

(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
2014 年 5 月 30 日 (30.05.2014)



(10) 国际公布号
WO 2014/079307 A1

- (51) 国际专利分类号:
G06F 21/56 (2013.01)
- (21) 国际申请号: PCT/CN2013/086233
- (22) 国际申请日: 2013 年 10 月 30 日 (30.10.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210475499.2 2012 年 11 月 21 日 (21.11.2012) CN
- (71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (72) 发明人: 鲁四喜 (LU, Sixi); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (74) 代理人: 北京东方亿思知识产权代理有限公司 (BEIJING EAST IP LTD.); 中国北京市东城区东长安街 1 号东方广场东方经贸城东 2 座 1601 室, Beijing 100738 (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, LT, 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, 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))。

(54) Title: METHOD AND DEVICE FOR MONITORING MALICIOUS LINK INJECTION OF WEBSITE SOURCE CODES

(54) 发明名称: 网站源代码恶意链接注入监控方法及装置

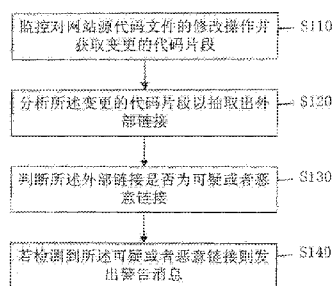


图 1 / FIG. 1

S110 MONITORING A MODIFYING OPERATION ON A WEBSITE SOURCE CODE FILE AND ACQUIRING A MODIFIED CODE FRAGMENT
S120 ANALYZING THE MODIFIED CODE FRAGMENT SO AS TO EXTRACT AN EXTERNAL LINK
S130 JUDGING WHETHER THE EXTERNAL LINK IS A SUSPICIOUS OR MALICIOUS LINK
S140 IF A SUSPICIOUS OR MALICIOUS LINK IS DETECTED, SENDING A WARNING MESSAGE

(57) Abstract: The present invention relates to a method for monitoring malicious link injections of website source codes, comprising: monitoring a modifying operation on a website source code file and acquiring a modified code fragment; analyzing the modified code fragment so as to extract an external link; judging whether the external link is a suspicious or malicious link; and if it is determined that the external link is a suspicious or malicious link, sending a warning message. The method for monitoring malicious link injection of website source codes can monitor modified contents of source codes in real time, effectively prohibiting the common virus transmission mode in which, after a system writing right is acquired by using a loophole in the operating system or a third-party application, a malicious redirected URL is injected into the page codes of a legal website. Furthermore, also provided is a device for monitoring malicious link injections of website source codes.

(57) 摘要: 本发明涉及一种网站-源代码恶意链接注入监控方法, 包括: 监控对网站源代码文件的修改操作并获取变更的代码片段; 分析所述变更的代码片段以抽取外部链接; 判断所述外部链接是否为可疑或者恶意链接; 以及若判定所述外部链接为可疑或者恶意链接则发出警告消息。上述的网站源代码恶意链接注入监控方法可实时监控源代码的变更内容, 有效的阻止了通过利用操作系统或第三方应用漏洞获取系统写权限后注入恶意的重定向网址到合法网站的页面代码中这样一类常见的病毒传播方式, 此外, 本发明还提供一种网站源代码恶意链接注入监控装置。

WO 2014/079307 A1

网站源代码恶意链接注入监控方法及装置

技术领域

本发明涉及网站安全技术，尤其涉及一种网站源代码恶意链接注入监控方法及装置。

背景技术

目前一种被普遍采用的传播病毒的方式是首先利用操作系统或第三方应用漏洞来获取系统的写权限，然后注入恶意的重定向网址到合法网站的页面代码中。如何检测网站是否被感染，目前的方案主要是：从外部抓取（crawling）网站内容，然后扫描页面内容是否有恶意代码。这类方法比较典型，如：symantec 的 safeweb 技术，McAfee 的 siteadvisor 技术等。

基于抓取技术的外部检测系统，存在着非实时性、漏报、误报等问题。病毒的传播性很强，可以在短时间内感染大量的网站，而从外部抓取网站内容无法在短时间内将所有网站内容抓取下来，故无法实时检测网站的安全性；这样会导致已经感染的页面因为非实时性而被误报为仍然安全，导致误报。

目前的网站的开发方式基本上为少量的源代码动态加载大量的数据库内容，对于数据库内容的安全性，如防止 SQL 注入、XSS 跨站攻击，目前都有较成熟的解决方案，而对源代码的保护却不够，而这部分也正是恶意网址注入的攻击点之一。

发明内容

有鉴于此，有必要提供一种网站源代码恶意链接注入监控方法及装置，其可提升网站源代码的安全性。

一种网站源代码恶意链接注入监控方法，包括：监控对网站源代码文

件的修改操作并获取变更的代码片段；分析所述变更的代码片段以抽取出外部链接；判断所述外部链接是否为可疑或者恶意链接；以及若判定所述外部链接为可疑或者恶意链接则发出警告消息。

一种网站源代码恶意链接注入监控装置，包括：代码监控单元，用于监控对网站源代码文件的修改操作并获取变更的代码片段；链接抽取单元，用于分析所述变更的代码片段以抽取出外部链接；链接分析单元，用于判断所述外部链接是否为可疑或者恶意链接；以及安全警告单元，用于若判定所述外部链接为可疑或者恶意链接则发出警告消息。

上述的网站源代码恶意链接注入监控方法及装置可实时监控源代码的变更内容，如果源代码的变更内容包含一些危险的外部链接元素，则立即发出警告给系统管理员，从而能够实时监控网站的安全性，进而有效的阻止了通过利用操作系统或第三方应用漏洞获取系统写权限后注入恶意的重定向网址到合法网站的页面代码中这样一类常见的病毒传播方式。

相比于传统的外部抓取方式，可以做到实时保护，避免了在等待被抓取期间恶意链接的传播。此外，由于网站源代码文件有限，并且相对来说变更的频率较低，故本实施例的方法对系统的性能影响较低。

为了让本发明的上述和其他目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附图式，作详细说明如下。

附图说明

图 1 为第一实施例提供的一种网站源代码恶意链接注入监控方法流程图。

图 2 为第二实施例提供的一种网站源代码恶意链接注入监控装置流程图。

具体实施方式

为更进一步阐述本发明为实现预定发明目的所采取的技术手段及功

效，以下结合附图及较佳实施例，对依据本发明的具体实施方式、结构、特征及其功效，详细说明如后。

实施例 1

参阅图 1，第一实施例提供一种网站源代码恶意链接注入监控方法，上述的监控方法包括：

步骤 S110、监控对网站源代码文件的修改操作并获取变更的代码片段。

一般来说，网站源代码文件会存储在一个或多个目录下，通过实时监控这些目录下的源代码文件，可以在有变更的时候抽取变更的代码段。例如，首先可将网站源代码文件进行备份，并对所有备份的源代码文件建立索引，存储其修改时间。然后通过比较监控的目录下源代码文件的修改时间与备份的源代码文件的修改时间即可获知源代码文件是否已经被修改。进一步地，比较两个版本的内容即可提取出变更的代码片段。

此外，可以理解，监控源代码文件的修改并不限于上述方法，例如，还可监测系统对磁盘的写操作，并在监测到对网站源代码目录内的文件进行的写操作时直接获取变更的代码片段。

步骤 S120、分析所述变更的代码片段以抽取出外部链接。

变更的代码片段可能是采用不同的编程语言例如 HTML、Javascripts、或者 PHP 等编写完成的。而不同的编程语言具有不同的语法，需要分别进行分析。具体地，步骤 S120 例如可包括：根据变更的代码片段所采用的编程语言加载相应的代码分析器；以及采用该代码分析器解析所述代码片段以抽取出所述外部链接。例如，采用文件物件模型（Document Object Model, DOM）加载分析 HTML 格式的代码片段以抽取出外部链接。

步骤 S130、判断所述外部链接是否为可疑或者恶意链接。

首先，可从链接自身及其父元素的属性来分析外部链接是否属于可疑

或恶意链接。例如，可判断外部链接是否位于像素值为 0 的页面元素中，或者是否位于坐标位置明显在屏幕之外的页面元素中。对于这些反常的链接，即位于像素值为 0 的页面元素中或者坐标位置明显在屏幕之外的页面元素中的外部链接，均可视为可疑链接。

判定可疑链接后，即可执行步骤 S140 发出警告消息。此外，为进一步确认可疑链接的安全性，还可进一步将可疑链接发送至第三方网址安全验证服务以验证该可疑链接是否为已知的恶意链接。例如 <http://aq.qq.com/cn2/safe-school/url-query-index> 就提供一种线上恶意链接验证服务。若确认所有可疑链接均为安全外部链接，则可不执行步骤 S140。

此外，除了将上述的可疑链接发送至第三方网址安全验证服务进行验证外，还可将所有提取出的外部链接发送至第三方网址安全验证服务进行验证。此时，可以不从链接自身及其父元素的属性来分析外部链接是否属于可疑或恶意链接，而直接进行线上验证。若第三方网址安全验证服务返回的结果表明存在可疑或者恶意链接则执行步骤 S140。

步骤 S140，若判定所述外部链接为可疑或者恶意链接则发出警告消息。

例如，发送邮件或者采用即时通讯软件发送消息告知系统管理员，进行人工确认。

此外，进一步地，在判定所述外部链接为可疑或者恶意链接后，还可启动保护机制以防止源代码监控系统文件被恶意删除、服务被恶意卸载或者终止。

本实施例的网站源代码恶意链接注入监控方法实时监控源代码的变更内容，如果源代码的变更内容包含一些危险的外部链接元素，则立即发出警告给系统管理员，从而能够实时监控网站的安全性，进而有效的阻止

了通过利用操作系统或第三方应用漏洞获取系统写权限后注入恶意的重定向网址到合法网站的页面代码中这样一类常见的病毒传播方式。

相比于传统的外部抓取方式，可以做到实时保护，避免了在等待被抓取期间恶意链接的传播。此外，由于网站源代码文件有限，并且相对来说变更的频率较低，故本实施例的方法对系统的性能影响较低。

实施例 2

参阅图 2，本发明第二实施例提供一种网站源代码恶意链接注入监控装置 200，包括：代码监控单元 210、链接抽取单元 220、链接分析单元 230、以及安全警告单元 240。

代码监控单元 210 用于监控对网站源代码文件的修改操作并获取变更的代码片段。一般来说，网站源代码文件会存储在一个或多个目录下，通过实时监控这些目录下的源代码文件，可以在有变更的时候抽取变更的代码段。例如，首先可将网站源代码文件进行备份，并对所有备份的源代码文件建立索引，存储其修改时间。然后通过比较监控的目录下源代码文件的修改时间与备份的源代码文件的修改时间即可获知源代码文件是否已经被修改。进一步地，比较两个版本的内容即可提取出变更的代码片段。

此外，可以理解，监控源代码文件的修改并不限于上述方法，例如，还可监测系统对磁盘的写操作，并在监测对网站源代码目录内的文件进行的写操作时直接获取变更的代码片段。

链接抽取单元 220 用于分析所述变更的代码片段以抽取出外部链接。变更的代码片段可能是采用不同的编程语言例如 HTML、Javascripts、或者 PHP 等编写完成的。而不同的编程语言具有不同的语法，需要分别进行分析。具体地，链接抽取单元 220 可用于：根据变更的代码片段所采用的编程语言加载相应的代码分析器；以及采用该代码分析器解析所述代码片段以抽取出所述外部链接。例如，采用文件物件模型（Document Object

Model, DOM) 加载分析 HTML 格式的代码片段以抽取出外部链接。

链接分析单元 230 用于判断所述外部链接是否为可疑或者恶意链接。首先,可从链接自身及其父元素的属性来分析外部链接是否属于可疑或恶意链接。例如,可判断外部链接是否位于像素值为 0 的页面元素中,或者是否位于坐标位置明显在屏幕之外的页面元素中。对于这些反常的链接,即位于像素值为 0 的页面元素中或者坐标位置明显在屏幕之外的页面元素中的外部链接,均可视为可疑链接。

判定可疑链接后,即可将可疑链接相关信息发送至安全警告单元 240,由安全警告单元发出警告消息。此外,为进一步确认可疑链接的安全性,还可进一步将可疑链接发送至第三方网址安全验证服务以验证该可疑链接是否为已知的恶意链接。例如 <http://aq.qq.com/cn2/safe-school/url-query-index> 就提供一种线上恶意链接验证服务。若确认所有可疑链接均为安全外部链接,则可不调用安全警告单元 240。

此外,链接分析单元 230 除了将上述的可疑链接发送至第三方网址安全验证服务进行验证外,还可将所有提取出的外部链接发送至第三方网址安全验证服务进行验证。此时,可以不从链接自身及其父元素的属性来分析外部链接是否属于恶意链接,而直接进行线上验证。若第三方网址安全验证服务返回的结果表明存在可疑或者恶意链接则将可疑或者恶意链接发送至安全警告单元 240。

安全警告单元 240 用于若判定所述外部链接为可疑或者恶意链接则发出警告消息。例如,发送邮件或者采用即时通讯软件发送消息告知系统管理员,进行人工确认。

此外,监控装置 200 还可包括安全防护单元 250,用于在判定所述外部链接为可疑或者恶意链接之后启动保护机制以防止监控装置 200 被恶意删除、服务被恶意卸载或者终止。例如,安全防护单元 250 可以驱动服

务的形式加载于操作系统内，监测并拦截外部程序对于监控装置 200 各功能模块的操作，以防止监控装置 200 被恶意删除、服务被恶意卸载或者终止。

本实施例的网站源代码恶意链接注入监控装置实时监控源代码的变更内容，如果源代码的变更内容包含一些危险的外部链接元素，则立即发出警告给系统管理员，从而能够实时监控网站的安全性，进而有效的阻止了通过利用操作系统或第三方应用漏洞获取系统写权限后注入恶意的重定向网址到合法网站的页面代码中这样一类常见的病毒传播方式。

相比于传统的外部抓取方式，可以做到实时保护，避免了在等待被抓取期间恶意链接的传播。此外，由于网站源代码文件有限，并且相对来说变更的频率较低，故本实施例的方法对系统的性能影响较低。

此外，本发明实施例还提供一种计算机可读存储介质，其内存储有计算机可执行指令，上述的计算机可读存储介质例如为非易失性存储器例如光盘、硬盘、或者闪存。上述的计算机可执行指令用于让计算机或者类似的运算装置完成上述的网站源代码恶意链接注入监控方法中的各种操作。

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示如上，然而并非用以限定本发明，任何本领域技术人员，在不脱离本发明技术方案范围内，当可利用上述揭示的技术内容做出些许更动或修饰为等同变化的等效实施例，但凡是未脱离本发明技术方案内容，依据本发明的技术实质对以上实施例所作的任何简介修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

权 利 要 求 书

1. 一种网站源代码恶意链接注入监控方法，包括：

监控对网站源代码文件的修改操作并获取变更的代码片段；

分析所述变更的代码片段以抽取出外部链接；

判断所述外部链接是否为可疑或者恶意链接；以及

若判定所述外部链接为可疑或者恶意链接则发出警告消息。

2. 如权利要求 1 所述的网站源代码恶意链接注入监控方法，其特征在于，还包括：在判定所述外部链接为可疑或者恶意链接之后，启动保护机制以防止系统文件被恶意删除、服务被恶意卸载或者终止。

3. 如权利要求 1 所述的网站源代码恶意链接注入监控方法，其特征在于，判断所述外部链接是否为可疑或者恶意链接包括：根据所述外部链接是否为位于像素值为 0 的页面元素中所包含的链接，或者为坐标位置明显在屏幕之外的页面元素所包含的链接判断所述外部链接是否为可疑或者恶意链接。

4. 如权利要求 1 所述的网站源代码恶意链接注入监控方法，其特征在于，判断所述外部链接是否为可疑或者恶意链接包括：将所述外部链接发送至第三方网址验证服务以验证所述外部链接是否为可疑或恶意链接。

5. 如权利要求 1 所述的网站源代码恶意链接注入监控方法，其特征在于，分析所述变更的代码片段以抽取出外部链接包括：根据所述代码片段所采用的编程语言加载相应的代码分析器；以及采用该代码分析器解析所述代码片段以抽取出所述外部链接。

6. 一种网站源代码恶意链接注入监控装置，包括：

代码监控单元，用于监控对网站源代码文件的修改操作并获取变更的代码片段；

链接抽取单元，用于分析所述变更的代码片段以抽取出外部链接；

链接分析单元，用于判断所述外部链接是否为可疑或者恶意链接；

安全警告单元，用于若判定所述外部链接为可疑或者恶意链接则发出警告消息。

7. 如权利要求 6 所述的网站源代码恶意链接注入监控装置，其特征在于，还包括安全防护单元，用于在判定所述外部链接为可疑或者恶意链接之后启动保护机制以防止系统文件被恶意删除、服务被恶意卸载或者终止。

8. 如权利要求 6 所述的网站源代码恶意链接注入监控装置，其特征在于，所述链接分析单元，用于根据所述外部链接是否为位于像素值为 0 的页面元素中所包含的链接，或者为坐标位置明显在屏幕之外的页面元素所包含的链接判断所述外部链接是否为可疑或者恶意链接。

9. 如权利要求 6 所述的网站源代码恶意链接注入监控装置，其特征在于，所述链接分析单元，用于将所述外部链接发送至第三方网址验证服务以验证所述外部链接是否为可疑或恶意链接。

10. 如权利要求 6 所述的网站源代码恶意链接注入监控装置，其特征在于，所述链接抽取单元，用于根据所述代码片段所采用的编程语言加载相应的代码分析器以及采用该代码分析器解析所述代码片段以抽取出所述外部链接。

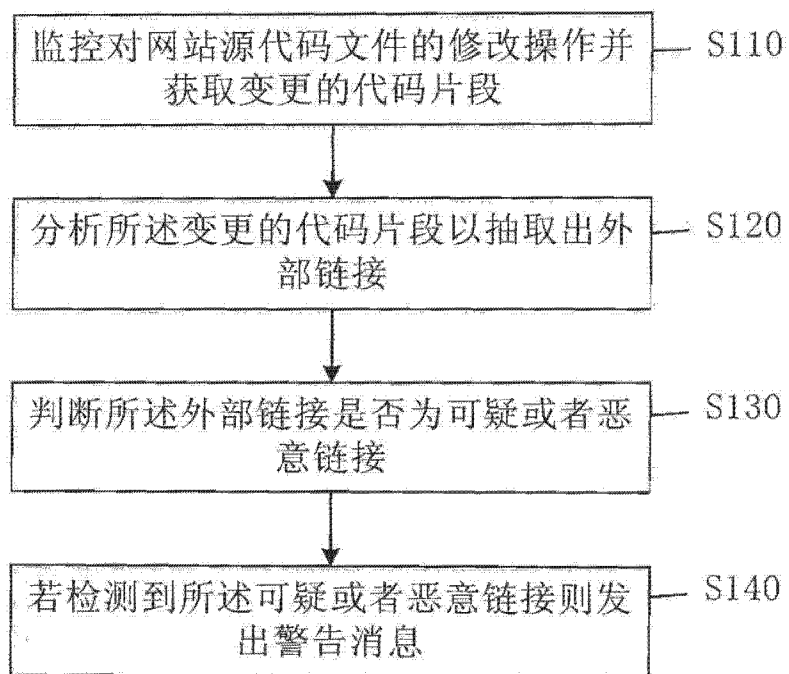


图 1

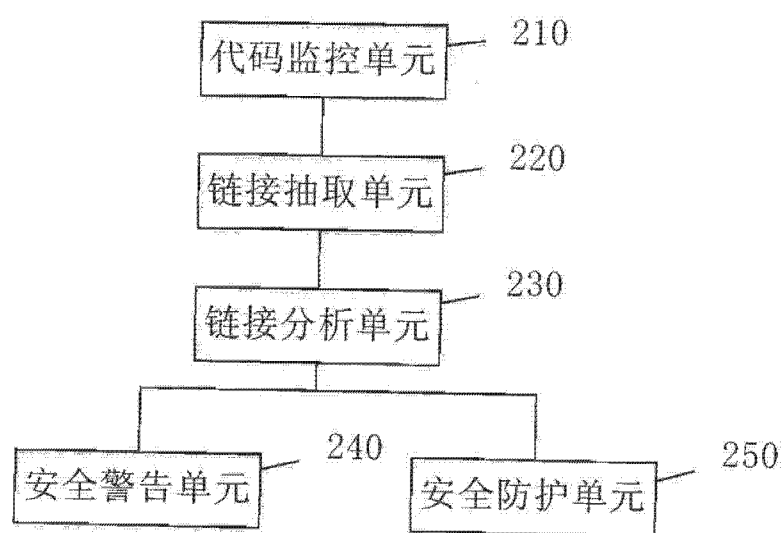


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/086233**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 21/56 (2013.01) 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)

IPC: G06F

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)

CNABS, CNTXT, DWPI: page, source code, malice, suspicious, real time, WEBSITE, WEBPAGE, CODE, MODIF+, ALTER+, CHANG+, HYPERLINK, LINK, DETECT, SUPERVIS+, MONITOR, INJECT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 1866817 A (BEIJING AHELIOS CONSULTING INC.), 22 November 2006 (22.11.2006), description, page 5, line 7 to page 7, line 6, and figures 1-2 and 4	1-10
Y	CN 102662840 A (TIANJIN UNIVERSITY), 12 September 2012 (12.09.2012), description, paragraphs [0038]-[0045], and figure 1	1-10
A	US 2010192224 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 29 July 2010 (29.07.2010), the whole document	1-10
A	US 2002010855 A1 (RESHEF, E. et al.), 24 January 2002 (24.01.2002), the whole document	1-10

☐ 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 26 December 2013 (26.12.2013)	Date of mailing of the international search report 20 February 2014 (20.02.2014)
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 HE, Minglun Telephone No.: (86-10) 61648107

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/086233

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1866817 A	22.11.2006	None	
CN 102662840 A	12.09.2012	None	
US 2010192224 A1	29.07.2010	None	
US 002010855 A1	24.01.2002	WO 0165330 A2	07.09.2001
		AU 3769601 A	12.09.2001
		EP 269286 A2	02.01.2003
		US 2003233581 A1	18.12.2003
		AT 414943 T	15.12.2008
		DE 60136616 D1	02.01.2009

A. 主题的分类

G06F 21/56 (2013.01) 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)

IPC: G06F

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))

CNABS, CNTXT, DWPI: 网站, 网页, 页面, 源代码, 源码, 代码, 修改, 变更, 改变, 更改, 链接, 注入, 监控, 检测, 监测, 恶意, 可疑, 实时, WEBSITE, WEBPAGE, CODE, MODIF+, ALTER+, CHANG+, HYPERLINK, LINK, DETECT, SUPERVIS+, MONITOR, INJECT

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
Y	CN 1866817 A (北京华景中天信息技术有限公司) 22.11 月 2006 (22.11.2006) 说明书第 5 页第 7 行-第 7 页第 6 行、图 1-2, 4	1-10
Y	CN 102662840 A (天津大学) 12.9 月 2012 (12.09.2012) 说明书第 [0038]-[0045]段、图 1	1-10
A	US 2010192224 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 29.7 月 2010 (29.07.2010) 全文	1-10
A	US 2002010855 A1 (RESHEF, Eran 等) 24.1 月 2002 (24.01.2002) 全文	1-10



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

26.12 月 2013 (26.12.2013)

国际检索报告邮寄日期

20.2 月 2014 (20.02.2014)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

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

何明伦

电话号码: (86-10) 61648107

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/086233

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 1866817 A	22. 11. 2006	无	
CN 102662840 A	12. 09. 2012	无	
US 2010192224 A1	29. 07. 2010	无	
US 2002010855 A1	24. 01. 2002	WO 0165330 A2	07. 09. 2001
		AU 3769601 A	12. 09. 2001
		EP 1269286 A2	02. 01. 2003
		US 2003233581 A1	18. 12. 2003
		AT 414943 T	15. 12. 2008
		DE 60136616 D1	02. 01. 2009