



(12) 发明专利申请

(10) 申请公布号 CN 103532938 A

(43) 申请公布日 2014. 01. 22

(21) 申请号 201310456260. 5

(22) 申请日 2013. 09. 29

(71) 申请人 东莞宇龙通信科技有限公司

地址 523500 广东省东莞市松山湖科技产业  
园区北部工业城C区

申请人 宇龙计算机通信科技(深圳)有限公  
司

(72) 发明人 余文姣

(74) 专利代理机构 北京中博世达专利商标代理  
有限公司 11274

代理人 申健

(51) Int. Cl.

H04L 29/06 (2006. 01)

G06F 21/12 (2013. 01)

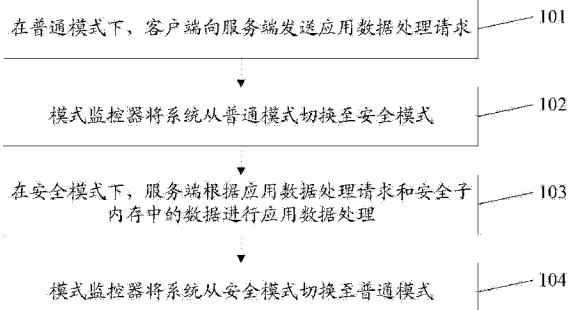
权利要求书3页 说明书8页 附图4页

(54) 发明名称

应用数据保护的方法和系统

(57) 摘要

本发明公开了一种应用数据保护的方法和系统，涉及通信技术领域，解决了对应用提供软件的保护，骇客可以利用系统漏洞攻击外设和内存来获取用户的私密信息的问题。本发明的方法可以包括：在普通模式下，客户端向服务端发送应用数据处理请求；模式监控器将系统从普通模式切换至安全模式；在安全模式下，服务端根据应用数据处理请求和安全子内存中的数据进行应用数据处理；模式监控器将系统从安全模式切换至普通模式；其中，内存被划分为安全子内存和普通子内存，在普通模式下，普通子内存中的数据允许被访问，在安全模式下，普通子内存中的数据允许被访问，且安全子内存中的数据允许被访问。可应用于应用数据的保护中。



1. 一种应用数据保护的方法,其特征在于,包括:

在普通模式下,客户端向服务端发送应用数据处理请求;

模式监控器将系统从所述普通模式切换至安全模式;

在所述安全模式下,所述服务端根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理;

所述模式监控器将所述系统从所述安全模式切换至所述普通模式;

其中,所述内存被划分为安全子内存和普通子内存,在所述普通模式下,所述普通子内存中的数据允许被所述服务端访问,在所述安全模式下,所述普通子内存中的数据允许被所述服务端访问,且安全子内存中的数据允许被所述服务端访问。

2. 根据权利要求1所述的应用数据保护的方法,其特征在于,所述模式监控器将系统从所述普通模式切换至安全模式,包括:

所述模式监控器判断所述客户端是否已向所述服务端发送了所述应用数据处理请求;

若是,则将所述系统从所述普通模式切换至所述安全模式;

所述模式监控器将所述系统从所述安全模式切换至所述普通模式,包括:

所述模式监控器判断所述客户端是否已接收所述服务端发送的应用数据处理响应,所述应用数据处理响应用于表征所述服务端已根据所述应用数据处理请求进行了应用数据处理;

若是,则将所述系统从所述安全模式切换至所述普通模式。

3. 根据权利要求1所述的应用数据保护的方法,其特征在于,在所述模式监控器将系统从所述普通模式切换至安全模式之后,所述方法还包括:

在所述安全模式下,所述模式监控器向地址控制器发送安全模式通知;

所述地址控制器根据当前待处理操作设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址;

将所述第一访问地址发送至所述服务端;

所述服务端根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理,包括:

所述服务端根据所述第一访问地址对所述普通子内存或所述安全子内存中的数据进行访问。

4. 根据权利要求3所述的应用数据保护的方法,其特征在于,所述地址控制器根据当前待处理操作设置第一访问地址,包括:

判断待处理操作是否为安全操作;

若是,则设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址;

若否,则设置第一访问地址,所述第一访问地址包括普通子内存的地址。

5. 根据权利要求1所述的应用数据保护的方法,其特征在于,在所述模式监控器将系统从所述安全模式切换至所述普通模式之后,所述方法还包括:

在所述普通模式下,所述模式监控器向地址控制器发送普通模式通知;

所述地址控制器根据当前待处理操作设置第二访问地址,所述第二访问地址包括普通

子内存的地址；

将所述第二访问地址发送至所述服务端；

所述服务端根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理，包括：

所述服务端根据所述第二访问地址对所述普通子内存中的数据进行访问。

6. 一种应用数据保护的系统，其特征在于，包括：

客户端，用于在普通模式下，向服务端发送应用数据处理请求；

所述服务端，用于在所述安全模式下，根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理；

模式监控器，用于在所述客户端向所述服务端发送所述应用数据处理请求之后，将所述系统从所述普通模式切换至安全模式；在根据所述应用数据处理请求进行应用数据处理之后，将所述系统从所述安全模式切换至所述普通模式；

其中，所述内存被划分为安全子内存和普通子内存，在所述普通模式下，所述普通子内存中的数据允许被所述服务端访问，在所述安全模式下，所述普通子内存中的数据允许被所述服务端访问，且安全子内存中的数据允许被所述服务端访问。

7. 根据权利要求 6 所述的应用数据保护的系统，其特征在于，

所述模式监控器，具体用于判断所述客户端是否已向所述服务端发送了所述应用数据处理请求；若是，则将所述系统从所述普通模式切换至所述安全模式；

所述模式监控器，具体用于判断所述客户端是否已接收所述服务端发送的应用数据处理响应，所述应用数据处理响应用于表征所述服务端已根据所述应用数据处理请求进行了应用数据处理；若是，则将所述系统从所述安全模式切换至所述普通模式。

8. 根据权利要求 6 所述的应用数据保护的系统，其特征在于，所述系统还包括：地址控制器；

所述模式监控器，还用于在所述模式监控器将系统从所述普通模式切换至安全模式之后，在所述安全模式下，向所述地址控制器发送安全模式通知；

所述地址控制器，用于根据当前待处理操作设置第一访问地址，所述第一访问地址包括如下地址中至少一项：所述安全子内存的地址、普通子内存的地址；将所述第一访问地址发送至所述服务端；

所述服务端，用于根据所述第一访问地址对所述普通子内存或所述安全子内存中的数据进行访问。

9. 根据权利要求 8 所述的应用数据保护的系统，其特征在于，所述地址控制器，具体用于判断待处理操作是否为安全操作；若是，则设置第一访问地址，所述第一访问地址包括如下地址中至少一项：所述安全子内存的地址、普通子内存的地址；若否，则设置第一访问地址，所述第一访问地址包括普通子内存的地址。

10. 根据权利要求 6 所述的应用数据保护的系统，其特征在于，所述系统还包括：地址控制器；

所述模式监控器，还用于在所述模式监控器将所述系统从所述安全模式切换至所述普通模式之后，在所述普通模式下，向所述地址控制器发送普通模式通知；

所述地址控制器，用于根据当前待处理操作设置第二访问地址，所述第二访问地址包

括普通子内存的地址；将所述第二访问地址发送至所述服务端；

所述服务端，用于根据所述第二访问地址对所述普通子内存中的数据进行访问。

## 应用数据保护的方法和系统

### 技术领域

[0001] 本发明涉及通信技术领域，尤其涉及应用数据保护的方法和系统。

### 背景技术

[0002] 当前终端系统中，可以通过软件方式对敏感的应用进行保护，并且每个应用的保护需要针对各自防御的重点进行单独设计和实现。

[0003] 在实现上述应用数据保护的过程中，发明人发现现有技术中至少存在如下问题：对应用提供软件的保护，骇客可以利用系统漏洞攻击外设和内存来获取用户的私密信息，如账号和密码等。

### 发明内容

[0004] 本发明的实施例提供一种应用数据保护的方法和系统，能够更好的对应用数据进行保护，更好的避免了应用数据被泄露。

[0005] 为达到上述目的，本发明的实施例采用如下技术方案：

[0006] 一方面，提供一种应用数据保护的方法，包括：

[0007] 在普通模式下，客户端向服务端发送应用数据处理请求；

[0008] 模式监控器将系统从所述普通模式切换至安全模式；

[0009] 在所述安全模式下，所述服务端根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理；

[0010] 所述模式监控器将所述系统从所述安全模式切换至所述普通模式；

[0011] 其中，所述内存被划分为安全子内存和普通子内存，在所述普通模式下，所述普通子内存中的数据允许被所述服务端访问，在所述安全模式下，所述普通子内存中的数据允许被所述服务端访问，且安全子内存中的数据允许被所述服务端访问。

[0012] 另一方面，提供一种应用数据保护的系统，包括：

[0013] 客户端，用于在普通模式下，向服务端发送应用数据处理请求；

[0014] 所述服务端，用于在所述安全模式下，根据所述应用数据处理请求和安全子内存中的数据进行应用数据处理；

[0015] 模式监控器，用于在所述客户端向所述服务端发送所述应用数据处理请求之后，将所述系统从所述普通模式切换至安全模式；在根据所述应用数据处理请求进行应用数据处理之后，将所述系统从所述安全模式切换至所述普通模式；

[0016] 其中，所述内存被划分为安全子内存和普通子内存，在所述普通模式下，所述普通子内存中的数据允许被所述服务端访问，在所述安全模式下，所述普通子内存中的数据允许被所述服务端访问，且安全子内存中的数据允许被所述服务端访问。

[0017] 本发明实施例提供的应用数据保护的方法和系统，采用上述方案后，在硬件上，将内存划分为普通子内存和安全子内存，在软件上，应用于终端设备中的系统设置了安全模式和普通模式，在安全模式下，系统中的服务端可以对普通子内存和安全子内存中的数据

进行访问，在普通模式下，服务端只可以对普通子内存中的数据进行访问。在系统执行安全要求较高的应用的过程中，需要切换至安全模式下执行，这样，可以对系统中执行的对安全要求较高的应用（该与安全要求较高的应用相关的数据可以存储于安全子内存中）提供全方位的保护，即只有在安全模式下执行相应的操作时，安全子内存中的数据才可能被允许访问，又由于该方案是基于硬件的设计，因此杜绝由于软件等因素引起的安全漏洞，安全性比现有技术中仅考虑软件层次的安全保护要可靠。

## 附图说明

[0018] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

- [0019] 图 1 为本实施例提供的一种应用数据保护的方法流程图；
- [0020] 图 2 为本实施例提供的另一种应用数据保护的方法流程图；
- [0021] 图 3 为图 2 所示的方法所应用的系统的硬件方面的结构示意图；
- [0022] 图 4 为图 2 所示的方法所应用的系统的软件方面的结构示意图；
- [0023] 图 5 为本实施例提供的例子的流程示意图；
- [0024] 图 6 为本实施例提供的例子的流程图；
- [0025] 图 7 为本实施例提供的一种应用数据保护的系统结构示意图；
- [0026] 图 8 为本实施例提供的另一种应用数据保护的系统结构示意图。

## 具体实施方式

[0027] 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作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0028] 现有技术中，对应用提供软件的保护，骇客可以利用系统漏洞攻击外设和内存来获取用户的私密信息，如账号和密码等。

[0029] 为了解决上述问题，本实施例提供一种应用数据保护的方法，为了可以更清楚的对以下实施例进行理解，首先对实施例所应用的系统进行简单描述，该系统可应用于终端设备中，终端设备可以但不限于包括：手机、电脑、平板电脑等，系统可以但不限于包括：客户端、服务端、模式监控器以及地址控制器等。

[0030] 其中，客户端是指与服务器相对应，为用户提供本地服务的程序。除了一些只在本地执行的应用程序之外，一般安装在普通的终端上，需要与服务端互相配合运行；服务端是为客户端服务的，服务的内容诸如向客户端提供资源，保存客户端数据等；模式监控器可以用于检测系统当前所述的状态，还可以控制状态的切换；地址控制器可以用于设置内存访问地址，以便服务器根据该访问地址对内存中的相应数据进行访问。

[0031] 为了可以对安全要求较高的应用数据进行更好的保护，可以将与安全要求较高的应用相关的数据存放至一个内存中较安全的位置，在执行安全要求较高的应用时，该内存

中较安全的位置中的数据可能不允许被访问。

[0032] 具体的,在硬件上,系统中的内存可以被划分为安全子内存和普通子内存,其中,安全子内存中可以存储与安全要求较高的应用相关的数据,普通子内存中可以存储与安全要求较低的应用相关的数据;在软件上,可以为系统设置普通模式和安全模式。

[0033] 在普通模式下,普通子内存中的任意数据允许被访问,在安全模式下,普通子内存中存储的任意数据允许被访问,且安全子内存中存储的相应的数据允许被访问,其中,安全子内存中可以但不限于存储与安全要求较高的应用相关的数据,换言之,安全要求较高的应用需要在安全模式下执行,安全要求较低的应用可以在普通模式或安全模式下执行。

[0034] 作为本实施例的一种实施方式,在安全模式下,正在执行安全要求较高的应用,若此时执行的操作不为安全操作时,为了避免安全子内存中存储的数据不被泄露,安全子内存中存储的相应的数据可能不允许被访问。

[0035] 如图1所示,本实施例提供的应用数据保护的方法可以包括:

[0036] 101、在普通模式下,客户端向服务端发送应用数据处理请求。

[0037] 在服务端执行相应应用之前,客户端可以根据用户输入的指令向服务端发送应用数据处理请求,以便服务端执行相应应用,由于客户端向服务端发送应用数据处理请求时并未执行该应用,因此可能不需要访问安全子内存中存储的数据,则该步骤可以在普通模式下执行。

[0038] 值得说明的是,本实施例中提供的应用数据处理请求可以用于请求执行安全要求较高的应用,与安全要求较高的应用相关的数据可以存储于安全子内存中。

[0039] 102、模式监控器将系统从普通模式切换至安全模式。

[0040] 由于,在客户端向服务端发送应用数据处理请求之后,服务端执行相应应用时,可能会访问与该应用相关的数据,即可能需要访问安全子内存中相应的数据,因此,在客户端向服务端发送应用数据处理请求之后,模式监控器可以将系统从普通模式切换至安全模式。

[0041] 103、在安全模式下,服务端根据应用数据处理请求和安全子内存中的数据进行应用数据处理。

[0042] 104、模式监控器将系统从安全模式切换至普通模式。

[0043] 采用上述方案后,在硬件上,将内存划分为普通子内存和安全子内存,在软件上,应用于终端设备中的系统设置了安全模式和普通模式,在安全模式下,系统中的服务端可以对普通子内存和安全子内存中的数据进行访问,在普通模式下,服务端只可以对普通子内存中的数据进行访问。在系统执行安全要求较高的应用过程中,需要切换至安全模式下执行,这样,可以对系统中执行的对安全要求较高的应用(该与安全要求较高的应用相关的数据可以存储于安全子内存中)提供全方位的保护,即只有在安全模式下执行相应的操作时,安全子内存中的数据才可能被允许访问,又由于该方案是基于硬件的设计,因此杜绝由于软件等因素引起的安全漏洞,安全性比现有技术中仅考虑软件层次的安全保护要可靠。

[0044] 现有技术中,通常对应用提供软件的保护,软件的保护具有差异性,面对不同的安全风险,不同的开发者需要针对不同的安全风险来分别设计软件来进行安全防护,这样,不仅浪费人力,而且随着时间的变化,安全威胁还会不断变化,如果软件的设计者稍微考虑的

不够全面,都会导致之前的工作变得毫无用处。

[0045] 为了解决上述问题和现有技术中的问题,本实施例提供另一种应用数据保护的方法,该方法是对图 1 所示的方法的进一步扩展和优化,如图 2 所示,具体可以包括:

[0046] 201、在普通模式下,客户端向服务端发送应用数据处理请求。

[0047] 在服务端执行相应的应用之前,客户端可以根据用户输入的指令向服务端发送应用数据处理请求,以便服务端执行相应地应用,由于客户端向服务端发送应用数据处理请求时并未执行该应用,因此可能不需要访问安全子内存中存储的数据,则该步骤可以在普通模式下执行。

[0048] 值得说明的是,本实施例中提供的应用数据处理请求可以用于请求执行安全要求较高的应用,与安全要求较高的应用相关的数据可以存储于安全子内存中。

[0049] 202、模式监控器判断客户端是否已向服务端发送了应用数据处理请求,若是,则执行步骤 203,若否,则执行步骤 202。

[0050] 模式监控器可以对客户端进行监控,可以根据客户端执行的相应操作对系统的模式进行设置,即模式监控器可以监控客户端是否已向服务端发送了应用数据处理请求。

[0051] 本实施例对模式监控器对客户端进行监控的方法不作限定,为本领域技术人员熟知的技术,且可以根据实际需要进行设定,在此不再赘述。

[0052] 203、模式监控器将系统从普通模式切换至安全模式。

[0053] 由于,在客户端向服务端发送应用数据处理请求之后,服务端执行相应地应用时,可能需要访问与该应用相关的数据,即可能需要访问安全子内存中相应的数据,因此,在客户端向服务端发送应用数据处理请求之后,模式监控器可以将系统从普通模式切换至安全模式。

[0054] 204、在安全模式下,服务端根据应用数据处理请求和安全子内存中的数据进行应用数据处理。

[0055] 在服务端根据应用数据处理请求进行应用数据处理时,服务端可能需要访问与该应用相关的数据,为了避免安全子内存中的数据被泄露,则可以在安全模式下执行本步骤,具体的,可以为只有在执行安全操作时,才允许安全子内存中的数据被访问,安全操作可以但不限于包括:已注册的操作或在执行可靠的操作。

[0056] 例如,在用户执行付款操作(即执行相应的付款应用)过程中,当输入相应的账户名称、支付密码以及登陆密码等私密信息(此操作为安全操作)时,需要在安全模式下进行,以便该付款应用相关的私密数据(如,可以但不限于包括账户名称、支付密码以及登陆密码等私密信息)不被泄露,其中,与付款应用相关数据可以被存储于安全子内存中。

[0057] 进一步的,在安全模式下,系统可以通过地址控制器设置相应的访问地址,以便服务端根据该访问地址对普通子内存和安全子内存中的相应数据进行访问。

[0058] 如图 3 所示,在所述模式监控器将系统从所述普通模式切换至安全模式之后,且在安全模式下,模式监控器(可以包括外设和 CPU(Central Processing Unit,中央处理器)等)向地址控制器发送安全模式通知;地址控制器根据当前待处理操作设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址;将所述第一访问地址发送至所述服务端;服务端根据第一访问地址对普通子内存或安全子内存中的数据进行访问。

[0059] 进一步的,地址控制器根据当前待处理操作设置第一访问地址可以包括:

[0060] 判断待处理操作是否为安全操作;

[0061] 若是,则设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址,此时,服务端根据该第一访问地址可以访问普通子内存和安全子内存中的相应数据;

[0062] 若否,则设置第一访问地址,所述第一访问地址包括普通子内存的地址,此时,服务端根据该第一访问地址可以访问普通子内存中的相应数据。

[0063] 这样,在安全模式下,若执行的操作不为安全操作,则安全子内存中的数据不被允许访问,此时服务端只可以访问普通子内存中的数据,进而避免了安全子内存中的数据的被泄露。

[0064] 其中,图3所示的安全应用1数据、安全应用2数据为安全子内存中存储的分别与安全应用1和安全应用2相关的数据,普通应用1数据、普通应用2数据为普通子内存中存储的分别与普通应用1和普通应用2相关的数据。

[0065] 205、模式监控器判断客户端是否已接收服务端发送的应用数据处理响应。若是,则执行步骤206,若否,则执行步骤205。

[0066] 其中,应用数据处理响应可以用于表征服务端已根据应用数据处理请求进行了应用数据处理。

[0067] 模式监控器可以对客户端进行监控,可以根据客户端执行的相应操作对系统的模式进行设置,即模式监控器可以监控客户端是否已接收服务端发送的应用数据处理响应。

[0068] 206、模式监控器将系统从安全模式切换至普通模式。

[0069] 由于,在服务端对应用数据处理完成之后,可能不需要访问与该应用相关的数据(即可能不再需要访问安全子内存中相应的数据),因此,在服务端对应用数据处理完成之后,模式监控器可以将系统从安全模式切换至普通模式。

[0070] 进一步的,如图3所示,在模式监控器将系统从安全模式切换至普通模式之后,且在普通模式下,模式监控器向地址控制器发送普通模式通知;地址控制器根据当前待处理操作设置第二访问地址,所述第二访问地址包括普通子内存的地址;将所述第二访问地址发送至所述服务端;服务端根据所述第二访问地址对所述普通子内存中的数据进行访问,此时服务端只可以访问普通子内存中的数据。

[0071] 如图4所示,为本实施例提供的软件结构示意图。在普通模式下,客户端可以与安全API(Application Programming Interface,应用程序编程接口)、安全API库进行数据交互,并通过安全驱动(即驱动层)与服务端进行数据交互;在安全模式下,服务端、服务端API、键盘驱动、NFC(Near Field Communication,近距离无线通讯)、显示驱动、驱动API可以执行相应的操作,内核可以指示模式监控器切换系统模式,另外,在安全模式下,还可以包括Secure boot(安全启动模组)。

[0072] 采用上述方案后,在硬件上,将内存划分为普通子内存和安全子内存,在软件上,应用于终端设备中的系统设置了安全模式和普通模式,在安全模式下,系统中的服务端可以对普通子内存和安全子内存中的数据进行访问,在普通模式下,服务端只可以对普通子内存中的数据进行访问。在系统执行安全要求较高的应用的过程中,需要切换至安全模式下执行,这样,可以对系统中执行的对安全要求较高的应用(该与安全要求较高的应用相关

的数据可以存储于安全子内存中)提供全方位的保护,即只有在安全模式下执行相应的操作时,安全子内存中的数据才可能被允许访问。另外,程序设计者不需要单独对应用程序做处理就可以运行在一个安全的环境中,这样节省了软件开发中安全方面的投入。又由于该方案是基于硬件的设计,因此杜绝由于软件等因素引起的安全漏洞,安全性比现有技术中仅考虑软件层次的安全保护要可靠。

[0073] 为了可以更好的对上述实施例进行理解,下面提供一个具体的例子进行简单说明。

[0074] 以下以通过 NFC 技术支付的过程为例进行说明,图 5 为该例子的流程示意图,图 6 为该例子的流程图,具体可以包括:

[0075] 1、在普通模式下(即图 5 中的“普通”),用户点击桌面的付款应用对应的图标,并向服务端发送付款应用请求;

[0076] 2、在普通模式下,在模式监视器监控到客户端已发送付款应用请求后,将系统切换到安全模式;

[0077] 3、在安全模式下,用户通过 NFC 技术得到结算消费账单,即开始执行支付应用,与支付应用相关的数据存储于安全子内存中;

[0078] 4、在安全模式下,用户在支付界面输入用户名和密码;

[0079] 5、在安全模式下,用户点击确认支付,由于步骤 4 和 5 为安全操作,因此允许服务端访问安全子内存;

[0080] 6、在安全模式下,获取安全子内存中存储的用户名和密码,并与用户输入的用户名和密码进行比对,判断是否相同,若相同,则执行步骤 7,若不同,则支付失败,执行步骤 8;

[0081] 7、在安全模式下,服务端根据消费账单和安全子内存中的数据进行账单结算,支付成功;

[0082] 8、在安全模式下,如果支付成功,则执行步骤 9,否则返回失败信息,执行步骤 4;

[0083] 9、在安全模式下,用户点击确认支付;

[0084] 10、支付完成,用户退出支付程序,同时在模式监视器检测到服务端已对付款应用处理完成后,将系统切换到普通模式。

[0085] 下面提供一下系统实施例,该系统实施例分别与上述提供的相应的方法实施例相对应。

[0086] 本实施例提供一种应用数据保护的系统,如图 7 所示,可以包括:

[0087] 客户端 71,用于在普通模式下,向服务端发送应用数据处理请求;

[0088] 服务端 72,用于在安全模式下,根据应用数据处理请求和安全子内存中的数据进行应用数据处理;

[0089] 模式监控器 73,用于在客户端向服务端发送应用数据处理请求之后,将系统从普通模式切换至安全模式;在根据应用数据处理请求进行应用数据处理之后,将系统从安全模式切换至普通模式;

[0090] 其中,所述内存被划分为安全子内存和普通子内存,在所述服务端 72 根据所述应用数据处理请求进行应用数据处理的过程中,在所述普通模式下,所述普通子内存中的数据允许被所述服务端 72 访问,在所述安全模式下,所述普通子内存中的数据允许被所述服

务端 72 访问,且安全子内存中的数据允许被所述服务端 72 访问。

[0091] 采用上述方案后,在硬件上,将内存划分为普通子内存和安全子内存,在软件上,应用于终端设备中的系统设置了安全模式和普通模式,在安全模式下,系统中的服务端可以对普通子内存和安全子内存中的数据进行访问,在普通模式下,服务端只可以对普通子内存中的数据进行访问。在系统执行安全要求较高的应用的过程中,需要切换至安全模式下执行,这样,可以对系统中执行的对安全要求较高的应用(该与安全要求较高的应用相关的数据可以存储于安全子内存中)提供全方位的保护,即只有在安全模式下执行相应的操作时,安全子内存中的数据才可能被允许访问,又由于该方案是基于硬件的设计,因此杜绝由于软件等因素引起的安全漏洞,安全性比现有技术中仅考虑软件层次的安全保护要可靠。

[0092] 本实施例提供另一种应用数据保护的系统,该系统是对图 6 所示的系统的进一步扩展和优化,如图 8 所示,可以包括:

[0093] 客户端 81,用于在普通模式下,向服务端发送应用数据处理请求;

[0094] 服务端 82,用于在安全模式下,根据应用数据处理请求和安全子内存中的数据进行应用数据处理;

[0095] 模式监控器 83,用于在客户端向服务端发送应用数据处理请求之后,将系统从普通模式切换至安全模式;在根据应用数据处理请求进行应用数据处理之后,将系统从安全模式切换至普通模式;

[0096] 其中,所述内存被划分为安全子内存和普通子内存,在所述服务端根据所述应用数据处理请求进行应用数据处理的过程中,在所述普通模式下,所述普通子内存中的数据允许被所述服务端访问,在所述安全模式下,所述普通子内存中的数据允许被所述服务端访问,且安全子内存中的数据允许被所述服务端访问

[0097] 进一步的,所述模式监控器 83,具体用于判断所述客户端是否已向所述服务端发送了所述应用数据处理请求;若是,则将所述系统从所述普通模式切换至所述安全模式;

[0098] 所述模式监控器 83,具体用于判断所述客户端是否已接收所述服务端发送的应用数据处理响应,所述应用数据处理响应用于表征所述服务端已根据所述应用数据处理请求进行了应用数据处理;若是,则将所述系统从所述安全模式切换至所述普通模式。

[0099] 进一步的,本实施例提供的应用数据保护的系统还可以包括:地址控制器 84;

[0100] 所述模式监控器 83,还用于在所述模式监控器将系统从所述普通模式切换至安全模式之后,在所述安全模式下,向所述地址控制器发送安全模式通知;

[0101] 所述地址控制器 84,用于根据当前待处理操作设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址;将所述第一访问地址发送至所述服务端;

[0102] 所述服务端 82,用于根据所述第一访问地址对所述普通子内存或所述安全子内存中的数据进行访问。

[0103] 进一步的,所述地址控制器 84,具体用于判断待处理操作是否为安全操作;若是,则设置第一访问地址,所述第一访问地址包括如下地址中至少一项:所述安全子内存的地址、普通子内存的地址;若否,则设置第一访问地址,所述第一访问地址包括普通子内存的地址。

[0104] 进一步的，模式监控器 83，还用于在所述模式监控器将所述系统从所述安全模式切换至所述普通模式之后，在普通模式下，向地址控制器发送普通模式通知；

[0105] 地址控制器 84，用于根据当前待处理操作设置第二访问地址，所述第二访问地址包括普通子内存的地址；将所述第二访问地址发送至所述服务端；

[0106] 所述服务端 82，用于根据所述第二访问地址对所述普通子内存中的数据进行访问。

[0107] 采用上述方案后，在硬件上，将内存划分为普通子内存和安全子内存，在软件上，应用于终端设备中的系统设置了安全模式和普通模式，在安全模式下，系统中的服务端可以对普通子内存和安全子内存中的数据进行访问，在普通模式下，服务端只可以对普通子内存中的数据进行访问。在系统执行安全要求较高的应用的过程中，需要切换至安全模式下执行，这样，可以对系统中执行的对安全要求较高的应用（该与安全要求较高的应用相关的数据可以存储于安全子内存中）提供全方位的保护，即只有在安全模式下执行相应的操作时，安全子内存中的数据才可能被允许访问。另外，程序设计者不需要单独对应用程序做处理就可以运行在一个安全的环境中，这样节省了软件开发中安全方面的投入。又由于该方案是基于硬件的设计，因此杜绝由于软件等因素引起的安全漏洞，安全性比现有技术中仅考虑软件层次的安全保护要可靠。

[0108] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。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可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务端，或者网络设备等）执行本发明各个实施例所述的方法。

[0109] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

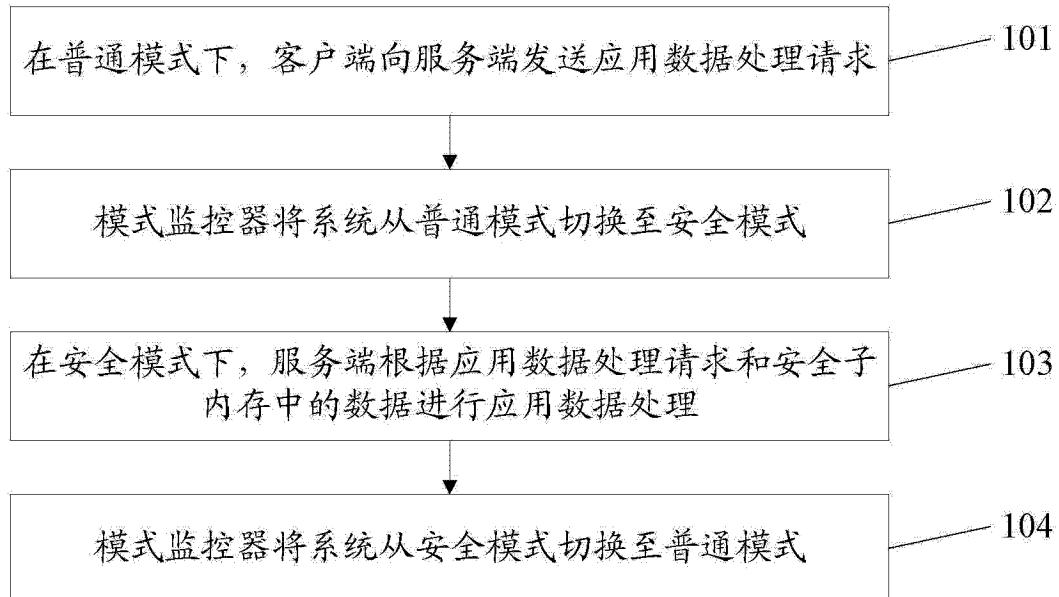


图 1

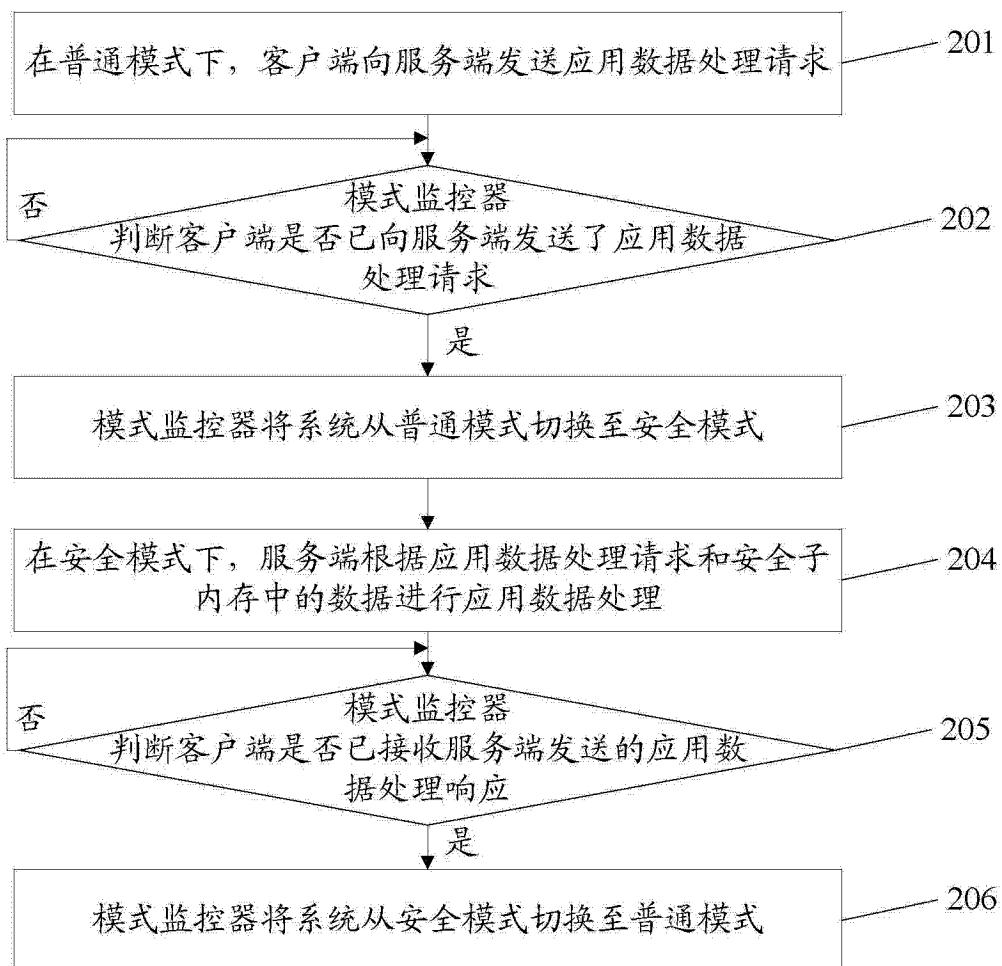


图 2

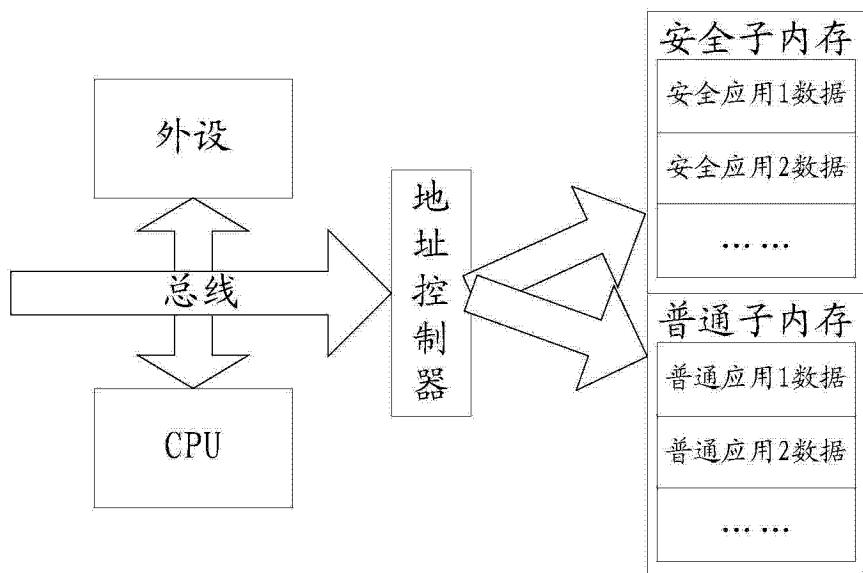


图 3

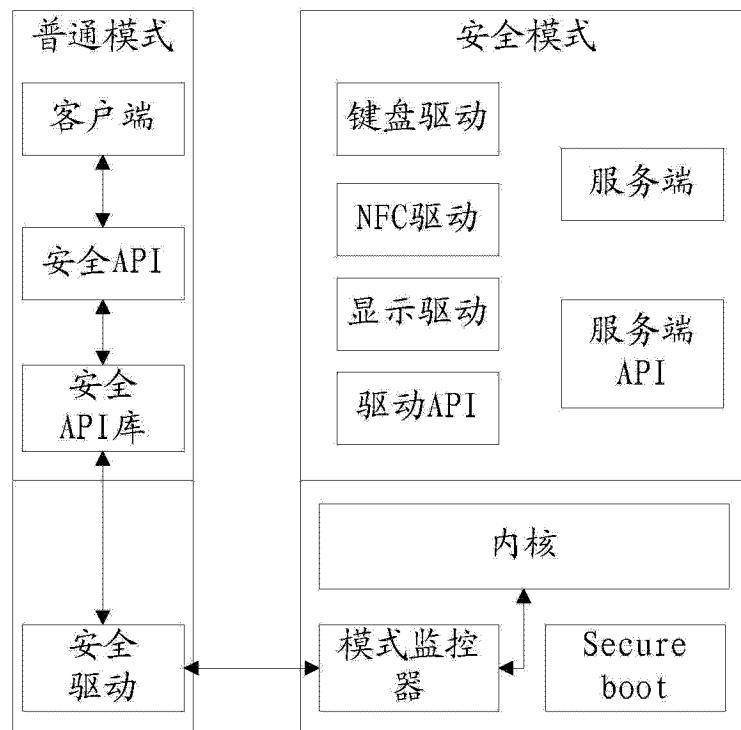


图 4

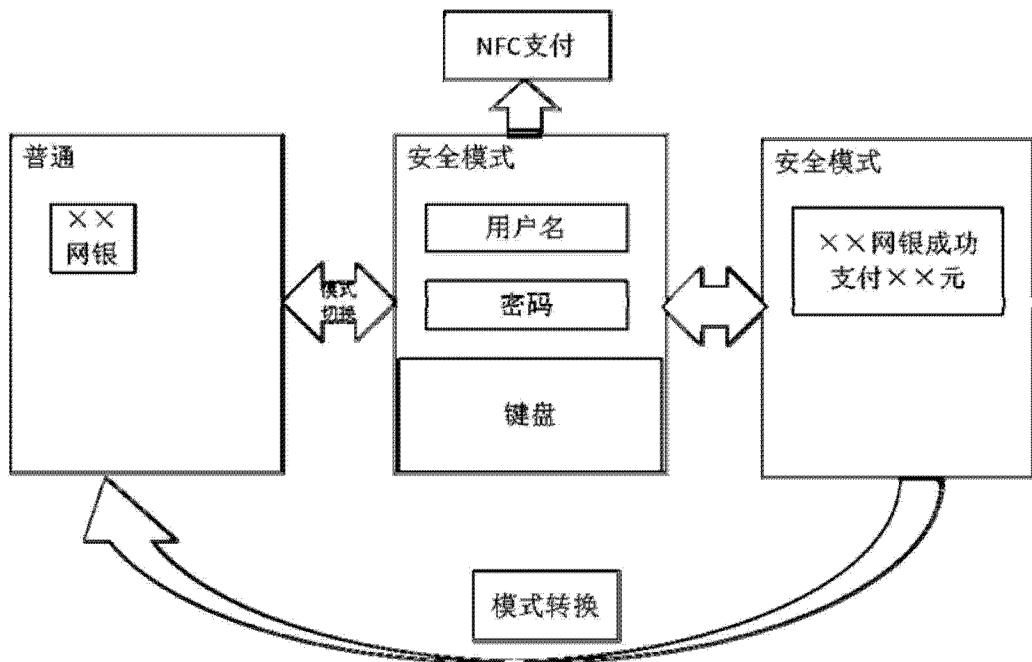


图 5

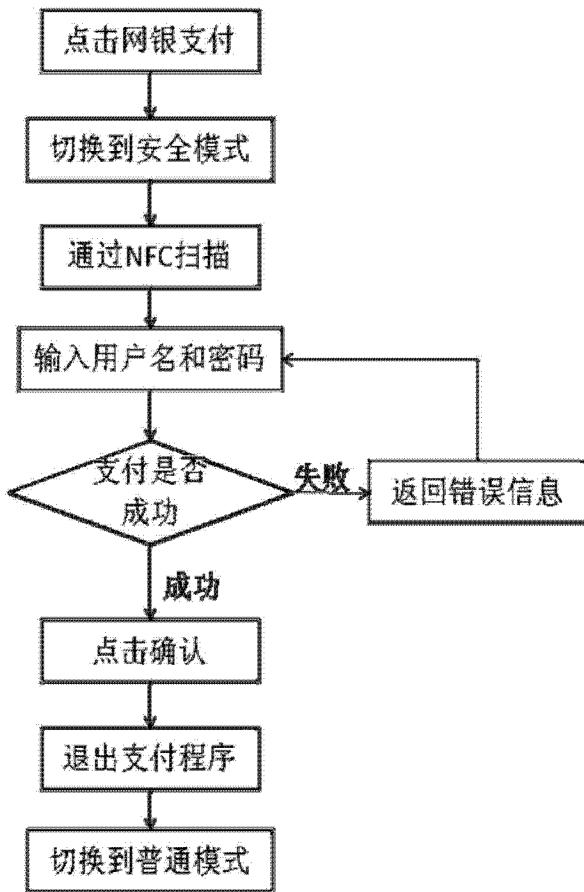


图 6

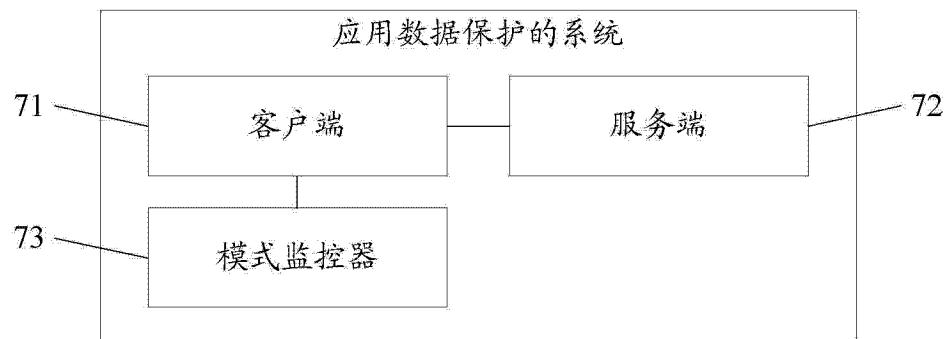


图 7

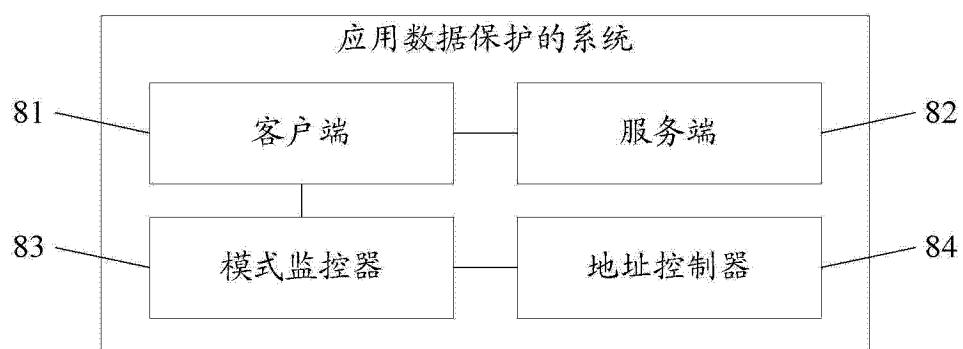


图 8