(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
2015 年 11 月 5 日 (05.11.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/165375 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04M 1/725* (2006.01)
H04L 12/26 (2006.01)

(21) 国际申请号: PCT/CN2015/077656

(22) 国际申请日: 2015 年 4 月 28 日 (28.04.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410175709.5 2014 年 4 月 28 日 (28.04.2014) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **陈杰 (CHEN, Jie)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京市隆安律师事务所 (BEIJING LONGAN LAW FIRM)**; 中国北京市朝阳区建国门外大街 21 号北京国际俱乐部 188 室, Beijing 100020 (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。

(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,

[见续页]

(54) **Title**: METHOD AND DEVICE FOR CAPTURING NETWORK DATA PACKET IN MOBILE TERMINAL

(54) **发明名称** : 在移动终端中抓取网络数据包的方法及装置

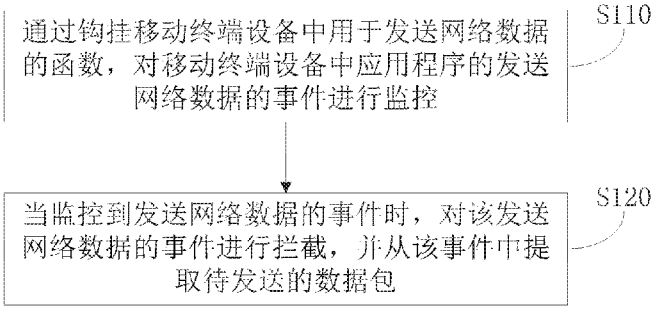

图 1 / FIG. 1

S110 MONITORING A NETWORK DATA TRANSMISSION EVENT OF AN APPLICATION PROGRAM IN A MOBILE TERMINAL DEVICE BY HOOKING A FUNCTION FOR TRANSMITTING NETWORK DATA INTO THE MOBILE TERMINAL DEVICE

S120 WHEN DETECTING THE NETWORK DATA TRANSMISSION EVENT, INTERCEPTING THE NETWORK DATA TRANSMISSION EVENT, AND EXTRACTING FROM THE EVENT THE DATA PACKET TO BE TRANSMITTED

(57) **Abstract**: Disclosed are a method and device for capturing a network data packet in a mobile terminal, the method comprising: monitoring a network data transmission event of an application program in a mobile terminal device by hooking a function for transmitting network data into the mobile terminal device, the function for transmitting the network data being an unified interface function provided by the operating system of the mobile terminal device and invoked for transmitting network data by each application installed in the mobile terminal device; when detecting the network data transmission event, intercepting the network data transmission event, and extracting from the event the data packet to be transmitted. The method effectively extracts the network data transmitted by the application program, and has wide applicability for various programs.

(57) **摘要**: 本发明公开了一种在移动终端中抓取网络数据包的方法及装置，其中所述方法包括：通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。通过该方法可以有效的提取应用程序所发送的网络数据，对于多种程序都具有广泛的适用性。

WO 2015/165375 A1

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))。

在移动终端中抓取网络数据包的方法及装置

技术领域

本发明涉及移动终端技术领域，具体涉及在移动终端中抓取网络数据包的方法及装置。

背景技术

为了便于应用，大多移动终端设备中会搭载相对大型的操作系统，操作系统负责管理移动终端设备的软硬件资源，控制其他程序的运行，并为其他程序的运行提供服务和支持。在操作系统之上用户可以安装各种功能丰富的软件应用，这些软件应用涉及到人们工作娱乐等等方面。在用户安装的软件应用中，不乏对运行环境要求较高的应用，诸如网络银行，一旦敏感的用户信息被恶意程序盗取，就可能会给用户带来损失；另外还有一些应用，可能会处于某种原因，在用户不知情的情况下，将终端设备中的一些用户数据上传到自己的服务器，等等。因此在移动终端设备上，还常常需要采取一定的安全措施，其中，在移动终端上对应用程序收发的数据包进行监控，并对收发的数据包进行安全性分析判断，在发现其中包含用户的敏感数据时，进行拦截或者向用户进行提示，便是其中的一种措施。在此过程中，如何抓取到应用收发的数据包是一个关键的问题。

对于一些使用 http 等传统的传输协议进行数据传输的情况而言，一般直接监控应用自身的收发数据事件，即可抓取到其收发的数据包。但是，对于 https 等传输协议而言，由于在传输数据包的过程中对数据包进行加密处理，因此，采用传统的方式对应用的收发事件进行监控时，抓取到的数据包往往是无法直接进行分析操作的。为此，现有技术中出现了一些网络数据监控工具，这些工具在抓取 https 数据包时，一般需要模拟成应用的客户端，如果应用或网站需要对数据进行加密，还需要提前获取和安装应用或者网站的证书，然后利用获取到的证书与服务器端进行通信，从中抓取到应用上传或者接收到的数据包。

这种方式虽然能够抓取到 https 数据包，但是往往只能针对特定的应用，例如某监控工具只能够对一款浏览器软件实现数据收发监控，对于层出不穷的移动终端应用，这种数据收发的监控工具或方式缺乏普遍的适用性，无法满足数

据安全的需求。此外，对于建立在加密的安全连接上的收据收发，这种抓取数据包的方式还需要在终端设备上安装对应的安全证书，才能够实现有效的安全监控，在无法获取安全证书的情况下，这种技术手段则仍然无法实现对移动终端所收发的数据包进行有效的抓取。

因此，如何更方便有效地抓取移动终端设备上收发的数据包，是迫切需要本领域技术人员解决的技术问题。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的在移动终端中抓取网络数据包的方法和相应的在移动终端中抓取网络数据包的装置。

依据本发明的一个方面，提供了在移动终端中抓取网络数据包的方法，包括：

通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；

当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

根据本发明的另一方面，提供了在移动终端中抓取网络数据包的装置，包括：

监控单元，用于通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；

数据提取单元，用于当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

根据本发明的另一个方面，提供了一种计算机程序，包括计算机可读代码，当所述计算机可读代码在移动终端上运行时，导致所述移动终端执行上述的在移动终端中抓取网络数据包的方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如上所述的计算机程序。

根据本发明的在移动终端中抓取网络数据包的方法，可以通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；进而，当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包，从应用程序发送网络数据的事件中可以有效的提取应用程序所发送的数据，并且，由于应用程序在发送网络数据时，常常需要调用所监控的统一的接口函数，从而本方法相对于现有技术，对于多种程序都具有广泛的适用性。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的在移动终端中抓取网络数据包的方法的流程图；

图 2 示出了根据本发明一个实施例的在移动终端中抓取网络数据包的装置的示意图；

图 3 示意性地示出了用于执行根据本发明的方法的移动终端的框图；以及

图 4 示意性地示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

附图实施例

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本

公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

图 1 示出了根据发明一个实施例的在移动终端中抓取网络数据包的方法的流程图，如图 1 所示，该在移动终端中抓取网络数据包的方法包括以下步骤：

S110：通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；

在移动终端设备中，通常安装了相对复杂的操作系统，为上层的应用程序提供支持。移动终端设备中的应用程序如果需要连接网络并通过网络收发数据，通常需要调用操作系统提供的接口。首先可以通过钩挂移动终端设备中用于收发网络数据的函数，对移动终端设备中应用程序收发网络数据的事件进行监控。通常，移动终端设备本地的应用程序要发送数据到特定的网络地址，需要调用移动终端设备中用于发送网络数据的函数，同样，在一些恶意程序需要发送用户的敏感数据时，也需要调用移动终端设备中的用于发送网络数据的函数，将本地的数据发送出去。因此，在本发明实施例提供的方法中，主要可以通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控，来获知应用程序发送网络数据的事件。

其中，用于发送网络数据的函数包括移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用的函数。例如，在苹果公司生产的移动终端设备中，所安装的操作系统为 iOS，在 iOS 操作系统中，应用程序如果需要发起加密连接，并向外发送数据时，需要调用 iOS 操作系统中提供的 sslread 函数。此时，可以通过钩挂搭载 iOS 操作系统的移动终端设备中的该函数，实现对其中运行的应用程序的发送网络数据的事件的监控。

此外，恶意应用程序还可以通过接收网络数据，实现接收黑客指令，下载恶意程序等恶意行为，因此除了监控对恶意应用程序发送本地敏感数据外，在本发明实施例提供的方法中，除了监控可能上传本地数据的发送网络数据的函数的调用事件，还可以对本地应用程序接收网络数据的事件进行监控，具体实现时，可以通过钩挂移动终端设备中用于接收网络数据的函数，对移动终端设备中应用程序的接收网络数据的事件进行监控；其中，用于接收网络数据的函

数包括移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要接收网络数据时，均需调用该函数。例如搭载 iOS 操作系统的移动终端中，本地应用程序如果需要接受网络数据，需要调用 sslwrite 函数，可以通过钩挂该函数，实现对移动终端设备中应用程序的接收网络数据的事件的监控。

S120：当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

当监控到本地应用程序触发的发送网络数据的事件后，可以拦截应用程序发送的网络数据，进一步的，可以从该事件中提取出待发送到数据包，对应用程序发送的数据进行分析，确定其安全性，或者确定其是否为用户的敏感数据。如前所述，在移动终端设备上的应用程序发送数据时，可以是基于加密连接的加密传输，要实现对这种数据传输中的数据捕获，如果不具备相应的解密手段，比如解密密钥或者证书，就很难实现进一步的数据分析，此时就需要在监控到移动终端设备中应用程序的发送网络数据的事件时，在应用程序对其所要发送的数据进行加密前，从函数调用事件中提取到待发送的未加密的数据包。具体实现时，可以利用钩挂机制，对应用程序所调用的操作系统的发送接口函数进行钩挂，这样，就可以在应用程序调用操作系统的发送接口函数时，获取应用程序向操作系统的发送接口函数传送的参数，在参数中有代表应用程序所要发送或接收的数据的函数参数，可以将此函数参数提取出来，从而实现对应用程序所要发送的数据包的获取。并且在这个过程中，所获取到的代表发送/接收数据的函数参数，是未经过加密的数据，便于实现后续的数据安全性分析。

如前所述，应用程序的恶意行为，除了发送用户的敏感数据，还可以有接收黑客指令，下载恶意程序等恶意行为，因此，还可以对应用程序接收网络数据的事件进行监控，以及对事件中应用程序所接收的数据包进行获取。具体的实现方式也可以是利用钩挂机制，对应用程序所调用的操作系统的接收接口函数进行钩挂。在数据包被加密的情况下，在提取数据时，可以在执行解密操作后再提取其中的数据，对应的，从接收网络数据的事件中提取的数据包为应用执行解密操作后的数据包。

例如在 iOS 操作系统中可以分别对应用程序收发数据时调用的接口函数，sslread 以及 sslwrite 进行钩挂，实现钩挂的函数原型可以如下：

MSHookFunction((void *)SSLWrite, (void *)_hook_SSLWrite, (void **)&_real_SSLWrite);

MSHookFunction((void *)SSLRead, (void *)_hook_SSLRead, (void **)&_real_SSLRead);

通过实现上述钩挂函数，可以在钩挂函数的代码中获取应用程序所要收发的数据。

在实现了对应用程序发送以及接收网络数据的事件的监控，以及对所有收发的数据包的获取后，可以进一步的对提取到的待发送数据包，或者待接收的数据包进行合法性分析；如果判定发送数据包中包括用户敏感数据，或者接收到数据为远程操控的恶意指令，或者下载恶意程序等行为等等，则进行拦截或者向用户发送提示信息，以提醒用户采取进一步的安全措施。

以上对本发明实施例提供的在移动终端中抓取网络数据包的方法进行了详细的介绍，通过该方法，可以通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；进而，当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包，从应用程序发送网络数据的事件中可以有效的提取应用程序所发送的数据，并且，由于应用程序在发送网络数据时，常常需要调用所监控的统一的接口函数，从而本方法相对于现有技术具有更加广泛的适用性。

与本发明实施例提供的在移动终端中抓取网络数据包的方法相对应，还提供了在移动终端中抓取网络数据包的装置，请参看图 2，为根据本发明一个实施例的在移动终端中抓取网络数据包的装置的示意图，如图所示，该装置可以包括：

监控单元 210，用于通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；

数据提取单元 220，用于当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

其中，从发送网络数据的事件中提取的待发送的数据包可以是应用程序执

行加密操作前的数据包。当移动终端设备所搭载的操作系统为 iOS 系统时，所钩挂的函数可以是用于发送网络数据的 sslread 函数。

在另一种实现方式下，该在移动终端中抓取网络数据包的装置还可以包括：

数据分析单元，用于对提取到的待发送数据包进行合法性分析；

数据拦截单元，用于如果判定出所述数据包中包括用户敏感数据，则进行拦截或者向用户发送提示信息。

当用于获取移动终端中应用程序接收的数据时，监控单元 210 还可以用于，通过钩挂移动终端设备中用于接收网络数据的函数，对移动终端设备中应用程序的接收网络数据的事件进行监控；其中，用于接收网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要接收网络数据时，均需调用该函数；

数据提取单元 220 还用于，当监控到接收网络数据的事件时，对该接收网络数据的事件进行拦截，并从该事件中提取接收到的数据包。

其中，如果是基于加密连接的数据传输，对应的从接收数据的事件中提取的接收到的数据包为应用执行解密操作后的数据包。当移动终端设备所搭载的操作系统为 iOS 系统时，所钩挂的数据接收函数可以是用于接收网络数据的 sslwrite 函数。

以上对本发明实施例提供的在移动终端中抓取网络数据包的装置进行了介绍，通过该装置，可以利用钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控。进而，当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包，从应用程序发送网络数据的事件中可以有效的提取应用程序所发送的数据，并且，由于应用程序在发送网络数据时，常常需要调用所监控的统一的接口函数，相对于现有技术具有更加广泛的适用性。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发

明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的在移动终端中抓取网络数据包的装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。

这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 3 示出了可以实现根据本发明的在移动终端中抓取网络数据包的方法的移动终端，例如手机、PAD 等。该移动终端传统上包括处理器 310 和以存储器 320 形式的计算机程序产品或者计算机可读介质。存储器 320 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 320 具有用于执行上述在移动终端中抓取网络数据包的方法中的任何方法步骤的程序代码 331 的存储空间 330。例如，用于程序代码的存储空间 330 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 331。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 4 所述的便携式或者固定存储单元。该存储单元可以具有与图 3 的移动终端中的存储器 320 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 331'，即可以由例如诸如 310 之类的处理器读取的代码，这些代码当由移动终端运行时，导致该移动终端执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包

括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

本申请可以应用于计算机系统/服务器，其可与众多其它通用或专用计算系统环境或配置一起操作。适于与计算机系统/服务器一起使用的众所周知的计算系统、环境和/或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

计算机系统/服务器可以在由计算机系统执行的计算机系统可执行指令（诸如程序模块）的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

权利要求书

1、一种在移动终端中抓取网络数据包的方法，包括:

通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数;

当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

2、如权利要求 1 所述的方法，所述从该事件中提取的待发送的数据包为应用程序执行加密操作前的数据包。

3、如权利要求 1 所述的方法，当所述操作系统为 iOS 系统时，所述用于发送网络数据的函数包括 sslread 函数。

4、如权利要求 1 至 3 任一项所述的方法，还包括:

对提取到的待发送数据包进行合法性分析;

如果判定出所述数据包中包括用户敏感数据，则进行拦截或者向用户发送提示信息。

5、如权利要求 1 至 3 任一项所述的方法，还包括:

通过钩挂移动终端设备中用于接收网络数据的函数，对移动终端设备中应用程序的接收网络数据的事件进行监控；其中，所述用于接收网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要接收网络数据时，均需调用该函数;

当监控到所述接收网络数据的事件时，对该接收网络数据的事件进行拦截，并从该事件中提取接收到的数据包。

6、如权利要求 5 所述的方法，所述从该事件中提取的接收到的数据包为应用执行解密操作后的数据包。

7、如权利要求 5 所述的方法，当所述操作系统为 iOS 系统时，所述用于接收网络数据的函数包括 sslwrite 函数。

8、一种在移动终端中抓取网络数据包的装置，包括:

监控单元，用于通过钩挂移动终端设备中用于发送网络数据的函数，对移

动终端设备中应用程序的发送网络数据的事件进行监控；其中，所述用于发送网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要发送网络数据时，均需调用该函数；

数据提取单元，用于当监控到所述发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包。

9、如权利要求 8 所述的装置，所述从该事件中提取的待发送的数据包为应用程序执行加密操作前的数据包。

10、如权利要求 8 所述的装置，当所述操作系统为 iOS 系统时，所述用于发送网络数据的函数包括 sslread 函数。

11、如权利要求 8 至 10 任一项所述的装置，还包括

数据分析单元，用于对提取到的待发送数据包进行合法性分析；

数据拦截单元，用于如果判定出所述数据包中包括用户敏感数据，则进行拦截或者向用户发送提示信息。

12、如权利要求 8 至 10 任一项所述的装置，所述监控单元还用于：

通过钩挂移动终端设备中用于接收网络数据的函数，对移动终端设备中应用程序的接收网络数据的事件进行监控；其中，所述用于接收网络数据的函数为移动终端设备的操作系统提供的统一的接口函数，移动终端设备中安装的各个应用在需要接收网络数据时，均需调用该函数；

所述数据提取单元还用于：当监控到所述接收网络数据的事件时，对该接收网络数据的事件进行拦截，并从该事件中提取接收到的数据包。

13、如权利要求 12 所述的装置，所述从该事件中提取的接收到的数据包为应用执行解密操作后的数据包。

14、如权利要求 12 所述的装置，当所述操作系统为 iOS 系统时，所述用于接收网络数据的函数包括 sslwrite 函数。

15、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在移动终端上运行时，导致所述移动终端执行根据权利要求 1-7 中的任一个所述的在移动终端中抓取网络数据包的方法。

16、一种计算机可读介质，其中存储了如权利要求 15 所述的计算机程序。

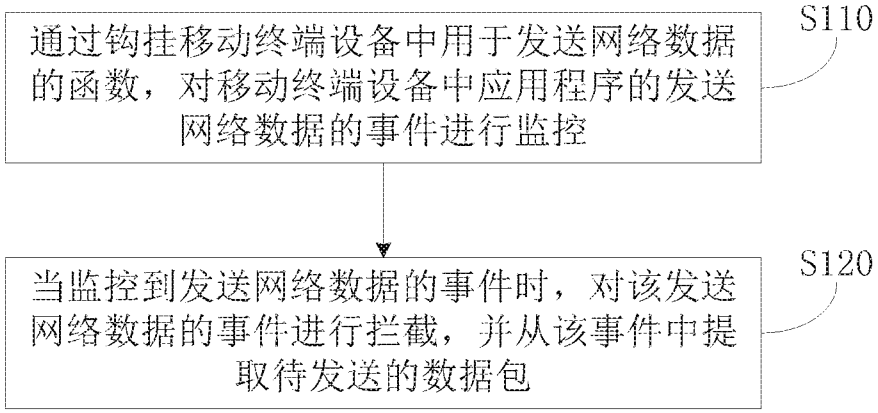
通过钩挂移动终端设备中用于发送网络数据的函数，对移动终端设备中应用程序的发送网络数据的事件进行监控
S110
当监控到发送网络数据的事件时，对该发送网络数据的事件进行拦截，并从该事件中提取待发送的数据包
S120

图 1

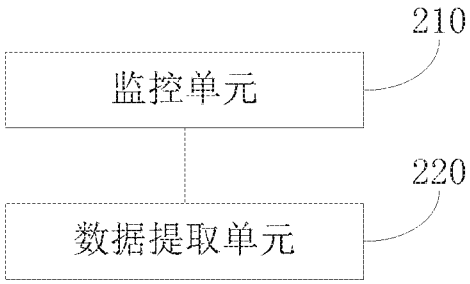
210
监控单元
220
数据提取单元

图 2

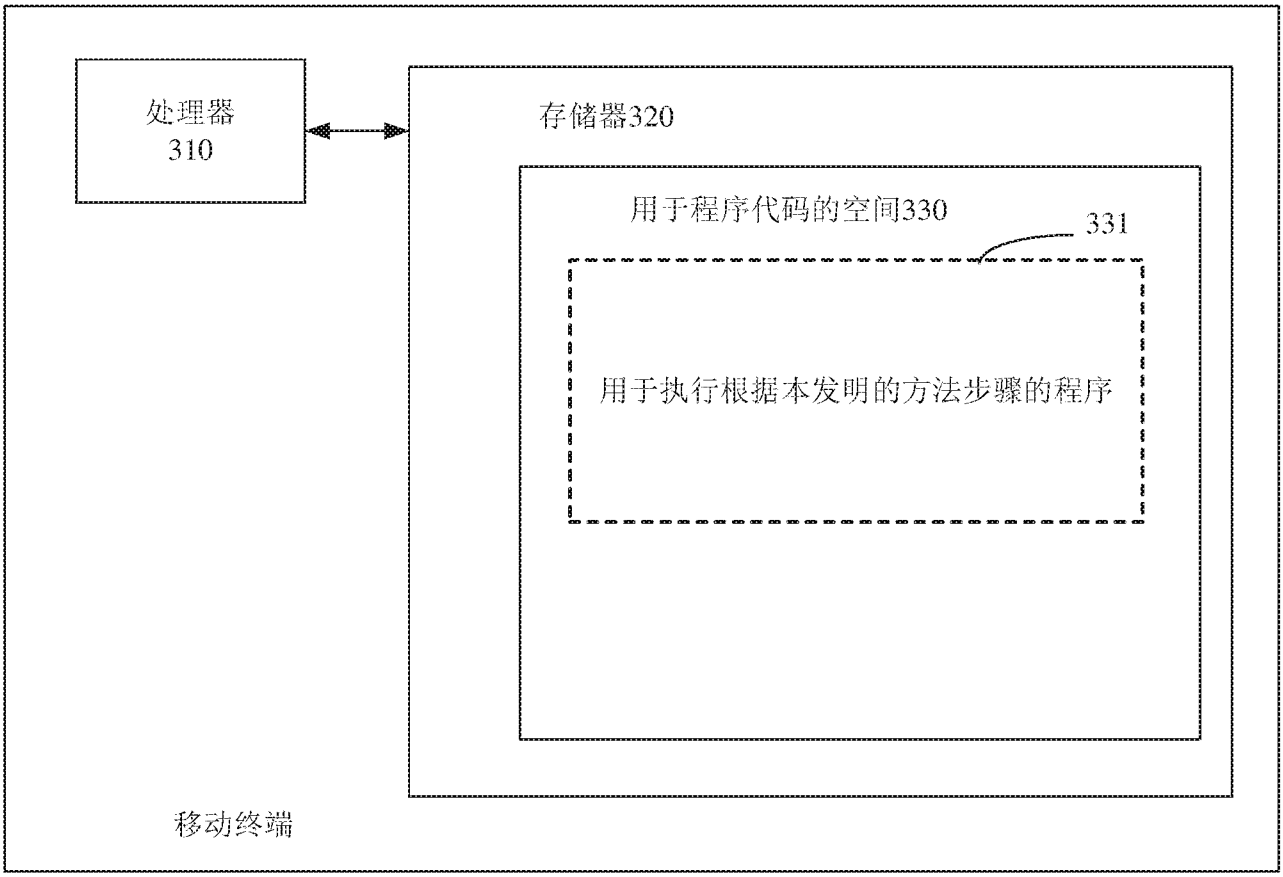
处理器
310
存储器320
用于程序代码的空间330
331
用于执行根据本发明的方法步骤的程序
移动终端

图 3

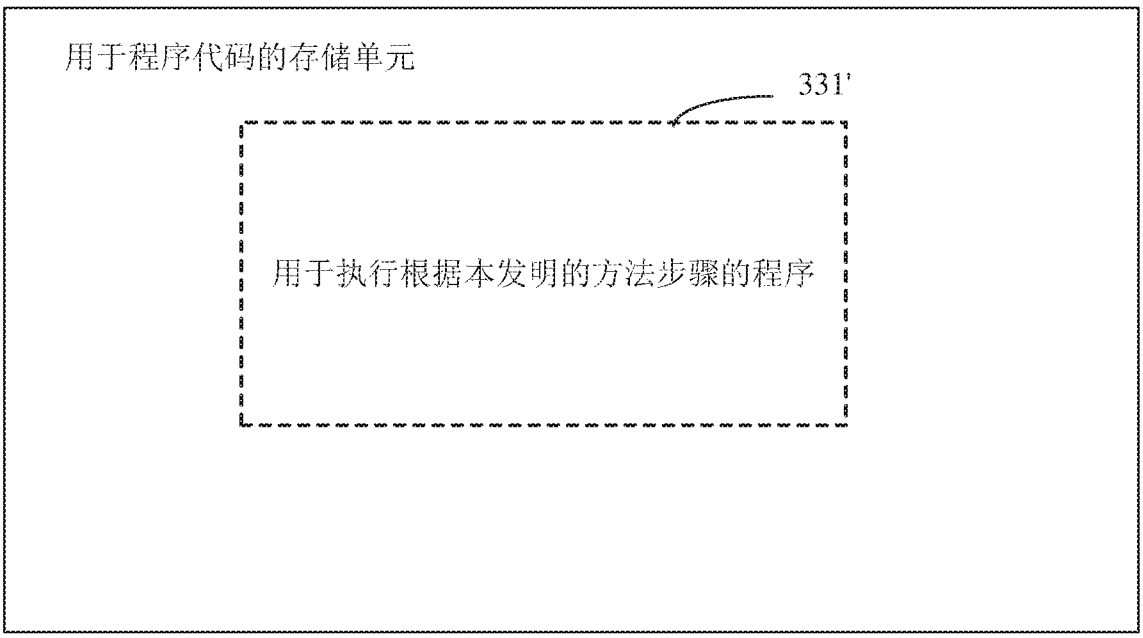
用于程序代码的存储单元
331'
用于执行根据本发明的方法步骤的程序

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/077656

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 12/26 (2006.01) i; H04M 1/725 (2006.01) 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)

H04L; H04M

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)

CNTXT; CNABS; VEN; CNKI: grasp, data packet, application, monitor, interface, capture, snatch, packet, terminal, leak, sensitive, function, app, ios, android

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103051617 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 17 April 2013 (17.04.2013), description, paragraphs [0023]-[0027], and figure 1	1-16
A	CN 103368978 A (THE THIRD INSTITUTE OF MINISTRY OF PUBLIC SECURITY), 23 October 2013 (23.10.2013), the whole document	1-16
A	CN 101286850 A (SHENZHEN POLYTECHNIC), 15 October 2008 (15.10.2008), the whole document	1-16
A	US 8561176 B1 (MCAFEE INC.), 15 October 2013 (15.10.2013), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2015 (20.07.2015)	**30 July 2015 (30.07.2015)**
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 **LI, Yan** Telephone No.: (86-10) **62088422**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/077656

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103051617 A	17 April 2013	WO 2014094470 A1	26 June 2014
CN 103368978 A	23 October 2013	None	
CN 101286850 A	15 October 2008	CN 101286850 B	15 December 2010
US 8561176 B1	15 October 2013	US 2013275950 A1	17 October 2013
		US 9027132 B2	05 May 2015
		US 2014059685 A1	27 February 2014

国际检索报告

国际申请号
PCT/CN2015/077656

A. 主题的分类

H04L 29/06(2006.01)i; H04L 12/26(2006.01)i; H04M 1/725(2006.01)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)

H04L; H04M

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）)

CNTXT;CNABS;VEN;CNKI:抓取，捕获，终端，数据包，泄露，敏感，函数，应用，监控，接口，安卓，capture, snatch,packet,terminal,leak,sensitive,function,app,ios,android

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
X	CN 103051617 A (北京奇虎科技有限公司等) 2013年 4月 17日 (2013-04-17) 说明书[0023]-[0027]段，图1	1-16
A	CN 103368978 A (公安部第三研究所) 2013年 10月 23日 (2013-10-23) 全文	1-16
A	CN 101286850 A (深圳职业技术学院) 2008年 10月 15日 (2008-10-15) 全文	1-16
A	US 8561176 B1 (MCAFEE INC) 2013年 10月 15日 (2013-10-15) 全文	1-16

☐ 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	国际检索报告邮寄日期
2015年 7月 20日	2015年 7月 30日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	李妍 电话号码 (86-10)62088422

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/077656

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	103051617	A	2013年 4月 17日	WO	2014094470	A1	2014年 6月 26日
CN	103368978	A	2013年 10月 23日		无		
CN	101286850	A	2008年 10月 15日	CN	101286850	B	2010年 12月 15日
US	8561176	B1	2013年 10月 15日	US	2013275950	A1	2013年 10月 17日
				US	9027132	B2	2015年 5月 5日
				US	2014059685	A1	2014年 2月 27日