(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 102902917 A
(43)申请公布日 2013.01.30

(21)申请号 201110215504.1

(22)申请日 2011.07.29

(71)申请人 国际商业机器公司
地址 美国纽约

(72)发明人 谢林 王斌 宋胤 张蕾 孙曼 李栋

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 张亚非 于静

(51)Int.Cl.
G06F 21/56(2013.01)

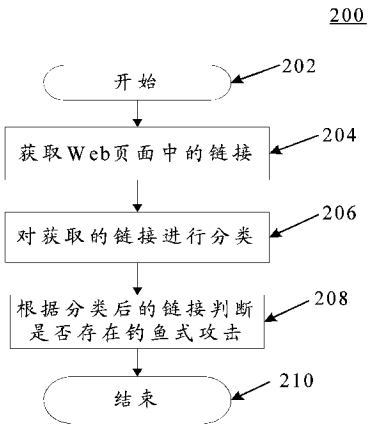
权利要求书 2 页 说明书 8 页 附图 3 页

(54)发明名称

用于预防钓鱼式攻击的方法和系统

(57)摘要

本公开提供了一种用于防止钓鱼式攻击的方法和系统，其中方法包括：获取Web页面中的链接；按照链接的类型对获取的链接进行分类；以及根据分类后的链接判断是否存在钓鱼式攻击，其中链接分为两种类型：与所述Web页面的地址属于相同域的内部链接以及与所述Web页面的地址属于不同域的外部链接。通过执行根据本公开实施例提供的上述一个或多个实施例的方法或系统，由于在向用户显示再现后的Web页面之前首先检测是否为钓鱼式攻击的假冒网站，并在检测到假冒网站时提示用户，这样避免了因钓鱼式攻击导致的不必要的损失。



CN 102902917 A

1. 一种用于防止钓鱼式攻击的方法，包括：

获取 Web 页面中的链接；

按照链接的类型对获取的链接进行分类；以及

根据分类后的链接判断是否存在钓鱼式攻击，

其中链接分为两种类型：与所述 Web 页面的地址属于相同域的内部链接以及与所述 Web 页面的地址属于不同域的外部链接。

2. 根据权利要求 1 的方法，其中根据分类后的链接判断是否存在钓鱼式攻击包括：

计算各类型的链接所占链接总数的百分比；

将计算的各类型的链接所占链接总数的百分比与预先设定的阈值进行比较；以及

利用所述比较结果判断是否存在钓鱼式攻击。

3. 根据权利要求 2 的方法，其中利用所述比较结果判断是否存在钓鱼式攻击包括：

响应于比较结果表明内部链接小于预先设定的阈值，提示用户可能存在钓鱼式攻击。

4. 根据权利要求 2 的方法，其中利用所述比较结果判断是否存在钓鱼式攻击包括：

响应于比较结果表明内部链接不小于预先设定的阈值，向用户显示 Web 页面。

5. 根据权利要求 2 的方法，其中利用所述比较结果判断是否存在钓鱼式攻击包括：

响应于比较结果表明外部链接不小于该预先设定的阈值，提示用户可能存在钓鱼式攻击。

6. 根据权利要求 2 的方法，其中利用所述比较结果判断是否存在钓鱼式攻击包括：

响应于比较结果表明外部链接小于预先设定的阈值，向用户显示 Web 页面。

7. 根据权利要求 1 的方法，其中通过扫描 Web 页面的源代码获取 Web 页面中的链接。

8. 根据权利要求 1 的方法，其中属于同一家公司的域名的链接类型相同。

9. 根据权利要求 1 的方法，进一步包括：

排除常见的提供服务的第三方合法网站的链接。

10. 一种用于防止钓鱼式攻击的系统，包括：

获取部件，被配置为获取 Web 页面中的链接；

分类部件，被配置为按照链接的类型对获取的链接进行分类；以及

判断部件，被配置为根据分类后的链接判断是否存在钓鱼式攻击，

其中链接分为两种类型：与所述 Web 页面的地址属于相同域的内部链接以及与所述 Web 页面的地址属于不同域的外部链接。

11. 根据权利要求 10 的系统，进一步包括：

计算部件，被配置为计算各类型的链接所占链接总数的百分比；以及

比较部件，被配置为将计算的各类型的链接所占链接总数的百分比与预先设定的阈值进行比较，

其中所述判断部件利用所述比较结果判断是否存在钓鱼式攻击。

12. 根据权利要求 11 的系统，进一步包括：

提示部件，被配置为响应于比较结果表明内部链接小于预先设定的阈值，提示用户可能存在钓鱼式攻击。

13. 根据权利要求 11 的系统，进一步包括：

显示部件，被配置为响应于比较结果表明内部链接不小于预先设定的阈值，向用户显

示 Web 页面。

14. 根据权利要求 11 的系统，进一步包括：

提示部件，被配置为响应于比较结果表明外部链接不小于该预先设定的阈值，提示用户可能存在钓鱼式攻击。

15. 根据权利要求 11 的系统，进一步包括：

显示部件，被配置为响应于比较结果表明外部链接小于预先设定的阈值，向用户显示 Web 页面。

16. 根据权利要求 10 的系统，其中获取部件进一步被配置为通过扫描 Web 页面的源代码获取 Web 页面中的链接。

17. 根据权利要求 10 的系统，其中属于同一家公司的域名的链接类型相同。

用于预防钓鱼式攻击的方法和系统

技术领域

[0001] 本发明涉及网络安全，更具体地，本发明涉及一种用于预防钓鱼式攻击(Phishing)的方法和系统。

背景技术

[0002] 钓鱼式攻击是一种企图利用电子通信伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程。这些通信往往声称自己来自网络银行、电子支付网站、在线零售商、信用卡公司或网络管理者等，以此来诱骗受害人的轻信。钓鱼式攻击通常是通过电子邮件或者即时通信进行。钓鱼式攻击往往将用户导引到界面外观与真正的合法网站非常相似的假冒网站以欺骗输入个人敏感信息。这些假冒网站通常是与网络银行、电子支付网站、在线零售商或信用卡公司等可信的品牌的页面非常相似的页面，受骗者往往会泄露自己的敏感信息，如信用卡号、银行卡账户、身份证号等内容。目前，已有多种方法和工具以帮助人们发现这些假冒网站并避免暴露他们的隐私信息。例如：通过 SSL 安全连接、数字证书，或者建立屏蔽钓鱼网站黑名单等。然而，这些方法虽然能解决一部分的问题，但也有各自的缺点。例如，即使通过 SSL 安全连接，要检测网站是否假冒网站实际上仍很困难。

发明内容

[0003] 本公开说明性实施例中认识到现有技术中存在的上述缺点。为此，本公开提供了一种轻量级的解决方案，能够帮助普通用户识别某一类普遍的钓鱼式攻击的方式并避免由此导致的不必要的损失。

[0004] 根据本公开的一个实施例，提供了一种用于防止钓鱼式攻击的方法，包括：对 Web 页面进行扫描；获取 Web 页面中的链接；按照链接的类型对获取的链接进行分类；以及根据分类后的链接判断是否存在钓鱼式攻击，其中链接分为两种类型：与所述 Web 页面的地址属于相同域的内部链接以及与所述 Web 页面的地址属于不同域的外部链接。

[0005] 根据本公开的另一个实施例，其中根据分类后的链接判断是否存在钓鱼式攻击包括计算各类型的链接所占链接总数的百分比；将计算的各类型的链接所占链接总数的百分比与预先设定的阈值进行比较；以及利用所述比较结果判断是否存在钓鱼式攻击。

[0006] 根据本公开的另一个实施例，其中利用所述比较结果判断是否存在钓鱼式攻击包括：响应于比较结果表明内部链接小于预先设定的阈值，提示用户可能存在钓鱼式攻击。

[0007] 根据本公开的另一个实施例，其中利用所述比较结果判断是否存在钓鱼式攻击包括：响应于比较结果表明内部链接不小于预先设定的阈值，向用户显示 Web 页面。

[0008] 根据本公开的另一个实施例，其中利用所述比较结果判断是否存在钓鱼式攻击包括：响应于比较结果表明外部链接不小于该预先设定的阈值，提示用户可能存在钓鱼式攻击。

[0009] 根据本公开的另一个实施例，其中利用所述比较结果判断是否存在钓鱼式攻击包

括：响应于比较结果表明外部链接小于预先设定的阈值，向用户显示 Web 页面。

[0010] 根据本公开的一个实施例，提供了一种用于防止钓鱼式攻击的系统，包括：获取部件，被配置为获取 Web 页面中的链接；分类部件，被配置为按照链接的类型对获取的链接进行分类；以及判断部件，被配置为根据分类后的链接判断是否存在钓鱼式攻击，其中链接分为两种类型：与所述 Web 页的地址属于相同域的内部链接以及与所述 Web 页的地址属于不同域的外部链接。

[0011] 此外，本公开的实施例还提供了与上述方法对应的计算机程序产品。

[0012] 通过执行根据本公开实施例提供的上述一个或多个实施例的方法或系统，由于在向用户显示再现后的 Web 页面之前首先检测是否为钓鱼式攻击的假冒网站，并在检测到假冒网站时提示用户，这样避免了因钓鱼式攻击导致的不必要的损失。

附图说明

[0013] 本公开可以通过参考下文中结合附图所给出的描述而得到更好的理解，其中在所有附图中使用了相同或相似的附图标记来表示相同或者相似的部件。所述附图连同下面的详细说明一起包含在本说明书中并且形成本说明书的一部分，而且用来进一步举例说明本公开的优选实施例和解释本公开的原理和优点。

[0014] 在附图中：

[0015] 图 1 显示了适于用来实现本发明实施方式的示例性计算系统 100 的框图；

[0016] 图 2 显示了根据本公开的实施例的用于预防钓鱼式攻击的方法 200 的流程图；

[0017] 图 3 显示了根据本公开的实施例的用于防止钓鱼式攻击的系统 300 的框图。

具体实施方式

[0018] 在下文中将结合附图对本公开的示范性实施例进行描述。为了清楚和简明起见，在说明书中并未描述实际实施方式的所有特征。然而，应该了解，在开发任何这种实际实施例的过程中必须做出很多特定于该实际实施方式的决定，以便实现开发人员的具体目标，例如，符合与系统及业务相关的那些限制条件，并且这些限制条件可能会随着实施方式的不同而有所改变。此外，还应该了解，虽然开发工作有可能是非常复杂和费时的，但对得益于本公开公开内容的本领域技术人员来说，这种开发工作仅仅是例行的任务。

[0019] 在此，还需要说明的一点是，为了避免因不必要的细节而模糊了本公开，在附图中仅仅示出了与根据本公开的方案密切相关的装置结构和 / 或处理步骤，而省略了与本公开关系不大的其他细节。

[0020] 钓鱼式攻击的攻击者往往利用真正的合法网站的资源来构建假冒网站，也就是说，假冒网站的版式、图像、链接等页面资源都会从真正的合法网站获取，这样，假冒网站的界面外观往往与真正的合法网站非常相似，因而也会非常容易取得用户的信任从而诱骗用户。攻击者通常将与真正的合法网站非常相似的假冒网站中涉及需要用户输入并提交个人敏感信息的部分指向预先设定好的地址，这样，当用户输入个人敏感信息并提交时，对用户来说，似乎是将其个人敏感信息提交给了真正的合法网站，但实际上是将其个人敏感信息提交给钓鱼攻击的攻击者。

[0021] 针对上面常见的钓鱼式攻击的方法，提出了根据本公开的一个或多个实施例的方

法和系统。

[0022] 下面结合附图详细介绍根据本公开的用于预防钓鱼式攻击的方法和系统的实施例。

[0023] 下面参见图 1，其中显示了适于用来实现本公开的一个或多个实施方式的示例性计算系统 100 的框图。如所示，计算机系统 100 可以包括 :CPU(中央处理单元)101、RAM(随机存取存储器)102、ROM(只读存储器)103、系统总线 104、硬盘控制器 105、键盘控制器 106、串行接口控制器 107、并行接口控制器 108、显示控制器 109、硬盘 110、键盘 111、串行外部设备 112、并行外部设备 113 和显示器 114。在这些设备中，与系统总线 104 耦合的有 CPU101、RAM 102、ROM 103、硬盘控制器 105、键盘控制器 106、串行控制器 107、并行控制器 108 和显示控制器 109。硬盘 110 与硬盘控制器 105 耦合，键盘 111 与键盘控制器 106 耦合，串行外部设备 112 与串行接口控制器 107 耦合，并行外部设备 113 与并行接口控制器 108 耦合，以及显示器 114 与显示控制器 109 耦合。应当理解，图 1 所述的结构框图仅仅为了示例的目的而示出的，而不是对本发明范围的限制。在某些情况下，可以根据具体情况而增加或者减少某些设备。

[0024] 下面参考图 2，其中显示了根据本公开的实施例的用于预防钓鱼式攻击的方法 200 的流程图。根据本公开的实施例的用于预防钓鱼式攻击的方法 200 从步骤 202 开始。

[0025] 接下来，方法 200 进入步骤 204，其中获取 Web 页面中的链接。通过对 Web 页面的源代码进行扫描进而获取 Web 页面中的链接。这些链接包括 :

[0026] HTML<a>href 属性，其中指定了链接所指向的地址 ;

[0027] HTML<script>src 属性，其中指定了外部脚本文件的源地址 ;

[0028] HTML<img>src 属性，其中指定了图像的源地址 ;

[0029] HTML<iFrame>src 属性，其中指定了要在 iFrame 中显示的文档的源地址 ;

[0030] HTML<Form>Action 属性，其中指定了表单提交的目的地址 ;

[0031] 等等。

[0032] 上面列出了 HTML 中一些涉及链接的属性的示例。应该理解，上面列出的只是 Web 页面中的链接的一些示例，其他涉及链接的 HTML 标签和属性，或者是 XHTML、XML 等其他标注语言中涉及的链接的标签、属性和内容对所属领域技术人员来说是知晓的，这里不再一一列举。

[0033] 根据本公开的发明人的观察，利用真正的合法网站的资源构建的假冒网站通常具有相同的特点，即

[0034] 1) 假冒网站的页面中的大部分资源从真正的合法网站获取 ;

[0035] 2) 需要用户输入并提交敏感信息的部分指向攻击者预先设定好的地址 ;

[0036] 3) 假冒网站的地址与真正的合法网站属于不同域 ;

[0037] 4) 攻击者预先设定好的地址与真正的合法网站属于不同域。

[0038] 以下是一个假冒网站的例子，攻击者假冒汇丰银行向用户发送电子邮件或即时通信的消息，当用户点击了攻击者发出的电子邮件或即时通信的消息中的链接，他将被导向地址为 http://qingadian.com/ 的假冒网站。该假冒网站具有与真正的汇丰银行的网站非常相似的页面以诱骗用户输入个人敏感信息。真正的合法的汇丰银行的网站地址为 http://www.hsbc.com.hk/。通过查看该假冒网站网站的代码可以看出 :该假冒网站页面中

的资源大部分都是从真正的合法网站获取的，参见下面给出的代码段。

[0039]

```
<script src='/1/PA_1_3_S5/content/hongkongpws/theme/js/pws_default.js' type="text/javascript"></script>
  <div class="containerGlobal"><div class="containerEntity"><div class="hsbcEntity">
  <div class="hsbcEntityTextArea01">Hong Kong</div>
  <div class="hsbcEntityTextArea02">
   <ul>
     <li class="hsbcEntityTabSelected"><a href="/1/2/home?fbc=HomeEngTopMenu">Home</a></li>
     <li><a href="/1/2/hk/personal?fbc=HomeEngTopMenu">Personal</a></li>
     <li><a href="/1/2/hsbcpremier/home?fbc=HomeEngTopMenu">HSBC Premier</a></li>
     <li><a href="/1/2/hsbcadvance/home?fbc=HomeEngTopMenu">HSBC Advance</a></li>
     <li><a href="http://www.commercial.hsbc.com.hk/1/2/commercial/home" 'width='+screen.width+', height=
'+screen.height*0.88+',location=yes,directories=no,menubar=yes,toolbar=yes,scrollbars=yes,status=yes,
resizable=yes,left=0,top=0');return false;">Commercial</a></li>
     <li><a href="http://www.hsbcnet.com/hsbc" target="_blank" onclick="window.open('http://www.hsbcnet.com/
hsbc','_blank','width='+screen.width+',height='+screen.height*0.88+',location=yes,directories=no,menubar=yes,
toolbar=yes,scrollbars=yes,status=yes,resizable=yes,left=0,top=0');return false;">Corporate</a></li>
     <li><a href="/1/2/mpf/home?fbc=HomeEngTopMenu">MPF</a></li>
     <li><a href="/1/2/hsbcgreaterchina?fbc=HomeEngTopMenu">Greater China</a></li>
     <li><a href="/1/2/about/home?fbc=HomeEngTopMenu">About HSBC</a></li>
     <li><a href="/1/2/careers/home?fbc=HomeEngTopMenu">Careers</a></li>
     <li><a href="/1/2/contact-us?fbc=HomeEngTopMenu">Contact us</a></li>
   </ul>
```

[0040]

```
   </div>
   </div>
   </div></div></div>
   … ….
 <p class="red"><strong>Personal Internet Banking</strong><br />
  <span style="display:block;float:left;"><a href="javascript:void(0)"
  onclick="window.open('http://qingadian.com/qingdaohuadian/CRM/login/IBlogin.html; 'width='+screen.
  width+',height='+screen.height*0.88+',location=no, directories=no,menubar=no,toolbar=no,scrollbars=yes,
  status=yes,resizable=yes,left=0,top=0'); onclick="window.open ">
  <img src="/1/PA_1_3_S5/content/hongkongpws/hk_home/images/logon.gif" alt="Logon" /></a></span>
```

[0041] 从上面给出的假冒网站的代码可以清楚的看出，假冒网站的页面资源大部分从真正的合法网站获取。而涉及到需要用户输入个人敏感信息部分指向了攻击者预先设定的地址，即 http://qingadian.com/qingdaohuadian/CRM/login/IBlogin.html。也就是说，用户在假冒网站上点击 Logon 按钮将被引导至上述地址。

[0042] 根据本公开的一个实施例，将链接分为两种类型：

[0043] 1) 内部链接，其链接地址与所述 Web 页面的地址属于相同域；

[0044] 2) 外部链接，其链接地址与所述 Web 页面的地址属于不同域；

[0045] 其中用户通过点击电子邮件或即时通信的消息中的链接访问所述 Web 页面。

[0046] 这里的域指的是域名。我们认为，属于同一家公司的不同域名的链接类型相同。例如 www.qq.com、www.tencent.com 等域名同属于腾讯公司，即涉及上述两个域名的链接是相同类型的链接；同理 www.sina.com、www.sinaimg.com 和 weibo.com 等域名同属于新浪公司；而 www.boc.cn、www.bankofchina.com 等域名同属于中国银行，等等。可以通过预先在数据库以列表或其他形式存储同属于一家公司的不同域名。也就是说，如果某一链接的地址对应的域名与所述 Web 页面的地址对应的域名相同或者属于同一家公司，那么该链接是内部链接。如果某一链接的地址对应的域名与所述 Web 页面的地址对应的域名不相同也不

属于同一家公司，那么该链接是外部链接。

[0047] 接下来，方法 200 进入步骤 206，其中对获取的链接进行分类。如前所述，根据本公开的一个实施例，将链接分为内部链接和外部链接两种类型。在步骤 206 中，根据链接的类型，即属于内部链接还是外部链接将获取的链接进行分类。这样，执行步骤 206 之后，得到属于内部链接的链接数量以及属于外部链接的链接数量。

[0048] 根据本公开的一个实施例，在获取 Web 页面中的链接或对链接进行分类的过程中可以排除常见的提供服务的第三方合法网站的链接，例如提供广告服务的 Google® AdWords®，或者提供搜索服务的Microsoft® Bing®等等。可以通过预先在数据库中以列表的形式存储这些需要排除的第三方合法网站，这样在获取 Web 页面的链接或链接进行分类的过程中可以通过查询列表的方式排除这些常见的提供服务的第三方合法网站的链接。

[0049] 接下来，方法 200 进入步骤 208，其中根据分类后的链接判断是否存在钓鱼式攻击。根据本公开的一个实施例，通过计算各类型的链接所占链接总数的百分比；以及将计算的各类型的链接所占链接总数的百分比与预先设定的阈值进行比较来根据分类后的链接判断是否存在钓鱼式攻击。根据本公开的一个实施例，链接分为内部链接和外部链接，计算内部链接和外部链接所占链接总数的百分比。之后，将计算出的内部链接所占链接总数的百分比与一个预先设定的阈值进行比较，如果比较结果表明内部链接小于该预先设定的阈值，则提示用户可能存在钓鱼式攻击。如果比较结果表明内部链接不小于预先设定的阈值，向用户显示再现后的 Web 页面。

[0050] 根据本公开的另一个实施例，将计算出的外部链接所占链接总数的百分比与一个预先设定的阈值进行比较，如果比较结果表明外部链接不小于该预先设定的阈值，则提示用户可能存在钓鱼式攻击。如果比较结果表明外部链接小于预先设定的阈值，向用户显示 Web 页面。

[0051] 我们以上面假冒网站为例，假设用户点击了攻击者发出的电子邮件或即时通信的消息中的链接，那么他将被导向地址 http://qingadian.com/。通过扫描上述地址对应的页面获取其中所有的链接。然后，根据链接的类型，即链接属于内部链接还是外部链接对获取的页面中的链接进行分类并计算各类型的链接所占链接总数的百分比。对于上述假冒网站，由于该假冒网站的页面资源大部分从真正的合法网站即 http://www.hsbc.com.hk/ 获取，因此与用户通过点击所访问的地址（即 http://qingadian.com/）属于相同域的内部链接的数量很少（通常只是需要用户输入个人敏感信息的部分对应的链接），而大部分链接来自于真正的合法网站，即 http://www.hsbc.com.hk/。如果用户通过点击所访问的是真正的合法网站，即 http://www.hsbc.com.hk，那么与用户通过点击所访问的该地址属于相同域的内部链接应该占多数。因此，我们假设预先设定的内部链接所占链接总数的阈值为 80％。如果用户通过点击所访问的假冒网站，那么与用户通过点击所访问的该地址属于相同域的内部链接应该很少。假设这时内部链接所占链接总数的比例大约为 5％。由于 5％远小于 80％，表明可能存在钓鱼式攻击，这时提示用户可能存在钓鱼式攻击。

[0052] 以上通过结合附图 2 对根据本公开的一个或多个实施例进行了，描述。附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序

段、或代码的一部分，所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和 / 或流程图中的每个方框、以及框图和 / 或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0053] 现在参考图 3，其中显示了根据本公开的实施例的用于防止钓鱼式攻击的系统 300 的框图。

[0054] 根据本公开的实施例的用于防止钓鱼式攻击的系统 300 包括 ：获取部件 302，被配置为获取 Web 页面中的链接 ；分类部件 304，被配置为按照链接的类型对获取的链接进行分类 ；以及判断部件 306，被配置为根据分类后的链接判断是否存在钓鱼式攻击，其中链接分为两种类型 ：与所述 Web 页面的地址属于相同域的内部链接以及与所述 Web 页面的地址属于不同域的外部链接。根据本公开的一个实施例，其中获取部件 302 进一步被配置为通过扫描 Web 页面的源代码获取 Web 页面中的链接。

[0055] 根据本公开的一个实施例，用于防止钓鱼式攻击的系统 300 进一步包括 ：计算部件（未显示），被配置为计算各类型的链接所占链接总数的百分比 ；以及比较部件（未显示），被配置为将计算的各类型的链接所占链接总数的百分比与预先设定的阈值进行比较。

[0056] 根据本公开的一个实施例，用于防止钓鱼式攻击的系统 300 进一步包括 ：提示部件（未显示），被配置为响应于比较结果表明内部链接小于预先设定的阈值，提示用户可能存在钓鱼式攻击 ；以及显示部件（未显示），被配置为响应于比较结果表明内部链接不小于预先设定的阈值，向用户显示 Web 页面。

[0057] 根据本公开的一个实施例，用于防止钓鱼式攻击的系统 300 进一步包括 ：提示部件（未显示），被配置为比较结果表明外部链接不小于该预先设定的阈值，则提示用户可能存在钓鱼式攻击 ；以及显示部件（未显示），被配置为响应于比较结果表明外部链接小于预先设定的阈值，向用户显示 Web 页面。

[0058] 所属技术领域的技术人员知道，本发明的多个方面可以体现为系统、方法或计算机程序产品。因此，本发明的多个方面可以具体实现为以下形式，即，可以是完全的硬件、完全的软件（包括固件、驻留软件、微代码等）、或者本文一般称为“电路”、“模块”或“系统”的软件部分与硬件部分的组合。此外，本发明的多个方面还可以采取体现在一个或多个计算机可读介质中的计算机程序产品的形式，该计算机可读介质中包含计算机可用的程序码。

[0059] 可以使用一个或多个计算机可读的介质的任何组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电的、磁的、光的、电磁的、红外线的、或半导体的系统、装置、器件或任何以上的组合。计算机可读存储介质的更具体的例子（非穷举的列表）包括以下 ：有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器 (RAM)、只读存储器 (ROM)、可擦式可编程只读存储器 (EPROM 或闪存)、光纤、便携式紧凑磁盘只读存储器 (CD-ROM)、光存储器件、磁存储器件、或者上述的任何合适的组合。在本文件的语境中，计算机可读存储介质可以是任何包含或存储程序的有形的介质，该程序被指令执行系统、装置或者器件使用或者

与其结合使用。

[0060] 计算机可读的信号介质可包括在基带中或者作为载波一部分传播的、其中体现计算机可读的程序码的传播的数据信号。这种传播的信号可以采用多种形式，包括——但不限于——电磁信号、光信号或任何以上合适的组合。计算机可读的信号介质可以是并非为计算机可读存储介质、但是能发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序的任何计算机可读介质。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、电线、光缆、RF 等等，或者任何合适的上述组合。

[0061] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、电线、光缆、RF 等等，或者任何合适的上述组合。

[0062] 用于执行本发明的操作的计算机程序码，可以以一种或多种程序设计语言的任何组合来编写，所述程序设计语言包括面向对象的程序设计语言 - 诸如 Java、Smalltalk、C++ 之类，还包括常规的过程式程序设计语言 - 诸如”C”程序设计语言或类似的程序设计语言。程序码可以完全地在用户的计算上执行、部分地在用户的计算机上执行、作为一个独立的软件包执行、部分在用户的计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在后一种情形中，远程计算机可以通过任何种类的网络——包括局域网 (LAN) 或广域网 (WAN)- 连接到用户的计算机，或者，可以（例如利用因特网服务提供商来通过因特网）连接到外部计算机。

[0063] 以下参照按照本发明实施例的方法、装置（系统）和计算机程序产品的流程图和 / 或框图描述本发明的多个方面。要明白的是，流程图和 / 或框图的每个方框以及流程图和 / 或框图中各方框的组合，都可以由计算机程序指令实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器，从而生产出一种机器，使得通过计算机或其它可编程数据处理装置执行的这些指令，产生实现流程图和 / 或框图中的方框中规定的功能 / 操作的装置。

[0064] 也可以把这些计算机程序指令存储在能指令计算机或其它可编程数据处理装置以特定方式工作的计算机可读介质中，这样，存储在计算机可读介质中的指令产生一个包括实现流程图和 / 或框图中的方框中规定的功能 / 操作的指令装置 (instruction means) 的制造品。

[0065] 也可以把计算机程序指令加载到计算机或其它可编程数据处理装置上，使得在计算机或其它可编程数据处理装置上执行一系列操作步骤，以产生计算机实现的过程，从而在计算机或其它可编程装置上执行的指令就提供实现流程图和 / 或框图中的方框中规定的功能 / 操作的过程。

[0066] 还需要指出的是，在本公开的装置和方法中，显然，各部件或各步骤是可以分解和 / 或重新组合的。这些分解和 / 或重新组合应视为本公开的等效方案。并且，执行上述系列处理的步骤可以自然地按照说明的顺序按时间顺序执行，但是并不需要一定按照时间顺序执行。某些步骤可以并行或彼此独立地执行。

[0067] 虽然已经详细说明了本公开及其优点，但是应当理解在不脱离由所附的权利要求所限定的本公开的精神和范围的情况下可以进行各种改变、替代和变换。而且，本申请的术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要

素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个.....”限定的要素，并不排除在包括所述要素的过程、方法、物品或者装置中还存在另外的相同要素。

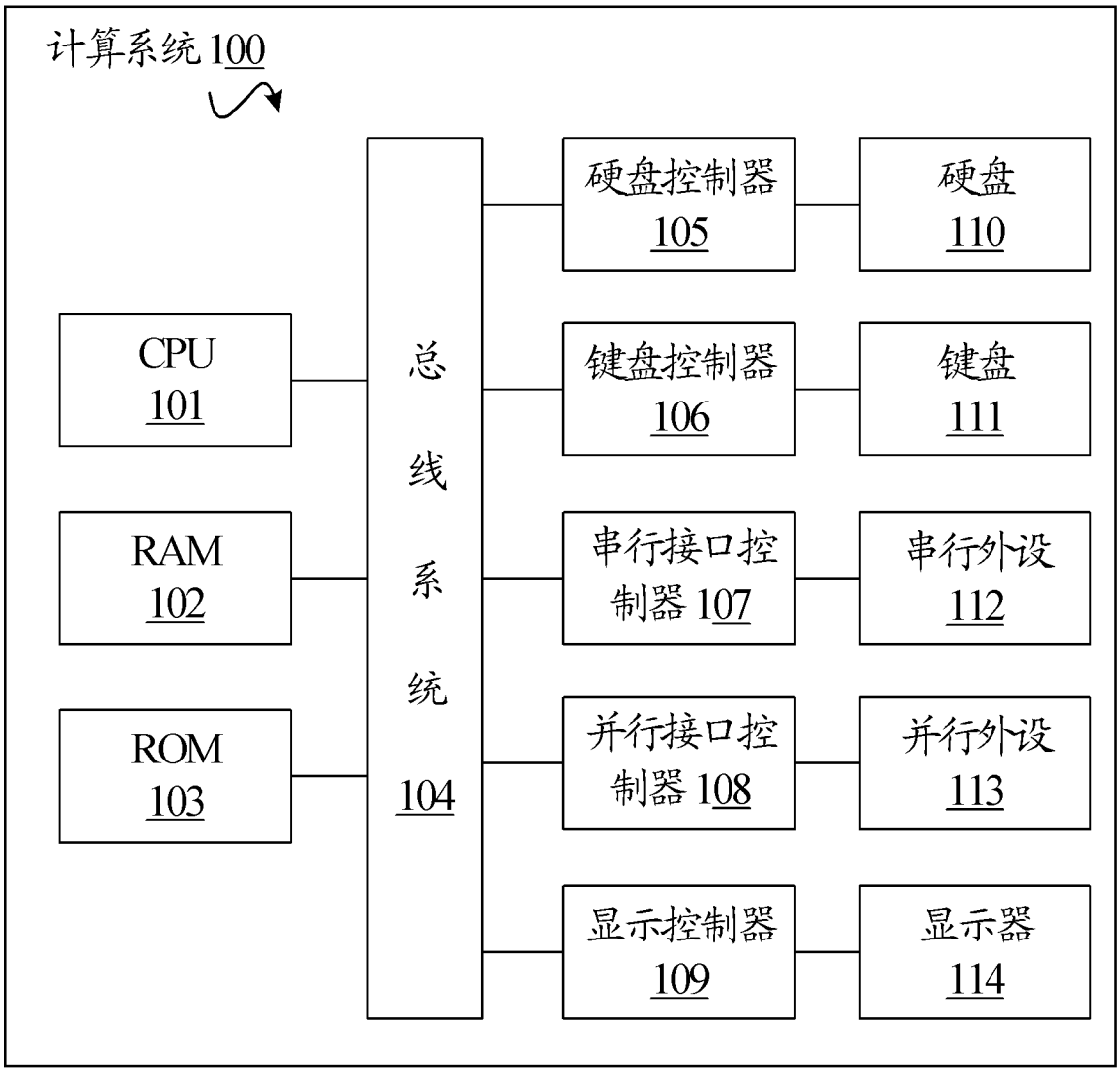

计算系统 100
CPU 101
RAM 102
ROM 103
总线系统 104
硬盘控制器 105
键盘控制器 106
串行接口控制器 107
并行接口控制器 108
显示控制器 109
硬盘 110
键盘 111
串行外设 112
并行外设 113
显示器 114

图 1

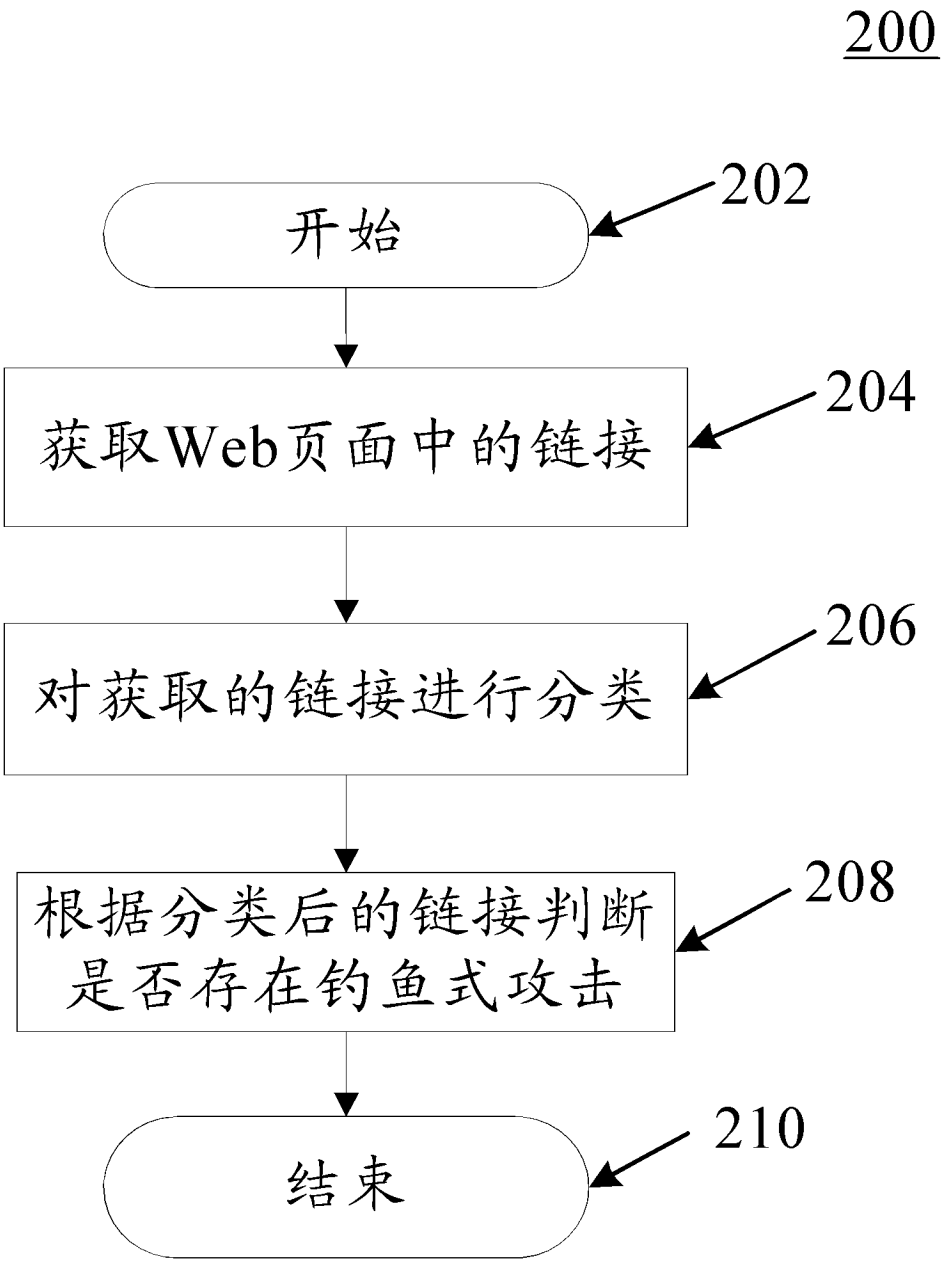

200
开始
202
获取Web页面中的链接
204
对获取的链接进行分类
206
根据分类后的链接判断是否存在钓鱼式攻击
208
结束
210

图 2

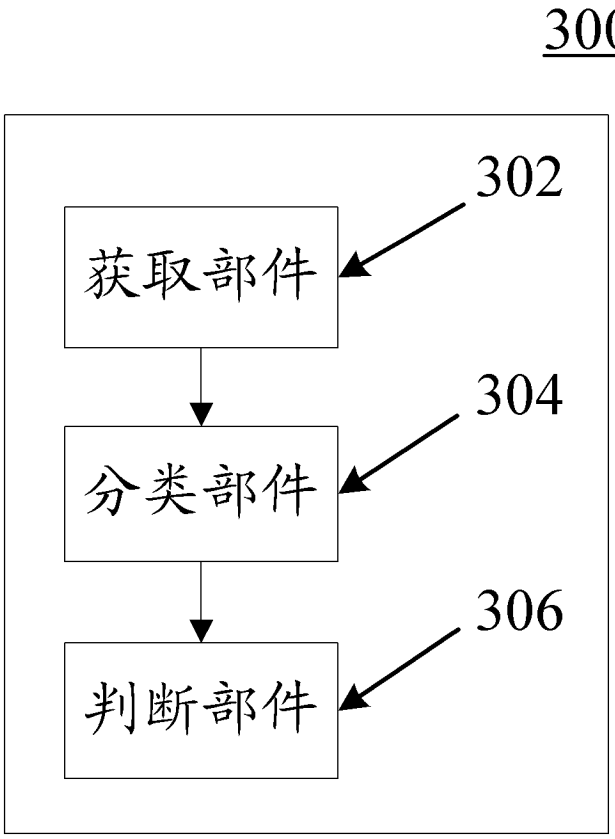


图 3