ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0120.5—2016

银行卡受理终端安全规范
第5部分：PIN输入设备

Security specification for bank card terminals—

Part 5: PIN entry device

2016-09-06 发布　　2016-09-06 实施

中国人民银行　发布

目　次

前　言

JR/T 0120—2016《银行卡受理终端安全规范》由以下五个部分组成：

——第1部分：销售点(POS)终端；

——第2部分：受理商户信息系统；

——第3部分：自助终端；

——第4部分：电话支付终端；

——第5部分：PIN输入设备。

本部分按照GB/T 1.1—2009 给出的规则起草。

本部分为《银行卡受理终端安全规范》的第5部分。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位：中国人民银行科技司、中国银联股份有限公司。

本部分起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国光大银行、招商银行、中国邮政储蓄银行、中国金融电子化公司、中金金融认证中心有限公司、北京银联金卡科技有限公司、银联商务有限公司、福建联迪商用设备有限公司、飞天诚信科技有限公司、无线网络安全技术国家工程实验室、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、信息产业信息安全测评中心。

本部分主要起草人：李伟、王永红、陆书春、李兴锋、杜宁、陈则栋、曲维民、汤沁莹、王禄禄、吴永强、赵哲、贾铮、周皓、王兰、杜磊、李伟（中国银联）、张志波、潘润红、邬向阳、杨倩、刘运、谭颖、严伟锋、夏庆凡、王治纲、王伯铮、于华东、李同勋、冯健诚、代伟、钱菲、李穗申、李石超、顾才泉、侯智勇、张晓琪、高志民、高强裔、李超、高峰、周诗扬、孙茂增、马哲、尚可、胡盖、张俊江、蒋利兵、郭鑫、林眺、于海涛、白艳雷、李琴、宋铮、刘健、董晶晶。

银行卡受理终端安全规范

第5部分：PIN输入设备

1 范围

本部分适用于所有受理银行卡终端完成PIN输入的设备或模块，本部分主要定义了该类设备基本的物理安全、逻辑安全以及相关安全管理要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0001 银行卡销售点（POS）终端技术规范

JR/T 0002 银行卡自动柜员机（ATM）终端技术规范

ISO 9564 银行业务 个人标识号管理与安全(Financial services Personal Identification Number(PIN) management and security)

ISO 11568 银行业 密钥管理程序(Banking-Key management)

ANSI X9.24 零售金融服务对称密钥管理（Retail Financial Services-Symmetric Key Management）

ANSI TR-31 通过对称算法密钥安全交换和密钥包规范（Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms）

3 术语和定义

JR/T 0001和JR/T 0002中界定的以及下列术语和定义适用于本文件。

3.1

终端主密钥 terminal master key（TMK）

用于加密终端工作密钥的密钥。

3.2

工作密钥 working key（WK）

PIN加密密钥、MAC计算的密钥和磁道加密密钥，也称为数据密钥。在联机更新的报文中，对工作密钥应用终端主密钥（TMK）加密，形成密文后进行传输，适用于有人值守的小区和便民点、单位办公室和无集中收银的商品批发市场的商用收单场景。

3.3

泄漏 compromise

一种对系统安全的侵害，该侵害有可能导致敏感数据被非法获得。

3.4

双重控制 dual control

通过两个以上的独立实体协同工作去保护敏感功能或信息的机制。

3.5

固件 firmware

在PIN输入设备内部与设备安全性相关所有程序代码称为固件，固件应符合本规范的安全要求。

3.6

IC卡读写器 IC card reader

用于对IC卡上的信息进行存取的设备。

3.7

数据完整性 data integrity

表明数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.8

密钥管理 key management

整个密钥生命周期中对密钥和相关参数的操作，包括生成、存储、分发、注入、使用、删除、销毁和存档等。

3.9

脱机PIN验证 offline PIN verification

持卡人身份的验证方式，该方式通过终端和IC卡的交互来比较持卡人输入的PIN与IC卡芯片内存储的PIN是否一致来验证持卡人身份。

3.10

联机PIN验证 online PIN verification

持卡人身份的验证方式，该方式将加密后的PIN值通过授权请求报文发送至发卡行，通过比较报文中PIN值与发卡行PIN值是否一致来验证持卡人身份。

3.11

逻辑安全性 logical security

设备在功能上抵御攻击的能力。

3.12

物理安全性 physical security

设备在物理构造上抵御攻击的能力。

3.13

防攻击 tamper-evident

能够提供被攻击证据的特性。

3.14

抗攻击 tamper-resistant

提供物理保护以抵御攻击的特性。

3.15

反攻击 tamper-responsive

针对已检测到的攻击自动反击以阻止攻击的特性。

3.16

攻击 tampering

对设备内部的探查或修改，或通过主动或被动的方法去探查或记录秘密数据的行为。

3.17

完整性 integrity

账户信息与交易数据未经授权不能改变的特性。即数据在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱续、重放、插入等行为的破坏和丢失的特性。

3.18

可用性 availability

处理、存储账户信息与交易数据的系统在规定条件下和规定时间内完成规定的功能的特性。可用性的测度包括：抗毁性、生存性和有效性。

3.19

敏感性 sensitivity

资源所具有的一种特征，意味着该资源的价值或重要性，包含资源的脆弱性。

3.20

知识分割 knowledge split

把消息分割成许多碎片的方法。分割后每一片所代表的信息足够小，但是把这些碎片重新组合在一起就能重现信息。

3.21

PIN输入设备 PIN entry device（PED）

输入PIN的设备机具。

3.22

加密密码键盘 encrypting PIN pad（EPP）

一种主要应用于无人值守终端（如ATM等）的PIN输入设备模块。

4 缩略语

JR/T 0120.1中界定的以及下列缩略语适用于本文件。

EPP　　加密密码键盘(Encrypting PIN Pad)
PED　　PIN输入设备(PIN Entry Device)

5　物理安全性要求

5.1　入侵检测机制

PIN输入设备应具备防攻击性机制，保证设备在被攻击后立即处于不可操作状态，并自动立即擦除设备中存放的秘密信息。这些机制可以使设备抵抗如下物理攻击手段（包括但不限于）：钻孔、激光、化学溶剂、通过外壳和通风口的探查。并且要求绕过这些机制插入PIN窃取装置或者获取敏感信息的可行方法至少需要26分（不包括对IC卡读写器的攻击）的攻击分值，其中实施攻击分至少13分。相关评分规则见附录B。

5.2　独立安全机制

设备的安全系统由至少两个以上的独立安全机制组成，设备的单个安全机制失效不会危及设备的安全。

5.3　内部访问响应

若允许访问PIN输入设备或IC卡读写器内部区域（如服务或维护等），则通过该区域插入PIN窃取装置是不可能的。设备内部设计可以保证（例如将敏感数据所在的组件由防攻击性和反攻击性机制保护）禁止直接访问PIN或者密钥等敏感数据，或设备安全机制可以在非法访问其内部区域时立即擦除敏感数据。

5.4　环境和操作条件改变的适应性

改变PIN输入设备的环境条件或操作条件不会影响其安全性(例如操作电压或环境温度超出PIN输入设备范围）。

5.5　敏感功能或信息保护

敏感功能或敏感信息只能在PIN输入设备受保护的区域内使用。对敏感信息和敏感功能进行攻击和修改至少需要26分的攻击分值（不包括对IC卡读写器的攻击），其中实施攻击分至少13分。

5.6　PIN 输入过程中可听到的音调

如果PIN输入时有声音提示，那么输入每一位PIN所发出的声音和输入其他位PIN所发出的声音应保持一致或声音随机，无法辨别。

5.7　PIN 输入过程中监控

即使在收银员或店员的协助下，通过监听PIN输入设备的声音、电磁辐射、能量消耗或其他任何可以从外部监听到的特征来探查PIN都至少需要26分的攻击分值，其中实施攻击分至少13分。

5.8　密钥识别分析

通过入侵或渗透PIN输入设备或IC卡读写器、监测PIN输入设备或IC卡读写器的辐射(包括能量波动）的方法获取在PIN输入设备或IC卡读写器中存储的任何与PIN安全相关的密钥，要求至少需要35分攻击分值，其中实施攻击分至少15分。

5.9 非 PIN 数据输入提示信息物理安全

输入非PIN数据时设备显示的提示内容应在安全模块的控制下，对非PIN数据的攻击至少需要18分攻击分值，其中实施攻击分至少9分。如果该提示内容是存储在安全模块内部，那么改变该提示内容会导致安全模块内密钥的擦除。如果该提示内容是存储在安全模块外部，那么设备安全机制要保证提示内容的完整性、正确使用和不被非法修改或使用（由厂商满足实现）。

5.10 移除检测（仅适用于 EPP）

安全组件不能擅自被拆除。如果要破坏或绕过该安全保护功能至少需要攻击分18分，其中实施攻击分至少9分。

5.11 防偷窥保护（不适用于 EPP）

PIN输入设备的设计应防止其他人对PIN输入的窥视，具体要求参考附录A。

5.12 独特外观（不适用于 EPP）

PIN输入设备或IC卡读写器应经过合理设计，以保证无法利用在零售市场上可买到的商品组件来组装PIN输入设备或IC卡读写器。例如，特有的设备外壳。

5.13 磁条读卡器（适用于任何带有集成式磁条读卡器的有人值守式 POS-PED，EPP 可选）

在攻击分值低于16分（实施攻击分8分）的条件下，通过入侵PIN输入设备安装附加物、替代或修改磁条阅读器的磁头和相关软硬件的方式，从而获取或修改磁道数据都是不可行的。

6 逻辑安全性要求

6.1 自检测试

PIN输入设备应具备自检功能，能够检查设备的固件、安全机制以及安全状态，自检在设备启动时进行并至少每天进行一次，设备每24小时内至少重新初始化内存。自检包括检查固件、针对篡改迹象的安全机制以及PED是否处于被攻破状态。一旦出现故障，PED及其功能会以安全的方式失去效用。

6.2 逻辑异常

PIN输入设备不应受异常逻辑的影响而泄露PIN的明文或其他敏感数据，这些异常逻辑包括但不限于：错误的命令序列、未知命令、错误模式下的命令和错误的参数。

6.3 固件认证

设备固件及对固件的任何改动都应经过严格的流程控制，以保证固件中不含隐藏的非法功能。

6.4 固件更新

如果PIN输入设备固件能够进行更新，那么设备应通过加密机制验证更新固件的完整性和真实性。如果未确认其完整性和真实性，那么设备应拒绝进行固件更新或清除设备中所有的密钥。

6.5 输入 PIN 区别

PIN输入设备在任何情况下都不显示或者泄漏PIN的明文。任何和PIN相关的数据应显示为无意义的字符（例如星号）或者输出无区别的信号等。同时应保证这些密码的输出只能输出至显示设备接口上，其他接口连接屏无法显示。

对于加密密码键盘，加密密码键盘从不向另外一个部件输出信息（比如，显示屏或设备控制器），从而能够对输入的PIN数字进行区分。

6.6 内存清除

PIN输入设备应严格控制敏感信息的存在时间和使用次数。设备在下面任一情况应自动清空其内部保存的敏感信息：

——交易已经完成；

——PIN输入设备等待持卡人或商户的响应超时。

6.7 敏感服务保护

设备的敏感服务用于访问敏感功能，敏感功能处理设备中如密钥、PIN和口令等敏感数据，使用设备的敏感服务应通过身份验证。进入或退出敏感服务不应泄露或改变设备中的敏感信息。

6.8 敏感服务限制

为保证设备的敏感服务不被非法使用，应对设备敏感服务的范围和使用时间进行限制，若超出服务范围和使用时间则PIN输入设备应退出敏感服务并返回到正常模式。

6.9 随机数

如果PIN输入设备产生的随机数与敏感数据有关系，则设备中的随机数产生器应经过评估，以保证其产生的随机数无法被预测。

6.10 PIN 防穷举

PIN输入设备应具有防止利用穷举探测PIN值的特性。

6.11 密钥管理

PIN输入设备中执行密钥管理技术需要符合ISO 11568和/或ANSI X9.24。有关TDES密钥组的密钥管理技术符合ANSI TR-31。

6.12 加密算法测试

PIN输入设备采用的PIN加密技术应遵循ISO 9564。

6.13 对设备中任意数据加解密

不能利用PIN输入设备内的工作密钥（WK）或密钥加密密钥（KEK）去加密或解密其他任意的数据。PIN输入设备应强制使数据密钥（指MAC密钥和磁道加密密钥），密钥加密密钥和PIN加密密钥有不同的值。

6.14 明文密钥安全

PIN输入设备的机制应保证：不允许输出私钥或密钥以及PIN的明文；不允许用（可能）已经泄密的密钥去加密其他密钥或PIN；不允许把密钥明文从高安全的组件传送至低安全的组件中去。

6.15 交易控制

输入其他交易数据的过程应和输入PIN的过程分开，以避免PIN的明文意外显示。如果其他交易数据和PIN是通过同一个键盘输入，那么输入其他交易数据和PIN时设备应有明显提示进行区别。

6.16 非PIN数据输入提示信息逻辑安全

6.16.1 改变用户界面提示攻击可能性分析

在未授权情况下，改变非PIN数据输入时显示的提示内容危及PIN安全（例如：当输出信息不加密时提示输入PIN）的攻击至少需要18分的攻击分值，其中实施攻击分至少9分（由厂商满足实现）。

6.16.2 基于加密的控制

对于具有可变显示功能的PIN输入设备，设备的显示应在安全模块控制下进行，设备的控制机制应保证不能通过改变设备的显示内容来获得明文PIN，并且提供特有效的认证机制和合适长度的密钥。在设计设备密钥管理方式或其他安全控制机制时应采用双重控制和知识分割的原则(允许第三方控制认证方法）。

6.16.3 设备多应用

如果设备支持多应用，应保证各应用间的相互独立，其中任何应用不能干扰其他应用和操作系统，包括不能修改属于其他应用的数据对象。

6.17 操作系统

设备的操作系统中只能包含设备内部操作及服务应用软件，操作系统应进行安全配置，开通尽量少的权限设置。

6.18 集成指南

供应商应提供完整详细的安全引导指南，方便集成商将安全设备集成到终端中去。

7 联机终端的安全要求

联机终端应满足以下密钥替换要求：

如果PIN输入设备能够保存多个PIN加密密钥而且能够在外部选择，那么设备安全机制应防止密钥被非法替换和使用。

8 脱机终端安全要求

8.1 防穿透保护

在要求攻击分值小于20分（实施攻击分10分）的情况下，任何渗透IC卡读写器从而附加、替换和修改IC卡读写器的软件或硬件，以获取或修改任何敏感数据的攻击都是不可行的。

注：读卡器可能包含不同保护级别的区域，例如IC卡读写器接口本身区域和退卡的区域。

8.2 IC卡读写器卡槽结构

在插入IC卡时，IC卡读写器插槽应没有空间被装入PIN窃取装置，要增大设备空间来容纳这种窃取装置也是不可行的。IC卡和其他任何外物不可能同时驻留在IC卡读卡器插槽内。

在卡插入过程中，IC卡插槽的入口处可完全处于持卡人的监控下，这样在插槽入口处的任何可疑物都可以被发觉。

8.3 IC卡读卡器构造（连线）

IC卡读写器的构造可以保证任何从IC卡读写槽到外部记录器或发射机（外部窃取装置）的连接线都可以被持卡人观察到。

8.4 PIN输入设备和IC卡读卡器间PIN传输保护

在PIN输入设备中传输时PIN的保护（至少满足下列的一条）：

——如果PIN输入设备和IC卡读写器没有集成在一起，且验证持卡人方式为加密PIN验证，那么在PIN输入设备和IC卡读写器之间传送的PIN BLOCK应通过IC卡上的加密密钥进行加密，或与ISO 9564加密要求保持一致；

——如果PIN输入设备和IC卡读写器没有集成在一起，且验证持卡人方式为明文PIN验证，那么从PIN输入设备向IC卡读写器传送的PIN BLOCK应按照ISO 9564要求进行加密；

——如果PIN输入设备和IC卡读写器集成在一起，且验证持卡人方式为加密PIN验证，那么PIN BLOCK应通过IC卡上的加密密钥进行加密；

——如果PIN输入设备和IC卡读写器集成在一起，且验证持卡人方式为明文PIN验证，那么PIN BLOCK在受保护环境（ISO 9564）中传输时不需加密。如果明文PIN在未受保护环境中从PIN输入设备传输至IC卡读写器，则PIN BLOCK应按照ISO 9564要求进行加密。

9 网络开放协议的安全要求

9.1 IP和链路层要求

为保证计算机网络相互连接通信安全，厂商应保证IP和链路层整体满足下列安全要求：

——应准确识别出系统平台中开放协议定义的所有链路层选项；

——对IP层和链路层进行受攻击脆弱性评估，以保证IP层和链路层没有受攻击弱点。通过以下方式实现：

- 根据安全文档进行评估；
- 根据公共域的信息反馈进行评估；
- 通过一些测试进行评估。

——供应商应不断更新维护安全指南，描述IP层和链路层如何被使用。安全指南提供给应用开发者、系统集成者以及终端用户如何使用的引导。安全指南应保证IP层和链路层使用的安全性；

——IP协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权形式进行更新，一旦认证不通过，应禁止更新。

9.2 IP协议要求

为保证计算机网络相互连接通信安全，IP协议应满足以下安全：

——应清楚地识别出系统平台中定义的所有IP协议项；

——对IP协议执行脆弱性评估，保证使用IP协议无明显容易受攻击的弱点。评估通过以下几种方式：

- 根据IP协议安全文档进行评估；

- 根据公共域信息反馈进行评估；
- 通过一些测试进行评估。

——供应商应维护安全指南，描述IP协议如何被使用。安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作的引导，应保证使用IP协议的安全性；

——IP协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权方式的更新，一旦认证不通过，应禁止更新。

9.3 安全协议要求

为保证计算机网络相互连接通信安全，厂商应实现满足安全协议的功能要求，如SSL/TLS，IPSec协议等，同时作为一个整体满足下列安全要求：

——应保证可以完全识别系统平台上开放协议定义的所有安全协议项；

——对安全协议进行脆弱性评估，以保证安全协议的使用不具有明显易受攻击弱点。评估采用以下方式实现：

- 根据安全协议文档进行评估；
- 根据公共域信息反馈进行评估；
- 通过一些测试进行评估。

——系统平台供应商应维护安全指南，描述安全协议如何被使用：

- 安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；
- 应保证使用安全协议的安全性；
- 安全指南应明确提出相关的安全协议是否能够作为金融应用或系统平台管理应用；
- 安全指南应明确指出安全协议相关配置是否能应用于金融应用或系统平台管理应用。

——协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权更新，一旦认证不通过，应禁止更新；

——系统平台供应商应进行密钥管理安全指南的管理和维护，描述密钥和证书应如何被使用：

- 密钥管理指南为系统平台中的内部使用者、应用开发者、系统集成者和终端使用者提供密钥管理的安全引导；
- 密钥管理安全指南要描述系统平台上所有密钥和证书的属性；
- 密钥管理安全指南保证密钥和证书使用的安全。

——安全协议应保证网络传输数据的保密性，加密机制采用适合相关算法的密钥长度，在安全模式下使用合理的密钥管理程序加密，如NIST SP800-21；

——安全协议为网络传输连接提供完整数据，采用MAC协议或数字签名实现数据完整性一致性，哈希算法采用SHA-224、SHA-256、SHA-384、SHA-512中的一种；

——安全协议对服务进行授权：

- 服务授权应使用对应相关算法合适的密钥长度；
- 系统平台能够验证接收到公钥的有效性；
- 系统平台能够验证接收到公钥的权限。

——安全协议能够监控信息反馈，并对异常进行处理；

——安全协议利用随机发生器校验NIST SP 800-22等。

9.4 IP服务要求

为保证计算机网络相互连接通信安全，厂商应实现IP服务的要求，如DNS、DHCP、HTTP、FTP等。

——应完全识别系统平台中开放协议定义的IP服务项；

——对IP服务进行脆弱性评估，以保证IP服务中不包含明显的易受攻击弱点。通过以下方式实现：

- 通过文档分析对服务安全性进行评估；
- 根据公共域信息反馈进行评估；
- 通过一些测试进行评估。

——供应商应维护安全指南，描述IP服务如何被使用：

- 安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；
- 应保证使用IP服务的安全性；
- 安全指南应明确提出相关的IP服务是否能够作为金融应用或系统平台管理应用；
- 安全指南应明确指出IP服务相关配置是否适用于金融应用或系统平台管理应用。

——IP服务的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权形式的更新，一旦认证不通过，应禁止更新；

——系统平台实现会话层管理：

- 系统平台保持对所有连接的跟踪，将活动的会话数量约束在最小必要范围值内；
- 系统平台对会话设置时间限制，保证会话开放时间限制在一定范围内。

——使用合理的安全协议保证IP服务的机密性和完整性，并实现对IP服务的密码授权和防止重复使用。

9.5 安全管理要求

——供应商应维护安全指南，对系统平台的配置管理作相关描述：

- 安全指南为系统平台提供内部使用者、应用开发者、系统集成者和终端使用者提供安全使用引导；
- 安全指南应覆盖整个系统平台，包括固件、应用软件、密钥和证书；
- 安全指南应覆盖整个系统平台的生命周期，从设计开发、出厂、交付使用及操作过程
- 安全指南应保证禁止未授权修改行为；
- 安全指南应保证任何对已通过认证系统平台做影响安全性能修改，会导致系统平台标识符改变。

——供应商推出安全维护的措施：

- 形成安全维护策略文档；
- 通过周期执行易受攻击脆弱性评估，保证及时检测易受攻击的弱点，例如报告分析、公共域信息反馈和测试；
- 应保证及时评估和分类最新发现的易受攻击弱点；
- 应保证及时建立缓解最新发现漏洞影响的机制。

——系统平台供应商对易受攻击的漏洞进行公开批露：

- 以文档形式保存相关漏洞信息；
- 保证及时公布最新发现易受攻击漏洞的信息，包括标识符、标书信息和漏洞相关的评估；
- 提供及时缓解漏洞危害的方法。

——系统平台可以被更新，供应商应维护更新机制描述，提供更新是如何实现：

- 更新机制采用恰当的、被认证的安全协议保证系统平台信息的机密性和完整性，对服务进行授权并防止重复使用。如果设备允许进行软件和配置更新，设备应采用加密授权，一旦授权不成功，则更新失败中止；
- 系统平台供应商为应用开发者、系统集成者和终端使用者提供更新最新系统平台的安全指南；
- 安全指南应覆盖固件、应用、密钥和证书的更新；

- 安全指南描述应用开发者、系统集成者和终端使用者的责任；
- 安全指南保证最新系统平台的及时安全更新。

10 集成安全要求

10.1 配置管理

任何依据该规范对设备集成到密码输入终端进行安全性评估时，应明确定义其物理和逻辑安全界定，如PIN输入和读卡器各自的功能。

10.2 PIN 输入功能集成

PIN输入功能集成安全要求：

——应保证已经通过认证的安全器件在集成到PIN输入设备时，不降低整个设备的保护级别；

——对密码输入器的密码输入区域和其周围区域进行设计或改造时，应保证不会增加密码输入器受攻击的风险。如对密码输入器的攻击至少需要攻击总分18分，其中实施攻击分9分。

10.3 终端集成

终端集成安全要求：

——密码输入终端将已认证的安全设备进行物理和逻辑集成时，应确保不引入新的攻击途径；

——密码输入终端应具有防止偷取支付卡机制（Lebanese Loop Attack黎巴嫩环攻击）；

——应保证在同一个设备中，安全器件与非安全组件之间要有比较清晰的逻辑和物理隔离；

——在应用执行过程中，显示给持卡人的动态信息和终端操作状态强制保持一致性。如果接收到来自外部设备更改持卡人动态显示信息和操作状态的命令，应保证该命令已被密码授权校验通过。对持卡人操作动态显示信息和系统操作状态之间修改的攻击，攻击总分至少18分，其中实施攻击分9分；

——PIN输入设备应保证只具有一个支付卡密码输入接口，例如一个键盘等。如果有其他可用于PIN输入接口，应限制该端口密码输入的使用，例如可采取无有效数字键、对输入的数字不可用；

——终端应具有防止未授权移除组件机制。攻击这种防止移除机制需要攻击总分18分，其中实施攻击分9分；

——供应商应对文档持续地维护更新，以保证终端集成使用者了解如何保护系统，对非法移除加以防止；

——对于嵌入式设备，应准确按照嵌入设备厂商提供的文档对系统加以保护，防止非法移除。

11 设备安全管理

11.1 生产期间的设备安全管理要求

设备在生产期间的安全管理要求：

——在设备生产过程中应采取变更控制机制，该机制可以保证当设备的任何物理或逻辑特性发生改变时，设备都应按照本规范的物理安全性要求或逻辑安全性要求进行重新评估；

——对通过评估的固件要合理地保护和存储，以防止被非法修改。对固件的保护应采用双重控制或密码验证方式进行；

——在生产过程中，用于组装PIN输入设备的组件应通过物理安全性要求的评估，并且这些组件没有被非法替换；
——设备所安装的软件在运送、存储和使用时，应遵循双重控制的原则，以防止在未授权情况下的对软件的修改或替换；
——在产品生产完成后且在出厂前，PIN输入设备和其任何组件都应存放在受保护的、进行访问控制的区域内，或将设备封装在具有防攻击特性的包装中，以防止非法接触设备或其组件；
——如果PIN输入设备在装载密钥时要对设备进行验证，且验证要素为生产过程中装入设备的秘密信息，那么该秘密信息的设置应对每台PIN输入设备唯一，任何人都不可知和不可预测该信息，并且该秘密信息在装入PIN输入设备时应在双重控制之下，以保证在装入期间不会泄露。

11.2 初始密钥注入前的设备安全管理要求

设备在初始密钥注入前的安全管理要求：
——PIN输入设备从生产厂家至初始密钥注入方的运送途中的存储过程都要受到控制和审计，以便及时确定设备在途中的地点；
——应设计合理的流程将对设备的安全责任从厂家递交给设备初始密钥注入方；
——在设备从生产厂家向初始密钥注入方运送的过程中，应该具备下列条件：

- 在具有防攻击特性的包装中存放并运送设备；
- 如果设备在存放和运送时存有秘密信息，那么当试图对设备做任何物理或功能上的改变时，该秘密信息应立即自动销毁。初始密钥注入方能验证该秘密信息完整性，但是未授权的个人无法获取该秘密信息。

附 录 A
（规范性附录）
防窥挡板的设计标准

A.1 满足PIN输入设备（密码键盘）防窥设计的挡板设计标准

A.1.1 设计样例

银行卡受理终端安全要求密码键盘设计，应具有以下防窥挡板的设计要求标准（如图 A.1 所示）。

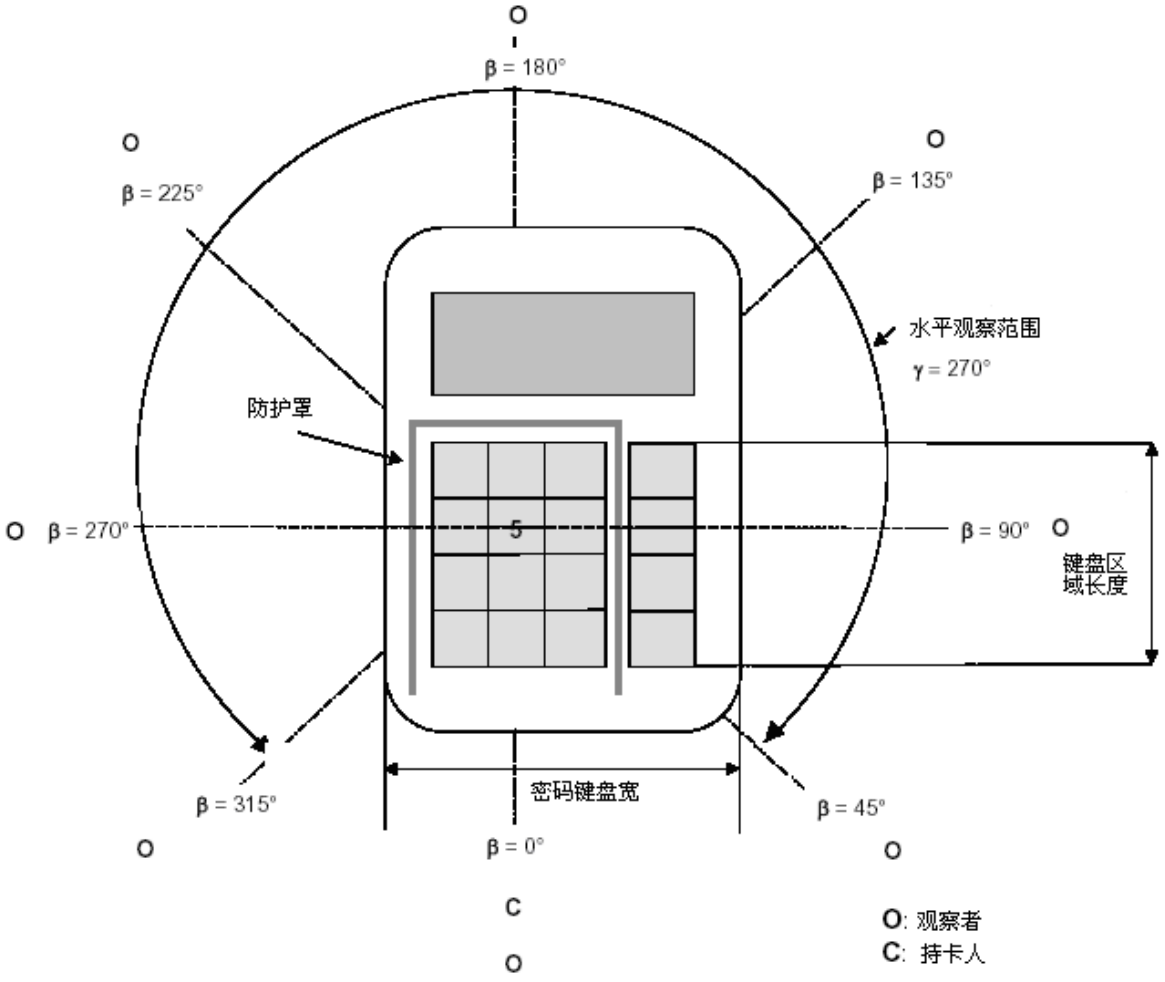

图 A.1 含有挡板设计的密码键盘样品俯视图

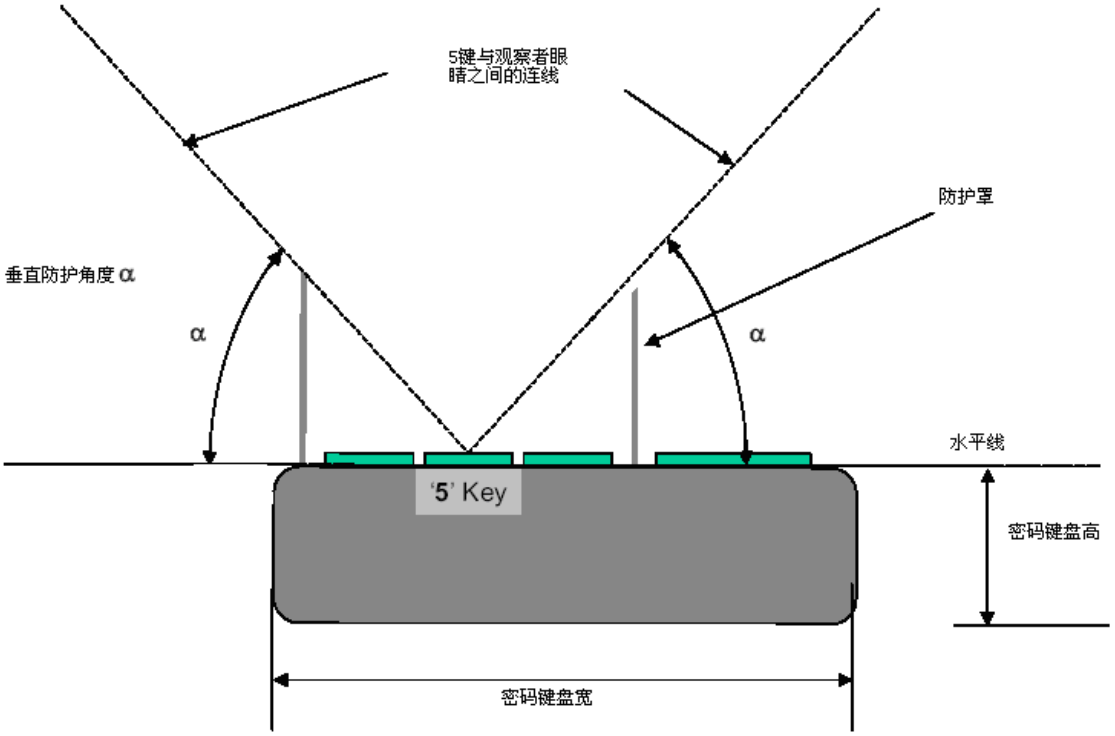

图 A.2 密码键盘样品正视图

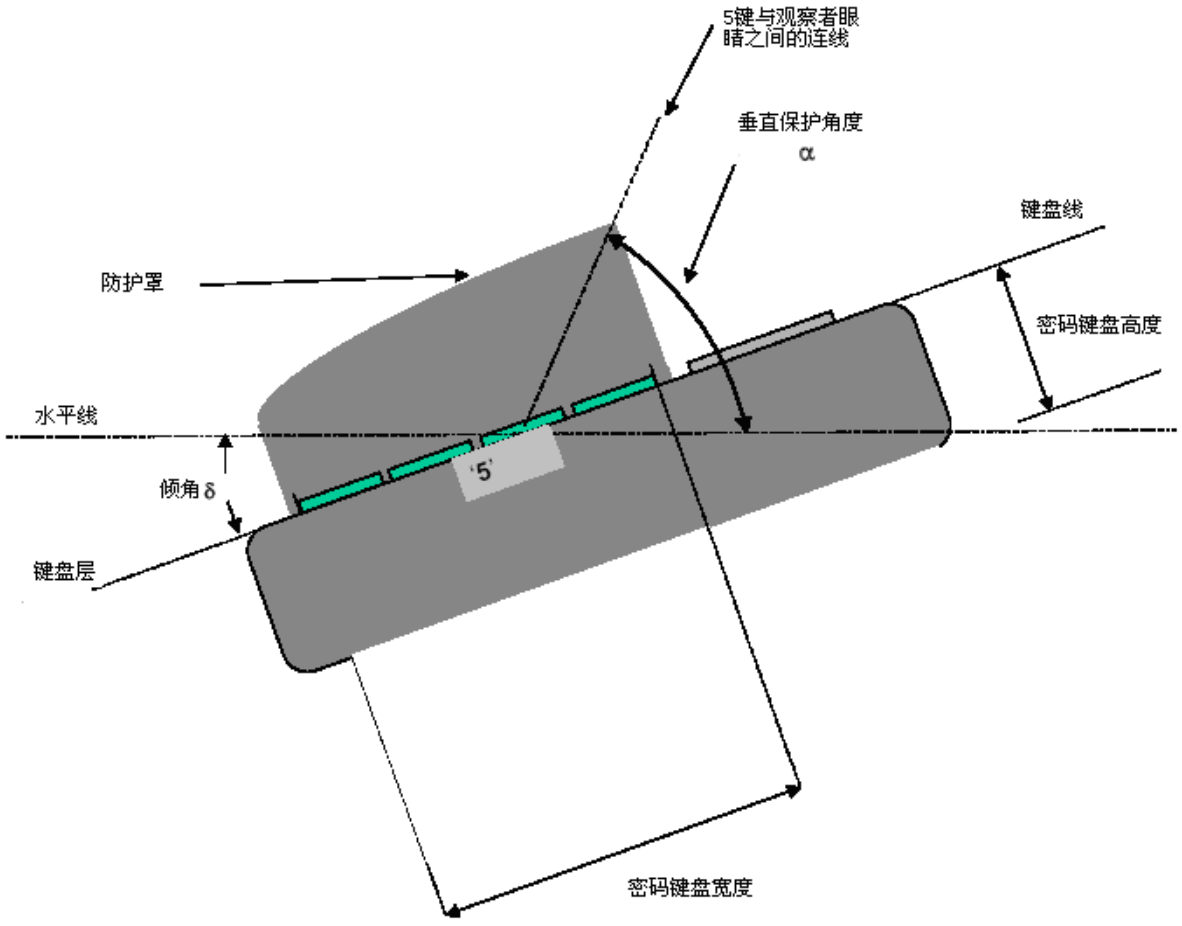

图 A.3：密码键盘样品侧视图

以上图中的角度定义如下：

α ：此角度是 5 键所在平面与连接 5 键与观测者视角的虚线之间的角度。

β ：观测者位置相对于操作员的位置之间的水平角度。

γ ：挡板存在的水平角度。

δ ：键盘区平面与水平面之间的角度。

A.1.2 设计原则

手持设备、有人职守设备以及无人职守设备有不同的设计要求，应明确设备的使用方式。如果其常备支撑或设备支架明显的表明 PIN 输入设备被装在一个旋转的支架上或类似工具上，该设备认定为桌上设备而不是手持设备。手持设备根据重量、功能、外型以及数字键盘区域的尺寸作为认定标准如下：

——重量不超过 500 克；

——设备功能及外型主机为手持型、便携式；

——数字键盘区域横向宽度不应超过 3inches 或者 7.62cm；

——数字键盘区域纵向长度不应超过 4inches 或者 10.16cm。

设备的防窥挡板应放置水平位置或有一定角度（0≤δ ≤45°），与垂直角度α 的要求范围有一定关系，如果 PIN 输入设备设计中键盘区向持卡人方向倾斜，则挡板后面的高度则可以适当降低，保护角度的具体要求见表 A.1：

表 A.1 测试角度要求

水平角度β	注释	垂直角度α
315°≤β ≤45°	在这个β 角度范围内，持卡人使用身体能将观测者的视角所遮挡。	NA
45°≤β ≤90° 270°≤β ≤315°	在这个β 角度范围内，观测键盘区的视线一部分被持卡人所遮挡。此时，保护角度α 应不小于 35 o。如果 PIN 输入设备倾斜放置，前面的挡板应该更高。	α 不小于 35°
90°≤β ≤270°	保护角度α 应不小于 40 °。如果键盘平面向下倾斜，则前挡板则可以适当的降低。	α 不小于 40°

如果 PIN 输入设备垂直放置或者放置角度大于 45 °，那么第三步将做适当的改变。使用垂直面代替水平面作为α 的参考平面。

此项保护针对于观测的视角，视角保护包括但不限于挡板防窥技术，例如 PIN 输入设备可采用触摸屏技术，即使用偏光器（触摸屏表面的模糊处理）制造视觉障碍，达到上述α 取值，或键盘采用随机数码显示，光学视角防窥技术，达到上述α 取值。

A.2 满足 PIN 输入设备放置环境的挡板设计标准

通过采用一些技术手段，在减低物理防护的一些要求（如α ≥25 °）的同时，保证对键盘区进行有效的遮挡。这些技术可以单独使用，也可同时使用。

——在验货台上实现视觉防窥挡板。这个挡板可以作为独立的挡板使用，也可作为一般通用验货台的一部分，如验货台的销售部位；

——PIN 输入设备成角度放置，使得 PIN 输入时难以进行偷窥，则应满足 A.1α 取值要求；

——PIN 输入设备安装可调节的支架，便于消费者将设备向旁边旋转、向前或向后倾斜一定位置，保证 PIN 输入时难以进行偷窥，应满足 A.1α 取值要求；

——键盘放置于终端旁安全摄像头的位置处，应不得看到 PIN 输入；

——提醒持卡人关于 PIN 输入的安全事项，可采用以下几种方式：

- 在PIN输入设备上标注；
- 在显示时进行提示，尽可能使用一个“单击确认”画面；
- 印在POS机具上；
- 安全PIN输入过程的一个标识。

设备厂商须提供恰当的技术文档，并包含针对不同观察区域安全所实施技术的矩阵，例如表 A.2：

表 A.2：观察区域以及 PIN 保护方法的矩阵样本

	观测途径				
方法	收银员	排队的顾客	非排队的顾客	现场的摄像机	远程摄像机
A 类 PIN 输入设备支架	M	H	L	L	L
B 类 PIN 输入设备支架	H	H	H	L	M
A 类收银台	L	M	M	L	H
B 类收银台	H	H	M	H	H
客户使用说明	H*	H*	H*	H*	H*

客户使用说明的方法可重复性低，因此应该与其他方法共同使用。

L：低等防护水平，M：中等防护水平，H：高等防护水平

矩阵中应明示 PIN 输入设备的购买方如何保护持卡人 PIN 的方法。应该根据所有的观察区域选择一个恰当的方法，以便于保持一个适当的保护级别。

附 录 B
（规范性附录）
攻击分值计算公式

B.1 计算攻击分值

本附录分析决定攻击分值的因素，并给出评估过程中如何避免一些主观因素的指导意见。除非评估人员认为这种方式并不适用于实际情况，否则这种方法应该被采纳。这样的话，就需要依据某个规则来认定这种方法是否适合于实际情况。

B.2 识别分析和实施攻击

攻击者在准备实施攻击已存在的漏洞时应首先识别分析出漏洞。所以将其分为两个步骤：识别分析和实施攻击。

B.3 需要考虑的因素

B.3.1 考虑因素概述

在分析漏洞攻击分值时，应当考虑下列因素：

——识别分析：

- 使用各种级别的专业技术，进行攻击所需的时间；
- 获取 PIN 输入设备的设计及操作原理知识的分值；
- 访问 PIN 输入设备的分值；
- 需要的设备，如进行分析所需的工具、组件、IT 硬件和软件；
- PIN 输入设备特定的零配件。

——实施攻击：

- 使用各种级别的专业技术，进行攻击所需的时间；
- 获取 PIN 输入设备的设计及操作原理知识的分值；
- 访问 PIN 输入设备的分值；
- 需要的设备，如进行分析所需的工具、组件、IT 硬件和软件；
- PIN 输入设备特定的备用组件。

这些因素并不互相依赖，但是在某种程度上却是可互相替代的。例如，专业技术或者软/硬件工具在某些情况下可以减少攻击所需的时间。

B.3.2 具体因素描述

B.3.2.1 攻击时间

攻击时间指攻击者识别分析或者实施攻击所需的时间（以小时为单位）。如果攻击由多步组成，则攻击时间累加起来从而获得攻击所需的总时间。应当统计实际的工作时间，而不是整个过程所耗费的时间，因为对采用的方法来说，没有一个最小的攻击时间(例如 进行旁路分析所需时间或者环氧变硬所需

的时间)。在那些无需人员职守的某攻击阶段，攻击时间应当以整个耗费时间的 1/3 来计算。

为了更好地计算实际工作时间，这里使用的转换关系为：1 天=8 个小时，1 周=40 小时，1 月=180 小时。

B.3.2.2 专业技术

专业技术指在应用领域或者产品类型等方面的通用知识等级。(例如，Unix 操作系统，网络协议)，分为以下等级：

——专家，对所采用的安全机制规则和理念非常熟悉，并对产品或系统类型相关的底层算法、协议、硬件、组织等方面也相当熟悉；

——精通，熟悉产品的安全特性的人。为了进行攻击，精通人员应具有使得攻击成功所需技能的资质；

——外行，和专家、精通的人相比是外行，没有专门技术。为了实施攻击，外行人员可以依据一个脚本或者既定流程，不需要特殊的技能。

如果某个攻击需要精通多个领域的技术，例如电子工程或者密码学，则可以假定需要专家级别的专门技术。

复合专家等级是指在多个技术领域达到专家等级的知识储备。这些领域都是为攻击技术所必须的。而复合专家所关心的领域应是不相同的，比如硬件操作和密码学。复合专家等级适用于那些需要培训等级的相关领域，而不是针对一次攻击所需要的实际个体数。在使用复合专家等级的时候应要提供非常充分的理由。

B.3.2.3 PIN 输入设备相关知识

PIN 输入设备相关的知识指具有特定的和 PIN 输入设备相关的专门技术。可分为以下等级：

——与PIN输入设备有关的公开信息（或者没有任何信息），每个人都很容易获取到（如从互联网获取）的信息，或者可由厂商提供给任何客户的信息，这些都被认为是公开的；

——与PIN输入设备有关受限制的信息（从厂商技术规格说明书中获取的信息），如果设备是先申请后发放，并且发放需要注册，则此类信息也被认为是受限制的信息；

——与PIN输入设备有关的敏感信息（内部设计的知识），需要利用“社交工程”或者彻底的逆向工程才能获取的信息。

应仔细区分用来分析漏洞和用来攻击的信息，特别是敏感信息更需要进行严格区分。实施攻击一般不需要敏感信息。

专家技术以及 PIN 输入设备的知识影响着有能力攻击 PIN 输入设备的攻击者所需信息的多少。攻击者的技术水平和在攻击中熟练使用设备的能力间有一些内在关系。攻击者的技术水平越低，熟练使用设备的能力越弱。同样的，技术水平越高，在攻击中使用设备的能力越强，具体关系不是唯一，须根据实际情况而定，如当环境因素限制专家级的攻击者使用设备，或者使用他人已开发并免费发布（通过互联网）的“傻瓜式”攻击工具。

B.3.2.4 访问 PIN 输入设备

机械样本是非功能性仅用来学习或者提供备份部件使用。没有工作密钥的功能性样本可用来测试设备的逻辑或者电气特性，不能用于网络支付和真正的支付卡支付。此种设备攻击者可购买到。注意，安装了测试密钥或者伪密钥的样本属于此类。带有工作密钥的功能性样本是全功能的设备，可用来验证一种攻击手段或实施攻击。如果在某个类别中需要超过 1 个样本，不可采用样本的数量乘以分数，而应当使用表 B.1 中的因子：

表 B.1 多个样本因子

设备的数量	因子
1	1
2	1.5
3-4	2
5-10	4
>10	5

B.3.2.5 分析设备工具

分析设备工具指用来分析或攻击漏洞的设备。可分成以下类别：

——标准设备：攻击者可快速使用分析漏洞或进行攻击的设备。这类设备较容易获取，如已在附近的仓库或从互联网下载的。可包含简单的攻击脚本、个人计算机、读卡器、模式发生器、简单光学显微镜、供电电源或者简单的机械装备；

——专门设备，攻击者不能马上获取，但可经过正当途径获得的设备。包括购买中等数量的设备，如专门的电子卡片、专用的测试平台、协议分析器、示波器、微探针工作站、化学工作台、精确铣床设备等等，或者开发更多的攻击脚本或程序；

——定制设备，指对公众还没有，需要专门定制的设备，如非常专业的软件，或设备太专业，控制发放甚至是严格限制。也可以是设备非常昂贵，如离子聚焦光束、扫描式电子显微镜，激光打磨器。可以租用到的定制设备可以视为专门设备，在分析阶段开发的软件也可认为是定制设备，在攻击阶段开发的则不算；

——芯片级别攻击设备，有必要时需进行芯片级攻击，其在市场上非广泛应用并且受到限制。该攻击使用的设备价格非常昂贵，因此将其单独进行分类。仅以下设备属于此类范畴：

- 聚焦离子束；
- 电子扫描显微镜；
- 激光研磨设备。

如果某个阶段（识别阶段或攻击阶段）需要使用不同级别的设备，应只保留其中最高等级即可。如果在识别阶段使用的设备，在攻击阶段也会重复利用，不能对同一设备进行两次评分。这种情况下，设备的分值应平均后分别用于识别阶段和攻击阶段中。

分析阶段使用多个设备能够保证在攻击阶段的成功率，但是在攻击阶段很少会使用多个设备。

B.3.2.6 隐藏攻击痕迹的组件

组件用来隐藏攻击痕迹、替换数据监控或安装通讯装置,。如果同样的零件在识别分析或者实施攻击过程中都使用，则只可以被统计一次。PIN 获取 bug 属于此类范畴。

——标准组件，攻击者较容易得到的部件，可通过市场购买或从同类型设备样本中拆来的部件；

——专用组件，不是攻击者已有，但可通过正当途径获得的部件。如通过市场订购且需要很长的运送时间，或需要按批购买的组件；

——定制组件，需要专门制造的部件。如果攻击需要专门定制部件，则这种攻击方式不大可行。

B.3.2.7 攻击成功率

a) 攻击率

攻击成功率仅在攻击的初始阶段使用，是一个用于对攻击的后续阶段可以重复利用设备、知识进行

优化，通过实验室评估的手段很难进行判定。在后续攻击阶段重复使用并用于计算的典型因素包括设备和知识两种。

在某些攻击场景中会导致总分以及攻击分值一致，但是其中之一会使得攻击阶段的耗费较低，除上面两个因素外的其他因素在评分时都要被考虑。

b) 攻击成功率

如果实施一个攻击的难度相当的大，导致成功的数量较少，此时需要依据限制条件应用多个设备。为了应对这类情况的出现，目标设备（例如攻击阶段使用带有工作密钥的功能性样本）的数量，应使用表 B.2 中的因子进行乘法运算：

表 B.2 成功率乘法因子

成功率	因子
P≥0.5	1
0.5>P≥0.25	1.5
P>0.25	2

一旦确认了攻击存在可能的因素，攻击的每一个步骤应分成独立的阶段，其中每个阶段都应具有其自己的可能性。总体的可能性是所有因子乘和得到。

一旦总体的可能性降低到 0.5 以下，需要出具一个恰当的文档。确定可能性的工作是基于终端实际攻击的基础上得到的，并行可能使用恰当的样本制作统计数据图表。

B.4 攻击分值计算方法

针对一个既定的攻击，须提出多种攻击场景计算分值。如替换专业人员的攻击时间和设备。当分析出一个漏洞且在公用域中，则识别分值应该选用攻击者在公用域中提出攻击方案的分值，而不采用最初的识别分值。攻击分值因素分值见表 B.3。

表 B.3 攻击分值因素分值

分值	范围	分析阶段	攻击阶段
攻击时间	< 1 小时	0	0
	<= 8 小时	2	2
	<= 24 小时	3	3
	<= 40 小时	3.5	3.5
	<= 80 小时	4	4
	<= 160 小时	5	5
	>160 小时	5.5	5.5
技术水平	外行	0	0
	精通	1.5	1.5
	专家	4	4
PIN 输入设备的知识	公开知识	0	0
	限制知识	2	2
	私有知识	3	3
攻击时需要获得 PIN 输入设备每个部件，如果需要多个部件，分值应当乘上上面的因子	设备样本	1	1
	没有工作密钥的功能性样本	2	2

分值	范围	分析阶段	攻击阶段
	带有工作密钥和软件的功能性样本	4	4
攻击需要的设备	无	0	0
	标准的	1	1
	专用的	3	3
	定做的	5	5
	芯片级攻击	7	7
特殊零件需求	无	0	0
	标准的	1	1
	专用的	3	3
	定做的	5	5

对于每个阶段而言，测试实验室应记录所有的必须的步骤。应包括所使用的技术水平，设备，特殊零件需求，以及操作所需的时间（按小时计算），如果涉及到成功率，也要予以明确。

上面表格中描述的所有项目是一个很好的汇总，能够帮助对于上述因素进行合理的选择。

B.5 攻击实例一

本攻击的目标是向PIN输入设备中插入一个PIN探测装置。插入一个PIN探测装置的攻击分值见表B.12。这个装置被放置在设备外壳下方的键盘板PCB附近，其目的在于监测键盘信号并且记录PIN的输入：

a) 识别阶段：

1) 对设备进行逆向工程以熟悉其设计原理，包括入侵检测信号以及传感器信号。电子专业的专家进行安全信号的走线的解析，也对键盘信号的扫描方式进行确认。随后，定位入侵检测机制，并且设计攻破或绕过这些机制的方法。因此，这个过程需要 60 个工作时，专家技能，标准的设备，以及一个机械样本。见表 B.4。

表 B.4 逆向工程

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	公开	无	1 个机械样本	60 小时

2) 定制用于监控键盘信号以及记录 PIN 输入的 bug。在此示例中，使用了简单的扫描技术，因此作出以下级别判定：专家，30 工作时，标准部件，标准设备，重复使用了机械样本。见表 B.5。

表 B.5 定制 bug

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	公开	标准	无	30 小时

3) 使用带有测试密钥的工作样本进行验证实验。注入测试密钥的操作以及对入侵响应的恢复工作需要有权使用密钥下载软件或者相关的说明，因此涉及到了限制知识。见表 B.6。

表 B.6 测试密钥

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	受限	标准	1 个带测试密钥的功能样本	40 小时

对整个识别阶段进行总结，结果见表 B.7。

表 B.7 识别阶段结果

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	受限	标准	1 个机械样本； 1 个带测试密钥的功能样本	130 小时

c） 攻击阶段：

攻击者使用带有密钥的功能样本进行实际的攻击，需要以下几个步骤：

1） 攻击入侵检测机制后，进入到终端内部。可以认为外壳能够被多余的部件替换，攻击每个检测机制的成功率可以达到 0.9，并且每个机制需要用时 1 小时。在这个示例中，总共有八个入侵检测机制，但是只有其中四个需要进行攻击。需要额外的 1 小时用于攻击的稳定性。

2） 尽管攻击方案被制定，仍然需要较好的机械技能以及保障成功的技巧。因此人员等级定为“精通”。见表 B.8。

表 B.8 攻击入侵检测机制

技术水平	设备	知识	部件	样本	攻击时间
精通	标准（重复利用）	公开	无	1 个带工作密钥的功能样本； P=0.94≈0.66	5 小时

3） 一旦进入到终端内部，攻击需要对终端较深层的敏感信号（例如，键盘扫描信号）进行定位，这些信号由更为难攻破的，其他的入侵检测机制进行保护。见表 B.9。

表 B.9 攻入终端内部

技术水平	设备	知识	部件	样本	攻击时间
专家	标准（重复利用）	公开	无	1 个带测试密钥的功能样本； P=0.8	12 小时

4） 一旦成功完成上述步骤，攻击者能够在键盘线上进行 bug 的安装，替换外壳，并对终端进行测试。恢复后的终端可以还回到原商户或商店。专用设备需要用来植入 bug，取决于前面步骤中的受限制的访问。见表 B.10。

表 B.10 bug 安装

技术水平	设备	知识	部件	样本	攻击时间
精通	专用	公开	标准（bug）	1 个带测试密钥的功能样本； P=1	6 小时

对攻击阶段进行总结，结论见表 B.11。

表 B.11 攻击阶段结论

技术水平	设备	知识	部件	样本	攻击时间
专家	专用	公开	标准	1 个带测试密钥的功能样本； P≈0.52； 因子为 1	23 小时

表 B.12 插入一个 PIN 探测装置的攻击分值

相关方面	识别分析值		实施攻击值	
攻击时间	<=160 小时	5	<=24 小时	3
技术水平	专家	4	专家	4
对设备的知识	限制	2	公开	0
对 PIN 输入设备的访问	1 个机械样本； 一个没有工作密钥的功能样本	4	有工作密钥的功能性样本 P≈0.52	4
设备	标准	1	专用	3
专用零件	标准	1	标准	1
每个阶段攻击分值		17		15
总共攻击分值		32		

B.6 攻击实例二

这个攻击的目标在于使用 DPA 确定 3DES 加密密钥，假定如下：

需要使用 PIN 输入设备的某个功能，这个功能提供 PIN 以供加密，此加密处理的密钥就是攻击目标。DPA 用到的数据，可从 PIN 输入设备外部接口获取。例如，没有对 PIN 输入设备执行进一步的物理攻击来获取需要的测试数据，并且 PIN 输入设备没有有效的防 DPA 的功能。攻击包含以下步骤：

a) 确定在 PIN 输入设备上运行 DPA 的方法。一般包含分析电子和逻辑接口。这个步骤需要专业的电子计算机知识。

b) 建立攻击方案，包含以一个自动控制的方式来操作 PIN 输入设备。由于需要大量的 PIN 输入，而这些输入很难手动进行，因此采用一种专门的机制来进行 PIN 的输入。该设备为定制设备，专门为这个攻击定做的，在分析阶段也会使用。

c) 得到一个 PIN 输入设备，并测试。需要观察至少 20000 个 PIN 输入以及随后的加密过程。在分析阶段可能会重复多次。由于需要穷举 PIN，所以 20000 个 PIN 输入至少需要 7 天。由于这么大量的交易不可能在真实的交易环境中出现，因此极有可能和一个模拟主机运行离线交易。

d) 分析采样数据，得到 PIN 加密密钥。

使用与第一个示例类似的手段，攻击分值的计算方法见表 B.13：

表 B.13 DPA 分析攻击分值例子

相关方面	识别值		攻击值	
攻击时间	＞160 小时	5.5	<80 小时	4
技术水平	专家	4	专家	4
对设备的知识	限制	2	公开	0
对 PIN 输入设备的访问	使用试验密钥的功能性样本	2	有工作密钥的功能性样本	4
设备	定做	5	专用	3
专用零件	标准	1	不需要其他的零件	0
每个阶段攻击分值		19.5		15
总共攻击分值		34.5		

参考文献

[1]ISO 13491-1 银行业 安全加密设备(零售) 第1部分：概念、需求以及评估方法(Banking Secure cryptographic devices (retail) Part 1: Concepts, requirements and evaluation methods)
[2] ISO 13491-2 银行业 安全加密设备(零售) 第2部分：用于磁条卡系统的设备安全符合性检测项目(Banking Secure cryptographic devices (retail) Part 2: Security compliance checklists for devices used in magnetic stripe card systems)
[3] Payment Card Industry PTS POI Security Requirement V3.0