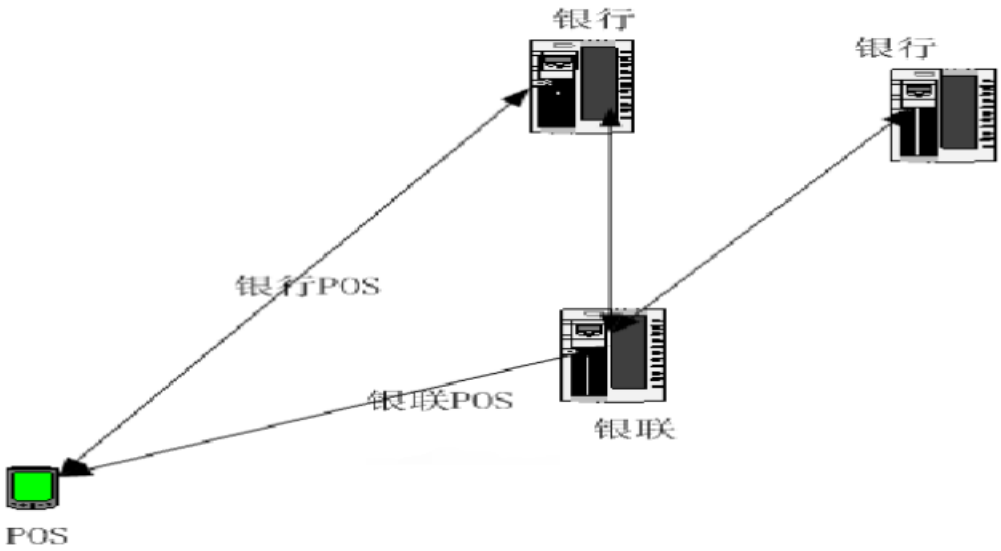
3) 如果是与银联后台连接的 POS，那么数据发给银联，

4) 银联收到报文后，根据卡号将报文另行组织并转发到卡号所对应的银行后台，

5) 银行后台数据处理后再将处理结果返回银联，

6) 银联再将数据转发回 POS，POS 根据相应的响应码进行相应的处理。

7) 如果是与银行直接相连的 POS，数据直接发给银行，后续处理相同（详见下图）



三、安全问题

- 身份认证、身份鉴别
- 网络安全
- 防止抵赖和篡改
- 交易数据的加密解密

四、安全策略

1. 身份认证——商户号和 POS 编号

移动服务器在移动 POS 机接入时，首先会检查并确认无线 POS 用户的身份，只有通过确认的 POS 机才分配以 IP 地址;交易数据送到银行 POS 主机后，再通过对该 POS 机的商户号和 POS 机编号等相关信息与数据库进行比对，进一步确保移动 POS 接入的合法性。

2. 网络安全——VPN 或者 SDH

现行的 GPRS 传输编码方式为 CS-1、CS-2，它们对传输数据都有加密保护，因此 GPRS 通道本身是安全的。GPRS 无线 POS 机系统可利用 VPN 或者 SDH 技术在移动数据公网上建立 POS 系统企业内部虚拟专用网使各地分散的无线 POS 机能安全地访问银行 POS 主机和银行内部网络资源，保证 POS 系统无线接入网络的可靠性和安全性。

3. 数字签名——SDA 和 DDA

金融 IC 卡借记/贷记应用中的 IC 卡数据认证在 IC 卡支付过程中的作用是进行脱机 IC 数据认证,包括:静态数据认证(SDA)和动态数据认证(DDA)。动态数据认证又包括:标准动态数据认证和复合动态数据认证。

静态数据认证

静态数据认证由终端验证卡片中的静态数据的数字签名来完成。其目的是确认存放在银联标准 IC 卡中关键的静态数据的合法性,可以发现在卡片个人化以后对卡内的发卡机构数据未经授权的改动,能有效地检测银联标准 IC 卡内关键静态数据的真实性。

整个银联标准 IC 卡静态数据认证的过程说明如下:

1)发卡机构的密钥管理系统产生发卡机构公/私钥对 Pi 和 Si,并将公钥 Pi 传送至根 CA;

2)根 CA 用自己的私钥 Sca 对发卡机构公钥 P;进行数字签名,产生发卡机构公钥证书,连同根 CA 公钥证书(包括 RID 及根 CA 公钥索引)返回给发卡机构密钥管理系统;

3)发卡机构密钥管理系统用发卡机构私钥 Si 对卡片静态数据进行数字签名,将签名结果、发卡机构公钥证书、RID 及根 CA 公钥索引传送至发卡系统;

4)发卡系统在个人化时将静态数字签名、发卡机构公钥证书、RID 及根 CA 公钥索引写入每一张卡片中;

5)根 CA 将其公钥 Pca，RID、根 CA 公钥索引及其它相关信息经收单机构传送至终端管理系统;

6)收单机构终端管理系统把根 CA 公钥 Pca，RID、根 CA 公钥索引及其它相关信息下载至终端;

7)银联标准 IC 卡进行交易时,脱机静态数据认证过程如下:

—终端从卡片中读取发卡机构公钥证书及签名数据,使用根 CA 公钥索引和 RID 找到根 CA 公钥 Pa ,由 Pa 恢复出发卡机构公钥 Pi 并验证其有效性;—终端使用恢复的发卡机构公钥 Pi 验证卡片签名数据的有效性。

动态数据认证

在动态数据认证(DDA)过程中,终端验证卡片上的静态数据以及卡片产生的当前动态交易数据的签名。DDA 能确认卡片上的发卡机构应用数据自卡片个人化后没有被非法篡改,更重要的是 DDA 还能确认卡片的真实性,防止卡片的非法复制和伪造。

可以是标准动态数据认证或复合动态数据认证/应用密文生成(CDA)。在动态数据认证方式下,银联标准 IC 卡将来自卡片的动态交易数据以及由动态数据认证数据对象列表(DDOL)所标识的终端数据生成一个数字签名。

银联标准 IC 卡标准动态数据认证整体过程说明如下:

1)发卡机构的密钥管理系统产生发卡机构公/私钥对 P;和 Si,并将发卡机构公钥 Pi 传送至根 CA;

2)根 CA 用自己的私钥 Sca 对发卡机构公钥 Pi 进行数字签名,产生发卡机构公钥证书,连同根 CA 公钥证书(包括 RID 及根 CA 公钥索引)返回给发卡机构密钥管理系统;

3)发卡机构密钥管理系统为每一张银联标准 IC 卡产生一对公私钥对 Sicc 和 Picc,并用发卡机构私钥 Si 对 IC 卡公钥 Picc 进行数字签名,产生 IC 卡公钥证书;

4)发卡机构密钥管理系统将发卡机构公钥证书、IC 卡公钥证书,IC 卡私钥,RID 及根 CA 公钥索引传送至发卡系统;

5)发卡系统在个人化时将发卡机构公钥证书、IC 卡公钥证书、IC 卡私钥、RID 及根 CA 公钥索引写入卡片中:

6)根 CA 将其公钥 Pca，RID、根 CA 公钥索引及其它相关信息经收单机构传送至终端管理系统:

7)收单机构终端管理系统把根 CA 公钥 Pc。RID，根 CA 公钥索引及其它相关信息下载至终端;

8)银联标准 IC 卡进行交易时,脱机静态数据认证过程如下:

终端从卡片中读取发卡机构公钥证书、IC 卡公钥证书,RID 及根 CA 公钥

索引,利用 RID 和根 CA 公钥索引定位根 CA 公钥 Pca,使用根 CA 公钥 Pca 恢复出发卡机构公钥 Pi 并验证其有效性,使用恢复的发卡机构公钥 P;恢复出 IC 卡公钥 Picc 并验证其有效性:

终端向 IC 卡发送内部认证命令请求一个动态签名:卡片对内部认证命令中的终端数据和 IC 卡交易动态数据进行连接，由 IC 卡私钥 Sicc 对该连接数据进行数字签名并返回给终端;

终端使用 IC 卡公钥 Picc 对上一步骤的数字签名进行验证。

在复合动态数据认证/应用密文生成方式中，在第一个请求应用密文命令发出后执行。银联标准 IC 卡将来自卡片的数据包括应用密文以及来自终端的数据生成一个数据签名。

银联标准 IC 卡复合动态数据认证/应用密文生成的整体过程如下:

1)发卡机构的密钥管理系统产生发卡机构公/私钥对 P;和 Si ,并将发卡机构公钥 Pi 传送至根 CA;

2)根 CA 用自己的私钥 Sca 对发卡机构公钥 Pi 进行数字签名,产生发卡机构公钥证书,连同根 CA 公钥证书(包括 RID 及根 CA 公钥索引)返回给发卡机构密钥管理系统;

3)发卡机构密钥管理系统为每一张银联标准 IC 卡产生一对公私钥对 Sicc 和 Picc,并用发卡机构私钥 Si;对 IC 卡公钥 Picc 进行数字签名,产生 IC 卡公钥证书;

4)发卡机构密钥管理系统将发卡机构公钥证书、IC 卡公钥证书、IC 卡私钥，RID 及根 CA 公钥索引传送至发卡系统;

5)发卡系统在个人化时将发卡机构公钥证书, IC 卡公钥证书, IC 卡私钥,

RID 及根 CA 公钥索引写入卡片中；

6)根 CA 将其公钥 Pca、RID、根 CA 公钥索引及其它相关信息经收单机构传送至终端管理系统；

7)收单机构终端管理系统把根 CA 公钥 Pca、RID、根 CA 公钥索引及其它相关信息下载至终端;

8)银联标准 IC 卡进行交易时,脱机静态数据认证过程如下:

终端从卡片中读取发卡机构公钥证书、IC 卡公钥证书，RID 及根 CA 公钥索引；

终端使用 Rid 和根 CA 公钥索引定位根 CA 公钥 Pca，使用根 CA 公钥 Pca 验证发卡机构公钥证书的签名并恢复出发卡机构公钥 Pi;

终端使用发卡机构公钥 Pi 验证 IC 卡公钥证书的签名并恢复出 IC 卡公钥 Picc;

终端生成一不可预知数并与其它相关数据一并传给 IC 卡;

IC 卡使用其自身的私钥 Sicc 对收到的终端数据(包括不可预知数、交易数据)和其它 IC 卡数据(包括 TC/ARQC)最数字签名并发送给终端;

终端使用 IC 卡公钥 Picc 验证 IC 卡传递的签名数据。

“所见即所签”的数字签名的功能的系统处理流程如下:

1)设置卡片支持静态数据认证(SDA)和动态数据(DDA)功能;

2)发卡行将该应用下将动态数据认证数据对象列表(DDOL)设置为“终端商户名称，应用主账号(PAN)，授权金额”，或者设置为“终端商户名称，应用主账号(PAN)，授权金额、不可预知数(随机数”以增强安全性;

3)在网银交易时，由主机(可能为 PC。手机、平板电脑等)传入“收款人名

称，收款人账号、交易金额"等信息到 POS 中。POS 将这些信息在显示屏上显示，供用户对交易进行确认；

4)如果用户已经对交易进行确认，则 POS 内部将收款人名称设置到终端商户名称域，将收款人账号设置到应用主账号域，将交易金额设置到授权金额域以及可选存在的不可预知数(随机数)；

5)POS 可选择执行"取交易选项命令(GPO)",来改变卡片内部参与签名的动态数据,以达到增加安全性的目的;

(步骤 5 为可选步骤)

6)调用动态数据认证(DDA)命令：

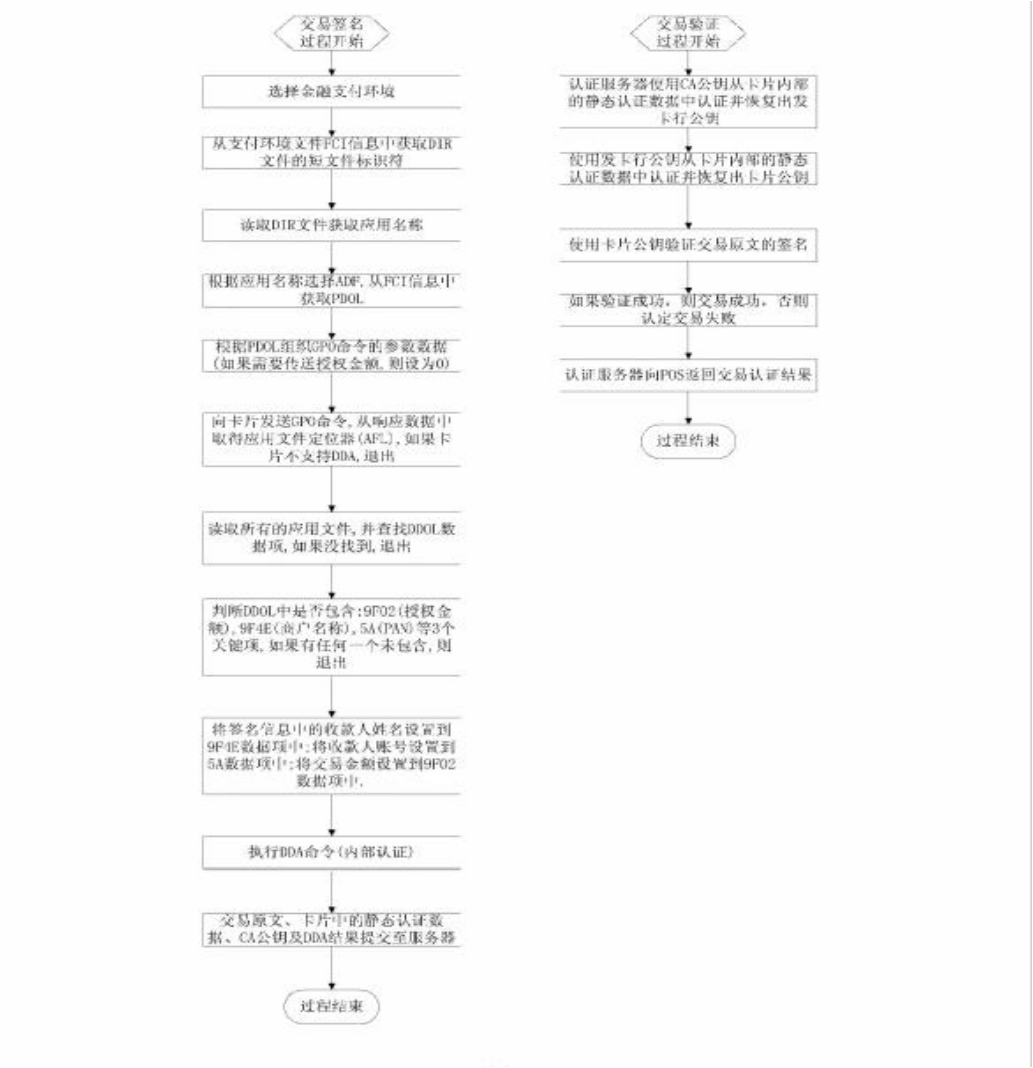
7)卡片内部执行动态数据认证过程，返回动态数据认证结果(即交易数据的签名结果；

8)P0S 获取卡片内部的应用交易序列号(ATC),连同卡片内部的静态认证数据一起返回给服务器;

9)服务器使用 CA 公钥从卡片内部的静态认证数据中恢复出卡片公钥；

10)服务器验证卡片的合法性,并使用卡片公钥验证交易数据的签名结果。如果验证成功,则认为交易有效,否则无效。

流程图：



4. 交易数据的加解密——ISO8583 和 3DES

无线 POS 机交易数据包与无线 POS 的交易数据包格式和加密方式一样都使用 ISO8583 模式传送交易数据，同样在应用层进行了数据加密保护和 MAC 鉴别以及完整性控制，对敏感数据如用户账号、密码等都采用了国际标准加密算法 3DES 进行加密保护，以确保无线 POS 系统交易数据的安全。

3DES，也称为 3DESede 或 TripleDES，是三重数据加密算法，相当于是对每个数据库应用三次 DES 的对称加密算法。由于 DES 密码长度容易被暴力破解，所以 3DES 算法通过对 DES 算法进行改进，增加 DES 的密钥长度来

避免类似的攻击，针对每个数据块进行三次 DES 加密；因此，3DES 加密算法并非什么新的加密算法，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。3DES 是 DES 向 AES 过渡的加密算法，它使用 2 个或者 3 个 56 位的密钥对数据进行三次加密。相比 DES，3DES 因密钥长度变长，安全性有所提高，但其处理速度不高。因此又出现了 AES 加密算法，AES 较于 3DES 速度更快、安全性更高。

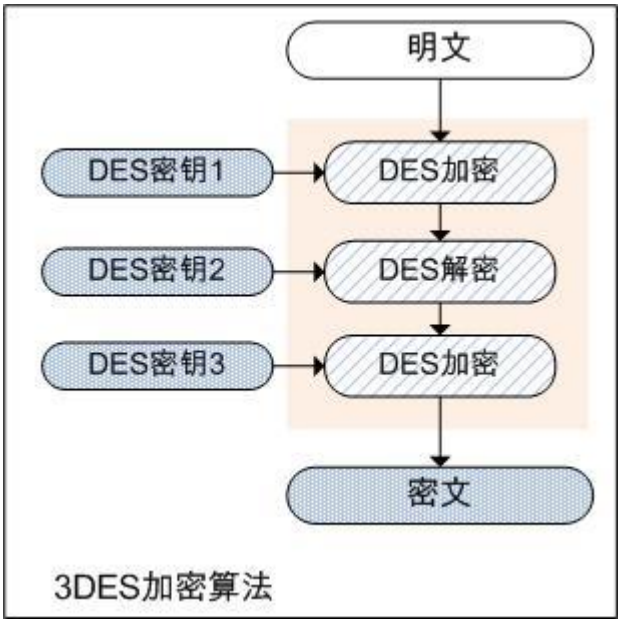
该算法的加解密过程分别是对明文/密文数据进行三次 DES 加密或解密，得到相应的密文或明文。

假设 EK（）和 DK（）分别表示 DES 的加密和解密函数，P 表示明文，C 表示密文，那么加解密的公式如下：

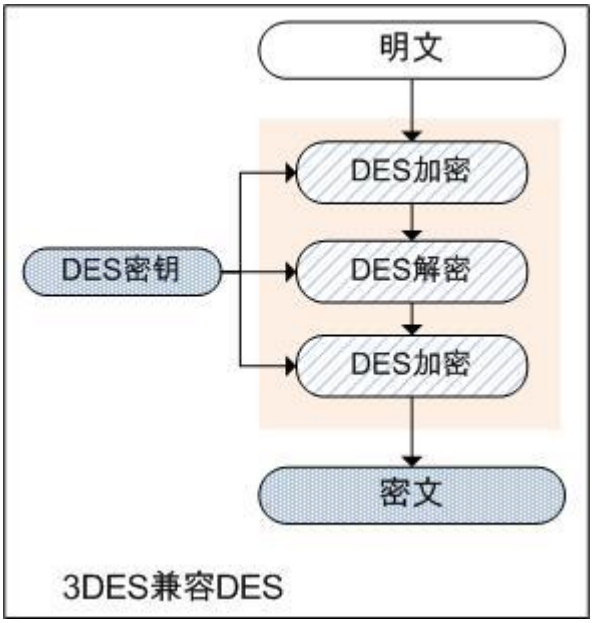
加密：C = EK3（ DK2（ EK1（P））），即对明文数据进行，加密 --> 解密 --> 加密的过程，最后得到密文数据；

解密：P = DK1（ EK2（ DK3（C））），即对密文数据进行，解密 --> 加密 --> 解密的过程，最后得到明文数据；

其中：K1 表示 3DES 中第一个 8 字节密钥，K2 表示第二个 8 字节密钥，K3 表示第三个 8 字节密钥，K1、K2、K3 决定了算法的安全性，若三个密钥互不相同，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。若数据对安全性要求不那么高，K1 可以等于 K3。在这种情况下，密钥的有效长度为 112 位，即 K1 对应 KL（左 8 字节），K2 对应 KR（右 8 字节），K3 对应 KL（左 8 字节）。



当三重密钥均相同时，前两步相互抵消，相当于仅实现了一次加密，因此可实现对普通 DES 加密算法的兼容。



五、参考文献

- 实现数字签名的方法以及用于实现数字签名的 POS 终端　周钰，严翔翔