(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105100048 B
(45)授权公告日 2018.06.01

(21)申请号 201510276364.7

(22)申请日 2015.05.26

(65)同一申请的已公布的文献号
申请公布号 CN 105100048 A

(43)申请公布日 2015.11.25

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 孟齐源 王万春

(74)专利代理机构 北京市隆安律师事务所 11323
代理人 权鲜枝 何立春

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 103841101 A,2014.06.04,
CN 104219670 A,2014.12.17,
CN 104270761 A,2015.01.07,

审查员 来文燕

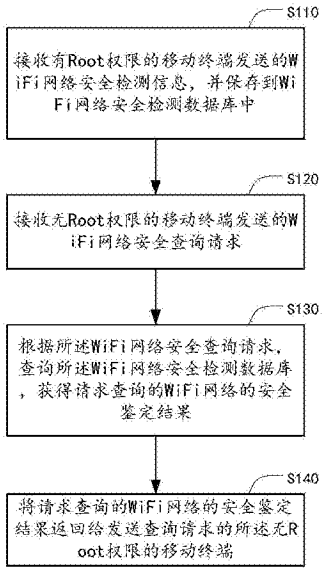
权利要求书3页 说明书13页 附图3页

(54)发明名称

WiFi网络安全鉴定方法、服务器、客户端装置和系统

(57)摘要

本发明公开了一种WiFi网络安全鉴定方法、服务器、客户端装置和系统。所述方法包括:接收有Root权限的移动终端发送的WiFi网络安全检测信息,并保存到WiFi网络安全检测数据库中;接收无Root权限的移动终端发送的WiFi网络安全查询请求;根据所述WiFi网络安全查询请求,查询所述WiFi网络安全检测数据库,获得请求查询的WiFi网络的安全鉴定结果;将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。本发明的技术方案,使得无Root权限的移动终端也能够获得WiFi安全性的鉴定信息。



CN 105100048 B

1.一种WiFi网络安全鉴定方法，其中，该方法包括：

接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；

接收无Root权限的移动终端发送的WiFi网络安全查询请求；

根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

2.如权利要求1所述的方法，其中，所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

移动终端检测到的地址解析协议ARP欺骗检测信息；

移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

移动终端本地的域名系统DNS服务器地址。

3.如权利要求1所述的方法，其中，根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果包括：

如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

4.如权利要求1-3中任一项所述的方法，其中，该方法进一步包括：

接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

向发送查询请求的所述有Root权限的移动终端返回判断结果。

5.一种WiFi网络安全鉴定方法，其中，该方法包括：

判断是否能够获取到移动终端的Root权限；

如果获取到Root权限，则检测移动终端所接入的WiFi网络的安全性，并向服务器发送WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

如果获取不到Root权限，则向服务器发送WiFi网络安全查询请求，接收服务器返回的安全鉴定结果并展示给用户。

6.如权利要求5所述的方法，其中，所述检测移动终端所接入的WiFi网络的安全性包括如下中的一种或多种：

在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

7.如权利要求5所述的方法，其中，所述向服务器发送WiFi网络安全检测信息包括：

WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

移动终端检测到的地址解析协议ARP欺骗检测信息；

移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

移动终端本地的域名系统DNS服务器地址。

8.如权利要求5所述的方法，其中，该方法进一步包括：

如果获取到Root权限，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

接收服务器返回的所述DNS服务器地址是否合法的判断结果。

9.一种WiFi网络安全鉴定服务器，其中，该服务器包括：

接收单元，适于接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；以及接收无Root权限的移动终端发送的WiFi网络安全查询请求；

存储单元，适于保存WiFi网络安全检测数据库；

鉴定单元，适于根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

发送单元，适于将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

10.如权利要求9所述的服务器，其中，所述接收单元接收的所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

移动终端检测到的地址解析协议ARP欺骗检测信息；

移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

移动终端本地的域名系统DNS服务器地址。

11.如权利要求9所述的服务器，其中，

所述鉴定单元，适于查询所述WiFi网络安全检测数据库，如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

12.如权利要求9-11中任一项所述的服务器，其中，

所述接收单元，进一步适于接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

所述鉴定单元，进一步适于根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

所述存储单元，进一步适于存储DNS库；

所述发送单元，进一步适于向发送查询请求的所述有Root权限的移动终端返回判断结果。

13.一种WiFi网络安全鉴定客户端装置，其中，该客户端装置包括：

判断单元，适于判断是否能够获取到移动终端的Root权限；

安全检测单元，适于在获取到Root权限时，检测移动终端所接入的WiFi网络的安全性，得到WiFi网络安全检测信息；

发送单元，适于向服务器发送所述WiFi网络安全检测信息，以使得服务器能够根据这

些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

以及所述发送单元，还适于在获取不到Root权限时，则向服务器发送WiFi网络安全查询请求；

接收单元，适于接收服务器返回的安全鉴定结果并展示给用户。

14.如权利要求13所述的客户端装置，其中，

所述安全检测单元，适于在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

和/或，

所述安全检测单元，适于根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

15.如权利要求13所述的客户端装置，其中，所述发送单元向服务器发送WiFi网络安全检测信息包括：

WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

移动终端检测到的地址解析协议ARP欺骗检测信息；

移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

移动终端本地的域名系统DNS服务器地址。

16.如权利要求13所述的客户端装置，其中，

所述发送单元，进一步适于在获取到Root权限时，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

所述接收单元，进一步适于接收服务器返回的所述DNS服务器地址是否合法的判断结果。

17.一种WiFi网络安全鉴定系统，其中，该系统包括：如权利要求9-12中任一项所述的WiFi网络安全鉴定服务器，和如权利要求13-16中任一项所述的WiFi网络安全鉴定客户端装置。

WiFi网络安全鉴定方法、服务器、客户端装置和系统

技术领域

[0001] 本发明涉及网络安全技术领域，具体涉及一种WiFi网络安全鉴定方法、服务器、客户端装置和系统。

背景技术

[0002] 当今社会网络通信技术发达，随着无线网络的普及，随处可见提供免费WiFi的标识。然而免费WiFi存在很大安全隐患，常见的有如下几种类型：第一种是DNS(域名系统)劫持，即通过篡改DNS进行劫持；第二种是中间人攻击，例如利用ARP(地址解析协议)欺骗、ICMP(互联网控制报文协议，Internet Control Message Protocol)劫持对用户所在的网络进行攻击。连入WiFi网络的移动终端(如手机)一旦被劫持，将会导致用户的各种上网的情况会被监控，数据被窃听，导致信息泄露，甚至访问的网站被劫持，直接导致受骗。

[0003] 这个问题在手机里的解决方案是，针对ARP欺骗、SMB欺骗需要手机有Root能力，即手机获先得Root权限，才能进一步利用发包等功能检测WiFi网络的安全性。由于大多数手机没有Root权限，便不能利用此项技术解决判断WiFi网络安全性的问题，即没有Root权限的手机无法获知WiFi网络是否存在风险。

发明内容

[0004] 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WiFi网络安全鉴定方法、服务器、客户端装置和系统。

[0005] 依据本发明的一个方面，提供了一种WiFi网络安全鉴定方法，该方法包括：

[0006] 接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；

[0007] 接收无Root权限的移动终端发送的WiFi网络安全查询请求；

[0008] 根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

[0009] 将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0010] 可选地，所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0011] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0012] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0013] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0014] 移动终端本地的域名系统DNS服务器地址。

[0015] 可选地，根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果包括：

[0016] 如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在

风险，否则确定请求查询的WiFi网络安全。

[0017] 可选地，该方法进一步包括：

[0018] 接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0019] 根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

[0020] 向发送查询请求的所述有权限的移动终端返回判断结果。

[0021] 根据本发明的另一方面，提供一种WiFi网络安全鉴定方法，该方法包括：

[0022] 判断是否能够获取到移动终端的Root权限；

[0023] 如果获取到root权限，则检测移动终端所接入的WiFi网络的安全性，并向服务器发送WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0024] 如果获取不到Root权限，则向服务器发送WiFi网络安全查询请求，接收服务器返回的安全鉴定结果并展示给用户。、

[0025] 可选地，述检测移动终端所接入的WiFi网络的安全性包括如下中的一种或多种：

[0026] 在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0027] 根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0028] 可选地，所述向服务器发送WiFi网络安全检测信息包括：

[0029] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0030] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0031] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0032] 移动终端本地的域名系统DNS服务器地址。

[0033] 可选地，该方法进一步包括：

[0034] 如果获取到Root权限，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0035] 接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0036] 根据本发明的另一方面，提供一种WiFi网络安全鉴定服务器，该服务器包括：

[0037] 接收单元，适于接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；以及接收无Root权限的移动终端发送的WiFi网络安全查询请求；

[0038] 存储单元，适于保存WiFi网络安全检测数据库；

[0039] 鉴定单元，适于根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

[0040] 发送单元，适于将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0041] 可选地，所述接收单元接收的所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0042] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0043] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0044] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0045] 移动终端本地的域名系统DNS服务器地址。

[0046] 可选地，所述鉴定单元，适于查询所述WiFi网络安全检测数据库，如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

[0047] 可选地，所述接收单元，进一步适于接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0048] 所述鉴定单元，进一步适于根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

[0049] 所述存储单元，进一步适于存储DNS库；

[0050] 所述发送单元，进一步适于向发送查询请求的所述有权限的移动终端返回判断结果。

[0051] 根据本发明的另一方面，提供一种WiFi网络安全鉴定客户端装置，该客户端装置包括：

[0052] 判断单元，适于判断是否能够获取到移动终端的Root权限；

[0053] 安全检测单元，适于在获取到root权限时，检测移动终端所接入的WiFi网络的安全性，得到WiFi网络安全检测信息；

[0054] 发送单元，适于向服务器发送所述WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0055] 以及所述发送单元，还适于在获取不到Root权限时，则向服务器发送WiFi网络安全查询请求；

[0056] 接收单元，适于接收服务器返回的安全鉴定结果并展示给用户。

[0057] 可选地，所述安全检测单元，适于在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0058] 和/或，

[0059] 所述安全检测单元，适于根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0060] 可选地，所述发送单元，进一步适于在获取到Root权限时，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0061] 所述接收单元，进一步适于接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0062] 根据本发明的另一方面，提供一种WiFi网络安全鉴定系统，该系统包括：如上述任一项所述的WiFi网络安全鉴定服务器，和如上述任一项所述的WiFi网络安全鉴定客户端装置。

[0063] 根据本发明的技术方案，可以通过有Root权限的移动终端提供WiFi安全状态的鉴定，将结果共享至云端WiFi网络安全检测数据库，使得无Root权限的移动终端不再需要Root，仅通过查询云端的网络安全检测数据库便可获得WiFi安全性的鉴定信息，由此解决了现有技术中手机必须通过Root才能验证WiFi安全性的技术问题。

[0064] 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

[0065] 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：

[0066] 图1示出了根据本发明一个实施例的一种WiFi网络安全鉴定方法；

[0067] 图2示出了根据本发明另一个实施例的种WiFi网络安全鉴定方法；

[0068] 图3示出了根据本发明另一个实施例的一种WiFi网络安全鉴定服务器的结构示意图；

[0069] 图4示出了根据本发明另一个实施例的一种WiFi网络安全鉴定客户端装置的结构示意图；以及

[0070] 图5示出了根据本发明另一个实施例的一种WiFi网络安全鉴定系统的示意图。

具体实施方式

[0071] 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。

[0072] 图1示出了根据本发明一个实施例的一种WiFi网络安全鉴定方法。如图1所示，该方法包括：

[0073] 步骤S110，接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中。

[0074] 这里，有Root权限的移动终端可以利用发包等功能检测WiFi网络的安全性。

[0075] 步骤S120，接收无Root权限的移动终端发送的WiFi网络安全查询请求。

[0076] WiFi网络安全查询请求中至少包括要查询的WiFi网络的标识。

[0077] 步骤S130，根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果。

[0078] 步骤S140，将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0079] 图1所示的方法中，通过有Root权限的移动终端进行WiFi网络安全检测获取网络安全检测信息并共享到服务器端的WiFi网络安全检测数据库，使得无Root权限的移动终端不需要Root，通过查询服务器端的WiFi网络安全检测数据库即可进行WiFi网络的安全鉴定。

[0080] 在本发明的一个实施例中，图1所示方法的步骤S110中所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0081] WiFi网络的标识以及WiFi网络是否存在风险的描述信息；WiFi网络是否存在风险

的描述信息包括如下信息中的一个或多个:移动终端检测到的地址解析协议ARP欺骗检测信息;移动终端检测到的互联网控制报文协议ICMP攻击检测信息;移动终端本地的域名系统DNS服务器地址。

[0082] WiFi网络的标识具体可以是:SSID,和/或BSSID。

[0083] 移动终端检测到的地址解析协议ARP欺骗检测信息具体可以是:存在ARP欺骗、不存在ARP欺骗或未知。ICMP攻击检测信息具体也可以是:存在、不存在或未知。

[0084] 在本发明的实施例中,通过发ARP请求包来看网络回应的ARP应答,进而判断是否存在ARP欺骗。发送一个ARP请求后,可能收到超过不止一个应答包,而且这种应答包的MAC地址是不一样的,那么这个时候代表网络里面一定存在这种劫持欺骗,那么移动终端就能识别出当前的WiFi网络中存在ARP欺骗。

[0085] 当检测发现有ARP攻击时:第一,阻止主机A对外发送广播包:因为广播包会被交换机泛洪,送到局域网内的每一台主机,而欺骗者主机可通过设置网卡混杂模式1,侦听到主机A的MAC,从而使主机A被局域网内的其它主机发现。第二,阻止主机A回应局域网内的ARP Request包(ARP请求包),防止主机A回应欺骗主机发送的ARP Request包。第三,放过发给网关的ARP Reply包(ARP回应包);如果本机向网关发送ARP Request包,需要拦截并修改为ARP Reply包发送给网关。因为必须放过ARP Replay,且修改ARP Request包为ARP Reply包并发送给网关才能够保证主机A能够访问广域网。

[0086] 对于ARP欺骗检测信息可以包括多种:防止篡改方法(即ARP缓存表保护策略)有多种,本实施例中采用了入口过滤欺骗包方法,即,判断入栈的ARP报文中的网关IP地址与网关MAC地址的对应关系与本机的ARP缓存表中的对应关系是否一致,若不一致,禁止修改本机的ARP缓存表;或者,判断入栈的ARP报文中的本机IP地址与本机MAC地址的对应关系与本机的ARP缓存表中的对应关系是否一致,若不一致,禁止修改本机的ARP缓存表。采用入口过滤方法,阻止非法ARP包,允许合法的ARP包,由于从入口进行了拦截,ARP地址表无法被欺骗。其优点在于,无需禁止用户对ARP地址表的操作即可实现ARP地址表保护功能。

[0087] 在本发明的一个实施例中,图1所示方法的步骤S130中根据所述WiFi网络安全查询请求,查询所述WiFi网络安全检测数据库,获得请求查询的WiFi网络的安全鉴定结果包括:

[0088] 如果WiFi网络安全检测数据库中的数据表明,在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险,则确定请求查询的WiFi网络存在风险,否则确定请求查询的WiFi网络安全。

[0089] 例如,WiFi网络安全查询请求查询的是SSID为12345678的WiFi网络,则根据WiFi网络安全检测数据库判断在过去的5分钟内是否有超过10个移动终端上报了该SSID为12345678的WiFi网络存在风险,是则确定存在风险,并通知查询者。

[0090] 在本发明的一个实施例中,图1所示方法进一步包括:接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求;根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法;向发送查询请求的所述有权限的移动终端返回判断结果。

[0091] 在本实施例中,客户端侧将DNS发送给云端服务器端,由服务器根据维护的DNS库进行判断。其中DNS库中可以包括DNS黑名单(恶意DNS列表)和白名单(合法DNS列表),白名

单记录中的安全网站都是事先经过安全验证的，而黑名单中的安全网站都是不安全的。因此可以向客户端反馈DNS是否安全。

[0092] 在本发明的一个实施例中，云端DNS库的主要判断规则，

[0093] 1.DNS的安全等级判断规则：如DNS与预先生成的恶意DNS列表匹配成功，则DNS安全等级为危险；如DNS与预先生成的合法DNS列表匹配成功，则DNS安全等级为安全；如DNS与预先生成的恶意DNS列表、预先生成的合法DNS列表均匹配失败，则DNS安全等级为警告。

[0094] 2.管理密码的安全等级判断规则：如管理密码为默认密码，则安全等级为危险；如管理密码为弱密码，则安全等级为警告；如管理密码不为默认密码且不为弱密码，则安全等级为安全。

[0095] 3.远端WEB管理的安全等级判断规则：如远端WEB管理开启，则安全等级为危险；如远端WEB管理未开启，则安全等级为安全。

[0096] 4.隔离区主机服务的安全等级判断规则：如隔离区主机服务开启，则安全等级为警告；如隔离区主机服务未开启，则安全等级为安全。

[0097] 5.无线网络安全配置的安全等级判断规则：如无线网络开启，且未设置密码或者密码认证方式不安全，则安全等级为警告；如无线网络未开启，或者无线网络密码认证方式安全，则安全等级为安全。

[0098] 在具体实现中，每一项网络配置均有对应的安全等级判断规则，安全等级判断规则可由安全厂商设置，保存在云检测端服务器中，定期或不定期进行更新。

[0099] 其中，DNS的安全等级判断规则为：如DNS符合第一DNS安全规则，则DNS安全等级为危险；如DNS符合第二DNS安全规则，则DNS安全等级为安全；如DNS符合第三DNS安全规则，则DNS安全等级为警告。

[0100] 进一步的，第一DNS安全规则为DNS与预先生成的恶意DNS列表(黑名单)匹配成功；第二DNS安全规则为DNS与预先生成的合法DNS列表(白名单)匹配成功；第三DNS安全规则为DNS与预先生成的恶意DNS列表、预先生成的合法DNS列表均匹配失败。

[0101] 预先生成的恶意DNS列表、合法DNS列表可以从第三方获得，也可以为由云检测端服务器数据库中分别预先收集的一组非法DNS地址、一组合法DNS地址，或者也可以为客户端数据库中分别预先收集的一组非法DNS地址、一组合法DNS地址，或者也可以为从云检测端服务器上下载至客户端数据库中的恶意DNS列表和合法DNS列表。

[0102] 终端的本地也可以配置DNS库，但需要不断的更新，且DNS库非常庞大，因此DNS劫持一般是通过云端查询来判断。

[0103] 由此，有效地遏制了黑客通过篡改DNS而给网民带来的诸如网络钓鱼、隐私窃取等安全风险。

[0104] 图2示出了根据本发明另一个实施例的一种WiFi网络安全鉴定方法。图2所示，该方法包括：

[0105] 步骤S210，判断是否能够获取到移动终端的Root权限；

[0106] 步骤S220，如果获取到root权限，则检测移动终端所接入的WiFi网络的安全性，并向服务器发送WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0107] 步骤S230，如果获取不到Root权限，则向服务器发送WiFi网络安全查询请求，接收

服务器返回的安全鉴定结果并展示给用户。

[0108] 图2所示的方法，使得移动终端在有Root权限，和无Root权限的情况下都能够获得WiFi网络的安全鉴定结果

[0109] 在本发明的一个实施例中，图2所示方法的步骤S220所述检测移动终端所接入的WiFi网络的安全性包括如下中的一种或多种：

[0110] 在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0111] 根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0112] 例如，移动终端连入WiFi的时候通过Root选项拿到Root权限，之后通过发ARP请求包来看网络回应的ARP应答。正常时，一个ARP请求出去，一般询问网关，那么网关肯定是在的，返回一个MAC地址。如果存在欺骗的话它是无差别的欺骗，当发送一个ARP请求后，可能收到超过不止一个应答包，而且这种应答包的MAC地址是不一样的，那么这个时候代表网络里面一定存在这种劫持欺骗，那么移动终端就能识别出当前的WiFi网络中存在ARP欺骗。

[0113] 在本发明的一个实施例中，图2所示方法的步骤S220所述向服务器发送WiFi网络安全检测信息包括：

[0114] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0115] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0116] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0117] 移动终端本地的域名系统DNS服务器地址。

[0118] 在本发明的一个实施例中，该方法进一步包括：如果获取到Root权限，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0119] 在本发明的一个实施例中，移动终端的本地也可以内置一个DNS库，在没有网络的时候，用DNS库进行判断。当WiFi网络对云鉴定有攻防的时候，通过该DNS库进行判断，如果能联网，则向服务器进行云查，本地的DNS也会传上去。

[0120] 图3示出了根据本发明另一个实施例的一种WiFi网络安全鉴定服务器的结构示意图。如图3所示，该WiFi网络安全鉴定服务器300包括：

[0121] 接收单元310，适于接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；以及接收无Root权限的移动终端发送的WiFi网络安全查询请求；

[0122] 存储单元320，适于保存WiFi网络安全检测数据库；

[0123] 鉴定单元330，适于根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

[0124] 发送单元340，适于将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0125] 图3所示的服务器，通过接收有Root权限的移动终端发送的WiFi网络安全检测信息，保存至WiFi网络安全检测数据库，使WiFi网络安全检测数据库得到及时的更新与完善，对接收的无Root权限移终端发送的WiFi网络安全查询请求予以回应，使得无Roor权限的移动终端也能够及时获得WiFi网络的安全鉴定结果。

[0126] 在本发明的一个实施例中，所述接收单元310接收的所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0127] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0128] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0129] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0130] 移动终端本地的域名系统DNS服务器地址。

[0131] 在本发明的一个实施例中，所述鉴定单元330，适于查询所述WiFi网络安全检测数据库，如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

[0132] 在本发明的一个实施例中，所述接收单元310，进一步适于接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0133] 所述鉴定单元330，进一步适于根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

[0134] 所述存储单元320，进一步适于存储DNS库；

[0135] 所述发送单元340，进一步适于向发送查询请求的所述有权限的移动终端返回判断结果。

[0136] 图4示出了根据本发明另一个实施例的一种WiFi网络安全鉴定客户端装置的结构示意图。如图4所示，该WiFi网络安全鉴定客户端装置400包括：

[0137] 判断单元410，适于判断是否能够获取到移动终端的Root权限；

[0138] 安全检测单元420，适于在获取到root权限时，检测移动终端所接入的WiFi网络的安全性，得到WiFi网络安全检测信息；

[0139] 发送单元430，适于向服务器发送所述WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0140] 以及所述发送单元430，还适于在获取不到Root权限时，则向服务器发送WiFi网络安全查询请求；

[0141] 接收单元440，适于接收服务器返回的安全鉴定结果并展示给用户。

[0142] 图4所示的客户端装置，使得移动终端在有Root权限和无Root权限的情况下都能够获得WiFi网络的安全鉴定结果。这样当移动终端到达一个新地点时，会扫描当地的所有WiFi网络，则通过本发明的方案可以获知所有扫描到的WiFi网络的安全鉴定信息，并对应展示的用户，从而使得用户能够选择一个安全的WiFi网络进行接入。

[0143] 在本发明的一个实施例中，

[0144] 所述安全检测单元420，适于在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0145] 和/或，

[0146] 所述安全检测单元，适于根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0147] 在本发明的一个实施例中，所述发送单元430向服务器发送WiFi网络安全检测信息包括：

[0148] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0149] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0150] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0151] 移动终端本地的域名系统DNS服务器地址。

[0152] 在本发明的一个实施例中，所述发送单元430，进一步适于在获取到Root权限时，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0153] 所述接收单元440，进一步适于接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0154] 图5示出了根据本发明另一个实施例的一种WiFi网络安全鉴定系统的示意图。如图5所示，该系统包括：WiFi网络安全鉴定服务器300，和WiFi网络安全鉴定客户端装置400。

[0155] 综上所述，发明的技术方案可以通过有Root权限的移动终端提供WiFi安全状态的鉴定，将结果共享至云端WiFi网络安全检测数据库，使得无Root权限的移动终端不再需要Root，仅通过查询云端的网络安全检测数据库便可获得WiFi安全性的鉴定信息，由此解决了现有技术中手机必须通过Root才能验证WiFi安全性的技术问题。

[0156] 需要说明的是：

[0157] 在此提供的算法和显示不与任何特定计算机、虚拟装置或者其它设备固有相关。各种通用装置也可以与基于在此的示教一起使用。根据上面的描述，构造这类装置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。

[0158] 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。

[0159] 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。

[0160] 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。

[0161] 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。

[0162] 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WiFi网络安全鉴定客户端装置和系统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。

[0163] 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。

[0164] 本发明公开了A 1、一种WiFi网络安全鉴定方法，其中，该方法包括：

[0165] 接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；

[0166] 接收无Root权限的移动终端发送的WiFi网络安全查询请求；

[0167] 根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

[0168] 将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0169] A2、如A1所述的方法，其中，所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0170] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0171] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0172] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0173] 移动终端本地的域名系统DNS服务器地址。

[0174] A 3、如A1所述的方法，其中，根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果包括：

[0175] 如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

[0176] A 4、如A1-A3中任一项所述的方法，其中，该方法进一步包括：

[0177] 接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0178] 根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

[0179] 向发送查询请求的所述有权限的移动终端返回判断结果。

[0180] 本发明还公开了B5、一种WiFi网络安全鉴定方法，其中，该方法包括：

[0181] 判断是否能够获取到移动终端的Root权限；

[0182] 如果获取到root权限，则检测移动终端所接入的WiFi网络的安全性，并向服务器发送WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0183] 如果获取不到Root权限，则向服务器发送WiFi网络安全查询请求，接收服务器返回的安全鉴定结果并展示给用户。

[0184] B6、如B5所述的方法，其中，所述检测移动终端所接入的WiFi网络的安全性包括如下中的一种或多种：

[0185] 在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0186] 根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0187] B7、如B5所述的方法，其中，所述向服务器发送WiFi网络安全检测信息包括：

[0188] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0189] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0190] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0191] 移动终端本地的域名系统DNS服务器地址。

[0192] B8、如B5所述的方法，其中，该方法进一步包括：

[0193] 如果获取到Root权限，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0194] 接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0195] 本发明还公开了C9、一种WiFi网络安全鉴定服务器，其中，该服务器包括：

[0196] 接收单元，适于接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中；以及接收无Root权限的移动终端发送的WiFi网络安全查询请求；

[0197] 存储单元，适于保存WiFi网络安全检测数据库；

[0198] 鉴定单元，适于根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果；

[0199] 发送单元，适于将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端。

[0200] C10、如C9所述的服务器，其中，所述接收单元接收的所述有Root权限的移动终端发送的WiFi网络安全检测信息包括：

[0201] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0202] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0203] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0204] 移动终端本地的域名系统DNS服务器地址。

[0205] C11、如C9所述的服务器，其中，

[0206] 所述鉴定单元，适于查询所述WiFi网络安全检测数据库，如果WiFi网络安全检测数据库中的数据表明，在指定的预设时间段内有超过预设值个数的移动终端上报了请求查询的WiFi网络存在风险，则确定请求查询的WiFi网络存在风险，否则确定请求查询的WiFi网络安全。

[0207] C12、如C9-C11中任一项所述的服务器，其中，

[0208] 所述接收单元，进一步适于接收有Root权限的移动终端发送的包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0209] 所述鉴定单元，进一步适于根据DNS库判断WiFi网络安全查询请求中的DNS服务器地址是否合法；

[0210] 所述存储单元，进一步适于存储DNS库；

[0211] 所述发送单元，进一步适于向发送查询请求的所述有权限的移动终端返回判断结果。

[0212] 本发明还公开了D13、一种WiFi网络安全鉴定客户端装置，其中，该客户端装置包括：

[0213] 判断单元，适于判断是否能够获取到移动终端的Root权限；

[0214] 安全检测单元，适于在获取到root权限时，检测移动终端所接入的WiFi网络的安全性，得到WiFi网络安全检测信息；

[0215] 发送单元，适于向服务器发送所述WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务；

[0216] 以及所述发送单元，还适于在获取不到Root权限时，则向服务器发送WiFi网络安全查询请求；

[0217] 接收单元，适于接收服务器返回的安全鉴定结果并展示给用户。

[0218] D14、如D13所述的客户端装置，其中，

[0219] 所述安全检测单元，适于在移动终端所接入的WiFi网络中发送ARP请求，如果该ARP请求的多个回包的MAC地址不一样，则确定该WiFi网络中存在ARP欺骗；

[0220] 和/或，

[0221] 所述安全检测单元，适于根据移动终端本地的DNS库判断移动终端本地的DNS服务器地址是否合法。

[0222] D15、如D13所述的客户端装置，其中，所述发送单元向服务器发送WiFi网络安全检测信息包括：

[0223] WiFi网络的标识以及关于该WiFi网络的如下信息中的一个或多个：

[0224] 移动终端检测到的地址解析协议ARP欺骗检测信息；

[0225] 移动终端检测到的互联网控制报文协议ICMP攻击检测信息；

[0226] 移动终端本地的域名系统DNS服务器地址。

[0227] D16、如D13所述的客户端装置，其中，

[0228] 所述发送单元，进一步适于在获取到Root权限时，向服务器发送包含WiFi标识和DNS服务器地址的WiFi网络安全查询请求；

[0229] 所述接收单元，进一步适于接收服务器返回的所述DNS服务器地址是否合法的判断结果。

[0230] 本发明还公开了E17、一种WiFi网络安全鉴定系统，其中，该系统包括：如权利要求C9-C12中任一项所述的WiFi网络安全鉴定服务器，和如权利要求D13-D16中任一项所述的WiFi网络安全鉴定客户端装置。

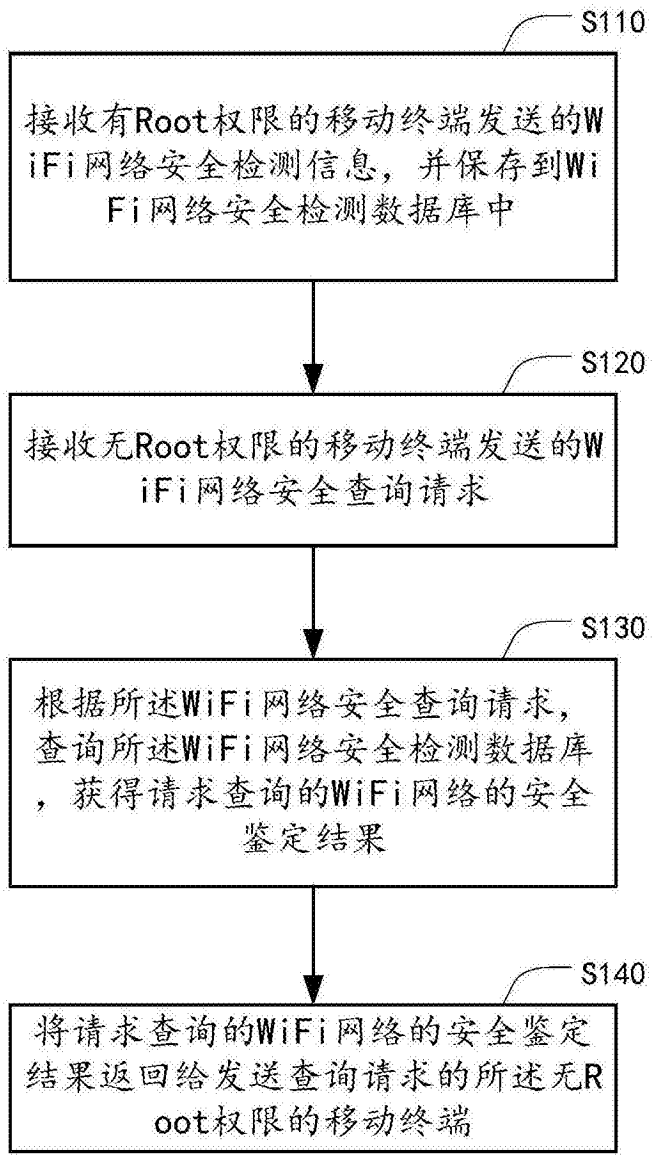

S110
接收有Root权限的移动终端发送的WiFi网络安全检测信息，并保存到WiFi网络安全检测数据库中
S120
接收无Root权限的移动终端发送的WiFi网络安全查询请求
S130
根据所述WiFi网络安全查询请求，查询所述WiFi网络安全检测数据库，获得请求查询的WiFi网络的安全鉴定结果
S140
将请求查询的WiFi网络的安全鉴定结果返回给发送查询请求的所述无Root权限的移动终端

图1

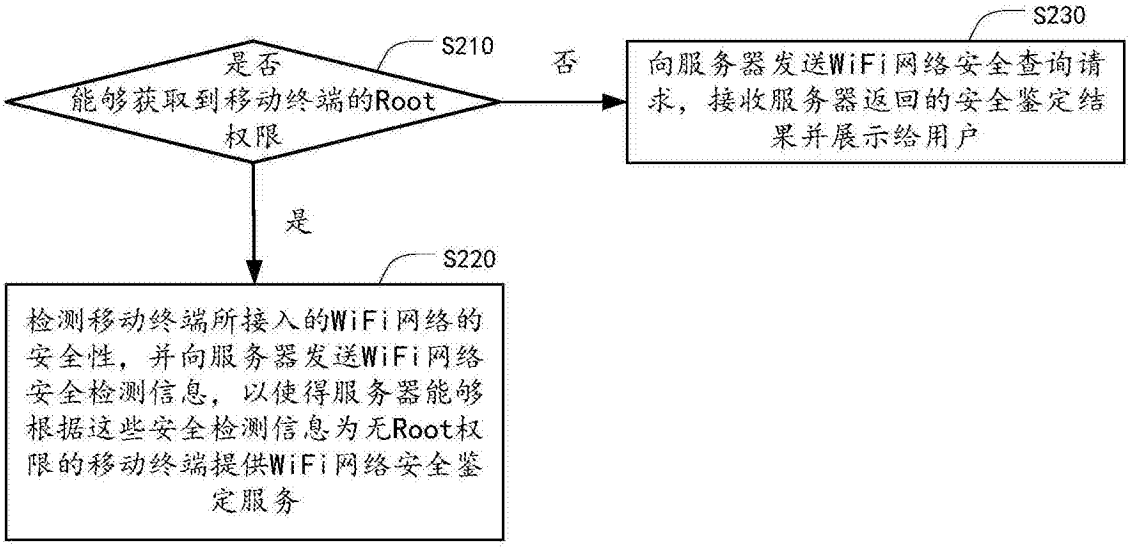

S210
是否能够获取到移动终端的Root权限
否
S230
向服务器发送WiFi网络安全查询请求，接收服务器返回的安全鉴定结果并展示给用户
是
S220
检测移动终端所接入的WiFi网络的安全性，并向服务器发送WiFi网络安全检测信息，以使得服务器能够根据这些安全检测信息为无Root权限的移动终端提供WiFi网络安全鉴定服务

图2

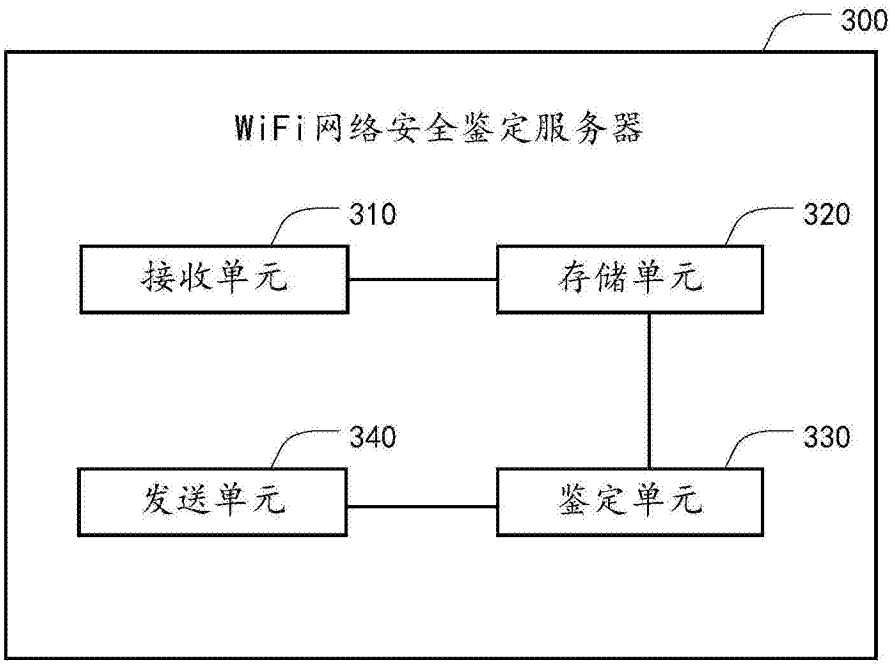

300
WiFi网络安全鉴定服务器
310
接收单元
320
存储单元
340
发送单元
330
鉴定单元

图3

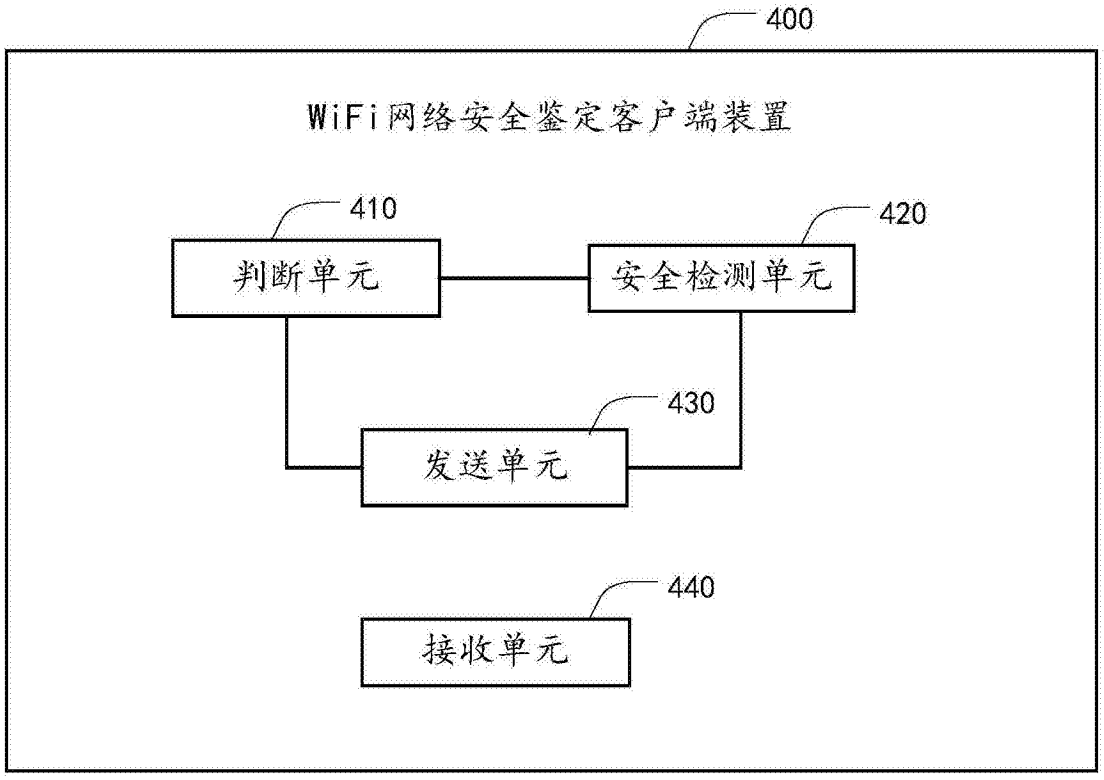

400
WiFi网络安全鉴定客户端装置
410
判断单元
420
安全检测单元
430
发送单元
440
接收单元

图4

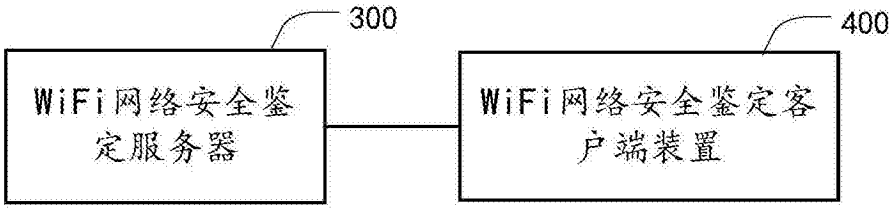

300
WiFi网络安全鉴定服务器
400
WiFi网络安全鉴定客户端装置

图5