

(12) 发明专利申请

(10) 申请公布号 CN 102708632 A

(43) 申请公布日 2012. 10. 03

(21) 申请号 201210165731. 2

(22) 申请日 2012. 05. 25

(71) 申请人 福建联迪商用设备有限公司

地址 350003 福建省福州市软件大道 89 号
福州软件园一区 23 号楼

(72) 发明人 洪逸轩 孟陆强 彭波涛

(74) 专利代理机构 福州市鼓楼区博深专利代理
事务所 (普通合伙) 35214

代理人 林志峥

(51) Int. Cl.

G07G 1/00 (2006. 01)

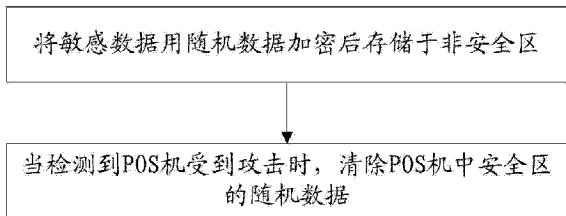
权利要求书 1 页 说明书 3 页 附图 1 页

(54) 发明名称

一种 POS 机中敏感数据的保护方法及保护装置

(57) 摘要

本发明公开一种 POS 机中敏感数据的保护方法, 所述 POS 机包括安全区和非安全区, 其中安全区存储有 POS 机出厂前随机生成的随机数据, 该方法包括以下步骤: 将敏感数据用随机数据加密后存储于非安全区; 检测到 POS 机受到攻击, 清除安全区的随机数据。本发明利用安全区的随机数据加密密钥后存储于非安全区, 在 POS 机受到攻击时清除安全区的随机数据, 由于安全区数据的随机性, 从而避免了 POS 机密钥被窃取情况的发生, 且降低了对安全区空间大小的要求, 提高了系统的灵活性。本发明同时公开一种 POS 机中敏感数据的保护装置。



1. 一种 POS 机中敏感数据的保护方法,其特征在于,所述 POS 机包括安全区和非安全区,其中安全区存储有 POS 机随机生成的随机数据,该方法包括以下步骤:

将敏感数据用随机数据加密后存储于非安全区;

当检测到 POS 机受到攻击时,清除 POS 机中安全区的随机数据。

2. 根据权利要求 1 所述的 POS 机中敏感数据的保护方法,其特征在于,所述敏感数据包括密钥,该密钥用于加密持卡人的安全数据。

3. 根据权利要求 1 所述的 POS 机中敏感数据的保护方法,其特征在于,所述攻击包括打开外壳、高温、高压、静电干扰中的至少一种。

4. 根据权利要求 1 所述的 POS 机中敏感数据的保护方法,其特征在于,在安全区中的随机数据被清除后,在使用 POS 机之前,重新生成随机数据和敏感数据,将该敏感数据用随机数据加密后存储于非安全区。

5. 一种 POS 机中敏感数据的保护装置,所述 POS 机包括安全区和非安全区,其中安全区存储有 POS 机随机生成的随机数据,其特征在于,该装置包括:

加密装置,用于将敏感数据用随机数据加密后存储于非安全区;

检测装置,用于检测 POS 机受到攻击,并当检测到攻击时,清除安全区的随机数据。

6. 根据权利要求 5 所述的 POS 机中敏感数据的保护装置,其特征在于,所述敏感数据包括密钥,该密钥用于加密持卡人的安全数据。

7. 根据权利要求 5 所述的 POS 机中敏感数据的保护装置,其特征在于,所述攻击类型包括打开外壳、高温、高压、静电干扰中的至少一种。

8. 根据权利要求 5 所述的 POS 机中敏感数据的保护装置,其特征在于,在安全区中的随机数据被清除后,在使用 POS 机之前,重新生成随机数据和敏感数据,将该敏感数据用随机数据加密后存储于非安全区。

一种 POS 机中敏感数据的保护方法及保护装置

技术领域

[0001] 本发明涉及一种 POS 机中敏感数据的保护方法及保护装置。

背景技术

[0002] 时下刷卡支付渐成为广大群众的消费习惯,电子支付也随之风生水起。相应的,作为电子支付的重要组成部分——POS 也成为人们日常生活中的必不可少的一部分。

[0003] POS 机做为一个电子金融交易的重要组成部分,主要实现将持卡人信息及相应的密码上送到后台的功能。整个数据的传输过程是在开放环境下进行的,为防止有人恶意监听网络数据进而获取到持卡人信息及相应的密码,需要用 POS 中的密钥对密码加密后再上送到后台。若 POS 机中保存的密钥泄密,相应的加密数据即可被解密,使得持卡人的密码泄密,危害社会的正常金融秩序。

发明内容

[0004] 为解决上述问题,本发明提出一种保护 POS 机中敏感数据的方法,避免敏感数据被非法获取情况的发生。本发明是采用以下技术方案实现的:一种 POS 机中敏感数据的保护方法,其特征在于,所述 POS 机包括安全区和非安全区,其中安全区存储有 POS 机随机生成的随机数据,该方法包括以下步骤:

[0005] 将敏感数据用随机数据加密后存储于非安全区;

[0006] 当检测到 POS 机受到攻击时,清除 POS 机中安全区的随机数据。

[0007] 其中,所述敏感数据包括密钥,该密钥用于加密持卡人的安全数据。

[0008] 其中,所述攻击包括打开外壳、高温、高压、静电干扰中的至少一种。

[0009] 其中,在安全区中的随机数据被清除后,在使用 POS 机之前,重新生成随机数据和敏感数据,将该敏感数据用随机数据加密后存储于非安全区。

[0010] 为解决上述问题,本发明同时公开一种 POS 机中敏感数据的保护装置,所述 POS 机包括安全区和非安全区,其中安全区存储有 POS 机随机生成的随机数据,其特征在于,该装置包括:

[0011] 加密装置,用于将敏感数据用随机数据加密后存储于非安全区;

[0012] 检测装置,用于检测 POS 机受到攻击,并当检测到攻击时,清除安全区的随机数据。

[0013] 其中,所述敏感数据包括密钥,该密钥用于加密持卡人的安全数据。

[0014] 其中,所述攻击类型包括打开外壳、高温、高压、静电干扰中的至少一种。

[0015] 其中,在安全区中的随机数据被清除后,在使用 POS 机之前,重新生成随机数据和敏感数据,将该敏感数据用随机数据加密后存储于非安全区。

[0016] 有益效果:

[0017] POS 机中的敏感数据只要经过安全区内部随机生成的数据加密后,就可以放置于非安全区域中,并在检测到外部攻击时自动清除安全区的数据,避免敏感数据被非法获取

情况的发生,提高了 POS 机的安全性。

附图说明

[0018] 图 1 为本发明实施例的 POS 机中敏感数据的保护方法流程图;

[0019] 图 2 为本发明实施例的 POS 机中敏感数据的保护装置结构原理图。

具体实施方式

[0020] 为详细说明本发明的技术内容、构造特征、所实现目的及效果,以下结合实施方式并配合附图详予说明。

[0021] 请参阅图 1,为本发明实施例的 POS 机中敏感数据的保护方法流程图。POS 机内部存储空间分为安全区和非安全区,安全区是 POS 芯片控制的一个区域,当芯片检测到 POS 外壳被打开之类的攻击后,芯片马上清除该区域的所有数据;非安全区,与安全区相对,当芯片检测到 POS 外壳被打开之类的攻击后,该区域数据不受影响。出厂前的每台 POS,均随机生成一串数据存储在安全区中,这保证了每台 POS 安全区的数据是完全不一样的,且 POS 的软件开发人员也无法预知安全区数据的内容。该保护方法包括以下步骤:

[0022] 将敏感数据用随机数据加密后存储于非安全区;

[0023] 检测到 POS 机受到攻击,清除安全区的随机数据。

[0024] 作为一实施例,本发明所述的敏感数据包括密钥,该密钥用以加密持卡人的安全数据,这里的安全数据包括持卡人在交易过程中使用的密码。保存在 POS 中的敏感数据,均经安全区数据加密后再保存于非安全区,即非安全区只保存敏感数据的密文。使用敏感数据前,使用安全区数据解密后再执行相应操作。

[0025] 当 POS 机检测到诸如打开外壳、温度、电压、静电干扰之类的攻击行为后,芯片立即清除安全区数据,并有明显的提示以警示用户该 POS 机已处于异常状态,无法再执行正常的金融交易。因为无法获取解密保存于非安全区的敏感数据密文的密钥,攻击者无法获取敏感数据的明文,所以保存于非安全区的敏感数据得到了保护。安全区数据被清除后,POS 机就无法继续执行正常的交易,只能通知专业维修人员,由维修人员对设备进行相关维修操作,重新生成 POS 安全区的随机数据,并重新生成随机敏感数据,将该敏感数据用随机数据加密后存储在非安全区。在保证 POS 没有被恶意破坏后,才能将 POS 重新返回给客户。

[0026] 请参考图 2,为本发明实施例的 POS 机中敏感数据的保护装置结构原理图。该装置包括:加密装置,用于将敏感数据用随机数据加密后存储于非安全区;检测装置,用于检测 POS 机受到攻击,并当检测到攻击时,清除安全区的随机数据。

[0027] 做为本发明的优选实施例,所述敏感数据包括交易过程用于加密持卡人的安全数据的密钥,比如用该密钥加密密码。上述的攻击类型包括打开外壳、高温、高压、静电干扰中的至少一种。

[0028] 上述方案中,安全区中的随机数据被清除后,再次使用 POS 机之前,需要重新生成随机数据和敏感数据,将该敏感数据用随机数据加密后存储于非安全区。

[0029] 实施本发明,敏感数据只要经过安全区内部随机生成的数据加密后,就可以放置于非安全区域中,提高了 POS 的安全性;由于芯片功能的制约,现有技术其清除的数据往往只是芯片特定的一段区域,但敏感数据所需的空间一般都比较大大,无法全部保存于安全区

中,只能部分或全部保存于非安全区中。本发明利用安全区的随机数据对敏感数据进行加密后存储在非安全区,降低了对安全区空间大小的要求,提高了系统的灵活性。

[0030] 以上所述仅为本发明的实施例,并非因此限制本发明的专利范围,凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本发明的专利保护范围内。

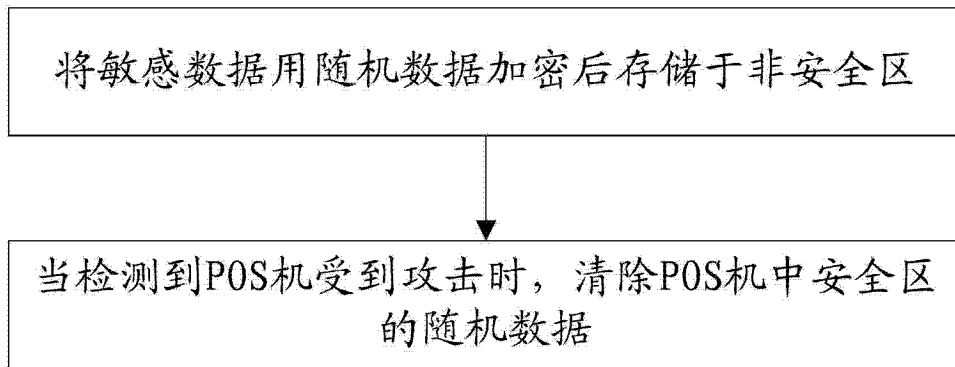


图 1

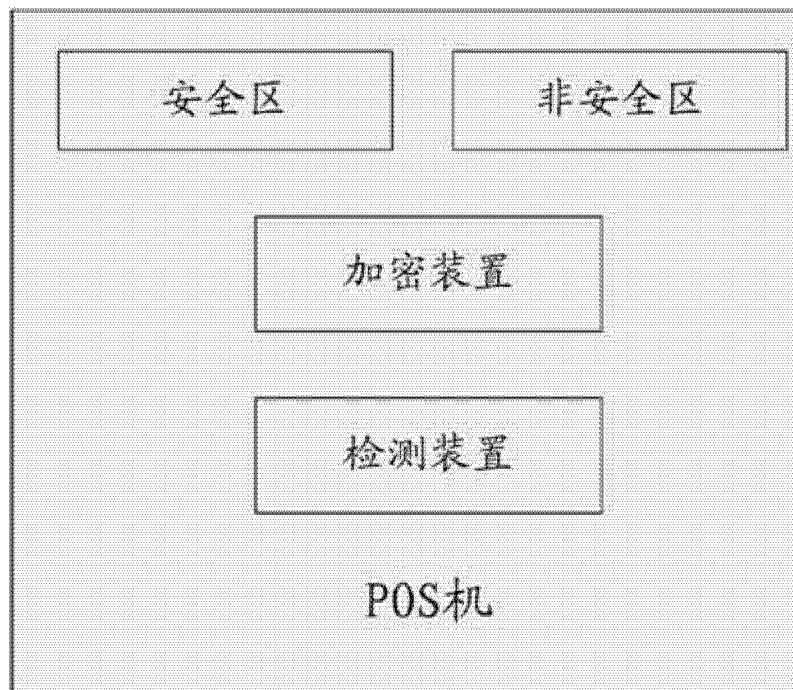


图 2