

(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
2017 年 5 月 18 日 (18.05.2017)



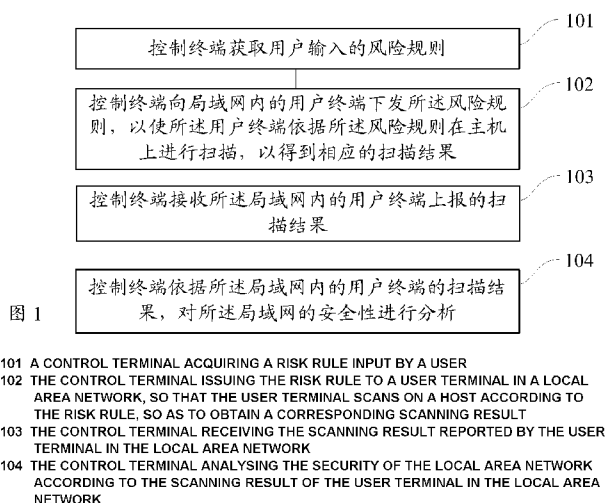
(10) 国际公布号
WO 2017/080424 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/104919
- (22) 国际申请日: 2016 年 11 月 7 日 (07.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510781407.7 2015 年 11 月 13 日 (13.11.2015) 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)。 北京奇安信科技有限公司 (BEIJING QIANXIN TECHNOLOGY CO.,LTD) [CN/CN]; 中国北京市朝阳区酒仙桥路甲 10 号 3 号楼 15 层 17 层 1701-26, Beijing 100015 (CN)。
- (72) 发明人: 江爱军 (JIANG, Aijun); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 赵小宁 (ZHAO, Xiaoning); 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: 北京润泽恒知识产权代理有限公司 (BEIJING RUNZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 7 层 702-703,715, Beijing 100081 (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, DJ, 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, KW, 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,

[见续页]

(54) Title: SECURITY DETECTION METHOD AND APPARATUS BASED ON LOCAL AREA NETWORK

(54) 发明名称: 一种基于局域网的安全检测方法和装置



(57) Abstract: Provided are a security detection method and apparatus based on a local area network. The method specifically comprises: a control terminal acquiring a risk rule input by a user; the control terminal issuing the risk rule to a user terminal in a local area network, so that the user terminal scans on a host according to the risk rule, so as to obtain a corresponding scanning result; the control terminal receiving the scanning result reported by the user terminal in the local area network; and the control terminal analysing the security of the local area network according to the scanning result of the user terminal in the local area network. By means of the embodiments of the present invention, unknown threats and security risks of a local area network can be detected more promptly by means of a risk rule, so that the timeliness of security detection can be improved, and effective prevention of viruses can be achieved.

(57) 摘要:

[见续页]



WO 2017/080424 A1



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))。

本发明实施例提供了一种基于局域网的安全检测方法和装置，其中的方法具体包括：控制终端获取用户输入的风险规则；控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；控制终端接收所述局域网内的用户终端上报的扫描结果；控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。本发明实施例能够通过风险规则更及时地检测出局域网的未知威胁和安全隐患，从而能够提高安全检测的及时性，且能够实现病毒的有效预防。

一种基于局域网的安全检测方法和装置

技术领域

本发明涉及计算机安全技术领域，特别是涉及一种基于局域网的安全检测方法和一种基于局域网的安全检测装置。

5 背景技术

随着互联网的迅速普及，局域网已成为企业发展中必不可少的一部分。然而，在为企业带来便利的同时，局域网也面临着各种各样的进攻和威胁，如机密泄漏、数据丢失、网络滥用、身份冒用、非法入侵等。

10 现有基于局域网的安全检测方案大多通过在企业网内部的终端上分别安装杀毒软件客户端，由该杀毒软件客户端基于病毒特征库发现终端上的病毒数量和病毒危害程度，并依据企业网内部所述终端的病毒数量和病毒危害程度进行企业网的安全评估。

15 对于病毒数量和病毒危害程度而言，尽管这种方法能够在一定程度上体现出企业网的安全状况，但是由于病毒特征库相对于病毒具有一定的滞后性，存在病毒的企业网已经处于危险状态，此种情况下的企业网已经属于不及格的网络环境，而对不及格的网络环境进行评分或进行检测，属于事后补救的范畴，因此无法有效保证企业网的安全性。

发明内容

20 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一种基于局域网的安全检测方法和一种基于局域网的安全检测装置。

依据本发明的一个方面，提供了一种基于局域网的安全检测方法，包括：
控制终端获取用户输入的风险规则；

25 控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

控制终端接收所述局域网内的用户终端上报的扫描结果；

控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

根据本发明的另一方面，提供了一种基于局域网的安全检测装置，应用于控制终端，包括：

5 获取模块，用于获取用户输入的风险规则；

下发模块，用于向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

接收模块，用于接收所述局域网内的用户终端上报的扫描结果；及

10 分析模块，用于依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

根据本发明实施例的一种基于局域网的安全检测方法和装置，可以使得控制终端的用户根据局域网的当前安全需求和实际情况，灵活地制定相应的风险规则，并根据所述风险规则对应的扫描结果分析得到局域网的安全状况，上述局域网的安全状况具体可以包括：安全、可疑、危险等状况；因此，
15 相对于传统的病毒特征库，本发明实施例能够通过风险规则更及时地检测出局域网的未知威胁和安全隐患，从而能够提高安全检测的及时性，且能够实现病毒的有效预防。

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
20 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

通过阅读下文可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。附图仅用于示出可选实施方式的目的，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
25 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一种基于局域网的安全检测方法的步骤流程示意图；

图2示出了根据本发明一个实施例的一种基于局域网的安全检测方法的

步骤流程示意图；

图 3 示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程示意图；

5 图 4 示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程示意图；

图 5 示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程示意图；

图 6 示出了根据本发明一个实施例的一种基于局域网的安全检测装置的结构示意；

10 图 7 是用于执行根据本发明的基于局域网的安全检测方法的计算设备的框图；

图 8 是用于为保持或者携带实现根据本发明的基于局域网的安全检测方法的程序代码的存储单元。

具体实施方式

15 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。

20 参照图 1，示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程图，具体可以包括如下步骤：

步骤 101、控制终端获取用户输入的风险规则；

步骤 102、控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

25 步骤 103、控制终端接收所述局域网内的用户终端上报的扫描结果；

步骤 104、控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

本发明实施例可以应用于企业网、政府网、校园网等局域网中；在上述

局域网中，所述控制终端是指局域网内用于控制其它用户终端进行安全检测的终端，所述用户终端是指局域网内响应控制终端的指令，与控制终端进行数据交互的终端。在实际应用中，可以在控制终端部署服务器代理模块，在用户终端部署软件客户端模块，以类似 C/S(客户端/ 服务器) 的架构，实现
5 局域网内控制终端对用户终端的控制功能，以及，用户终端的控制响应及通信功能。其中，上述控制终端和上述用户终端之间可以通过标准协议或者私有协议进行通信，其中，私有协议具有封闭性和安全性高的优点；可以理解，本发明实施例对于控制终端与用户终端之间的具体通信方式不加以限制。

在实际应用中，控制终端的用户可以是网络管理员等具有一定的网络安全知识的高级用户，因此，控制终端的用户可以根据局域网的当前安全需求和实际情况，灵活地制定相应的风险规则，从而，可以根据所述风险规则对应的扫描结果分析得到局域网的安全状况。

在本发明的一种可选实施例中，所述风险规则具体可以包括：与风险对象相关的规则，所述风险对象具体可以包括如下对象中的至少一种：进程、
15 服务、计划任务、安装应用、端口、文件、操作系统、注册表、用户账号和用户权限。可以理解，本发明实施例对于具体的风险对象和具体的风险规则不加以限制。

在本发明的一种可选实施例中，上述风险规则可以与 APT(高级持续性威胁，Advanced Persistent Threat)攻击相关，传统 APT 攻击的变种多，更新
20 快，故对于未知病毒而言并无样本可依，而本发明实施例中，控制终端的用户可以依据 APT 攻击的特性确定相应的风险对象，从而制定相应的风险规则。可以理解，本发明实施例对于风险对象的具体依据不加以限制。

在本发明的一种应用示例中，控制终端的用户发现 APT 攻击与 QQ 应用有关，故打算获知局域网内 QQ 的使用状态，则可以将 QQ 应用作为风险
25 对象并制定相应的风险规则，该风险规则可用于扫描主机上是否安装有 QQ、安装 QQ 的时间、安装 QQ 的版本、QQ 的安装路径等。

在本发明的另一种应用示例中，控制终端的用户发现局域网中一台主机的速度变慢了，进一步研究发现该主机上多出了一个未知服务，故可以将该

未知服务作为风险对象并制定相应的风险规则，该风险规则可用于扫描主机上是否存在该未知服务、该未知服务进入该主机的时间、该未知服务在该主机上的路径等。

在本发明的再一种应用示例中，控制终端的用户发现局域网的安全性与用户终端的密码有关，故可以将用户终端的密码作为风险对象并制定相应的风险规则，该风险规则可用于扫描用户终端的密码是否符合预置的复杂性要求等。

可以理解，上述制定风险规则的方式只是作为示例，实际上，本领域技术人员还可以根据实际应用需求采用其他制定风险规则的方式，如依据步骤104 输出的安全性分析结果制定风险规则等，本发明实施例对于风险规则的具体制定方式不加以限制。

需要说明的是，本发明实施例可以向用户提供风险规则的输入接口，该输入接口可以支持检索式的检索，且可以支持与、或等逻辑运算，可以理解，本发明实施例对于用户输入风险规则的具体方式不加以限制。

在实际应用中，本发明实施例可以作为局域网的安全检测的辅助分析工具，例如，本发明实施例分析得到的安全状况可以作为未知病毒的判定依据，或者，本发明实施例还可以与传统的病毒特征库等杀毒软件结合使用，本发明实施例对于具体的应用场景不加以限制。

在实际应用中，用户终端可以依据上述风险规则在主机上进行扫描，得到的扫描结果具体可以包括：命中风险规则的命中结果，或者，命中风险规则的命中结果等。在本发明的一种可选实施例中，用户终端可以在得到扫描结果后向控制终端上报上述扫描结果，或者，用户终端还可以仅仅向控制终端上报命中结果，而可以不向控制终端上报命中结果，因此可以节省命中结果的传输资源。

综上，由于传统的病毒特征库相对于病毒具有一定的滞后性，故无法检测出未知病毒；而本发明实施例可以使得控制终端的用户根据局域网的当前安全需求和实际情况，灵活地制定相应的风险规则，并根据所述风险规则对应的扫描结果分析得到局域网的安全状况，上述局域网的安全状况具体可以

包括：安全、可疑、危险等状况；因此，相对于传统的病毒特征库，本发明实施例能够通过风险规则更及时地检测出局域网的未知威胁和安全隐患，从而能够提高安全检测的及时性，且能够实现病毒的有效预防。

5 参照图 2，示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程图，具体可以包括如下步骤：

步骤 201、控制终端获取用户输入的风险规则；

步骤 202、控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

10 步骤 203、控制终端接收所述局域网内的用户终端上报的扫描结果；

步骤 204、控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析；

相对于图 1 所示实施例，本实施例的所述风险规则具体可以包括：与风险对象相关的规则，则所述控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析的步骤 204，具体可以包括：

15 步骤 241、控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性。

本实施例可以风险对象为粒度，分析风险对象的风险性。例如，在风险对象为未知服务时，可以根据局域网内的所有用户终端的扫描结果，分析得到该未知服务的风险性，因此，相对于传统的病毒特征库，本发明实施例能够更及时地检测出局域网的风险对象。

在本发明的一种可选实施例中，所述控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性的步骤，具体可以包括：

25 步骤 A1、控制终端依据所述局域网内的用户终端在一个时间段内的扫描结果，分析得到所述风险对象的生长趋势；

步骤 A2、依据所述风险对象的生长趋势，判定所述风险对象的风险性。

对于某个文件而言，由于其未通过 MD5（信息摘要算法 5，Message-Digest Algorithm 5）的校验，故将其列为风险对象；假设局域网内

的用户终端在一个时间段内的扫描结果表明，该文件在一周内从一台主机扩散到一千台主机，故可以依据该文件的生长趋势，判断该文件为未知隐患。其中，可以依据生长趋势对应的速率、风险对象的最大值等参数判定风险对象的风险性，本发明实施例对于风险对象的风险性的具体判定方法不加以限制。

在实际应用中，可以表格、柱状图、曲线等形式展现上述风险对象的生长趋势，以提高分析结果的直观性。另外，可以理解，上述分析得到所述风险对象的生长趋势只是作为可选实施例，实际上，本领域技术人员还可以根据实际应用需求，首先分析得到风险对象在局域网中的分布或比例、风险对象的生命周期等特性，再依据风险对象的特性判定所述风险对象的风险性，本发明实施例对于风险对象的特性不加以限制。

参照图 3，示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程图，具体可以包括如下步骤：

步骤 301、控制终端获取用户输入的风险规则；所述风险规则具体可以包括：与风险对象相关的规则；

步骤 302、控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

步骤 303、控制终端接收所述局域网内的用户终端上报的扫描结果；

步骤 304、控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析；所述分析具体可以包括：控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性；

相对于图 2 所示实施例，本实施例的方法还可以包括：

步骤 305、在所述风险对象的风险性符合预置条件时，生成用于清理所述风险对象的风险规则；

步骤 306、将所生成的风险规则输入至所述控制终端向局域网内的用户终端下发所述风险规则的步骤 302。

本发明实施例的预置条件可以为依据风险对象的风险性预置的条件，例

如，在本发明的一种应用示例中，上述预置条件具体可以包括：安全、可疑、危险等风险等级对应的条件，其中，上述风险等级对应的预置条件可以包括如下条件中的任一：风险对象在局域网中的分布或比例、风险对象的生命周期、风险对象在一个时间段内的生长趋势等，本发明实施例对于具体的预置条件不加以限制。

在本发明的一种应用示例中，风险规则可用于扫描主机上是否安装有QQ、安装QQ的时间、安装QQ的版本、QQ的安装路径等，则在该风险规则对应的QQ应用的风险性符合预置条件时，可以生成用于清理QQ应用的风险规则，以使用户终端在主机上卸载QQ应用并删除QQ应用对应的文件和痕迹。

在本发明的另一种应用示例中，风险规则可用于扫描主机上是否存在该未知服务、该未知服务进入该主机的时间、该未知服务在该主机上的路径等，则在该风险规则对应的未知服务的风险性符合预置条件时，可以生成用于清理未知服务的风险规则，以使用户终端在自身的主机上清理掉该未知服务。

综上，本实施例生成并清理所述风险对象的风险规则，能够在及时地检测出局域网的未知威胁和安全隐患的基础上，进一步将局域网的未知威胁和安全隐患停止在萌芽状态，从而可以提高局域网的安全性。

参照图4，示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程图，具体可以包括如下步骤：

步骤401、控制终端获取用户输入的风险规则；所述风险规则具体可以包括：与风险对象相关的规则；

步骤402、控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

步骤403、控制终端接收所述局域网内的用户终端上报的扫描结果；

步骤404、控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析；所述分析具体可以包括：控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性；

相对于图 2 所示实施例，本实施例的方法还可以包括：

步骤 405、在所述风险对象的风险性符合预置条件时，依据所述局域网内首次出现的风险对象的信息，对所述风险对象对应的攻击源进行追踪。

5 本实施例可以在遭到网络攻击的情况下，对上述网络攻击的攻击源进行追踪，以对新类型的网络攻击具有智能学习能力，并且还可以对网络攻击具有良好的识别和控制能力。

在实际应用中，可以采用入侵取证技术对上述风险对象对应的攻击源进行追踪。具体地，可以利用计算机的软硬件技术，按照符合法律规范的方式，对首次出现的风险对象对应攻击源的入侵、破坏、欺诈、攻击等攻击行为进行识别、保存、分析和提交数字证据。例如，可以依据上述风险对象对应的 IP 地址、MAC 地址追踪攻击源的地址，又如，可以依据系统的日志记录中记录的用户登陆痕迹记录攻击源的登陆痕迹，或者，可以依据防火墙日志中记录的攻击源的原地址信息确定攻击源的地址等，本发明实施例对于对所述风险对象对应的攻击源进行追踪的具体过程不加以限制。

15

参照图 5，示出了根据本发明一个实施例的一种基于局域网的安全检测方法的步骤流程图，具体可以包括如下步骤：

步骤 501、控制终端获取用户输入的风险规则；

20 步骤 502、控制终端获取用户输入的修复规则，所述修复规则用于用户终端的扫描结果命中所述风险规则时的安全性修复；

步骤 503、控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

步骤 504、控制终端向局域网内的用户终端下发所述修复规则，以使所述用户终端在扫描结果命中所述风险规则时进行安全性修复；

25 步骤 505、控制终端接收所述局域网内的用户终端上报的扫描结果；

步骤 506、控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

相对于图 1 所示实施例，本实施例的控制终端还可以向局域网内的用户

终端下发修复规则，以使所述用户终端在扫描结果命中所述风险规则时进行安全性修复；其中，控制终端可以向用户终端同时下发上述风险规则和上述修复，以使用户终端在扫描结果命中所述风险规则时，及时地进行安全性修复。

5 例如，在将用户终端的密码作为风险对象时，该风险对象对应的风险规则可用于扫描用户终端的密码是否符合预置的复杂性要求等；该风险对象对应的修复规则中包括有修复指示值；其中，修复指示值等于 1，表示在扫描结果命中风险规则时，不向控制终端上报扫描结果；修复指示值等于 2，表示在扫描结果命中风险规则时，向控制终端上报扫描结果；修复指示值等于 3，表示除了在扫描结果命中风险规则时向控制终端上报扫描结果外，还提示用户修改密码；修复指示值等于 4，表示除了在扫描结果命中风险规则时向控制终端上报扫描结果外，锁定计算机，并强制用户修改密码。其中，上述修复指示值可以依据扫描结果确定，例如，在密码的复杂度符合第一复杂度条件时，确定修复指示值的值为 1；在密码的复杂度符合第二复杂度条件时，确定修复指示值的值为 2；在密码的复杂度符合第三复杂度条件时，确定修复指示值的值为 3；在密码的复杂度符合第四复杂度条件时，确定修复指示值的值为 4，其中，第一复杂度条件、第二复杂度条件、第三复杂度条件和第四复杂度条件对应的复杂度递减。

20 可以理解，上述依据修复规则进行安全性修复的过程只是作为示例，实际上本领域技术人员可以根据实际应用需求，采用风险对象或者风险规则对应的修复规则，本发明实施例对于具体的修复规则不加以限制。

25 对于方法实施例，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，本发明实施例并不受所描述的动作顺序的限制，因为依据本发明实施例，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可选实施例，所涉及的动作并不一定是本发明实施例所必须的。

参照图 6，示出了根据本发明一个实施例的一种基于局域网的安全检测

装置的结构框图，具体可以包括如下模块：

获取模块 601，配置为获取用户输入的风险规则；

下发模块 602，配置为向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

接收模块 603，配置为接收所述局域网内的用户终端上报的扫描结果；

及

分析模块 604，配置为依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

在本发明的一种可选实施例中，所述风险规则具体可以包括：与风险对象相关的规则，则所述分析模块 604，具体可以包括：

分析子模块，配置为依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性。

在本发明的另一种可选实施例中，所述分析子模块，具体可以包括：

趋势分析单元，配置为依据所述局域网内的用户终端在一个时间段内的扫描结果，分析得到所述风险对象的生长趋势；及

判定单元，配置为依据所述风险对象的生长趋势，判定所述风险对象的风险性。

在本发明的再一种可选实施例中，所述装置还可以包括：

生成模块，配置为在所述风险对象的风险性符合预置条件时，生成用于清理所述风险对象的风险规则；

输入模块，配置为将所生成的风险规则输入至所述下发模块。

在本发明的又一种可选实施例中，所述装置还可以包括：

追踪模块，配置为在所述风险对象的风险性符合预置条件时，依据所述局域网内首次出现的风险对象的信息，对所述风险对象对应的攻击源进行追踪。

在本发明的一种可选实施例中，所述获取模块 601，还可以配置为获取用户输入的修复规则，所述修复规则用于用户终端的扫描结果命中所述风险

规则时的安全性修复;

所述下发模块 602, 还可以配置为向局域网内的用户终端下发所述修复规则, 以使所述用户终端在扫描结果命中所述风险规则时进行安全性修复。

在本发明的另一种可选实施例中, 所述风险规则具体可以包括: 与风险对象相关的规则, 所述风险对象具体可以包括如下对象中的至少一种:

进程、服务、计划任务、安装应用、端口、文件、操作系统、注册表、用户账号和用户权限。

对于装置实施例而言, 由于其与方法实施例基本相似, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。

10

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
5 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
10 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
10 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
15 理解，可以在实践中使用微处理器或者数字信号处理器（DSP，Digital Signal
Process）来实现根据本发明实施例的基于局域网的安全检测方法和装置中的
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，
20 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平台上下
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 7 示出了用于执行根据本发明的基于局域网的安全检测方法的
计算设备。该计算设备传统上包括处理器 710 和以存储器 720 形式的
程序产品或者可读介质。存储器 720 可以是诸如闪存、EEPROM（电可
25 擦除可编程只读存储器）、EPROM 或者 ROM 之类的电子存储器。存储器
720 具有用于执行上述方法中的任何方法步骤的程序代码 731 的存储
空间 730。例如，用于程序代码的存储空间 730 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 731。这些程序代码可以从一个或

者多个程序产品中读出或者写入到这一个或者多个程序产品中。这些程序产品包括诸如存储卡之类的程序代码载体。这样的程序产品通常为如参考图 8 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 7 的计算设备中的存储器 720 类似布置的存储段、存储空间等。程序代码
5 可以例如以适当形式进行压缩。通常，存储单元包括可读代码 731'，即可以由例如诸如 710 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

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
10 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“包括”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
15 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。

权 利 要 求 书

1、一种基于局域网的安全检测方法，包括：

控制终端获取用户输入的风险规则；

控制终端向局域网内的用户终端下发所述风险规则，以使所述用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

5 控制终端接收所述局域网内的用户终端上报的扫描结果；

控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析。

2、如权利要求 1 所述的方法，其特征在于，所述风险规则包括：与风险对象相关的规则，则所述控制终端依据所述局域网内的用户终端的扫描结果，对所述局域网的安全性进行分析的步骤，包括：

控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性。

3、如权利要求 2 所述的方法，其特征在于，所述控制终端依据所述局域网内的用户终端的扫描结果，分析得到所述风险对象的风险性的步骤，包括：

控制终端依据所述局域网内的用户终端在一个时间段内的扫描结果，分析得到所述风险对象的生长趋势；

依据所述风险对象的生长趋势，判定所述风险对象的风险性。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述方法还包括：

20 在所述风险对象的风险性符合预置条件时，生成用于清理所述风险对象的风险规则；

将所生成的风险规则输入至所述控制终端向局域网内的用户终端下发所述风险规则的步骤。

5、如权利要求 2 或 3 所述的方法，其特征在于，所述方法还包括：

25 在所述风险对象的风险性符合预置条件时，依据所述局域网内首次出现的风险对象的信息，对所述风险对象对应的攻击源进行追踪。

6、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述方法还包括：

控制终端获取用户输入的修复规则，所述修复规则用于用户终端的扫描

结果命中所述风险规则时的安全性修复；

控制终端向局域网内的用户终端下发所述修复规则，以使所述用户终端在扫描结果命中所述风险规则时进行安全性修复。

7、如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述风险规则包
5 括：与风险对象相关的规则，所述风险对象包括如下对象中的至少一种：

进程、服务、计划任务、安装应用、端口、文件、操作系统、注册表、
用户账号和用户权限。

8、一种基于局域网的安全检测装置，应用于控制终端，包括：
10 获取模块，配置为获取用户输入的风险规则；

下发模块，配置为向局域网内的用户终端下发所述风险规则，以使所述
用户终端依据所述风险规则在主机上进行扫描，以得到相应的扫描结果；

接收模块，配置为接收所述局域网内的用户终端上报的扫描结果；及

15 分析模块，配置为依据所述局域网内的用户终端的扫描结果，对所述局
域网的安全性进行分析。

9、如权利要求 8 所述的装置，其特征在于，所述风险规则包括：与风
险对象相关的规则，则所述分析模块，包括：

分析子模块，配置为依据所述局域网内的用户终端的扫描结果，分析得
到所述风险对象的风险性。

20 10、如权利要求 9 所述的装置，其特征在于，所述分析子模块，包括：

趋势分析单元，配置为依据所述局域网内的用户终端在一个时间段内的
扫描结果，分析得到所述风险对象的生长趋势；及

判定单元，配置为依据所述风险对象的生长趋势，判定所述风险对象的
风险性。

25 11、如权利要求 9 或 10 所述的装置，其特征在于，所述装置还包括：

生成模块，配置为在所述风险对象的风险性符合预置条件时，生成用于
清理所述风险对象的风险规则；

输入模块，配置为将所生成的风险规则输入至所述下发模块。

12、如权利要求 9 或 10 所述的装置，其特征在于，所述装置还包括：

追踪模块，配置为在所述风险对象的风险性符合预置条件时，依据所述局域网内首次出现的风险对象的信息，对所述风险对象对应的攻击源进行追踪。

5 13、如权利要求 8 或 9 或 10 所述的装置，其特征在于，所述获取模块，还配置为获取用户输入的修复规则，所述修复规则用于用户终端的扫描结果命中所述风险规则时的安全性修复；

所述下发模块，还配置为向局域网内的用户终端下发所述修复规则，以使所述用户终端在扫描结果命中所述风险规则时进行安全性修复。

10 14、如权利要求 8 或 9 或 10 所述的装置，其特征在于，所述风险规则包括：与风险对象相关的规则，所述风险对象包括如下对象中的至少一种：

进程、服务、计划任务、安装应用、端口、文件、操作系统、注册表、用户账号和用户权限。

15 15、一种程序，包括可读代码，当所述可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1 至 7 中的任一项所述的基于局域网的安全检测方法。

16、一种可读介质，其中存储了如权利要求 15 所述的程序。

说明书附图

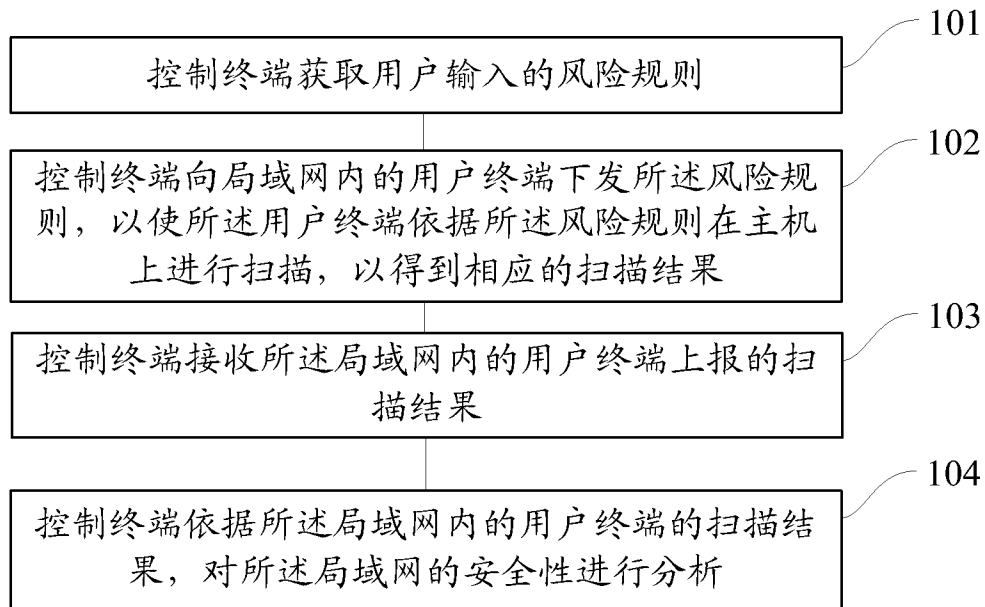


图 1

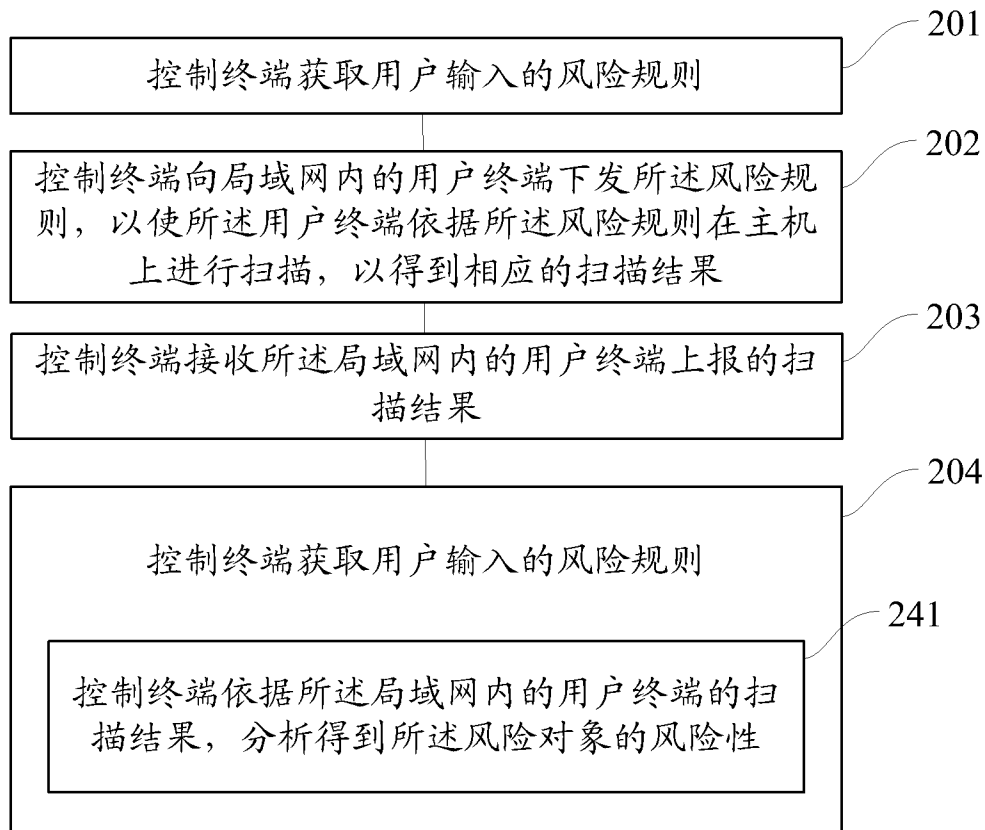


图 2

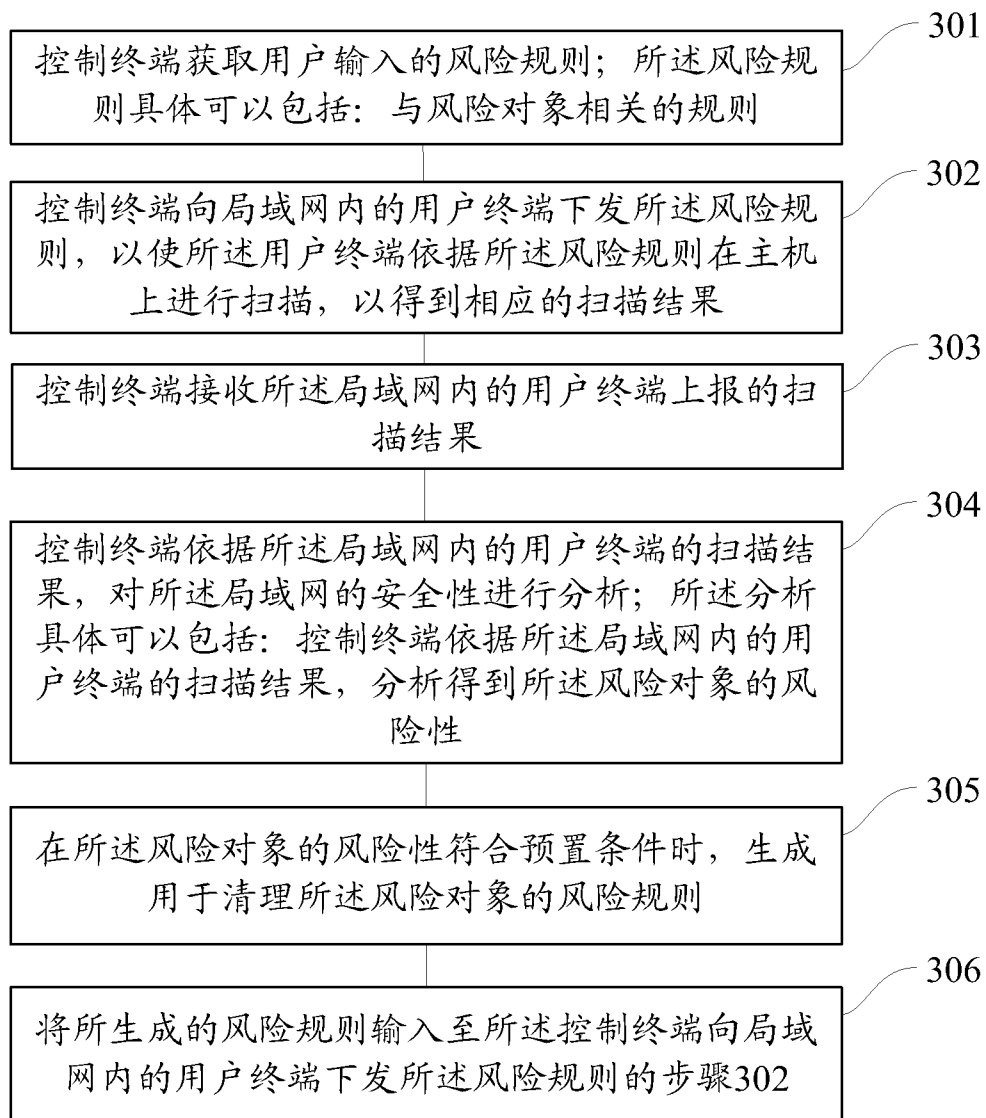


图 3

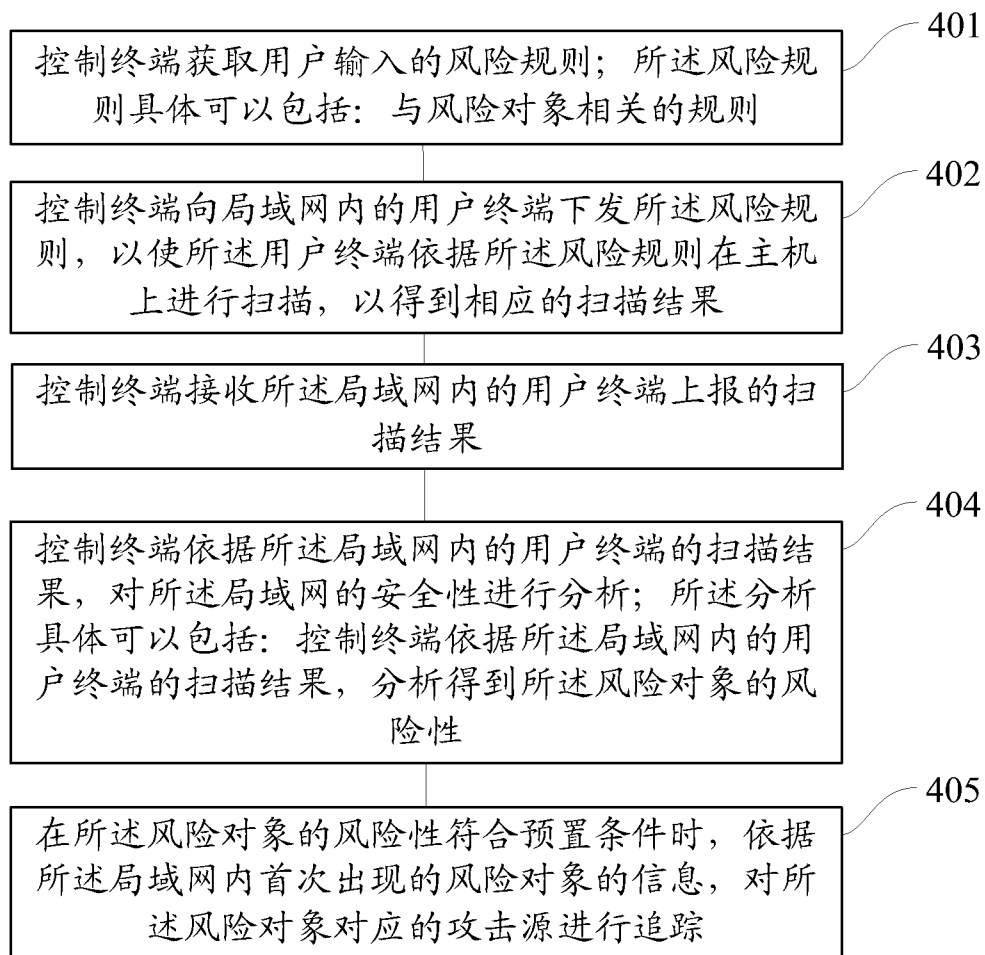


图 4

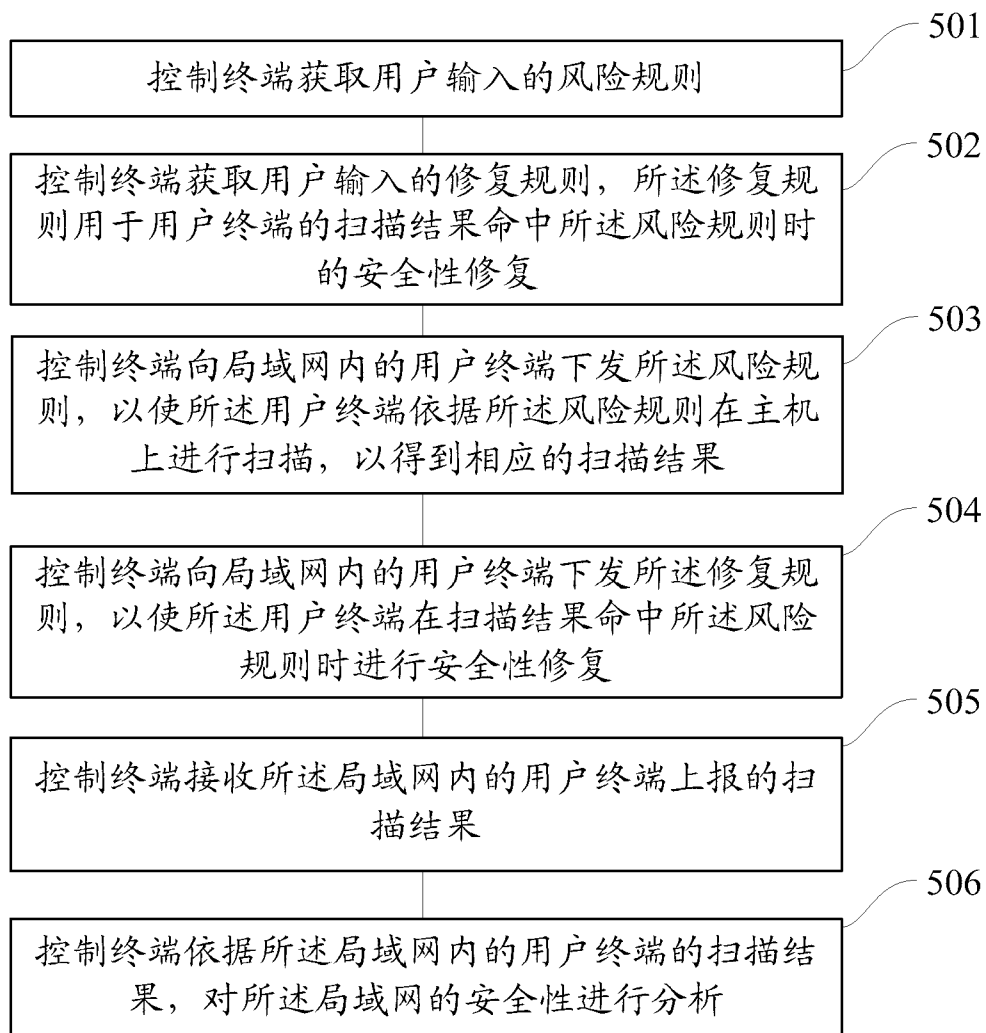


图 5

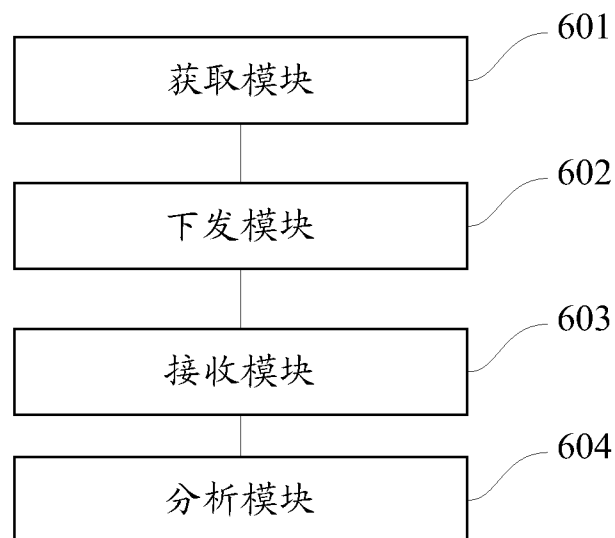


图 6

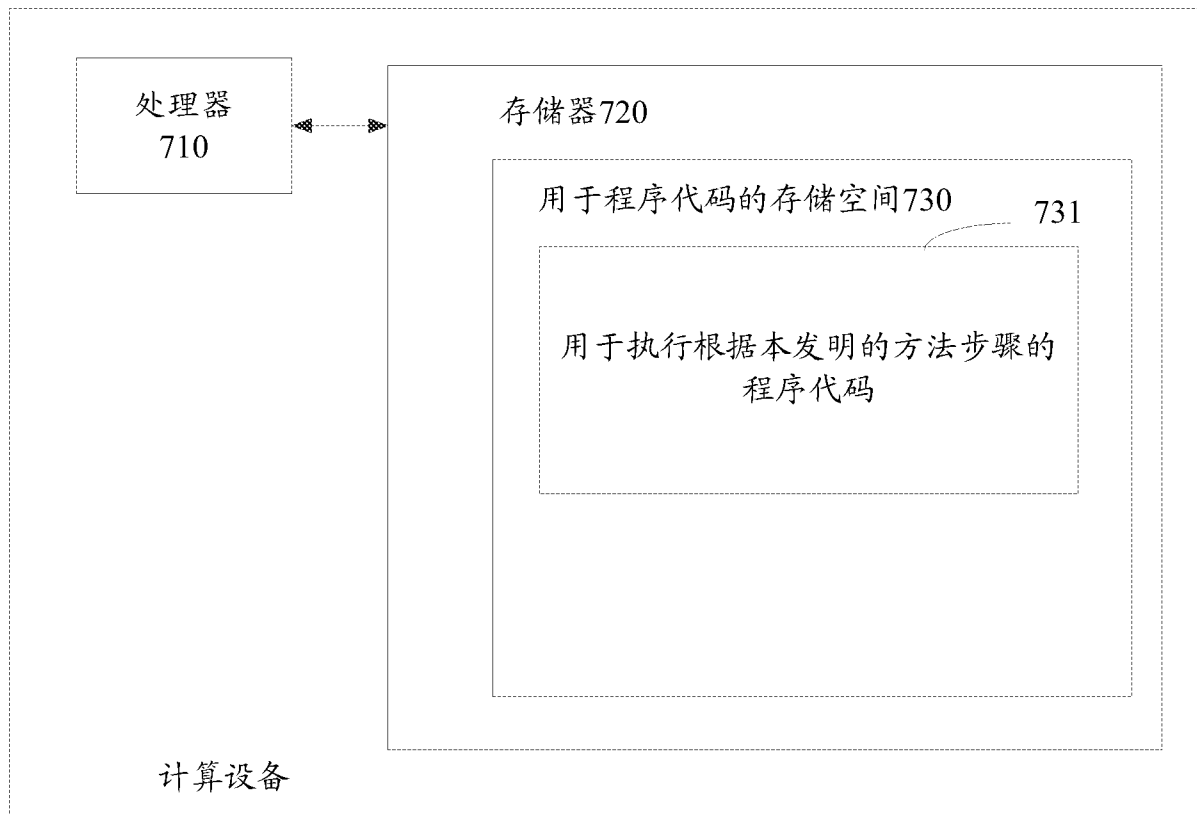


图 7

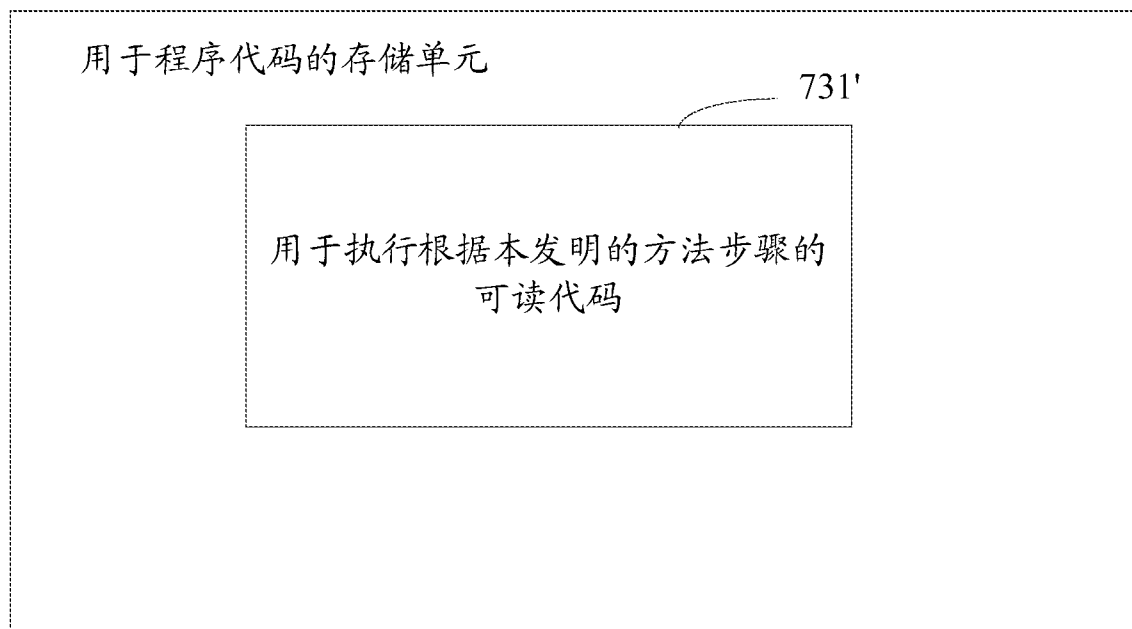


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/104919

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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

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)

CNKI, CNPAT, WPI, EPODOC: wireless, local area network, threaten, bug, feature, host machine, repair, strategy, hidden trouble, unknown, potential, user, port, authority, account number, process, file, environment, virus, wooden horse, enterprise network, campus network, score, grade, WLAN, terminal, local, area, network, scanning, risk, rule, report, control, security, detection, LAN, host, input

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105262777 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 20 January 2016 (20.01.2016), description, paragraphs 0006-0037 and 0046-0096	1-16
X	CN 102413011 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 11 April 2012 (11.04.2012), description, paragraphs 0008-0040 and 0088-0135	1-16
A	CN 101835144 A (UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA), 15 September 2010 (15.09.2010), the whole document	1-16
A	WO 2007066333 A1 (SWARTZ, A.R. et al.), 14 June 2007 (14.06.2007), the whole document	1-16

☐ 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 10 January 2017 (10.01.2017)	Date of mailing of the international search report 25 January 2017 (25.01.2017)
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 NIU, Xiaojia Telephone No.: (86-10) 61648247

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/104919

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105262777 A	20 January 2016	None	
CN 102413011 A	11 April 2012	CN 102413011 B	30 September 2015
CN 101835144 A	15 September 2010	None	
WO 2007066333 A1	14 June 2007	EP 1958116 A1	20 August 2008
		IL 191687 D0	11 February 2009
		JP 2009521020 A	28 May 2009
		US 2007180509 A1	02 August 2007

A. 主题的分类 H04L 29/06 (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 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)) CNKI, CNPAT, WPI, EPODOC: 无线, 局域网, 安全, 检测, 威胁, 漏洞, 特征, 规则, 扫描, 主机, 修复, 策略, 隐患, 未知, 潜在, 危险, 终端, 用户, 端口, 权限, 账号, 进程, 文件, 环境, 病毒, 木马, 企业网, 校园网, 评分, 等级, 评级, WLAN, terminal, local, area, network, scanning, risk, rule, report, control, security, detection, LAN, host, input																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 105262777 A (北京奇虎科技有限公司等) 2016年 1月 20日 (2016 - 01 - 20) 说明书第0006-0037, 0046-0096段</td> <td>1-16</td> </tr> <tr> <td>X</td> <td>CN 102413011 A (奇智软件北京有限公司) 2012年 4月 11日 (2012 - 04 - 11) 说明书第0008-0040, 0088-0135段</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 101835144 A (中国科学技术大学) 2010年 9月 15日 (2010 - 09 - 15) 全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>WO 2007066333 A1 (SWARTZ, ALON, R. 等) 2007年 6月 14日 (2007 - 06 - 14) 全文</td> <td>1-16</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 105262777 A (北京奇虎科技有限公司等) 2016年 1月 20日 (2016 - 01 - 20) 说明书第0006-0037, 0046-0096段	1-16	X	CN 102413011 A (奇智软件北京有限公司) 2012年 4月 11日 (2012 - 04 - 11) 说明书第0008-0040, 0088-0135段	1-16	A	CN 101835144 A (中国科学技术大学) 2010年 9月 15日 (2010 - 09 - 15) 全文	1-16	A	WO 2007066333 A1 (SWARTZ, ALON, R. 等) 2007年 6月 14日 (2007 - 06 - 14) 全文	1-16
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	CN 105262777 A (北京奇虎科技有限公司等) 2016年 1月 20日 (2016 - 01 - 20) 说明书第0006-0037, 0046-0096段	1-16															
X	CN 102413011 A (奇智软件北京有限公司) 2012年 4月 11日 (2012 - 04 - 11) 说明书第0008-0040, 0088-0135段	1-16															
A	CN 101835144 A (中国科学技术大学) 2010年 9月 15日 (2010 - 09 - 15) 全文	1-16															
A	WO 2007066333 A1 (SWARTZ, ALON, R. 等) 2007年 6月 14日 (2007 - 06 - 14) 全文	1-16															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。 <table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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													
* 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 2017年 1月 10日		国际检索报告邮寄日期 2017年 1月 25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		受权官员 牛晓佳 电话号码 (86-10) 61648247															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/104919

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	105262777	A	2016年 1月 20日	无			
CN	102413011	A	2012年 4月 11日	CN	102413011	B	2015年 9月 30日
CN	101835144	A	2010年 9月 15日	无			
WO	2007066333	A1	2007年 6月 14日	EP	1958116	A1	2008年 8月 20日
				IL	191687	D0	2009年 2月 11日
				JP	2009521020	A	2009年 5月 28日
				US	2007180509	A1	2007年 8月 2日