EMV96 的潜在缺陷和改进意见

沈 炜, 陈 纯
(1. 浙江大学计算机系, 浙江杭州 310027; 2. 浙江大学信雅达计算机信息安全研究中心, 浙江杭州 310027)

摘 要: EMV96 是 Europay、MasterCard、Visa 提出的目前具有代表性的 IC 卡交易规范. 相当多的 IC 卡交易系统和规范都建立 EMV96 的基础之上. 本文系统地分析了 EMV96 的交易协议中的安全机制, 得出 EMV96 用以实现应用的一些重要安全性假设; 进一步分析表明: EMV96 的一些假设使得 EMV96 不能很好地满足交易的四个条件, 在不改变交易流程的前提下, 针对 EMV96 的潜在缺陷, 提出相应的改进意见.

关键词: EMV96; IC 卡; 支付协议
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2002) 05-0731-03

Some Potential Defects in EMV96 and Improvement Advice

SHEN Wei, CHEN Chun
(1. Department of Computer, Zhejiang University, Hangzhou, Zhejiang 310027, China;
2. Computer Information Security Center of Xinyada, Zhejiang University, Hangzhou, Zhejiang 310027, China)

Abstract: EMV96 is a representative IC card payment specification presented by Europay, MasterCard and Visa. Many IC card payment schemes are implemented based on it. In this paper, we analyze the security mechanism of payment protocols of EMV96 and put forward some assumptions based on which EMV96 sets up its payment application. Further analysis shows that EMV96 can't satisfy secure payment based on those assumptions. Finally, we present our improvement advice without modifying the flow of application.

Key words: EMV96; IC card; payment protocol

1 引言

EMV96[1] 是 Europay、MasterCard 和 Visa 提出的目前具有代表性的 IC 卡交易规范, 整个规范分为卡、终端和应用三大部分, 对物理设备、传输协议、交易流程都作了极为详细的分析和规定, 形成一个相当严密、完整的结构体系. 目前许多 IC 卡支付系统都使用 EMV96 作为交易规范. 中国人民银行也在 EMV96 的基础上结合国内的实际情况制定了5中国金融集成电路(IC)卡规范5[2].

本文系统地分析了 EMV96 在交易中所使用的通讯协议的安全机制, 得出作为 EMV96 交易协议安全性基础的一些重要假设. 进一步分析表明: 一些假设使得 EMV96 不能很好地满足交易所必须满足的四个条件, 因而存在安全上的弱点. 这样的弱点会使交易中的支付和授权凭证作为防抵赖证据而言是弱的, 同时对内部攻击的防御也是弱的. 我们提出适当修改传输中的数据内容, 使得支付和授权凭证带有提供者的特征信息, 从而增强 EMV96 的安全性.

2 一些约定与记号

X_C: X 的数字证书, 包含 X 的公钥和证书签发者对该公钥的签名;

P_X, S_X: X 的公钥和私钥;

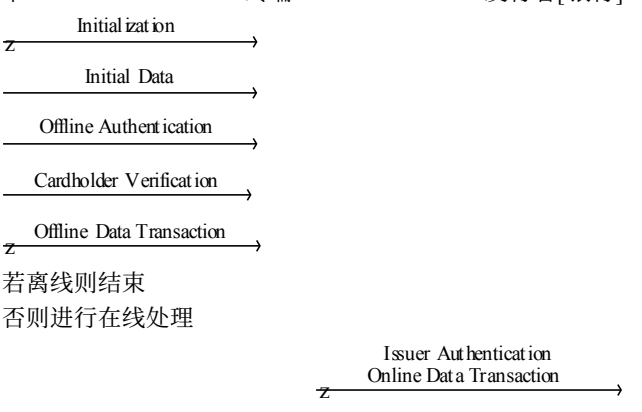
$Sign_k(DATA)$, $Recover_k(DATA)$: 使用密钥 k 对数据 DATA 进行签名和对被签名 DATA 数据进行恢复, EMV96 使用 RSA 作为签名算法, $Sign_k(\ )$ 和 $Recover_k(\ )$ 成立关系: $Recover_{P_X}(Sign_{S_X}(DATA)) = Recover_{S_X}(Sign_{P_X}(DATA)) = DATA$;

Hash(DATA): 对 DATA 求 Hash 值, EMV96 使用 SHA-1 作为 Hash 算法;

$MAC_k(DATA)$: 使用密钥 k 求 DATA 的消息认证码(MAC), EMV96 使用 DES 或 Triple-DES 作为加密和 MAC 算法, 所使用的密钥 k 都从一个由 IC 卡和发行者共享的主密钥 K_M 动态生成.

3 EMV96 的交易流程

EMV96 给出的一个典型的交易过程如下所示:



其中 Initial Data 包含 IC_C、I_C 和其它交易相关数据等.

离线认证分为静态认证和动态认证, 如下所示.

静态认证:

收稿日期: 2001-06-04; 修回日期: 2002-01-04

卡 终端

$Sign_{S_{CA}}(P_I + Hash(P_I))$
$Sign_{S_I}(CARD\_DATA + Hash(CARD\_DATA))$ →

$Recover_{P_{CA}}(Sign_{S_{CA}}(P_I + Hash(P_I)))$
$= P_I + Hash(P_I)$
校验 $Hash(P_I)$
$Recover_{P_I}(Sign_{S_I}(CARD\_DATA + Hash(CARD\_DATA)))$
$= CARD\_DATA + Hash(CARD\_DATA)$
校验 $Hash(CARD\_DATA)$

其中 $Sign_{S_{CA}}(P_I + Hash(P_I))$ 为 CA(Certification Authority)对 P_I 的签名,存在于 I_C 中; $Sign_{S_I}(CARD\_DATA + Hash(CARD\_DATA))$ 为卡个性化时发行者使用签发的关键数据.

动态认证:

卡 终端

$Sign_{S_{CA}}(P_I + Hash(P_I))$
$Sign_{S_I}(P_{IC} + Hash(P_{IC}))$ →

$Recover_{P_{CA}}(Sign_{S_{CA}}(P_I + Hash(P_I))) = P_I + Hash(P_I)$
校验 $Hash(P_I)$
$Recover_{P_I}(Sign_{S_I}(P_{IC} + Hash(P_{IC}))) = P_{IC} + Hash(P_{IC})$
校验 $Hash(P_{IC})$

INTERNAL AUTHENTICATE(DATA) →

$Sign_{S_{IC}}(DATA + Hash(DATA))$ →

$Recover_{P_{IC}}(Sign_{S_{IC}}(DATA + Hash(DATA))) = DATA + Hash(DATA)$
校验 $Hash(DATA)$

其中 $Sign_{S_I}(P_{IC} + Hash(P_{IC}))$ 为发行者对 P_{IC} 的签名,存在于 IC_C 中,DATA 为动态认证数据.

持卡者认证分为离线认证和在线认证,都通过校验 PIN 来确定持卡者身份.

持卡者认证(离线):

卡 终端

GET DATA →
PIN Try Count →

若 PIN Try Count = 0 则中止
否则进行 PIN 输入操作

VERIFY $Recover_{P_{IC}}(PIN)$ →

$Sign_{S_{IC}}(Recover_{P_{IC}}(PIN)) = PIN$
校验 PIN
Result (OK or FAIL) →

持卡者认证(在线):

终端 发行者[银行]

PIN 输入操作
PIN →
校验(PIN)
Result = OK or FAIL →

离线和在线数据处理如下进行:

离线数据处理:

卡 终端

GENERATE AC(TD) →
TC or AAC →

GENERATE AC: Generate Application Cryptogram 命令,TD 为其参数;TD: Transaction Data,包含时戳和终端标识 TERM_ID;TC: Transaction Certificate,由标志信息和 $MAC_k(TD)$ 组成,表示接受 TD;AAC: Application Authentication Cryptogram,表示拒绝接受 TD.

在线认证及数据处理:

卡 终端 发行者[银行]

GENERATE AC(TD) →
ARQC →
ARQC + TD →
IAD →
GENERATE AC(IAD, TD) →
TC or AAC →

ARQC: Authorization Request Cryptogram,表示对 TD 的授权申请,

由标志信息和 MAC_k(TD)组成; IAD: Issuer Authentication Data, 对 ARQC 的授权结果, 由标志信息和 MAC_k(TD, I. C)组成; TC: 由标志信息和 MAC_k(IAD, TD)组成.

4　弱点及改进建议

我们从 EMV96 中分析得出若干重要安全性假设, 列举如下: (1)信任假设: 发行者是可信的; 终端信任发行者; 终端对卡和发行者来说是可信的. (2)通讯安全假设: 卡与终端之间的通讯是安全的; 发行者与终端之间的通讯是安全的; 发行者相信终端的写卡操作是正确的. (3)交易连续性假设: 整个交易过程是由同一张卡完成的.

从交易流程可以看出上述假设所起的作用: 由于有假设 1 和 2 的存在, 所以没有对发行者的认证, 没有对终端的认证, 终端对来自发行者的数据也没有任何的验证, 在线方式中, 终端的写卡操作也没有给发行者任何结果; 由于有假设 3 的存在, 交易过程中对卡认证结束之后, 没有任何的机制保证参与交易的卡与完成交易中的所有与卡相关操作的卡在物理上是相同的.

但一个交易应该满足以下条件: (a) 交易信息对非参与者是保密的; (b) 参与者之间依赖某种机制建立相互信任关系; (c) 参与者的行为是不可抵赖的; (d) 整个交易过程中的资金流动是可追踪的.

EMV96 对这四个条件的支持如下:

条件(a): 由 IC 卡的防篡扰特性和假设 2 保证.

条件(b): 由假设 1, 卡信任终端, 卡信任发行者, 终端信任发行者; 终端通过认证和假设(3)信任卡; 通过 PIN 检验, 卡与持卡者建立信任关系.

条件(c): 离线方式下, 卡将 TC(包含 MAC_k(TD))作为交易凭证给终端; 在线方式下, 发行者将 IAD(包含 MAC_k(TD, I. C))给终端作为交易授权, 卡将 TC(包含 MAC_k(IAD, TD))作为交易凭证给终端; 假设 1 保证终端不会抵赖.

条件(d): 资金的流动包含在 TD(内含时戳)的流动中, 各方获得的凭证标志了 TD 的流动过程.

显然, 条件(a)的支持是强的.

条件(b)的支持是弱的: 在 EMV96 中, 不存在对终端的认证, 因而也就不存在对终端所有者(一般是商家)的认证; 同时, 在线 PIN 检验中, 发行者返回的验证结果没有任何证据证明该结果是由发行者提供的.

支持条件(c)的证据是弱的: TC 中, 没有包含任何卡的特征信息; 发行者返回的 IAD 虽然包含 MAC_k(TD, I. C), 但 I. C 是公开的, 因而也没有任何发行者的特征信息.

条件(d)的保证是弱的: 由于条件(c)是弱的.

因此, 基于 EMV96 的交易系统需要提供另外的机制来弥补下面这四个最主要的问题: (1)在线 PIN 检验, 如何保证发行者验证结果的真实性; (2)写卡操作前, 如何验证发行者授权的真实性; (3)写卡操作后, 如何验证卡返回结果的真实性; (4)如何保证终端的可靠性.

由于三个假设是确定 EMV96 交易流程的基础, 因此修改这些假设势必将加入新的认证过程, 将会改变 EMV96 现有的交易应用的体系结构, 这对于 EMV96 的实现是不利的. 最好的结果是在不改变已有的交易流程的基础上提供相应的机制解决上述四个问题. 对此, 我们提出以下建议: (1)在线 PIN 检验, 发行者返回 $Sign_{S_I}$(Result); (2)在线数据处理, 发行者返回的 IAD 中的 MAC_k(TD, I. C)变为 $Sign_{S_I}$(MAC_k(TD)); (3)在线数据处理写卡操作后, 卡返回 TC 中 MAC_k(IAD, TD)变为 $Sign_{S_{IC}}$(MAC_k(IAD, TD)); (4)增加对终端的认证可以建立对终端的信任, 但这样会改变 EMV96 的体系结构, 一个折衷的方法是终端由发行者提供并拥有所有权而不是商家. 上述修改不改变交易流程, 但各关键信息带有提供者的私钥签名, 因此既可作为消息认证, 同时也是交易授权和支付凭证, 可以作为资金的流动证据, 加强了对四个条件的支持. 另外, 由于最后卡的返回值 TC 带有卡的识别特征, 因此对假设 3 也提供有力的保障.

5　结论

EMV96 使用对称加密机制建立了从卡至终端、从终端至发行者的安全信道, 在这个信道上, 进行各方认证完成交易. 因此, EMV96 的交易方式对抗非参与者的攻击是强的. 但由于用于认证的信息缺乏提供者的特征标志, 因此 EMV96 对抗内部攻击和防抵赖机制不令人乐观.

本文的建议在不修改已有的交易规范的结构和流程前提下, 适当改变传输数据的内容, 使得重要的交易信息带有提供者的私钥签名, 因此能有效地抗击内部攻击, 增强防抵赖机制, 增加了 EMV96 安全性.

参考文献:

[1] Europay, Mastercard, Visa. EMV96 integrated circuit card specification for payment systems, integrated circuit card terminal specifications for payment systems and integrated circuit card application specification for payment systems, version 3.1.1 [Z]. 1998.

[2] 中国人民银行. 中国金融集成电路(IC)卡规范, V1.0 [Z]. 1998.

作者简介:

沈　炜　男, 1973 年 7 月出生于浙江省杭州市, 1995 年获杭州师范学院数学系理学学士学位, 1998 年获杭州大学计算机系工学硕士学位, 目前在浙江大学计算机系攻读博士学位, 研究方向为网络安全和电子商务.

陈　纯　男, 1955 年 12 月出生于浙江象山, 教授, 博士生导师, 主要研究方向为计算机协同工作、电子商务、移动/嵌入式数据库、人工智能等, 已完成多项国家自然科学基金项目, 目前正主持国家计委的/面向区域经济发展的高技术产品开发系统0项目.