

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 12 月 8 日 (08.12.2016)



(10) 国际公布号
WO 2016/192453 A1

- (51) 国际专利分类号:
G06Q 20/32 (2012.01)
- (21) 国际申请号: PCT/CN2016/077958
- (22) 国际申请日: 2016 年 3 月 31 日 (31.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510290962.X 2015 年 5 月 30 日 (30.05.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中
国广东省深圳市南山区科技园北区梦溪道 2 号,
Guangdong 518057 (CN)。
- (72) 发明人: 张子敬 (ZHANG, Zijing); 中国广东省深圳
市南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 张晴 (ZHANG, Qing); 中国广东省深圳市
南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。
- (74) 代理人: 北京友联知识产权代理事务所(普通合
伙) (YOULINK INTELLECTUAL PROPERTY
LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,
CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA,
RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST,
SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: SAFETY CONTROL METHOD AND APPARATUS, AND TERMINAL

(54) 发明名称: 一种安全控制方法、装置和终端

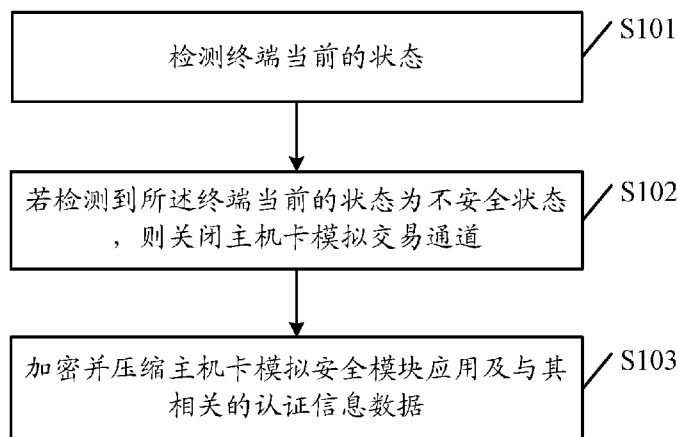


图 1

- S101 Detect a current state of a terminal
- S102 If it is detected that the current state of the terminal is an unsafe state, close a host card simulated transaction channel
- S103 Encrypt and compress a host card simulated safety module application and authentication information data related to the host card simulated safety module application

(57) Abstract: A safety control method and apparatus (300, 400), and a terminal. The safety control method comprises: detecting a current state of a terminal (S101); if it is detected that the current state of the terminal is an unsafe state, closing a host card simulated transaction channel (S102); and encrypting and compressing a host card simulated safety module application and authentication information data related to the host card simulated safety module application (S103). Therefore, safety control of an NFC service is implemented by using a host card simulation-based technology.

(57) 摘要: 一种安全控制方法、装置 (300, 400) 和终端, 所述安全控制方法包括: 检测终端当前的状态 (S101); 若检测到所述终端当前的状态为不安全状态, 则关闭主机卡模拟交易通道 (S102); 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据 (S103)。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

WO 2016/192453 A1



(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ,

CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种安全控制方法、装置和终端

技术领域

本发明涉及通信领域，具体涉及了一种安全控制方法、装置和终端。

背景技术

目前，基于 Android4.4 的 NFC（Near Field Communication，近距离无线通讯技术）支付引入了一个新的开放式架构，即 HCE（Host-based Card Emulation，主机卡模拟）技术，从而在配备 NFC 功能的终端中实现卡模块后，终端不需要提供物理 SE（Security Elements，安全模块），使得 NFC 的应用更加简单与灵活。

但是 HCE 技术只是模拟了 NFC 和 SE 通信的协议和实现，也即以虚拟 SE 的方式完成 NFC 业务的安全保证，并没有实现 SE。现有基于 HCE 技术的 SE 解决方案，可以通过本地应用程序的模拟或者云端服务器的模拟来实现，但是在这两种方案下，由于 Android 系统本身的安全性问题导致数据安全性不够，比如当系统被 Root（获取超级用户权限）以后，系统中的所有数据都将受到安全威胁，系统中存储的 SE 或认证信息很容易被获取。那么如何在基于 HCE 技术下实现 NFC 业务的安全控制是一个亟待解决的问题。

发明内容

本发明实施例提供了一种安全控制方法、装置和终端，以期可以在基于 HCE 技术下实现 NFC 业务的安全控制。

本发明实施例第一方面提供了一种安全控制方法，包括：

检测终端当前的状态；

若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

本发明实施例第二方面提供了一种安全控制装置，包括：

第一检测模块，用于检测终端当前的状态；

关闭模块，用于若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；

加密模块，用于加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

本发明还提供了一种终端，包括如上述任一技术方案所述的安全控制装置。

可以看出，在本发明实施例提供的技术方案中，检测终端当前的状态；若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道，从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道；加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例提供的一种安全控制方法的流程示意图；

图 2 是本发明实施例提供的另一种安全控制方法的流程示意图；

图 3 是本发明实施例提供的一种安全控制装置的结构示意图；

图 4 是本发明实施例提供的另一种安全控制装置的结构示意图；

图 5 是本发明实施例提供的又一种安全控制装置的结构示意图；

图 6 是本发明实施例提供的一种终端的结构示意图。

具体实施方式

本发明实施例提供了一种安全控制方法、装置和终端，以期可以在基于 HCE 技术下实现 NFC 业务的安全控制。

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第

三”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

本发明实施例的一种安全控制方法的一个实施例，一种安全控制方法包括：检测终端当前的状态；若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

首先参见图 1，图 1 是本发明的一个实施例提供的一种安全控制方法的流程示意图。其中，如图 1 所示，本发明的一个实施例提供的一种安全控制方法可以包括：

S101、检测终端当前的状态。

其中，终端为手机、平板电脑等能安装 Android 系统的智能终端，支持 HCE，具备 NFC 功能。终端当前的状态指终端当前的运行环境的状态，比如是否安全等。

其中，HCE 指基于主机的卡模拟，在配备 NFC 功能的终端上实现卡模拟时，不需要提供 SE，由在终端上运行的一个应用或者云端的服务器来完成 SE 的功能，此时 NFC 芯片接收到的数据由操作系统、或发送至终端中的应用、或通过移动网络发送云端的服务端来完成交互。例如，在 NFC 手机中，可以通过手机中的应用来模拟安全模块 SE。

其中，安全模块 SE 指用于存储 NFC 应用和用户敏感数据以及实现安全密钥运算的芯片模块，是 NFC 卡模拟的核心，安全模块还通过非接前端与外部读写设备进行通信，实现数据存储及交易过程的安全性。

可选地，在本发明的一些可能的实施方式中，NFC 终端可包括硬件安全模块 SE，提供对敏感信息的安全存储和为交易事务提供一个安全的执行环境，其中，SE 可以集成到 SIM 卡、SD 卡或终端芯片中。

可选地，在本发明的一些可能的实施方式中，可在具有 NFC 功能的终端上安装 Android4.4 系统，由于 Android4.4 系统支持 HCE 功能，从而可在 Android4.4 系统上实现 HCE 功能，利用 HCE 模拟 SE 应用。

可选地，在本发明的其它一些可能的实施方式中，如果具有 NFC 功能的终端系统是 Android4.4 之前的版本，则可以将终端系统升级到 Android4.4 系统。从而可以实现对 HCE 功能的支持。

可选地，在本发明的一些可能的实施方式中，支持 HCE 功能的终端可在终端上用 APP (Application, 应用程序) 应用程序模拟卡，实现主机卡模拟的功能，同时该终端也支持其它传统的 SE 模拟卡技术，如硬件 SE 模块，也即终端同时兼容 HCE 和传统的 SE。

举例进行说明，对于一个具有 NFC 功能的 Android4.4 系统的手机终端，支持 HCE 功能，从而可通过 HCE 实现对 SE 的卡模块，同时该手机终端上具有硬件 SE 模块，所以可以理解，该手机终端同时兼容 HCE 卡模拟以及传统的硬件 SE 功能。

可选地，在本发明的一些可能的实施方式中，终端当前的状态可以为安全状态，也可以为不安全状态。

可选地，在本发明的一些可能的实施方式中，终端在 HCE 模拟交易通道开启后，以一定的频率检测终端当前的安全状态。

S102、若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道。

其中，不安全状态指终端的运行环境不安全，导致运行在终端当前的数据有可能被窃取或者破坏，从而导致终端当前所进行的交易不安全。

其中，主机卡模块交易通道（即 HCE 卡模拟交易通道）是指利用 HCE 技术模拟 SE 安全模块完成 NFC 交易的通道，此时 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到模拟 SE 的应用，然后由模拟 SE 的应用进行回复。而传统的基于硬件的 NFC 交易通道是 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到 SE，然后由 SE 进行回复。

例如，在一部具有 HCE 功能的 NFC 手机中，通过 APP 应用模拟 SE，从而实现 HCE 模拟交易通道，即主机卡模拟交易通道。

举例说明，在本发明的一些可能的实施方式中，当终端为手机时，利用手机 NFC 进行支付，当手机的系统被 Root 后，存储在手机系统中的数据很容易被窃取或破坏，此时终端的当前状态为不安全状态，那么关闭 HCE 模拟交易通道，从而终止该通道所进行的支付交易。

可以理解，关闭主机卡模拟交易通道可以在终端当前状态为不安全状态时不再使用该交易通道进行交易，从而阻止了不安全交易的发生。

S103、加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

其中，在 NFC 终端中，主机卡模拟安全模块应用（即 HCE 模拟 SE 应用）指在具有 HCE 卡模拟功能的终端上模拟 SE 安全模块的 APP 应用，与其相关的认证信息数据是指存储在 HCE 模拟 SE 应用中的 NFC 交易中用于认证的数据和用户敏感数据。例如，在 NFC 支付中，该认证信息数据可以为支付双方的用户信息、密码、以及与支付相关的其它数据等。

可选地，在本发明的一些可能的实施方式中，也可以压缩并加密 HCE 卡模拟安全模块应用及与其相关的认证信息数据，从而保证交易数据的安全性。

举例说明，在手机 NFC 移动支付时，若支付环境出现安全风险，此时关闭 HCE 模拟支付通道，并将与支付相关的用户信息、密码以及其它相关的数据进行加密并压缩，保证数据的安全性。

可以理解，通过一定的方式加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据将加强这些数据的安全性。

可以看出，本实施例的方案中，检测终端当前的状态；若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道，从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道；加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现关闭 HCE 卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，所述检测终端当前的状态包括以下方式中的至少一种：

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

其中，终端当前的安全状态包括终端自身运行环境是否安全以及终端运行的软件是否合格，当检测到终端系统被获取超级用户权限或终端安装的应用受到病毒入侵时，判断为终端自身的运行环境不安全，也即终端的状态为不安全状态，此时关闭 HCE 卡模拟交易通道。

可以理解,在上述几种情况下将会使得终端运行的应用及数据的安全受到威胁,如终端正在进行支付时,若终端被获取到超级用户权限,则和支付相关的信息将会被获取,支付交易不安全。

可选地,在本发明其它的一些可能的实施方式中,所述检测终端当前的状态还可以包括检测终端安装的应用是否为不合法应用或无权限应用,以及检测终端其它异常情况。

可选地,在本发明的一些可能的实施方式中,所述方法还包括:

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用则拒绝所述应用访问所述主机卡模拟交易通道。

可以理解,若检测到所述终端安装的应用为非官方发布应用、合法应用或无权限应用时,此时只是终端的应用不合格,而终端本身不存在 Root 或其它安全风险时,此时只限制该应用对 HCE 卡模拟交易通道的访问,而不去关闭 HCE 卡模拟交易通道,使得操作简单,也能不影响其它官方应用、合法应用以及有权限应用对 HCE 卡模拟交易通道的访问。

可选地,在本发明的一些可能的实施方式中,所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后,所述方法还包括:

将所述主机卡模拟交易通道路由到安全模块实体中。

可以理解,当终端当前的状态为不安全状态时,关闭 HCE 卡模拟交易通道,并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后,从而 NFC 交易则无法进行,那么此时将 HCE 卡模拟交易通道路由到传统的 SE 模块中保证了交易的顺利进行,同时保证了数据的安全性。

可选地,在本发明的一些可能的实施方式中,所述安全模块实体为硬件实体 SE 模块。

举例说明,在本发明的一些可能的实施方式中,当利用手机进行 NFC 移动支付时,若检测到手机被 Root,为了保证支付的安全性,关闭 HCE 模拟交易通道,加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据,并同时 will HCE 模拟交易通道路由到实体 SE 中,从而消除了支付风险并保证了交易的顺利进行。

可选地,在本发明的一些可能的实施方式中,所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据,包括:

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据还可以通过其它以一定的编码规则形成的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可以理解，利用主机卡模拟手机钱包对应的个人识别密码（主机 HCE 钱包 PIN 码）对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密符合 NFC 交易中的密码设置方式，保证密码安全性。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后，所述方法还包括：

检测所述终端当前的状态；

若检测到所述终端当前的状态为安全状态，开启所述主机卡模拟交易通道；
解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

可选地，在本发明的一些可能的实施方式中，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，继续以一定的频率检测终端当前的状态。

可以理解，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，再持续不断地以一定的频率检测终端当前的状态，并在终端当前的状态为安全状态后，开启 HCE 模拟交易通道，并恢复 HCE 模拟 SE 应用及相关认证信息数据，从而可以在终端的安全状态恢复后，及时恢复 HCE 模拟交易通道。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现开启 HCE 卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，恢复 HCE 模拟交易通道时，可以解密并解压主机卡模拟安全模块应用及与其相关的认证信息数据。

可选地，在本发明的一些可能的实施方式中，若检测到所述终端当前的状态为安全状态，则再次将 HCE 卡模拟交易通道从 SE 实体中路由到 HCE 卡模拟交易通道中。

举例说明，在手机 NFC 支付时，当系统被 Root 后，对模拟支付通道进行关

闭并将 HCE 模拟 SE 应用以及相关认证信息数据进行保护,同时将 HCE 模拟交易通路由到实体 SE 模拟中后,继续检测终端的安全状态,当检测到终端的不安全因素已经排除后,则开启原有的 HCE 模拟支付通道,将相关应用及数据进行释放,并再次将交易通道从实体 SE 路由到 HCE 模拟支付通道中,恢复 HCE 卡模拟交易功能。

为了便于更好理解和实施本发明实施例的上述方案,下面结合一些具体的应用场景进行举例说明。

请参见图 2,图 2 是本发明的另一个实施例提供的另一种安全控制方法的流程示意图,其中,如图 2 所示,本发明的另一个实施例提供的另一种安全控制方法可以包括:

S201、检测终端当前的状态。

其中,终端为手机、平板电脑等能安装 Android 系统的智能终端,支持 HCE,具备 NFC 功能。终端当前的状态指终端当前的运行环境的状态,比如是否安全等。

其中,HCE 指基于主机的卡模拟,在配备 NFC 功能的终端上实现卡模拟时,不需要提供 SE,由在终端上运行的一个应用或者云端的服务器来完成 SE 的功能,此时 NFC 芯片接收到的数据由操作系统、或发送至终端中的应用、或通过移动网络发送至云端的服务器来完成交互。例如,在 NFC 手机中,可以通过手机中的应用来模拟安全模块 SE。

其中,安全模块 SE 指用于存储 NFC 应用和用户敏感数据以及实现安全密钥运算的芯片模块,是 NFC 卡模拟的核心,安全模块还通过非接前端与外部读写设备进行通信,实现数据存储及交易过程的安全性。

可选地,在本发明的一些可能的实施方式中,NFC 终端可包括硬件安全模块 SE,提供对敏感信息的安全存储和为交易事务提供一个安全的执行环境,其中,SE 可以集成到 SIM 卡、SD 卡或终端芯片中。

可选地,在本发明的一些可能的实施方式中,可在具有 NFC 功能的终端上安装 Android4.4 系统,由于 Android4.4 系统支持 HCE 功能,从而可在 Android4.4 系统上实现 HCE 功能,利用 HCE 模拟 SE 应用。

可选地,在本发明的其它一些可能的实施方式中,如果具有 NFC 功能的终端系统是 Android4.4 之前的版本,则可以将终端系统升级到 Android4.4 系统。

从而可以实现对 HCE 功能的支持。

可选地，在本发明的一些可能的实施方式中，支持 HCE 功能的终端可在终端上用 APP (Application, 应用程序) 应用程序模拟卡，实现主机卡模拟的功能，同时该终端也支持其它传统的 SE 方案，如硬件 SE 模块，也即终端同时兼容 HCE 和传统的 SE。

举例进行说明，在本发明的一些可能的实施方式中，对于一个具有 NFC 功能的 Android4.4 系统的手机终端，支持 HCE 功能，从而可通过 HCE 实现对 SE 的卡模块，同时该手机终端上具有硬件 SE 模块，所以可以理解，该手机终端同时兼容 HCE 卡模拟以及传统的硬件 SE 功能。

可选地，在本发明的一些可能的实施方式中，终端当前的状态可以为安全状态，也可以为不安全状态。

可选地，在本发明的一些可能的实施方式中，终端在 HCE 模拟交易通道开启后，以一定的频率检测终端当前的安全状态。

可选地，在本发明的一些可能的实施方式中，所述检测终端当前的状态包括以下方式中的至少一种：

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

其中，终端当前的安全状态包括终端自身运行环境是否安全以及终端运行的软件是否合格，当检测到终端系统被获取超级用户权限或终端安装的应用受到病毒入侵时，判断为终端自身的运行环境不安全，也即终端的状态为不安全状态，此时关闭 HCE 卡模拟交易通道。

可以理解，在上述几种情况下将会使得终端运行的应用及数据的安全受到威胁，如终端正在进行支付时，若终端被获取到超级用户权限，则和支付相关的信息将会被获取，支付交易不安全。

可选地，在本发明其它的一些可能的实施方式中，所述检测终端当前的状态还可以包括其它检测影响终端运行环境安全的情况。

S202、若检测到终端当前的状态为不安全状态，则关闭主机卡模拟交易通道。

其中，不安全状态指终端的运行环境不安全，导致运行在终端当前的数据有可能被窃取或者破坏，从而导致终端当前所进行的交易不安全，如终端系统

被 Root、终端安装的应用否受到病毒入侵等。

其中，主机卡模块交易通道（即 HCE 卡模拟交易通道）是指利用 HCE 技术模拟 SE 安全模块完成 NFC 交易的通道，此时 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到模拟 SE 的应用，然后由模拟 SE 的应用进行回复。而传统的基于硬件的 NFC 交易通道是 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到 SE，然后由 SE 进行回复。

例如，在一部具有 HCE 功能的 NFC 手机中，通过 APP 应用模拟 SE，从而实现 HCE 模拟交易通道，即主机卡模拟交易通道。

举例说明，在本发明的一些可能的实施方式中，当终端为手机时，利用手机 NFC 进行支付，当手机的系统被 Root 后，存储在手机系统中的数据很容易被窃取或破坏，此时终端的当前状态为不安全状态，那么关闭 HCE 模拟交易通道，从而终止该通道所进行的支付交易。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现关闭 HCE 卡模拟交易通道。

可以理解，关闭主机卡模拟交易通道可以在终端当前状态为不安全状态时不再使用该交易通道进行交易，从而阻止了不安全交易的发生。

可选地，在本发明的一些可能的实施方式中，所述方法还包括：

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用，则拒绝所述应用访问所述主机卡模拟交易通道。

可以理解，若检测到所述终端安装的应用为非官方发布应用、合法应用或无权限应用时，此时只是终端的应用不合格，而终端本身不存在 Root 或其它安全风险时，此时只限制该应用对 HCE 卡模拟交易通道的访问，而不去关闭 HCE 卡模拟交易通道，使得操作简单，也能不影响其它官方应用、合法应用以及有权限应用对 HCE 卡模拟交易通道的访问。

S203、加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

其中，在 NFC 终端中，主机卡模拟安全模块应用（即 HCE 模拟 SE 应用）指在具有 HCE 卡模拟功能的终端上模拟 SE 安全模块的 APP 应用，与其相关的认证信息数据是指存储在 HCE 模拟 SE 应用中的 NFC 交易中用于认证的数据和用户敏感数据。例如，在 NFC 支付中，该认证信息数据可以为支付双方的用户信息、密码、以及与支付相关的其它数据等。

可选地，在本发明的一些可能的实施方式中，也可以压缩并加密 HCE 卡模拟安全模块应用及与其相关的认证信息数据，从而保证交易数据的安全性。

举例说明，在手机 NFC 移动支付时，若支付环境出现安全风险，此时关闭 HCE 模拟支付通道，并将与支付相关的用户信息、密码以及其它相关的数据进行加密并压缩，保证数据的安全性。

可以理解，通过一定的方式加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据将加强这些数据的安全性。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，包括：

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据还可以通过其它以一定的编码规则形成的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可以理解，利用主机卡模拟手机钱包对应的个人识别密码（主机 HCE 钱包 PIN 码）对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密符合 NFC 交易中的密码设置方式，保证密码安全性。

S204、将主机卡模拟交易通道路由到安全模块实体中。

可以理解，当终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，从而 NFC 交易则无法进行，那么此时将 HCE 卡模拟交易通道路由到传统的 SE 模块中保证了交易的顺利进行，同时保证了数据的安全性。

可选地，在本发明的一些可能的实施方式中，所述安全模块实体为硬件实体 SE 模块。

举例说明，在本发明的一些可能的实施方式中，当利用手机进行 NFC 移动支付时，若检测到手机被 Root，为了保证支付的安全性，关闭 HCE 模拟交易通道，加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，并同时 will HCE 模拟交易通道路由到实体 SE 中，从而消除了支付风险并保证了交易的顺利进行。

S205、再次检测终端当前的状态。

可选地，在本发明的一些可能的实施方式中，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，继续以一定的频率检测终端当前的状态。

可以理解，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，再持续不断地以一定的频率检测终端当前的状态，可以实时观察终端的状态，在终端的状态发生改变时及时做出响应。

S206、若检测到终端当前的状态为安全状态，开启主机卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现开启 HCE 卡模拟交易通道。

可选地，若再次检测到终端当前的状态为不安全状态时，不进行任何动作。

S207、解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

可选地，在本发明的一些可能的实施方式中，若保护主机卡模拟安全模块应用及与其相关的认证信息数据的动作为压缩并加密时，可以解密并解压主机卡模拟安全模块应用及与其相关的认证信息数据。

可以理解，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，再持续不断地以一定的频率检测终端当前的状态，并在终端当前的状态为安全状态后，开启 HCE 模拟交易通道，并恢复 HCE 模拟 SE 应用及相关认证信息数据，从而可以在终端的安全状态恢复后，及时恢复 HCE 模拟交易通道。

可选地，在本发明的一些可能的实施方式中，解密主机卡模拟安全模块应用及与其相关的认证信息数据的密码为加密主机卡模拟安全模块应用及与其相关的认证信息数据时的密码，一般为主机 HCE 钱包 PIN 码。

举例说明，在手机 NFC 支付时，当系统被 Root 后，对模拟支付通道进行关闭并将 HCE 模拟 SE 应用以及相关认证信息数据进行保护，同时将 HCE 模拟交易通道路由到实体 SE 模拟中后，继续检测终端的安全状态，当检测到终端的不安全因素已经排除后，则开启原有的 HCE 模拟支付通道，将相关应用及数据进行释放，并再次将交易通道从实体 SE 路由到 HCE 模拟支付通道中，恢复 HCE 卡模拟交易功能。

可以看出, 本实施例的方案中, 检测终端当前的状态; 若检测到所述终端当前的状态为不安全状态, 则关闭主机卡模拟交易通道, 从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道; 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据, 实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

下面再举例一个更为具体的应用场景。

例如, 当终端为安装 Android4.4 系统的手机时, 具有 NFC 功能, 支持 HCE 技术, 从而可在手机上通过 HCE 模拟 SE 应用来实现 NFC 的软件模拟。当利用 NFC 进行移动支付时, 首先检测手机的状态, 如手机是否被 Root、支付软件是否官方发布、手机上安装的软件是否受到病毒入侵等, 若检测到手机被 Root, 用户可以取得系统的最高权限, 从而就可以取得存储的 SE 或认证信息, 恶意用户可能通过其它方式访问终端的存储系统, 并且获取存储于应用中的敏感数据去完成一些伪卡的交易, 这将会给支付者带来极大的安全风险, 所以手机在检测到该安全风险后, 再通过 NFC 控制器关闭 HCE 卡模拟交易通道, 同时通过 HCE 手机钱包对应的 PIN 码加密并压缩存储 HCE 模拟 SE 应用及相关认证数据信息, 保证数据的安全性。

更进一步地, 当检测到支付软件为非官方发布软件时, 拒绝该支付软件访问 HCE 卡模拟交易通道, 从而可以杜绝支付软件带来的不安全因素。

更进一步地, 当关闭 HCE 卡模拟交易通道后, 可以将 HCE 卡模拟交易通道路由到 SE 实体中。

更进一步地, 当关闭手机 Root 权限后, 再次检测手机的状态是否安全时, 此时将检测到手机的状态为安全状态, 恢复 HCE 卡模拟交易通道, 同时解压并解密 HCE 模拟 SE 应用及相关认证数据信息, 此时不再由实体 SE 进行 NFC 交易。

请参见图 3, 图 3 是本发明的一个实施例提供的一种安全控制装置的结构示意图, 其中, 如图 3 所示, 本发明的一个实施例提供的一种安全控制装置 300 可以包括:

第一检测模块 310、关闭模块 320 和加密模块 330。

其中, 第一检测模块 310 用于检测终端当前的状态。

其中, 终端为手机、平板电脑等能安装 Android 系统的智能终端, 支持 HCE,

具备 NFC 功能。终端当前的状态指终端当前的运行环境的状态，比如是否安全等。

其中，HCE 指基于主机的卡模拟，在配备 NFC 功能的终端上实现卡模拟时，不需要提供 SE，由在终端上运行的一个应用或者云端的服务器来完成 SE 的功能，此时 NFC 芯片接收到的数据由操作系统、或发送至终端中的应用、或通过移动网络发送至云端的服务器来完成交互。例如，在 NFC 手机中，可以通过手机中的应用来模拟安全模块 SE。

其中，安全模块 SE 指用于存储 NFC 应用和用户敏感数据以及实现安全密钥运算的芯片模块，是 NFC 卡模拟的核心，安全模块还通过非接前端与外部读写设备进行通信，实现数据存储及交易过程的安全性。

可选地，在本发明的一些可能的实施方式中，NFC 终端可包括硬件安全模块 SE，提供对敏感信息的安全存储和为交易事务提供一个安全的执行环境，其中，SE 可以集成到 SIM 卡、SD 卡或终端芯片中。

可选地，在本发明的一些可能的实施方式中，可在具有 NFC 功能的终端上安装 Android4.4 系统，由于 Android4.4 系统支持 HCE 功能，从而可在 Android4.4 系统上实现 HCE 功能，利用 HCE 模拟 SE 应用。

可选地，在本发明的其它一些可能的实施方式中，如果具有 NFC 功能的终端系统是 Android4.4 之前的版本，则可以将终端系统升级到 Android4.4 系统。从而可以实现对 HCE 功能的支持。

可选地，在本发明的一些可能的实施方式中，支持 HCE 功能的终端可在终端上用 APP (Application, 应用程序) 应用程序模拟卡，实现主机卡模拟的功能，同时该终端也支持其它传统的 SE 模拟卡技术，如硬件 SE 模块，也即终端同时兼容 HCE 和传统的 SE。

举例进行说明，对于一个具有 NFC 功能的 Android4.4 系统的手机终端，支持 HCE 功能，从而可通过 HCE 实现对 SE 的卡模块，同时该手机终端上具有硬件 SE 模块，所以可以理解，该手机终端同时兼容 HCE 卡模拟以及传统的硬件 SE 功能。

可选地，在本发明的一些可能的实施方式中，终端当前的状态可以为安全状态，也可以为不安全状态。

可选地，在本发明的一些可能的实施方式中，终端在 HCE 模拟交易通道开

启后，以一定的频率检测终端当前的安全状态。

关闭模块 320，用于若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道。

其中，不安全状态指终端的运行环境不安全，导致运行在终端当前的数据有可能被窃取或者破坏，从而导致终端当前所进行的交易不安全。

其中，主机卡模块交易通道（即 HCE 卡模拟交易通道）是指利用 HCE 技术模拟 SE 安全模块完成 NFC 交易的通道，此时 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到模拟 SE 的应用，然后由模拟 SE 的应用进行回复。而传统的基于硬件的 NFC 交易通道是 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到 SE，然后由 SE 进行回复。

例如，在一部具有 HCE 功能的 NFC 手机中，通过 APP 应用模拟 SE，从而实现 HCE 模拟交易通道，即主机卡模拟交易通道。

举例说明，在本发明的一些可能的实施方式中，当终端为手机时，利用手机 NFC 进行支付，当手机的系统被 Root 后，存储在手机系统中的数据很容易被窃取或破坏，此时终端的当前状态为不安全状态，那么关闭 HCE 模拟交易通道，从而终止该通道所进行的支付交易。

可以理解，关闭主机卡模拟交易通道可以在终端当前状态为不安全状态时不再使用该交易通道进行交易，从而阻止了不安全交易的发生。

加密模块 330，用于加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

其中，在 NFC 终端中，主机卡模拟安全模块应用（即 HCE 模拟 SE 应用）指在具有 HCE 卡模拟功能的终端上模拟 SE 安全模块的 APP 应用，与其相关的认证信息数据是指存储在 HCE 模拟 SE 应用中的 NFC 交易中用于认证的数据和用户敏感数据。例如，在 NFC 支付中，该认证信息数据可以为支付双方的用户信息、密码、以及与支付相关的其它数据等。

可选地，在本发明的一些可能的实施方式中，也可以压缩并加密 HCE 卡模拟安全模块应用及与其相关的认证信息数据，从而保证交易数据的安全性。

举例说明，在手机 NFC 移动支付时，若支付环境出现安全风险，此时关闭 HCE 模拟支付通道，并将与支付相关的用户信息、密码以及其它相关的数据进行加密并压缩，保证数据的安全性。

可以理解,通过一定的方式加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据将加强这些数据的安全性。

可以理解的是,本实施例的安全控制装置 300 的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

可以看出,本实施例的方案中,安全控制装置 300 检测终端当前的状态;安全控制装置 300 若检测到所述终端当前的状态为不安全状态,则关闭主机卡模拟交易通道,从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道;安全控制装置 300 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据,实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

请参见图 4,图 4 是本发明的另一个实施例提供的另一种安全控制装置的结构示意图,其中,如图 4 所示,本发明的另一个实施例提供的另一种安全控制装置 400 可以包括:

第一检测模块 410、关闭模块 420 和加密模块 430。

其中,第一检测模块 410 用于检测终端当前的状态。

其中,终端为手机、平板电脑等能安装 Android 系统的智能终端,支持 HCE,具备 NFC 功能。终端当前的状态指终端当前的运行环境的状态,比如是否安全等。

其中,HCE 指基于主机的卡模拟,在配备 NFC 功能的终端上实现卡模拟时,不需要提供 SE,由在终端上运行的一个应用或者云端的服务器来完成 SE 的功能,此时 NFC 芯片接收到的数据由操作系统、或发送至终端中的应用、或通过移动网络发送至云端的服务器来完成交互。例如,在 NFC 手机中,可以通过手机中的应用来模拟安全模块 SE。

其中,安全模块 SE 指用于存储 NFC 应用和用户敏感数据以及实现安全密钥运算的芯片模块,是 NFC 卡模拟的核心,安全模块还通过非接前端与外部读写设备进行通信,实现数据存储及交易过程的安全性。

可选地,在本发明的一些可能的实施方式中,NFC 终端可包括硬件安全模块 SE,提供对敏感信息的安全存储和为交易事务提供一个安全的执行环境,其中,SE 可以集成到 SIM 卡、SD 卡或终端芯片中。

可选地，在本发明的一些可能的实施方式中，可在具有 NFC 功能的终端上安装 Android4.4 系统，由于 Android4.4 系统支持 HCE 功能，从而可在 Android4.4 系统上实现 HCE 功能，利用 HCE 模拟 SE 应用。

可选地，在本发明的其它一些可能的实施方式中，如果具有 NFC 功能的终端系统是 Android4.4 之前的版本，则可以将终端系统升级到 Android4.4 系统。从而可以实现对 HCE 功能的支持。

可选地，在本发明的一些可能的实施方式中，支持 HCE 功能的终端可在终端上用 APP (Application, 应用程序) 应用程序模拟卡，实现主机卡模拟的功能，同时该终端也支持其它传统的 SE 模拟卡技术，如硬件 SE 模块，也即终端同时兼容 HCE 和传统的 SE。

举例进行说明，对于一个具有 NFC 功能的 Android4.4 系统的手机终端，支持 HCE 功能，从而可通过 HCE 实现对 SE 的卡模块，同时该手机终端上具有硬件 SE 模块，所以可以理解，该手机终端同时兼容 HCE 卡模拟以及传统的硬件 SE 功能。

可选地，在本发明的一些可能的实施方式中，终端当前的状态可以为安全状态，也可以为不安全状态。

可选地，在本发明的一些可能的实施方式中，终端在 HCE 模拟交易通道开启后，以一定的频率检测终端当前的安全状态。

关闭模块 420，用于若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道。

其中，不安全状态指终端的运行环境不安全，导致运行在终端当前的数据有可能被窃取或者破坏，从而导致终端当前所进行的交易不安全。

其中，主机卡模块交易通道（即 HCE 卡模拟交易通道）是指利用 HCE 技术模拟 SE 安全模块完成 NFC 交易的通道，此时 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到模拟 SE 的应用，然后由模拟 SE 的应用进行回复。而传统的基于硬件的 NFC 交易通道是 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到 SE，然后由 SE 进行回复。

例如，在一部具有 HCE 功能的 NFC 手机中，通过 APP 应用模拟 SE，从而实现 HCE 模拟交易通道，即主机卡模拟交易通道。

举例说明，在本发明的一些可能的实施方式中，当终端为手机时，利用手

机 NFC 进行支付, 当手机的系统被 Root 后, 存储在手机系统中的数据很容易被窃取或破坏, 此时终端的当前状态为不安全状态, 那么关闭 HCE 模拟交易通道, 从而终止该通道所进行的支付交易。

可以理解, 关闭主机卡模拟交易通道可以在终端当前状态为不安全状态时不再使用该交易通道进行交易, 从而阻止了不安全交易的发生。

加密模块 430, 用于加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

其中, 在 NFC 终端中, 主机卡模拟安全模块应用 (即 HCE 模拟 SE 应用) 指在具有 HCE 卡模拟功能的终端上模拟 SE 安全模块的 APP 应用, 与其相关的认证信息数据是指存储在 HCE 模拟 SE 应用中的 NFC 交易中用于认证的数据和用户敏感数据。例如, 在 NFC 支付中, 该认证信息数据可以为支付双方的用户信息、密码、以及与支付相关的其它数据等。

可选地, 在本发明的一些可能的实施方式中, 也可以压缩并加密 HCE 卡模拟安全模块应用及与其相关的认证信息数据, 从而保证交易数据的安全性。

举例说明, 在手机 NFC 移动支付时, 若支付环境出现安全风险, 此时关闭 HCE 模拟支付通道, 并将与支付相关的用户信息、密码以及其它相关的数据进行加密并压缩, 保证数据的安全性。

可以理解, 通过一定的方式加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据将加强这些数据的安全性。

可选地, 在本发明的一些可能的实施方式中, 可由主机或者 NFC 控制器来实现关闭 HCE 卡模拟交易通道。

可选地, 在本发明的一些可能的实施方式中, 所述检测模块 410 检测终端当前的状态包括以下方式中的至少一种:

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

其中, 终端当前的安全状态包括终端自身运行环境是否安全以及终端运行的软件是否合格, 当检测到终端系统被获取超级用户权限或终端安装的应用受到病毒入侵时, 判断为终端自身的运行环境不安全, 也即终端的状态为不安全状态, 此时关闭 HCE 卡模拟交易通道。

可以理解, 在上述几种情况下将会使得终端运行的应用及数据的安全受到

威胁，如终端正在进行支付时，若终端被获取到超级用户权限，则和支付相关的信息将会被获取，支付交易不安全。

可选地，在本发明其它的一些可能的实施方式中，所述检测终端当前的状态还可以包括检测终端安装的应用是否为不合法应用或无权限应用，以及检测终端其它异常情况。

可选地，在本发明的一些可能的实施方式中，所述检测模块 410 还用于：

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用，则拒绝所述应用访问所述主机卡模拟交易通道。

可以理解，若检测到所述终端安装的应用为非官方发布应用、合法应用或无权限应用时，此时只是终端的应用不合格，而终端本身不存在 Root 或其它安全风险时，此时只限制该应用对 HCE 卡模拟交易通道的访问，而不去关闭 HCE 卡模拟交易通道，使得操作简单，也能不影响其它官方应用、合法应用以及有权限应用对 HCE 卡模拟交易通道的访问。

可选地，在本发明的一些可能的实施方式中，所述安全控制装置 400 还包括：

路由模块 440，用于将所述主机卡模拟交易通道路由到安全模块实体中。

可以理解，当终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，从而 NFC 交易则无法进行，那么此时将 HCE 卡模拟交易通道路由到传统的 SE 模块中保证了交易的顺利进行，同时保证了数据的安全性。

可选地，在本发明的一些可能的实施方式中，所述安全模块实体为硬件实体 SE 模块。

举例说明，在本发明的一些可能的实施方式中，当利用手机进行 NFC 移动支付时，若检测到手机被 Root，为了保证支付的安全性，关闭 HCE 模拟交易通道，加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，并同时 will HCE 模拟交易通道路由到实体 SE 中，从而消除了支付风险并保证了交易的顺利进行。

可选地，在本发明的一些可能的实施方式中，所述加密模块 430 具体用于：

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据还可以通过其它以一定的编码规则形成的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可以理解，利用主机卡模拟手机钱包对应的个人识别密码（主机 HCE 钱包 PIN 码）对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密符合 NFC 交易中的密码设置方式，保证密码安全性。

可选地，在本发明的一些可能的实施方式中，在所述加密模块 430 后，所述安全控制装置 400 还包括：

第二检测模块 450，用于检测所述终端当前的状态；

开启模块 460，用于若检测到所述终端当前的状态为安全状态，开启所述主机卡模拟交易通道；

解密模块 470，用于解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

其中，第二检测模块 450 可以与第一检测模块 410 不同，用于在 HCE 卡模拟交易通道关闭后检测所述终端当前的安全状态，也可以与第一检测模块 410 集成在同一个模块中，用于检测所述终端当前的状态。

可选地，在本发明的一些可能的实施方式中，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，第二检测模块 450 继续以一定的频率检测终端当前的状态。

可以理解，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，再持续不断地以一定的频率检测终端当前的状态，并在终端当前的状态为安全状态后，开启 HCE 模拟交易通道，并恢复 HCE 模拟 SE 应用及相关认证信息数据，从而可以在终端的安全状态恢复后，及时恢复 HCE 模拟交易通道。

可选地，在本发明的一些可能的实施方式中，开启模块 460 可由主机或者 NFC 控制器来实现开启 HCE 卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，恢复 HCE 模拟交易通道时，解密模块 470 可以解密并解压主机卡模拟安全模块应用及与其相关的认证信息

数据。

可选地，在本发明的一些可能的实施方式中，若检测到所述终端当前的状态为安全状态，则再次将 HCE 卡模拟交易通道从 SE 实体中路由到 HCE 卡模拟交易通道中。

举例说明，在手机 NCF 支付时，当系统被 Root 后，对模拟支付通道进行关闭并将 HCE 模拟 SE 应用以及相关认证信息数据进行保护，同时将 HCE 模拟交易通道路由到实体 SE 模拟中后，继续检测终端的安全状态，当检测到终端的不安全因素已经排除后，则开启原有的 HCE 模拟支付通道，将相关应用及数据进行释放，并再次将交易通道从实体 SE 路由到 HCE 模拟支付通道中，恢复 HCE 卡模拟交易功能。

可以理解的是，本实施例的安全控制装置 400 的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

可以看出，本实施例的方案中，安全控制装置 400 检测终端当前的状态；安全控制装置 400 若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道，从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道；安全控制装置 400 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

参见图 5，图 5 是本发明的又一个实施例提供的又一种安全控制装置的结构示意图。如图 5 所示，本发明的又一个实施例提供的又一种安全控制装置 500 可以包括：至少一个总线 501、与总线相连的至少一个处理器 502 以及与总线相连的至少一个存储器 503。

其中，处理器 502 通过总线 501，调用存储器 503 中存储的代码以用于检测终端当前的状态；若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

其中，终端为手机、平板电脑等能安装 Android 系统的智能终端，支持 HCE，具备 NFC 功能。终端当前的状态指终端当前的运行环境的状态，比如是否安全等。

其中, HCE 指基于主机的卡模拟, 在配备 NFC 功能的终端上实现卡模拟时, 不需要提供 SE, 由在终端上运行的一个应用或者云端的服务器来完成 SE 的功能, 此时 NFC 芯片接收到的数据由操作系统、或发送至终端中的应用、或通过移动网络发送至云端的服务器来完成交互。例如, 在 NFC 手机中, 可以通过手机中的应用来模拟安全模块 SE。

其中, 安全模块 SE 指用于存储 NFC 应用和用户敏感数据以及实现安全密钥运算的芯片模块, 是 NFC 卡模拟的核心, 安全模块还通过非接前端与外部读写设备进行通信, 实现数据存储及交易过程的安全性。

可选地, 在本发明的一些可能的实施方式中, NFC 终端可包括硬件安全模块 SE, 提供对敏感信息的安全存储和为交易事务提供一个安全的执行环境, 其中, SE 可以集成到 SIM 卡、SD 卡或终端芯片中。

可选地, 在本发明的一些可能的实施方式中, 可在具有 NFC 功能的终端上安装 Android4.4 系统, 由于 Android4.4 系统支持 HCE 功能, 从而可在 Android4.4 系统上实现 HCE 功能, 利用 HCE 模拟 SE 应用。

可选地, 在本发明的其它一些可能的实施方式中, 如果具有 NFC 功能的终端系统是 Android4.4 之前的版本, 则可以将终端系统升级到 Android4.4 系统。从而可以实现对 HCE 功能的支持。

可选地, 在本发明的一些可能的实施方式中, 支持 HCE 功能的终端可在终端上用 APP (Application, 应用程序) 应用程序模拟卡, 实现主机卡模拟的功能, 同时该终端也支持其它传统的 SE 模拟卡技术, 如硬件 SE 模块, 也即终端同时兼容 HCE 和传统的 SE。

可选地, 在本发明的一些可能的实施方式中, 终端当前的状态可以为安全状态, 也可以为不安全状态。

可选地, 在本发明的一些可能的实施方式中, 终端在 HCE 模拟交易通道开启后, 以一定的频率检测终端当前的安全状态。

其中, 不安全状态指终端的运行环境不安全, 导致运行在终端当前的数据有可能被窃取或者破坏, 从而导致终端当前所进行的交易不安全。

其中, 主机卡模块交易通道 (即 HCE 卡模拟交易通道) 是指利用 HCE 技术模拟 SE 安全模块完成 NFC 交易的通道, 此时 NFC 芯片作为非接触通讯前端, 将从外部读写器接收到命令, 转发到模拟 SE 的应用, 然后由模拟 SE 的应用进

行回复。而传统的基于硬件的 NFC 交易通道是 NFC 芯片作为非接触通讯前端，将从外部读写器接收到命令，转发到 SE，然后由 SE 进行回复。

其中，在 NFC 终端中，主机卡模拟安全模块应用（即 HCE 模拟 SE 应用）指在具有 HCE 卡模拟功能的终端上模拟 SE 安全模块的 APP 应用，与其相关的认证信息数据是指存储在 HCE 模拟 SE 应用中的 NFC 交易中用于认证的数据和用户敏感数据。例如，在 NFC 支付中，该认证信息数据可以为支付双方的用户信息、密码、以及与支付相关的其它数据等。

可选地，在本发明的一些可能的实施方式中，也可以压缩并加密 HCE 卡模拟安全模块应用及与其相关的认证信息数据，从而保证交易数据的安全性。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现关闭 HCE 卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，处理器 502 检测终端当前的状态包括以下方式中的至少一种：

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

其中，终端当前的安全状态包括终端自身运行环境是否安全以及终端运行的软件是否合格，当检测到终端系统被获取超级用户权限或终端安装的应用受到病毒入侵时，判断为终端自身的运行环境不安全，也即终端的状态为不安全状态，此时关闭 HCE 卡模拟交易通道。

可选地，在本发明其它的一些可能的实施方式中，所述检测终端当前的状态还可以包括其它检测影响终端运行环境安全的情况。

可选地，在本发明其它的一些可能的实施方式中，所述检测终端当前的状态还可以包括检测终端安装的应用是否为不合法应用或无权限应用，以及检测终端其它异常情况。

可选地，在本发明的一些可能的实施方式中，处理器 502 还可以：

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用，则拒绝所述应用访问所述主机卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，处理器 502 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后，处理器 502 还可以：

将所述主机卡模拟交易通道路由到安全模块实体中。

可选地，在本发明的一些可能的实施方式中，所述安全模块实体为硬件实体 SE 模块。

可选地，在本发明的一些可能的实施方式中，处理器 502 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，处理器 502 可以：

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可选地，在本发明的一些可能的实施方式中，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据还可以通过其它以一定的编码规则形成的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

可选地，在本发明的一些可能的实施方式中，处理器 502 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后，处理器 502 还包括：

检测所述终端当前的状态；

若检测到所述终端当前的状态为安全状态，开启所述主机卡模拟交易通道；
解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

可选地，在本发明的一些可能的实施方式中，在终端当前的状态为不安全状态时，关闭 HCE 卡模拟交易通道，并同时加密并压缩 HCE 模拟 SE 应用以及与其相关的认证信息数据后，继续以一定的频率检测终端当前的状态。

可选地，在本发明的一些可能的实施方式中，可由主机或者 NFC 控制器来实现开启 HCE 卡模拟交易通道。

可选地，在本发明的一些可能的实施方式中，恢复 HCE 模拟交易通道时，处理器 502 可以解密并解压主机卡模拟安全模块应用及与其相关的认证信息数据。

可选地，在本发明的一些可能的实施方式中，若检测到所述终端当前的状态为安全状态，处理器 502 则再次将 HCE 卡模拟交易通道从 SE 实体中路由到 HCE 卡模拟交易通道中。

可以理解的是，本实施例的安全控制装置 500 的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

可以看出，本实施例的方案中，安全控制装置 500 检测终端当前的状态；

安全控制装置 500 若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道，从而在终端状态为不安全状态时不再继续使用主机卡模拟交易通道；安全控制装置 500 加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，实现了对交易过程中数据的保护。从而在基于主机卡模拟的技术下实现了对 NFC 业务的安全控制。

参见图 6，图 6 是本发明的一个实施例提供的终端。本发明还提供了一种终端 500，包括如上述任一技术方案所述的安全控制装置 400。

本发明实施例还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时包括上述方法实施例中记载的任何一种消息交互方法的部分或全部步骤。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中沒有详述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明的各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元

中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、只读存储器（ROM, Read-Only Memory）、随机存取存储器（RAM, Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权 利 要 求 书

1、一种安全控制方法，其特征在于，所述方法包括：

检测终端当前的状态；

若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；
加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据。

2、如权利要求1所述的方法，其特征在于，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后，所述方法还包括：

将所述主机卡模拟交易通道路由到安全模块实体中。

3、如权利要求1所述的方法，其特征在于，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据后，所述方法还包括：

检测所述终端当前的状态；

若检测到所述终端当前的状态为安全状态，开启所述主机卡模拟交易通道；
解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

4、如权利要求1或3所述的方法，其特征在于，所述检测终端当前的状态包括以下方式中的至少一种：

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

5、如权利要求1所述的方法，其特征在于，所述加密并压缩主机卡模拟安全模块应用及与其相关的认证信息数据，包括：

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

6、如权利要求1所述的方法，其特征在于，所述方法还包括：

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用，则拒绝所述应用访问所述主机卡模拟交易通道。

7、一种安全控制装置，其特征在于，所述装置包括：

第一检测模块，用于检测终端当前的状态；

关闭模块，用于若检测到所述终端当前的状态为不安全状态，则关闭主机卡模拟交易通道；

加密模块，用于加密并压缩主机卡模拟安全模块应用及与其相关的认证信

息数据。

8、如权利要求 7 所述的装置，其特征在于，所述装置还包括：

路由模块，用于将所述主机卡模拟交易通道路由到安全模块实体中。

9、如权利要求 7 所述的装置，其特征在于，在所述加密模块后，所述装置还包括：

第二检测模块，用于检测所述终端当前的状态；

开启模块，用于若检测到所述终端当前的状态为安全状态，开启所述主机卡模拟交易通道；

解密模块，用于解压并解密主机卡模拟安全模块应用及与其相关的认证信息数据。

10、如权利要求 6 或 9 所述的装置，其特征在于，所述检测模块检测终端当前的状态包括以下方式中的至少一种：

检测所述终端系统是否被获取超级用户权限、检测所述终端安装的应用是否官方发布、检测所述终端安装的应用是否受到病毒入侵。

11、如权利要求 7 所述的装置，其特征在于，所述加密模块具体用于：

通过主机卡模拟手机钱包对应的个人识别密码或用户自设定的密码对所述主机卡模拟安全模块应用及与其相关的认证信息数据进行加密。

12、如权利要求 7 所述的装置，其特征在于，所述检测模块还用于：

若检测到所述终端安装的应用为非官方发布应用、不合法应用或无权限应用，则拒绝所述应用访问所述主机卡模拟交易通道。

13、一种终端，其特征在于，包括如权利要求 7 至 12 中任一项所述的安全控制装置。

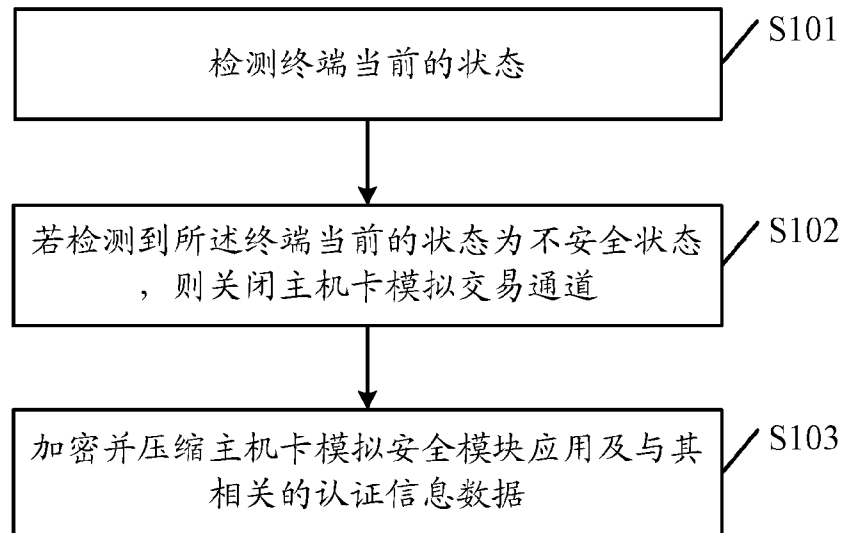


图 1

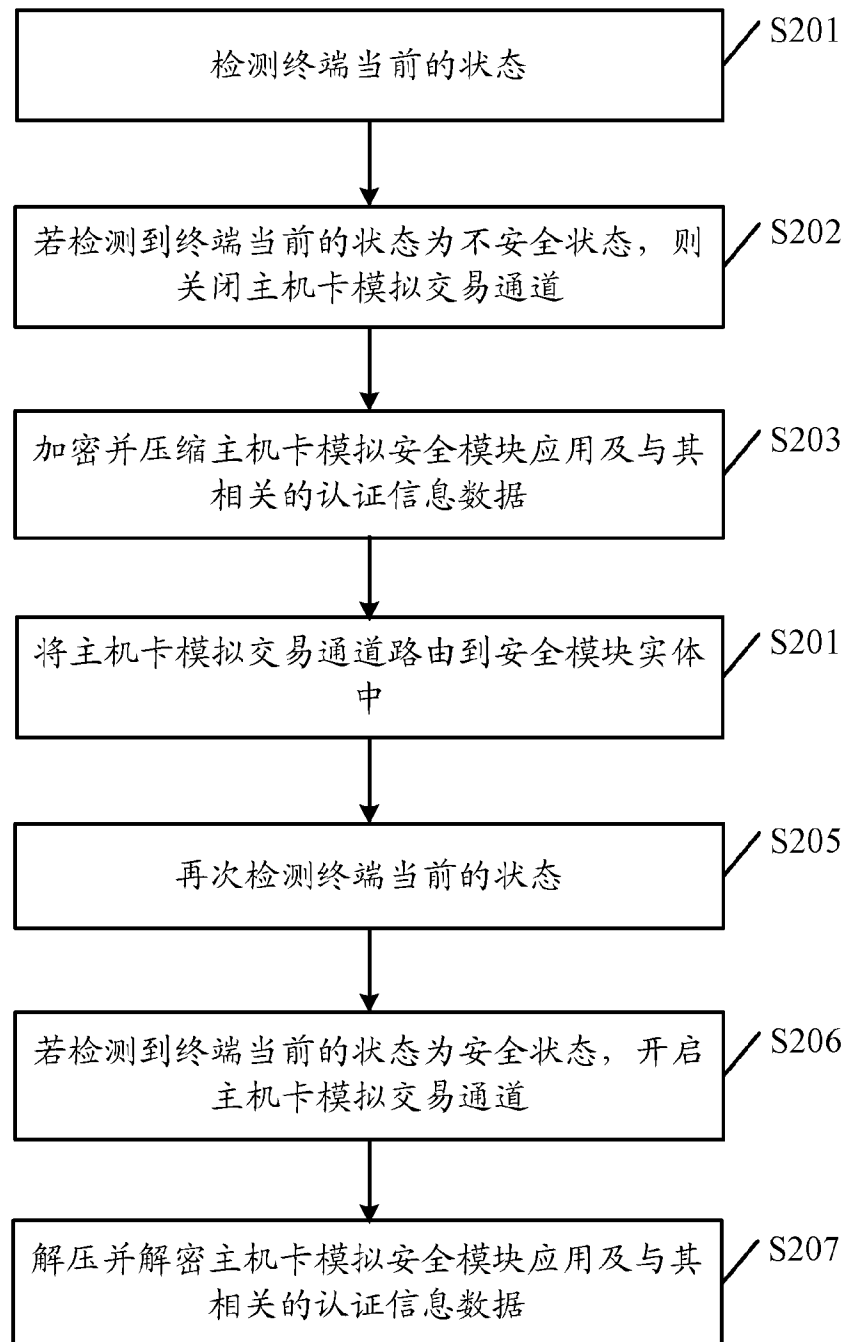


图 2

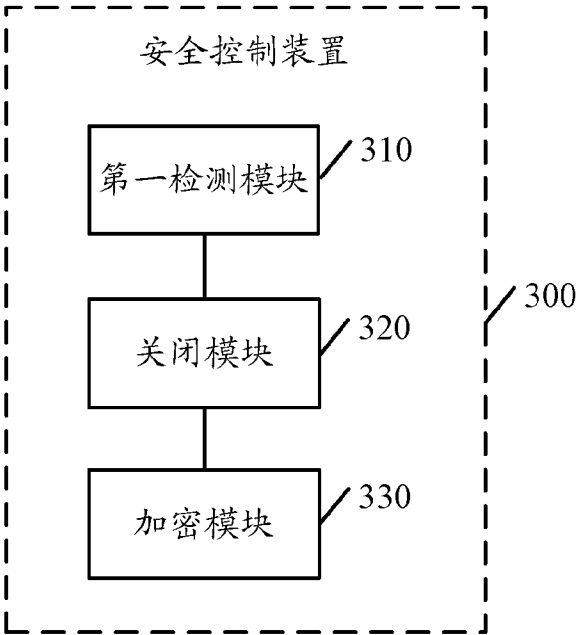


图 3

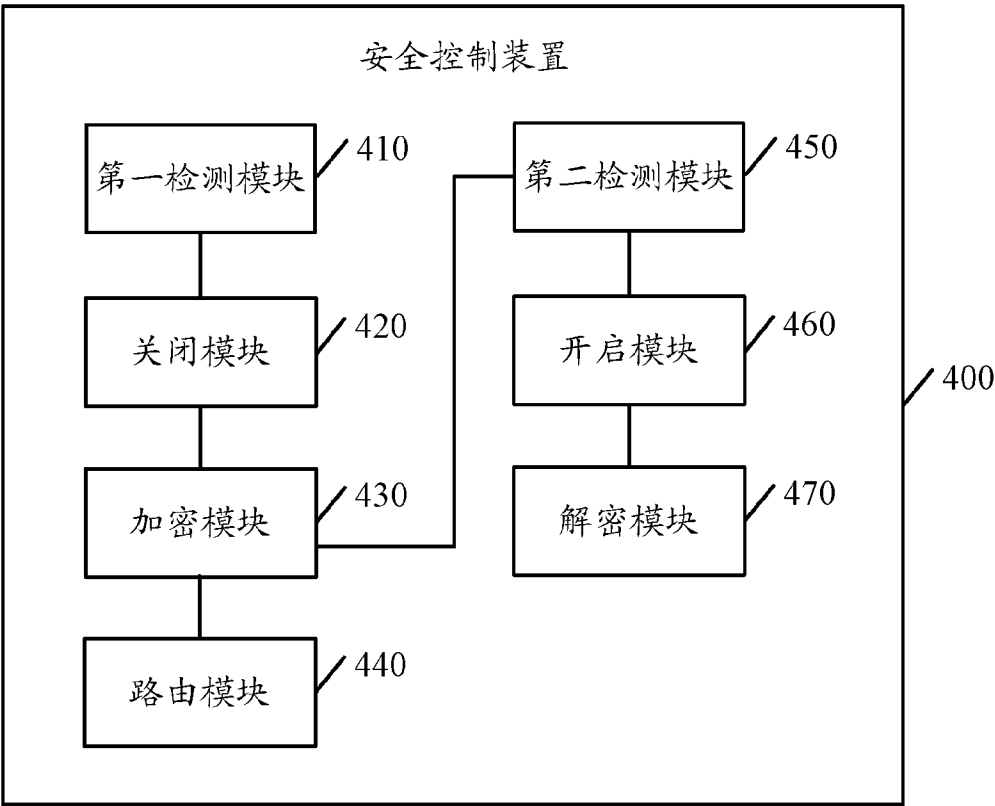


图 4

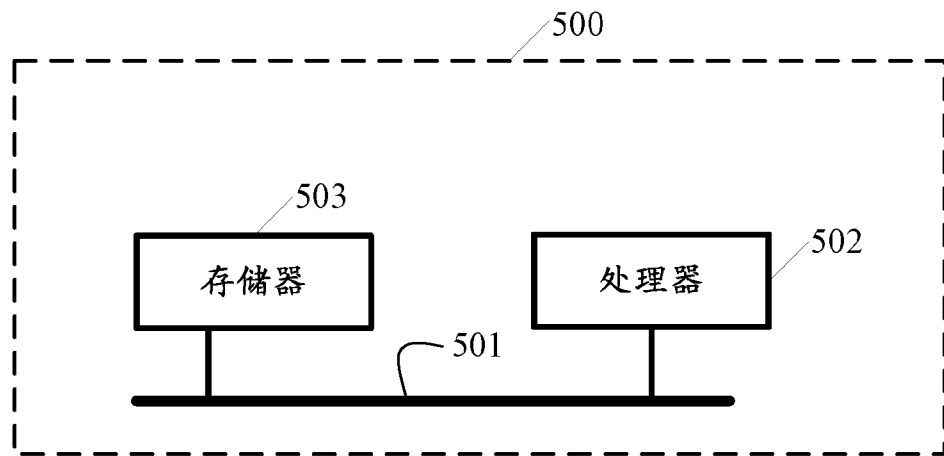


图 5

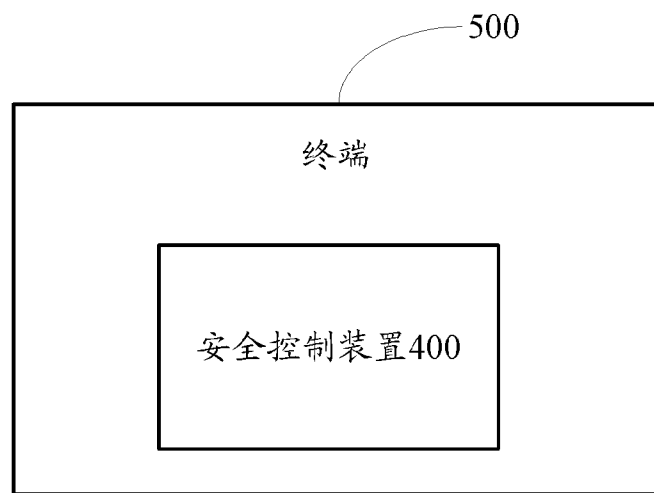


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/077958

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, EPODOC, WPI, GOOGLE, CNKI: secure, pay, terminal, status, close, detection, stop, encrypt, compress, application, authentication, password, accounts, HCE, NFC, SE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104240085 A (ZTE CORP.), 24 December 2014 (24.12.2014), description, paragraphs [0002] and [0004]-[0015]	1-13
Y	CN 103617382 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 05 March 2014 (05.03.2014), description, paragraphs [0003]-[0007]	1-13
Y	CN 101079090 A (FEITIAN TECHNOLOGIES CO., LTD.), 28 November 2007 (28.11.2007), description, page 3, paragraph 4 to page 4, paragraph 2 and page 6, paragraph 2	1-13
A	US 2015006319 A1 (BARKLEY, INC.), 01 January 2015 (01.01.2015), the whole document	1-13

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 06 June 2016 (06.06.2016)	Date of mailing of the international search report 28 June 2016 (28.06.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer MA, Lili Telephone No.: (86-10) 62413996

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/077958

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104240085 A	24 December 2014	WO 2014194592 A1	11 December 2014
		EP 3007363 A1	13 April 2016
		US 2016150408 A1	26 May 2016
CN 103617382 A	05 March 2014	None	
CN 101079090 A	28 November 2007	CN 101079090 B	21 April 2010
US 2015006319 A1	01 January 2015	None	

国际检索报告

国际申请号

PCT/CN2016/077958

A. 主题的分类

G06Q 20/32 (2012.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNPAT, EPDOC, WPI, GOOGLE, CNKI: 安全, 支付, 终端, 状态, 关闭, 检测, 停止, 加密, 压缩, 应用, 认证, 密码, 帐号, secure, pay, terminal, status, close, detection, stop, encrypt, compress, application, authentication, password, accounts, HCE, NFC, SE

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 104240085 A (中兴通讯股份有限公司) 2014年 12月 24日 (2014 - 12 - 24) 说明书第[0002]、[0004]-[0015]段	1-13
Y	CN 103617382 A (北京奇虎科技有限公司 等) 2014年 3月 5日 (2014 - 03 - 05) 说明书第[0003]-[0007]段	1-13
Y	CN 101079090 A (北京飞天诚信科技有限公司) 2007年 11月 28日 (2007 - 11 - 28) 说明书第3页第4段-第4页第2段, 第6页第2段	1-13
A	US 2015006319 A1 (BARKLEY, INC.) 2015年 1月 1日 (2015 - 01 - 01) 全文	1-13

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 6月 6日

国际检索报告邮寄日期

2016年 6月 28日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10) 62019451

授权官员

马丽莉

电话号码 (86-10) 62413996

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/077958

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104240085	A	2014年 12月 24日	WO	2014194592	A1	2014年 12月 11日
				EP	3007363	A1	2016年 4月 13日
				US	2016150408	A1	2016年 5月 26日
CN	103617382	A	2014年 3月 5日	无			
CN	101079090	A	2007年 11月 28日	CN	101079090	B	2010年 4月 21日
US	2015006319	A1	2015年 1月 1日	无			