(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105471807 A
(43)申请公布日 2016.04.06

(21)申请号 201410230457.1

(22)申请日 2014.05.28

(71)申请人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 赵隽 曹越 肖全举

(74)专利代理机构 上海波拓知识产权代理有限公司 31264
代理人 杨波

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

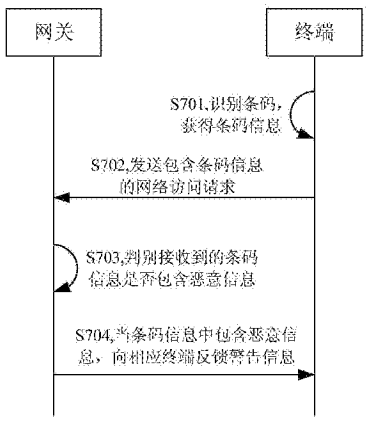
权利要求书2页 说明书7页 附图5页

(54)发明名称

基于条码信息的网络访问安全性检测方法及系统

(57)摘要

本发明提出一种基于条码信息的网络访问安全性检测方法及系统，其基于条码信息的网络访问安全性检测方法包括：终端识别条码，获得条码信息；终端向网关发送包含所述条码信息的网络访问请求；网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息；当所述条码信息中包含恶意信息，则网关向发送所述网络访问请求的相应终端反馈警告信息。本发明可以大大提高终端扫码的安全性，并且可以消除在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。



CN 105471807 A

1. 一种基于条码信息的网络访问安全性检测方法，用于至少一个终端通过网关进行网络访问时检测条码信息的安全性，其特征在于，包括：

终端识别条码，获得条码信息；

终端向网关发送包含所述条码信息的网络访问请求；

网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息；

当所述条码信息中包含恶意信息，则网关向发送所述网络访问请求的相应终端反馈警告信息。

2. 如权利要求 1 所述的基于条码信息的网络访问安全性检测方法，其特征在于，所述网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息的步骤包括：

网关将所述条码信息与预设的恶意信息库进行比对；

网关根据比对结果，判断所述条码信息中是否包含所述恶意信息库中的恶意信息。

3. 如权利要求 1 所述的基于条码信息的网络访问安全性检测方法，其特征在于，所述网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息的步骤包括：

网关将所述条码信息发送给远端检测服务器，并由远端检测服务器对条码信息进行检测；

网关接受远端检测服务器反馈来的检测结果，并根据检测结果判断所述条码信息中是否包含恶意信息。

4. 如权利要求 1 ～ 3 任一项所述的基于条码信息的网络访问安全性检测方法，其特征在于，所述网关向发送所述网络访问请求的相应终端反馈警告信息的步骤中，所述警告信息包括恶意信息的类型以及避让逻辑。

5. 一种条码信息安全性检测方法，其特征在于，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测，所述条码信息安全性检测方法包括：

获取所述网络访问请求中的条码信息；

判别获取的所述条码信息中是否包含恶意信息；

当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。

6. 如权利要求 5 所述的条码信息安全性检测方法，其特征在于，所述判别获取的所述条码信息中是否包含恶意信息的步骤包括：

将所述条码信息与预设的恶意信息库进行比对；

根据比对结果，判断所述条码信息中是否包含所述恶意信息库中的恶意信息。

7. 如权利要求 5 所述的条码信息安全性检测方法，其特征在于，所述判别获取的所述条码信息中是否包含恶意信息的步骤包括：

将所述条码信息发送给远端检测服务器，并由远端检测服务器对条码信息进行检测；

接受远端检测服务器反馈来的检测结果，并根据检测结果判断所述条码信息中是否包含恶意信息。

8. 如权利要求 5 ～ 7 任一项所述的条码信息安全性检测方法，其特征在于，所述向发出所述网络访问请求的相应终端反馈警告信息的步骤中，所述警告信息包括恶意信息的类型以及避让逻辑。

9. 一种基于条码信息的网络访问安全性检测系统，包括至少一个网关和至少一个终

端，所述一个网关与至少一个终端连接，并形成网络，其特征在于，所述基于条码信息的网络访问安全性检测系统包括：

终端，用于识别条码，获得条码信息，并向网关发送包含所述条码信息的网络访问请求；

网关，用于判别接收到的所述网络访问请求中的条码信息是否包含恶意信息，并当所述条码信息中包含恶意信息时，向发送所述网络访问请求的相应终端反馈警告信息。

10. 如权利要求 9 所述的基于条码信息的网络访问安全性检测系统，其特征在于，所述网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息时包括：所述网关将所述条码信息与预设的恶意信息库进行比对，并根据比对结果，判断所述条码信息中是否包含所述恶意信息库中的恶意信息。

11. 如权利要求 9 所述的基于条码信息的网络访问安全性检测系统，其特征在于，所述系统还包括：

远端服务器，用于接收所述网关发送来的条码信息，对条码信息进行检测，并将检测结果反馈给所述网关，以由所述网关根据检测结果判断所述条码信息中是否包含恶意信息。

12. 如权利要求 9 ～ 11 任一项所述的基于条码信息的网络访问安全性检测系统，其特征在于，所述警告信息包括恶意信息的类型以及避让逻辑。

13. 一种条码信息安全性检测装置，其特征在于，设置于网关，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测，所述条码信息安全性检测装置包括：

条码信息获取模块，用于获取所述网络访问请求中的条码信息；

恶意信息判别模块，用于判别获取的所述条码信息中是否包含恶意信息；

警告信息反馈模块，用于当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。

14. 如权利要求 13 所述的条码信息安全性检测装置，其特征在于，所述恶意信息判别模块进一步包括：

比对单元，用于将所述条码信息与预设的恶意信息库进行比对；

判断单元，用于根据比对结果，判断所述条码信息中是否包含所述恶意信息库中的恶意信息。

15. 如权利要求 13 所述的条码信息安全性检测装置，其特征在于，所述恶意信息判别模块进一步包括：

发送单元，用于将所述条码信息发送给远端检测服务器，并由远端检测服务器对条码信息进行检测；

接收单元，用于接受远端检测服务器反馈来的检测结果；

判别单元，用于根据检测结果判断所述条码信息中是否包含恶意信息。

16. 如权利要求 13 ～ 15 任一项所述的条码信息安全性检测装置，其特征在于，所述警告信息包括恶意信息的类型以及避让逻辑。

基于条码信息的网络访问安全性检测方法及系统

技术领域

[0001] 本发明涉及信息安全技术领域，特别涉及一种基于条码信息的网络访问安全性检测方法及系统。

背景技术

[0002] 二维码（two-dimension code），又称二维条码，它是在一维条码的基础上扩展出另一维具有可读性的条码，二维码用特定的几何图形按一定规律在平面（二维方向）上分布的黑白相间的图形，是所有信息数据的一把钥匙。目前，二维码因其具有的信息存储量大、保密性高、成本低等特点，在工商业、交通运输、金融、医疗等领域逐渐应用推广。而近年来，移动通信领域蓬勃发展起来的移动终端二维码业务，使移动终端用户进入信息随手可得的时代，由此带来的巨大商机在国内外日益显现。

[0003] 在实际应用中，例如用二维码上网时，首先要利用移动终端自带的摄像头拍摄下二维码的图片，然后从二维码图片中设别出其中包含的网址信息，从而才能访问与该网址相应的网站。但是，如果扫描解码后得到的是一条恶意网址链接，或运行非法程序，就可能泄露移动终端通讯录、银行卡号密码等一切与移动终端绑定的隐私，以及造成系统崩溃更或财产损失等严重后果。

[0004] 针对二维码的安全问题，虽然目前市场上出现了一些安装于移动终端的安全扫描软件，这些安全扫描软件可以对解码后二维码信息的安全性行识别，但是，这类安全扫描软件对二维码信息安全性的判断通常都是软件附带功能，经常不会被启用，而且还具有一定的局限性：第一，必须使用安装有安全扫描软件的移动终端进行扫码，才能对二维码信息的安全性进行判断；第二，必须使用特定的安全扫描软件才能对二维码信息的安全性进行判断。然而，绝大部门用户使用二维码扫描时都不会想到会对自己的设备及账号造成威胁，对二维码的警惕性较低，所以大部分用户都不会在移动终端特别安装这类安全扫描软件，因此这类安全扫描软件的使用率很低，无法真正解决二维码的安全问题，因而目前需要一种方案，从根本上解决二维码的安全隐患。

发明内容

[0005] 本发明实施例的目的是提供一种基于条码信息的网络访问安全性检测方法及系统，以解决条码扫描信息的完全问题。

[0006] 本发明实施例提出一种基于条码信息的网络访问安全性检测方法，用于至少一个终端通过网关进行网络访问时检测条码信息的安全性，包括：

[0007] 终端识别条码，获得条码信息；

[0008] 终端向网关发送包含所述条码信息的网络访问请求；

[0009] 网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息；

[0010] 当所述条码信息中包含恶意信息，则网关向发送所述网络访问请求的相应终端反馈警告信息。

[0011] 本发明实施例另提出一种条码信息安全性检测方法，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测，所述条码信息安全性检测方法包括：

[0012] 获取所述网络访问请求中的条码信息；

[0013] 判别获取的所述条码信息中是否包含恶意信息；

[0014] 当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。

[0015] 本发明实施例还提出一种基于条码信息的网络访问安全性检测系统，包括至少一个网关和至少一个终端，所述一个网关与至少一个终端连接，并形成网络，所述基于条码信息的网络访问安全性检测系统包括：

[0016] 终端，用于识别条码，获得条码信息，并向网关发送包含所述条码信息的网络访问请求；

[0017] 网关，用于判别接收到的所述网络访问请求中的条码信息是否包含恶意信息，并当所述条码信息中包含恶意信息时，向发送所述网络访问请求的相应终端反馈警告信息。

[0018] 本发明实施例还提出一种条码信息安全性检测装置，设置于网关，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测，所述条码信息安全性检测装置包括：

[0019] 条码信息获取模块，用于获取所述网络访问请求中的条码信息；

[0020] 恶意信息判别模块，用于判别获取的所述条码信息中是否包含恶意信息；

[0021] 警告信息反馈模块，用于当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。

[0022] 相对于现有技术，本发明的有益效果是：本实施例的条码信息安全性检测方法，会对终端发出的网络访问请求中的条码信息进行监测，当发现恶意信息后立刻向对应的终端发出警告，从而大大提高了局域网中终端扫码的安全性。而且，通过本实施例的装置，可以对局域网中终端扫码获得的条码信息的安全性进行统一检测，从而消除了在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。

附图说明

[0023] 图 1 为本发明实施例的一种基于条码信息的网络访问安全性检测系统的架构图；

[0024] 图 2 为本发明实施例的一种显示在终端显示屏上的警告信息；

[0025] 图 3 为本发明实施例的另一种基于条码信息的网络访问安全性检测系统的架构图；

[0026] 图 4 为本发明实施例的一种条码信息安全性检测装置的结构图；

[0027] 图 5 为本发明实施例的一种恶意信息判别模块的结构图；

[0028] 图 6 为本发明实施例的另一种恶意信息判别模块的结构图；

[0029] 图 7 为本发明实施例的一种基于条码信息的网络访问安全性检测方法的流程图；

[0030] 图 8 为本发明实施例的另一种基于条码信息的网络访问安全性检测方法的流程图；

[0031] 图 9 为本发明实施例的一种条码信息安全性检测方法的流程图。

具体实施方式

[0032] 有关本发明的前述及其他技术内容、特点及功效，在以下配合参考图式的较佳实施例详细说明中将可清楚的呈现。通过具体实施方式的说明，当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解，然而所附图式仅是提供参考与说明之用，并非用来对本发明加以限制。

[0033] 请参见图 1，其为本发明实施例的一种基于条码信息的网络访问安全性检测系统的架构图，该系统包括多个网关 11 和多个终端 12（为便于说明，图 1 中仅绘示了两个网关 11），网关 11 与互联网 13 连接，每个网关 11 均与多个终端 12 连接，并形成局部的网络。终端 12 可以通过网关 11 向互联网 13 发出网络访问请求，以访问互联网 13 中的网络服务器（图 1 中未绘示）。其中，终端 12 可以是平板电脑、手机、电子阅读器、遥控器、PC、笔记本电脑、车载设备、可穿戴设备等具有拍摄以及网络功能的智能设备。所述网关 11 可以是具有路由功能的路由器、启用了路由协议的服务器、代理服务器等。特别的，可以在普通 PC 上连接创建局域网络的硬件设备（如创建 wifi 的硬件设备），并以该 PC 为基础创建所述网关 11。

[0034] 本实施例中，终端 12 可以通过自带的拍摄功能对条码进行扫描，并识别出其中的条码信息。这里所述的条码可以包括一维条码（也称为条形码）、二维条码（也称为二维码）、三维条码（也称为三维条码）等记录各类信息的图形标记。所述的条码信息可以是隐含在条码图形中的数字、符号、图片等数据。当条码信息中包含需要访问互联网 13 的信息时（例如条码信息中包含一个待访问的网址），那么终端 12 可以向网关 11 发送包含所述条码信息的网络访问请求。

[0035] 网关 11 接收到包含条码信息的网络访问请求后，会提取出其中的条码信息，并判断提取出的条码信息中是否包含恶意信息。如果条码信息中包含恶意信息，例如条码信息中包含恶意网址、负面词汇或黄色图片等，那么网关 11 则拦截该网络访问，并向发出该网络访问请求的相应终端反馈警告信息。而如果条码信息中不包含恶意信息，则允许终端 12 正常访问互联网 13。

[0036] 进一步来说，在网关 11 判别接收到的网络访问请求中的条码信息是否包含恶意信息时，可以将条码信息与网关 11 本地预设的恶意信息库进行比对，所述的恶意信息库中预存有大量恶意信息，如果匹配到条码信息中的某一个信息与恶意信息库中的一个信息一致，则说明该信息为恶意信息，则向相应的终端 12 反馈警告信息。

[0037] 所述的警告信息可以包括恶意信息的类型以及避让逻辑。请参见图 2，其为本发明实施例的一种显示在终端 12 显示屏上的警告信息。其中恶意信息为网址“http://www.12321412212.com”，恶意信息的类型为“病毒木马风险”，避让逻辑为“建议您停止访问”。当然，警告信息中包含的内容也不以此为限，可以根据需要来设定。

[0038] 本实施例的系统会对终端发出的网络访问请求中的条码信息进行监测，当发现恶意信息后立刻向对应的终端发出警告，从而大大提高了局域网中终端扫码的安全性，可以有效防止终端对恶意网站的访问，也进一步地避免了终端上隐私信息的泄露，以及非法程序对终端的入侵造成的系统崩溃更或财产损失等严重后果。

[0039] 此外，本实施例的系统通过网关对网络访问请求中的条码信息进行监测，只要局域网中的终端扫码条码后，并基于条码信息发出网络访问请求，都由被网关对条码信息进

行检测，换言之，终端上无须再安装特定的安全扫码软件，而是由网关统一对局域网中终端扫码获得的条码信息的安全性进行检测，从而消除了在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。

[0040] 请参见图 3，其为本发明实施例的一种基于条码信息的网络访问安全性检测系统的架构图。藉于一些网关 11 的存储能力有限，不足以存放恶意信息库，或者一些网关 11 的运算处理能力不足，本实施例的基于条码信息的网络访问安全性检测系统与图 1 的实施例相比，还增加了远端服务器 14。

[0041] 当网关 11 接收到包含条码信息的网络访问请求后，会提取出其中的条码信息，并将该条码信息发送给远端服务器 14 进行检测。远端服务器 14 中存储有恶意信息库，远端服务器 14 会利用恶意信息库检测网关 11 发送来的条码信息中是否存在恶意信息，并将检测结果反馈给网关 11。网关 11 接收到检测结果后，根据检测结果判断哪些网络访问请求的条码信息中包含恶意信息，并向包含恶意信息的网络访问请求对应的终端 12 反馈警告信息。由此可见，本实施例的网关 11 无须做大量的运算处理，对网关 11 的硬件要求较低，也便于网络的布局及推广。

[0042] 本发明实施例还提出一种条码信息安全性检测装置，其设置于网关中，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测。请参见图 4，其为本实施例的装置包括 ：条码信息获取模块 41、恶意信息判别模块 42 以及警告信息反馈模块 43。

[0043] 条码信息获取模块 41 用于获取网络访问请求中的条码信息。终端 12 访问互联网 13 时都需要向网关发送请求，条码信息获取模块 41 便可以筛选出其中包含条码信息的网络访问请求，并提取出其中的条码信息。

[0044] 恶意信息判别模块 42 用于判别条码信息获取模块 41 获取的所述条码信息中是否包含恶意信息。恶意信息判别模块 42 对条码信息的识别可以直接通过本地系统完成，或者也可以利用远程的检测服务器来完成。具体来说，如果网关是设置在 PC 上的，例如通过在 PC 上连接创建局域网络的硬件设备（如创建 wifi 的硬件设备），并以该 PC 为基础创建网关，由于 PC 一般都有一定的存储能力，因而可以将恶意信息库直接保存在 PC 的存储器中，恶意信息判别模块 42 可以将待检测的条码信息直接与本地存储的恶意信息库进行匹配，如果条码信息中的某一条信息与恶意信息库中的信息一致，则说明这条信息是恶意信息。另一种情况，如果网关只是单纯路由功能的设备，那么这个网关就不会有很强的运算能力和存储空间，那么恶意信息判别模块 42 可以将待检测的条码信息发送给远端检测服务器，由远端检测服务器对条码信息进行检测，并且根据远端检测服务器反馈回来的检测结果判断所述条码信息中是否包含恶意信息，这样就对本地硬件的运算能力和存储能力要求都会很低，便于装置的布局及推广。

[0045] 警告信息反馈模块 43 用于当恶意信息判别模块 42 判别出所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。所述警告信息可以包括恶意信息的类型以及避让逻辑。

[0046] 请参见图 5，藉于恶意信息判别模块 42 在本地对条码信息进行检测的方式，恶意信息判别模块 42 可以进一步包括 ：比对单元 421 和判断单元 422。比对单元 421 用于将条码信息与预设的恶意信息库进行比对。判断单元 422 用于根据比对单元 421 输出的比对结果，判断条码信息中是否包含所述恶意信息库中的恶意信息。

[0047] 请参见图6，藉于恶意信息判别模块42利用远端检测服务器对条码信息进行检测的方式，恶意信息判别模块42可以进一步包括：发送单元423、接收单元424和判别单元425。发送单元423用于将条码信息发送给远端检测服务器，以由远端检测服务器对条码信息进行检测。接收单元424用于接受远端检测服务器反馈来的检测结果。判别单元425用于根据接收单元424接收到的检测结果判断所述条码信息中是否包含恶意信息。

[0048] 本实施例的装置会对终端发出的网络访问请求中的条码信息进行监测，当发现恶意信息后立刻向对应的终端发出警告，从而大大提高了局域网中终端扫码的安全性。而且，通过本实施例的装置，可以对局域网中终端扫码获得的条码信息的安全性进行统一检测，从而消除了在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。

[0049] 本发明实施例还提出一种基于条码信息的网络访问安全性检测方法，用于在终端根据条码信息发出网络访问请求时，对条码信息的安全性进行检测，请参见图7，其包括以下步骤：

[0050] S701，终端识别条码，获得条码信息。

[0051] S702，终端向网关发送包含所述条码信息的网络访问请求。

[0052] S703，网关判别接收到的所述网络访问请求中的条码信息是否包含恶意信息。

[0053] 网关对条码信息的识别可以直接通过本地系统完成。具体来说，如果网关是设置在PC上的，例如通过在PC上连接创建局域网络的硬件设备（如创建wifi的硬件设备），并以该PC为基础创建网关，由于PC一般都有一定的存储能力，因而可以将恶意信息库直接保存在PC的存储器中，网关可以将待检测的条码信息直接与本地存储的恶意信息库进行比对，如果条码信息中的某一条信息与恶意信息库中的信息一致，则说明这条信息是恶意信息。

[0054] S704，当所述条码信息中包含恶意信息，则网关向发送所述网络访问请求的相应终端反馈警告信息。所述的警告信息可以包括恶意信息的类型以及避让逻辑。

[0055] 请参见图8，其为本发明实施例的另一种基于条码信息的网络访问安全性检测方法的流程图，其包括以下步骤：

[0056] S801，终端识别条码，获得条码信息。

[0057] S802，终端向网关发送包含所述条码信息的网络访问请求。

[0058] S803，网关将所述条码信息发送给远端检测服务器。

[0059] S804，远端检测服务器对条码信息安全性进行检测。

[0060] S805，远端检测服务器将检测结果反馈给网关。

[0061] S806，网关根据检测结果判断条码信息中是否包含恶意信息。

[0062] S807，当所述条码信息中包含恶意信息，则网关向发送所述网络访问请求的相应终端反馈警告信息。

[0063] 在一般情况下，如果网关只是单纯路由功能的设备，那么这个网关就不会有很强的运算能力和存储空间，所以本实施例的方法将待检测的条码信息发送给远端检测服务器，由远端检测服务器对条码信息进行检测，并且根据远端检测服务器反馈回来的检测结果判断所述条码信息中是否包含恶意信息，这样就对本地硬件的运算能力和存储能力要求都会很低，也便于网络的布局及推广。

[0064] 本发明实施例的基于条码信息的网络访问安全性检测方法，会对终端发出的网络访问请求中的条码信息进行监测，当发现恶意信息后立刻向对应的终端发出警告，从而大

大提高了局域网中终端扫码的安全性，可以有效防止终端对恶意网站的访问，也进一步地避免了终端上隐私信息的泄露，以及非法程序对终端的入侵造成的系统崩溃更或财产损失等严重后果。

[0065] 此外，本发明实施例的基于条码信息的网络访问安全性检测方法，通过网关对网络访问请求中的条码信息进行监测，只要局域网中的终端扫码条码后，并基于条码信息发出网络访问请求，都由被网关对条码信息进行检测，换言之，终端上无须再安装特定的安全扫码软件，而是由网关统一对局域网中终端扫码获得的条码信息的安全性进行检测，从而消除了在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。

[0066] 本发明实施例还提出一种条码信息安全性检测方法，用于对网关接收到的网络访问请求中的条码信息的安全性进行检测，请参见图 9，其包括以下步骤：

[0067] S901，获取所述网络访问请求中的条码信息。

[0068] S902，判别获取的所述条码信息中是否包含恶意信息。对条码信息的判别可以直接通过本地系统完成，或者也可以利用远程的检测服务器来完成。

[0069] 具体来说，如果网关是设置在 PC 上的，例如通过在 PC 上连接创建局域网络的硬件设备（如创建 wifi 的硬件设备），并以该 PC 为基础创建网关，由于 PC 一般都有一定的存储能力，因而可以将恶意信息库直接保存在 PC 的存储器中，检测条码信息时可以将条码信息直接与本地存储的恶意信息库进行比对，如果条码信息中的某一条信息与恶意信息库中的信息一致，则说明这条信息是恶意信息。另一种情况，如果网关只是单纯路由功能的设备，那么这个网关就不会有很强的运算能力和存储空间，那么可以将待检测的条码信息发送给远端检测服务器，由远端检测服务器对条码信息进行检测，并且根据远端检测服务器反馈回来的检测结果判断所述条码信息中是否包含恶意信息，这样就对本地硬件的运算能力和存储能力要求都会很低，便于装置的布局及推广。

[0070] S903，当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息。所述警告信息包括恶意信息的类型以及避让逻辑。

[0071] 本实施例的条码信息安全性检测方法，会对终端发出的网络访问请求中的条码信息进行监测，当发现恶意信息后立刻向对应的终端发出警告，从而大大提高了局域网中终端扫码的安全性。而且，通过本实施例的装置，可以对局域网中终端扫码获得的条码信息的安全性进行统一检测，从而消除了在终端安全扫码的操作门槛，真正解决了终端扫码的安全问题。

[0072] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明实施例可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明实施例的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，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，服务器，或网络设备等）执行本发明实施例各个实施场景所述的方法。

[0073] 以上所述，仅是本发明的较佳实施例而已，并非对本发明作任何形式上的限制，虽然本发明已以较佳实施例揭露如上，然而并非用以限定本发明，任何熟悉本专业的技术人员，在不脱离本申请技术方案范围内，当可利用上述揭示的技术内容作出些许更动或修饰为等同变化的等效实施例，但凡是未脱离本申请技术方案内容，依据本发明的技术实质对

以上实施例所作的任何简单修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

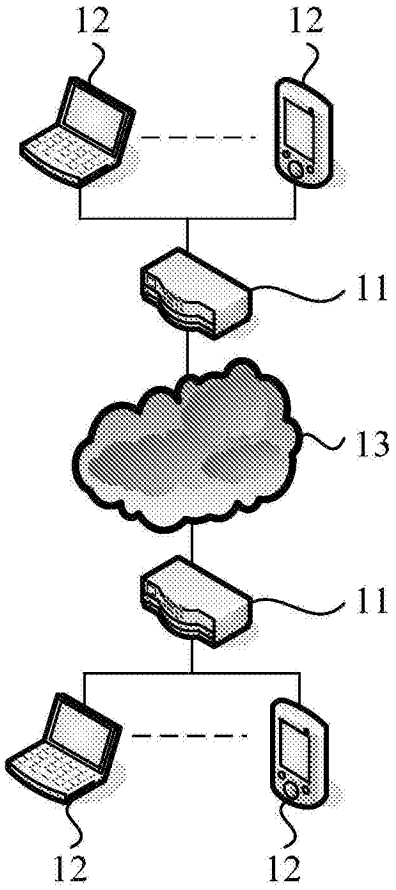

12
12
11
13
11
12
12

图 1


网站存在病毒风险！
危险！当前页面存在病毒木马风险，
建议您停止访问！
网址：http://www.1232141221 3.com
关闭此页
我了解风险，仍然访问

图 2

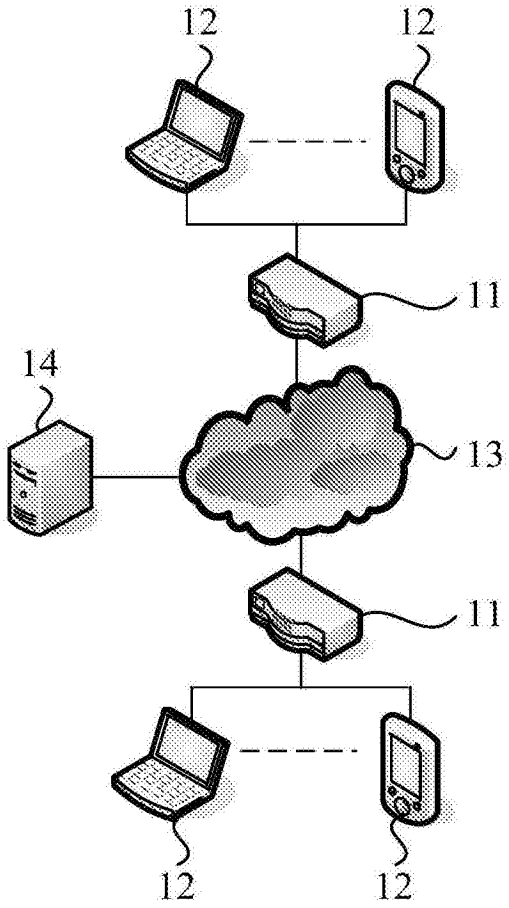

12
12
11
14
13
11
12
12

图 3

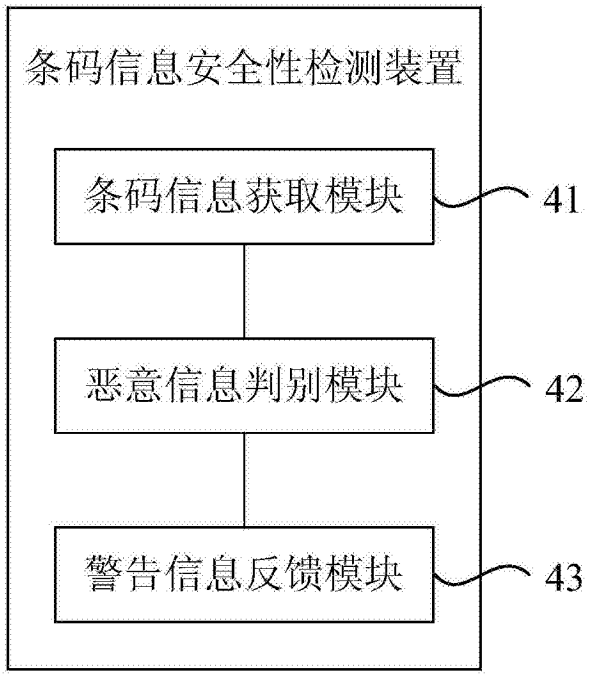

条码信息安全性检测装置
条码信息获取模块
41
恶意信息判别模块
42
警告信息反馈模块
43

图 4

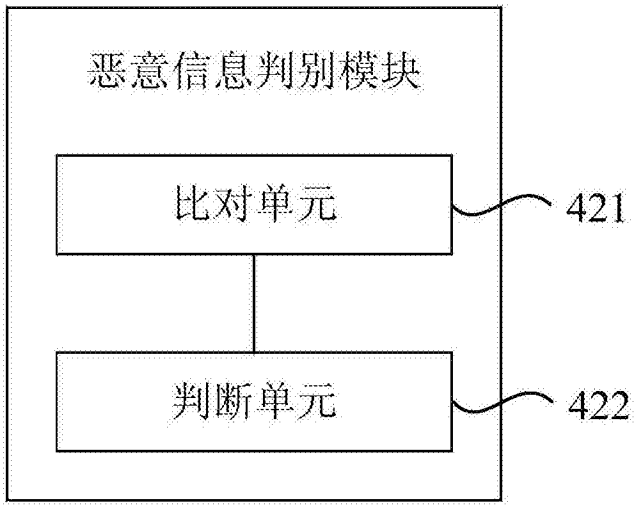

恶意信息判别模块
比对单元
421
判断单元
422

图 5

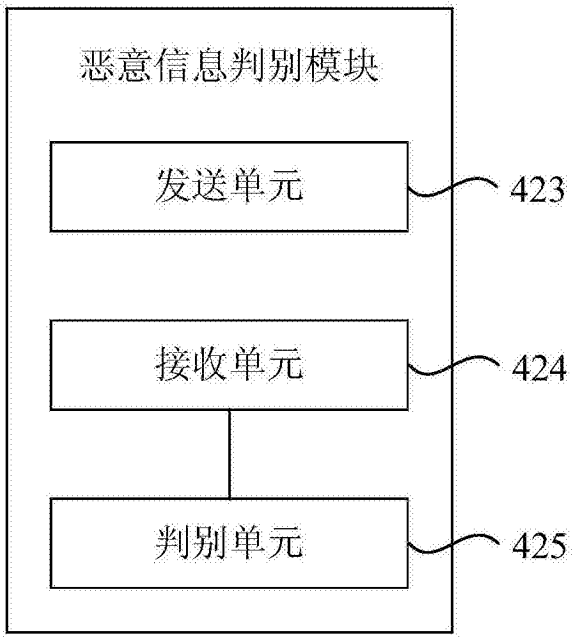

恶意信息判别模块
发送单元
423
接收单元
424
判别单元
425

图 6

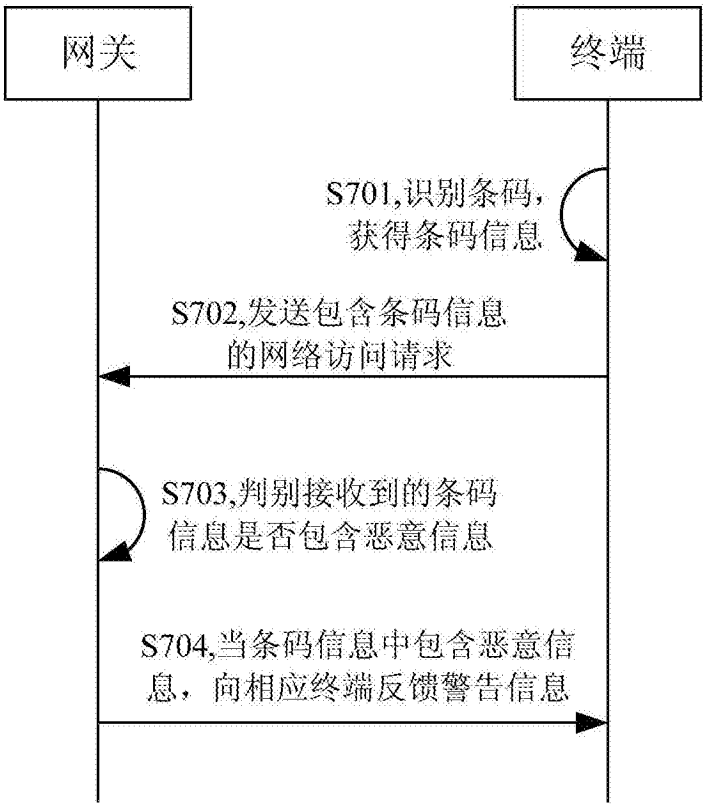

网关
终端
S701,识别条码，
获得条码信息
S702,发送包含条码信息
的网络访问请求
S703,判别接收到的条码
信息是否包含恶意信息
S704,当条码信息中包含恶意信
息，向相应终端反馈警告信息

图 7

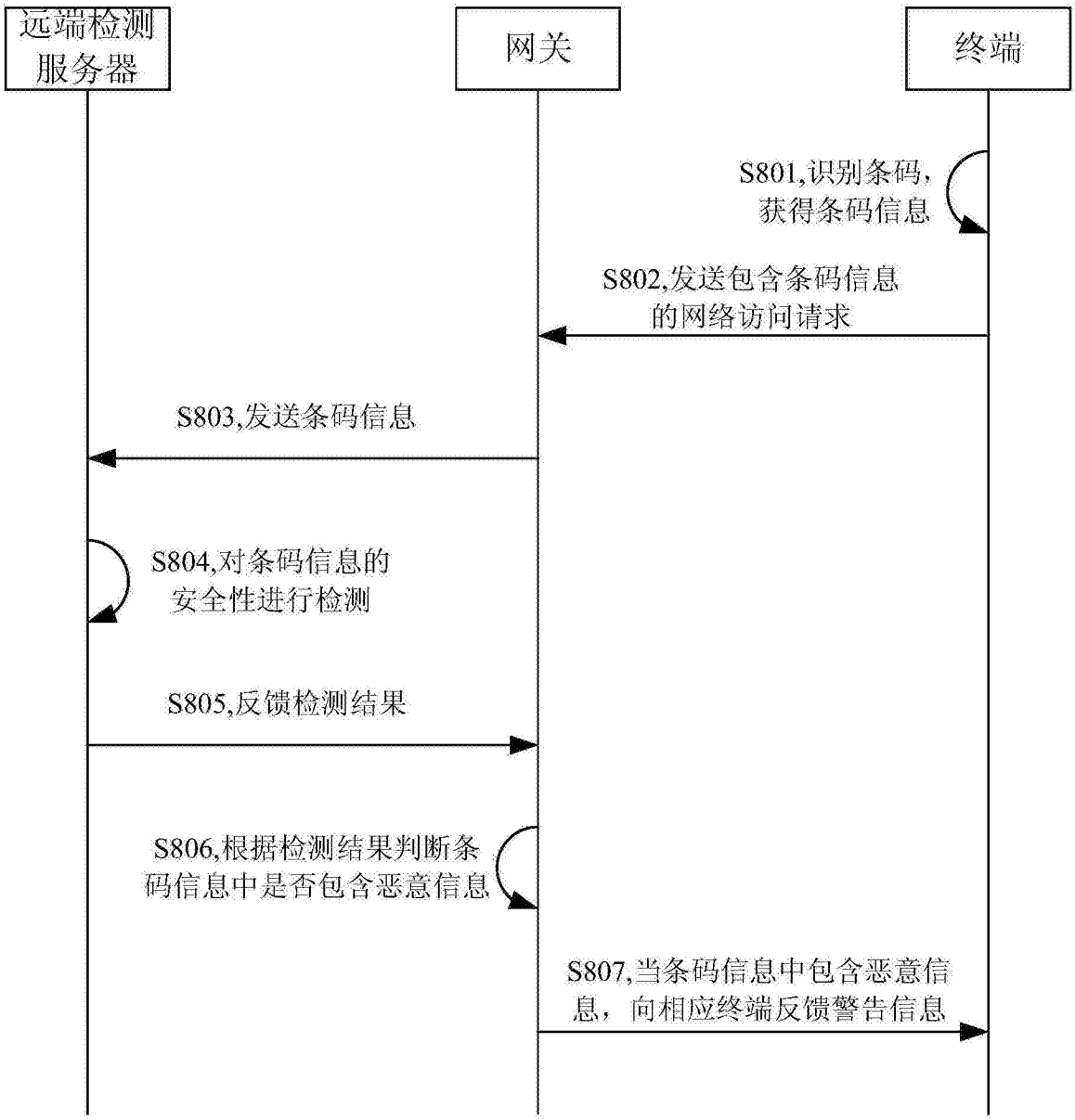

远端检测服务器
网关
终端
S801,识别条码，获得条码信息
S802,发送包含条码信息的网络访问请求
S803,发送条码信息
S804,对条码信息的安全性进行检测
S805,反馈检测结果
S806,根据检测结果判断条码信息中是否包含恶意信息
S807,当条码信息中包含恶意信息，向相应终端反馈警告信息

图 8

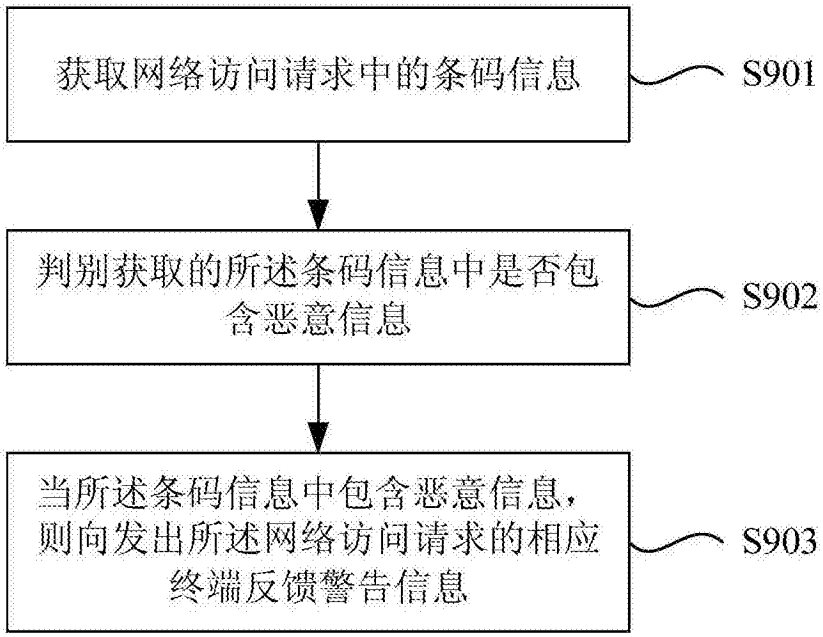

获取网络访问请求中的条码信息
S901
判别获取的所述条码信息中是否包含恶意信息
S902
当所述条码信息中包含恶意信息，则向发出所述网络访问请求的相应终端反馈警告信息
S903

图 9