(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 101296087 B
(45)授权公告日 2011.09.21

(21)申请号 200810092320.9

(22)申请日 2008.04.22

(30)优先权数据
11/738,912 2007.04.23 US

(73)专利权人 SAP股份公司
地址 德国瓦尔多夫

(72)发明人 弗洛里安·克施鲍姆

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邵亚丽

(51)Int.Cl.
H04L 9/36(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 20040003293 A1,2004.01.01, 全文.
US 20040168083 A1,2004.08.26, 全文.
CN 1870493 A,2006.11.29, 全文.

审查员 李博

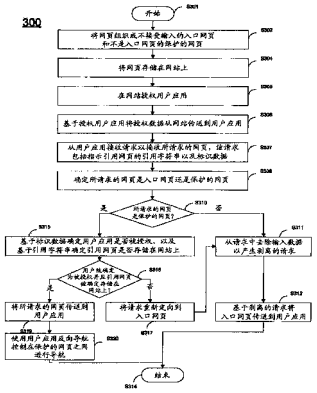
权利要求书 2 页 说明书 14 页 附图 9 页

(54)发明名称

用于防止跨站攻击的方法和系统

(57)摘要

公开了有效跨站攻击的防护,其方法包括:将网页被存储在网站上,该网页被组织成不接受输入的入口网页和不是入口网页的保护的网页;从用户应用接收请求以接收所请求的网页,该请求包括指示引用网页的引用字符串以及标识数据;确定所请求的网页是入口网页还是保护的网页,并且如果所请求的网页被确定为保护的网页,则进一步基于所述标识数据确定所述用户应用是否被授权;基于所述引用字符串确定所述引用网页是否存储在网站上;如果所述用户应用被确定为被授权并且所述引用网页被确定存储在网站上,则将所请求的网页传送到所述用户应用;以及如果所述用户应用被确定为未被授权或者所述引用网页被确定没有存储在网站上,则将该请求重新定向到所述入口网页之一。



CN 101296087 B

1. 一种用于防止跨站攻击的方法，包括：

将网页存储在网站上，该网页被组织成不接受输入的入口网页和不是入口网页的保护的网页；

从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据；

确定所请求的网页是入口网页还是保护的网页；

如果所请求的网页被确定为保护的网页，则基于所述标识数据确定所述用户应用是否被授权，以及基于所述引用字符串确定所述引用网页是否存储在网站上；

如果所述用户应用被确定为被授权并且如果所述引用网页被确定存储在网站上，则将所请求的网页传送到所述用户应用；以及

如果所述用户应用被确定为未被授权或者如果所述引用网页被确定没有存储在网站上，则将该请求重新定向到所述入口网页之一。

2. 如权利要求 1 所述的方法，还包括：

如果所请求的网页被确定为入口网页或者该请求被重新定向到入口网页，则从请求中去除输入数据，由此产生剥离的请求；以及

基于所述剥离的请求将所述入口网页之一传送到所述用户应用。

3. 如权利要求 1 所述的方法，还包括：

在网站授权所述用户应用。

4. 如权利要求 3 所述的方法，其中，所述授权所述用户应用还包括认证所述用户应用。

5. 如权利要求 4 所述的方法，其中，使用秘密密钥、使用会话统一资源定位符（" URL"）、使用超文本传输协议（" HTTP"）认证、或用户应用端的安全套接字协议层（" SSL"）授权所述用户应用。

6. 如权利要求 3 所述的方法，还包括：

基于授权所述用户应用，将所述标识数据从网站传送到所述用户应用。

7. 如权利要求 1 所述的方法，其中，所述标识数据是 cookie。

8. 如权利要求 1 所述的方法，还包括在所述网站将所述网页组织成入口网页和保护的网页。

9. 如权利要求 1 所述的方法，其中，所述请求在网关被接收。

10. 如权利要求 1 所述的方法，其中，所述保护的网页还包括应用、小服务程序或脚本。

11. 如权利要求 1 所述的方法，还包括使用用户应用反向导航控制在保护的网页之间进行导航。

12. 如权利要求 1 所述的方法，其中，所述用户应用是网络浏览器应用。

13. 如权利要求 1 所述的方法，其中，所述用户应用在用户设备上执行。

14. 如权利要求 1 所述的方法，其中，所述引用字符串是超文本传输协议（" HTTP"）引用字符串。

15. 如权利要求 1 所述的方法，其中，所述引用字符串存储引用网页的统一资源定位符（" URL"）。

16. 如权利要求 1 所述的方法，其中，至少一个入口网页是登录页、主页或入口扉页。

17. 如权利要求 1 所述的方法，其中，所述保护的网页是在线银行交易页、在线银行菜

单页、在线银行认证页、在线拍卖搜索结果页、在线拍卖登录页、在线拍卖认证页、在线拍卖投标入口页、在线拍卖投标验证页、在线零售商搜索结果页、在线零售商购物推车页、在线零售商登录页、在线零售商信用卡地址验证页、在线零售商确认页、网络邮件认证页、网络菜单页、网络邮件发送页、网络邮件搜索页、网络邮件读取页、搜索引擎搜索结果页、SAP®入口认证页或SAP®入口菜单页。

18. 如权利要求 1 所述的方法，其中，所述标识数据指示用户被授权但是未被认证。

19. 一种用于防止跨站攻击的系统，包括：

服务器，包括：

用于存储网页的装置，该网页被组织成不接受输入的入口网页和不是入口网页的保护的网页；和

网关，包括：

用于从用户应用接收请求以接收所请求的网页的装置，该请求包括指示引用网页的引用字符串以及标识数据；

用于确定所请求的网页是入口网页还是保护的网页的装置；

用于如果所请求的网页被确定为保护的网页，则基于所述标识数据确定所述用户应用是否被授权，以及基于所述引用字符串确定所述引用网页是否存储在网站上的装置；

用于如果所述用户应用被确定为被授权并且如果所述引用网页被确定存储在网站上，则将所请求的网页传送到所述用户应用的装置；以及

用于如果所述用户应用被确定为未被授权或者如果所述引用网页被确定没有存储在网站上，则将该请求重新定向到所述入口网页之一的装置。

20. 一种用于防止跨站攻击的装置，包括：

用于将网页存储在网站上的装置，该网页被组织成不接受输入的入口网页和不是入口网页的保护的网页；

用于从用户应用接收请求以接收所请求的网页的装置，该请求包括指示引用网页的引用字符串以及标识数据；

用于确定所请求的网页是入口网页还是保护的网页的装置；

用于如果所请求的网页被确定为保护的网页、则基于所述标识数据确定所述用户应用是否被授权、以及基于所述引用字符串确定所述引用网页是否存储在网站上的装置；

用于如果所述用户应用被确定为被授权并且所述引用网页被确定存储在网站上、则将所请求的网页传送到所述用户应用的装置；以及

用于如果所述用户应用被确定为未被授权或者如果所述引用网页被确定没有存储在网站上、则将该请求重新定向到所述入口网页之一的装置。

用于防止跨站攻击的方法和系统

技术领域

[0001] 本发明一般涉及跨站 (cross-site) 攻击的防护，并且至少一个特定实施方式涉及跨站脚本 (cross-site scripting) 和跨站请求伪造 (forgery) 攻击的防护。

背景技术

[0002] 虽然网络应用在虚拟环境中运行，但是它们中的一些，包括在线拍卖或银行应用，涉及真实世界的货币交易。网络用户和网站两者都在保护这些货币交易中存在既得利益 (vested interest)，这就给黑客操控提供了有吸引力的目标。

[0003] 对这些安全性很重要的网络应用的关键弱点的恶意利用被持续的开发设计出来，其中跨站脚本和跨站请求伪造攻击特别受黑客偏爱。这些攻击的先锋 (vanguard) 是恶意链接，这样的恶意链接被感染了脚本或伪造的输入，它们通过电子通信被呈现给合法的用户。当合法用户无辜地 (innocently) 选择这个恶意链接时，就使得脚本能够在用户浏览器和目标网站的安全上下文中执行。

[0004] 虽然存在传统的客户端和服务器端技术来保护免于跨站攻击，但是这些方案通常是不完善的。例如，这些典型的方案中的一些仅针对会话盗窃攻击，所述会话盗窃攻击对会话的完整性进行攻击。

发明内容

[0005] 根据一个一般的实施方式，网页存储在网站上，所述网页被组织成不接受输入的入口网页 (entry pages) 和不是入口网页的保护的网页 (protectedpages)，以及基于用户标识符和秘密密钥在网站对网络浏览器应用进行认证。基于认证网络浏览器应用，标识 cookie 被从网站传送到网络浏览器应用，并且在网关接收来自网络浏览器应用的请求以接收所请求的网页和标识 cookie，该请求包括超文本传输协议 (Hypertext Transfer Protocol，“HTTP”) 引用字符串 (referer string)，该引用字符串包括引用网页 (referring web page) 的统一资源定位符 (“URL”)。在网关确定所请求的网页是入口网页还是保护的网页。如果确定所请求的网页是保护的网页，则基于所接收的标识 cookie 进一步在网关确定网络浏览器是否被认证，以及基于 HTTP 引用字符串来确定该引用网页是否存储在网站上。如果网络浏览器应用被确定为被认证并且如果引用网页被确定为存储在网站上，则所请求的网页被从网站传送到网络浏览器应用，而如果网络浏览器应用被确定为未被认证或者引用网页被确定为没有存储在网站上，则所述请求在网关被重新定向 (redirect) 到入口网页之一。如果所请求的网页被确定为入口网页或者该请求被重新定向到入口网页，则在网关去除来自请求的输入数据，由此产生剥离的 (stripped) 请求，并且如果所请求的网页被确定为入口网页或者该请求被重新定向到入口网页，则基于产生剥离的请求，将入口网页之一从网站传送到网络浏览器。

[0006] 根据另一个一般的实施方式，网页存储在网站上，所述网页被组织成不接受输入的入口网页和不是入口网页的保护的网页。从用户应用接收请求以接收所请求的网页，该

请求包括指示引用网页的引用字符串以及标识数据，并且确定所请求的网页是入口网页还是保护的网页。如果所请求的网页被确定为保护的网页，则基于所述标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站上，并且如果用户应用被确定为被授权并且引用网页被确定为存储在网站上，则所请求的网页被传送到用户应用。如果用户应用被确定为未被授权或者引用网页被确定为没有存储在网站上，则该请求被重新定向到入口网页之一。

[0007] 实施方式可以包括一个或多个以下特征。例如，如果所请求的网页被确定为入口网页或者该请求被重新定向到入口网页，则从该请求中去除输入数据，由此产生剥离的请求，并基于剥离的请求，入口网页可以被传送到用户应用。用户应用可以在网站被授权或被认证，例如，使用秘密密钥、使用会话 URL、使用 HTTP 认证、或用户应用端的安全套接字协议层（“SSL”）。基于认证用户应用，可能是 cookie 的标识数据可以从网站传送到用户应用。网页可以在网站被组织成入口网页和保护的网页。可以在网关接收该请求。保护的网页还可以包括应用、小服务程序、或脚本。使用用户应用反向导航控制 (backward navigation control)，可以进行保护的网页之间的导航。用户应用可以是在用户设备上执行的网络浏览器应用。引用字符串可以是 HTTP 引用字符串，并且可以存储引用网页的 URL。

[0008] 在此外的示例中，至少一个入口网页可以是登录页、主页、或入口扉页 (portal front page)。网站可以是在线银行网站、拍卖网站、在线零售网站、网络邮件网站、搜索引擎网站、或SAP®入口网站。保护的网页可以是在线银行交易页、在线银行菜单页、在线银行认证页、在线拍卖搜索结果页、在线拍卖登录页、在线拍卖认证页、在线拍卖投标输入页、在线拍卖投标验证页、在线零售商搜索结果页、在线零售商购物推车页、在线零售商登录页、在线零售商信用卡地址验证页、在线零售商确认页、网络邮件认证页、网络菜单页、网络邮件发送页、网络邮件搜索页、网络邮件读取页、搜索引擎搜索结果页、SAP®入口认证页、或 SAP®入口菜单页。标识数据可以指示用户被授权但是未被认证。

[0009] 根据另一个一般实施方式，系统包括服务器和网关。服务器被配置来存储网页，所述网页被组织成不接受输入的入口网页和不是入口网页的保护的网页。网关被配置来从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据，确定所请求的网页是入口网页还是保护的网页，如果所请求的网页被确定为保护的网页，则基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站上，如果用户应用被确定为被授权并且如果引用网页被确定为存储在网站上，则实行所请求的网页到用户应用的传送，而如果用户应用被确定为未授权或者如果引用网页被确定为没有存储在网站上，则将该请求重新定向到入口网页之一。

[0010] 根据另一个一般实施方式，计算机程序产品被有形地体现在机器可读存储介质中。计算机程序产品包括指令，当由机器读取时，该指令操作以使数据处理装置将网页存储在网站上，所述网页被组织成不接受输入的入口网页和不是入口网页的保护的网页，从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据，以及确定所请求的网页是入口网页还是保护的网页。该计算机程序产品还包括指令，当由机器读取时，该指令操作以使数据处理装置在所请求的网页被确定为保护的网页的情况下，基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储

在网站上，如果用户应用被确定为被授权并且如果引用网页被确定为存储在网站上，则将所请求的网页传送到用户应用，而如果用户应用被确定为未被授权或者如果引用网页被确定为没有存储在网站上，则将该请求重新定向到入口网页之一。

[0011] 以下在附图和说明书中阐述一个或多个实施方式的细节。从说明书、附图以及权利要求书中，公开内容的其它潜在的特征和优点将变得更加清楚。

附图说明

[0012] 图 1 示出了根据一个一般实施方式的示范系统的外观。

[0013] 图 2 示出了图 1 的计算机的示范内部体系结构。

[0014] 图 3 是示出用于实施增强的跨站攻击防护的示范处理的流程图。

[0015] 图 4 示出了示范系统，包括目标网站、以及分别与合法用户和黑客相关联的计算机。

[0016] 图 5 到图 10 示出了各种示范在线应用的入口网页和保护的网页的组织。

[0017] 图 11 是示出使用图 3 中描述的示范处理防护跨站脚本攻击的游动图 (swim diagram)。

[0018] 相似的参考标号总是代表相应的部分。

具体实施方式

[0019] 图 1 示出了示例系统 100 的外观，包括网关计算机 101、网站 102、由合法网络用户使用的计算机 104、以及由黑客使用的计算机 105，全部经由网络 106 相连接。以下，为了描述增强的跨站攻击防护方案的目的，黑客（或“攻击者”）是用户或用户应用，其中，他们的目的在于通过他们自身动作或通过无辜第三方的中间动作 (intervening action) 来启动跨站攻击。但是，合法网络用户或用户应用没有启动跨站攻击的企图，虽然他们的动作不知不觉地或者鲁莽地导致了攻击的发生。例如，黑客是将包括跨站攻击脚本输入的恶意链接发送到一个或多个合法网络用户的人或程序，并且知道合法网络用户可能将选择发起跨站攻击的恶意链接。选择了恶意链接但是并不知道该链接会启动跨站攻击的恶意链接的接收者被视为合法网络用户，即使合法网络用户可能知道选择未知或非可信来源的链接通常是个坏习惯。

[0020] 简单来讲，网站 102 被配置来存储网页，所述网页被组织成不接受输入的入口网页和不是入口网页的保护的网页。合法网络用户使用的计算机 104 被配置来从用户应用发送请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据。网关计算机 101 被配置来接收请求，确定所请求的网页是入口网页还是保护的网页，并且如果所请求的网页被确定为保护的网页，则基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站 102。网关计算机 101 还被配置来在用户应用被确定为被授权并且引用网页被确定存储在网站 102 上的情况下，实行所请求的网页到用户应用的传送，以及如果用户应用被确定为未被授权或者如果引用网页被确定没有存储在网站 102 上，则将该请求重新定向到入口网页之

[0021] 更具体地说，网关计算机 101 的硬件环境包括用于向用户显示文本和图像的显示监视器 108、用于输入文本数据和用户命令到网关计算机 101 中的键盘 109、用于指示、选

择和操作显示在显示监视器 108 上的对象的鼠标 110、固定盘驱动 111、可移动盘驱动 112、磁带驱动 114、硬拷贝 (hardcopy) 输出设备 115、计算机网络连接 116、以及数字输入设备 117。

[0022] 显示图形、图像、以及文本显示监视器 108 包括网关计算机 101 使用的软件应用的用户接口、以及操作网关计算机 101 所需要的操作系统程序。用户使用键盘 109 输入命令和数据来操作和控制计算机操作系统程序以及应用程序。用户使用鼠标 110 来选择和操作显示在显示监视器 108 上的图形和文本对象，作为与网关计算机 101 和运行在网关计算机 101 上的应用的交互的一部分和网关计算机 101 和运行在网关计算机 101 上的应用的控制的一部分。鼠标 110 是任何类型的指示设备，并且可以是操纵杆、跟踪球、触摸板、或其它指示设备。而且，数字输入设备 117 允许网关计算机 101 捕捉数字图象，并且可以是扫描仪、数字相机、数字摄像机、或其它数字输入设备。用来提供有效跨站攻击防护的软件在本地被存储计算机可读存储介质上，比如固定盘驱动 111。

[0023] 在另外的实施方式中，固定盘驱动 111 本身可以包括许多物理驱动单元，比如独立盘的冗余阵列 (“RAID”)、或者可以是在物理上位于分离的计算单元中的特大容量盘驱动 (disk drive farm) 或盘阵列。这样的计算机可读存储介质允许网关计算机 101 访问存储在可移动或非可移动存储介质上的计算机可执行处理步骤、应用程序等。

[0024] 无线和有线 (wireline) 计算机网络连接 116 可以是调制解调器连接、包括以太网的局域网 (“LAN”) 连接、或宽带广域网 (“WAN”) 连接，比如数字用户线路 (“DSL”)、电缆高速互联网连接、拨号连接、T-1 线路、T-3 线路、光纤连接、或卫星连接。网络 106 可以是 LAN 网络、公司或政府 WAN 网络、因特网、或其它网络中的一个或多个。网关计算机 101 直接或间接耦合到网站 102、合法用户使用的计算机 104、和 / 或黑客使用的计算机 105，以便在网关计算机 101、网站 102、和 / 或计算机 104 和 105 之间实行单向或双向的数据传输。

[0025] 计算机网络连接 116 使用有线或无线连接器。示例的无线连接器包括，例如，INFRARED DATA ASSOCIATION®(“IrDA®”)无线连接器、光无线连接器、INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS®(“IEEE®”)标准 802.11 无线连接器、BLUETOOTH®无线连接器、近场通信 (“NFC”) 连接器、正交频分复用 (“OFDM”) 超宽带 (“UWB”) 无线连接器、时间调制超宽带 (“TM-UWB”) 无线连接器、或其它无线连接器。示例的无线连接器包括，例如，IEEE®-1394 FIREWIRE®连接器、通用串行总线 (“USB”) 连接器、串行端口连接器、并行端口连接器、或其它有线连接器。

[0026] 可移动盘驱动 112 是可移动存储设备，用来从网关计算机 101 下载数据或向网关计算机 101 上载数据。可移动盘驱动 112 可以是软盘驱动、IOMEGA®ZIP®驱动、只读压缩盘存储器 (“CD-ROM”) 驱动、可记录 CD(“CD-R”) 驱动、可重写 CD(“CD-RW”) 驱动、闪存、USB 闪存驱动、外部硬盘驱动、thumb 驱动、pen 驱动、键驱动、高密度数字多功能盘 (“HD-DVD”) 光盘驱动、蓝光光盘驱动、全息数字数据存储 (“HDDS”) 光盘驱动、或者各种可记录或可重写数字多功能盘 (“DVD”) 驱动中的任何一个，比如可记录 DVD(“DVD-R”或“DVD+R”)、可重写 DVD(“DVD-RW”或“DVD+RW”)、或 DVD-RAM。操作系统程序、应用、以及各种数据文件被存储在盘上，它们存储在固定盘驱动 111 上或可移动盘驱动 112 的可移动介

质上。

[0027] 磁带驱动 114 是磁带存储设备，用来从网关计算机 101 下载数据或向网关计算机 101 上载数据。磁带驱动 114 可以是四分之一英寸盒式磁带 (cartridge)（“QIC”）、4 毫米数字音频磁带（“DAT”）、8 毫米数字线性磁带（“DLT”）驱动、或者其它类型的磁带。

[0028] 硬拷贝输出设备 115 为操作系统程序和应用提供输出功能。硬拷贝输出设备 115 可以是打印机或任何产生有形输出对象的输出设备，所述输出对象包括文本或图像数据，或者文本或图像数据的图形表示。虽然硬拷贝输出设备 115 被示为直接连接到网关计算机 101，但并不需要如此。例如，硬拷贝输出设备 115 可以经由诸如有线或无线网络的网络接口连接到计算机 101。

[0029] 网站 102 在远端存在于网络 106 上，并且包括一个或多个联网的 (networked) 数据服务器设备或服务器。网站 102 执行服务于由网关计算机 101 发送的请求的软件，其中网站 102 可以包括特大容量服务器 (server farm)、特大容量存储器 (storage farm)、或存储服务器。在替代的实施方式中，网站 102 被省略，与网站 102 相关联的功能实际上由网关计算机 101 执行。网站 102 可以是在线银行网站、在线零售网站、网络邮件网站、搜索引擎网站、SAP®入口网站、或其它类型的网站。

[0030] 而且，虽然网关计算机 101 在图 1 中示出为台式机 PC，但是在另外的实施方式中，网关计算机 101 可以是笔记本计算机、工作站、中型计算机、大型机、嵌入式系统、电话、手持或平板计算机 (tablet computer)、PDA、或其它类型的计算机。

[0031] 虽然为了简洁目的而省略了组成网站 102、合法网络用户使用的计算机 104、以及黑客使用的计算机 105 的组件的描述，但是说出下面的内容就足够了：组成网站 102、合法网络用户使用的计算机 104、和 / 或黑客使用的计算机 105 的计算机或各个联网的计算机的硬件环境类似于这里对于网关计算机 101 所描述的示范硬件环境。在替代的实施方式中，任何网关计算机 101、网站 102、合法网络用户使用的计算机 104、和 / 或黑客使用的计算机 105 的功能被合并到单一或多个组合硬件环境中。例如，单一公共计算机可以先被黑客使用，随后被合法网络用户使用。

[0032] 图 2 示出了网关计算机 101 的内部体系结构的示例。计算环境包括：计算机中央处理单元（“CPU”）200，在那里处理包括操作系统或应用的计算机指令；显示接口 202，其提供通信接口，并处理在显示监视器 108 上呈现 (rendering) 图形、图像和文本的功能；键盘接口 204，其提供到键盘 109 的通信接口；指示设备接口 205，其提供到鼠标 110 或等同的指示设备的通信接口；数字输入接口 206，其提供到数字输入设备 117 的通信接口；硬拷贝输出设备接口 208，其提供到硬拷贝输出设备 115 的通信接口；随机存取存储器（“RAM”）210，在其中计算机指令和数据被存储在易失性存储设备中，用于由计算机 CPU 200 进行处理；只读存储器（“ROM”）211，在其中用于基本系统功能的不变低级系统代码或数据，比如基础输入和输出（“I/O”）、启动、或接收来自键盘 109 的键击，被存储在非易失性存储设备中；存储器 220 或其它适合类型的存储器（例如，随机存取存储器（“RAM”）、只读存储器（“ROM”）、可编程只读存储器（“PROM”）、可擦除可编程只读存储器（“EPROM”）、电可擦除可编程只读存储器（“EEPROM”）、磁盘、光盘、软盘、硬盘、可移动盒式磁带、闪存驱动），在其中存储包括操作系统 221、应用程序 222（包括增强的跨站攻击防护应用 223、认证应用 224、以及其它所需应用 225）、和数据文件 226 的文件；以及计算机网络接口 216，其通过计算机网络连接

116 提供到网络 106 的通信接口。组件设备与计算机 CPU 200 通过计算机总线 227 相互通信。

[0033] 简单来讲，增强的跨站攻击防护应用 223 被有形地体现在盘 220，一种机器可读存储介质中。增强的跨站攻击防护应用 223 包括指令，所述指令操作以使计算机将网页存储在网站 102 上，所述网页被组织成不接受输入的入口网页和不是入口网页的保护的网页，以从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据，并确定所请求的网页是入口网页还是保护的网页。增强的跨站攻击防护应用 223 还包括指令，所述指令操作以使计算机在所请求的网页在被确定为保护的网页的情况下，基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站 102 上，如果用户应用被确定为被授权并且引用网页被确定为存储在网站 102 上，则将所请求的网页传送到用户应用，而如果用户应用被确定为未被授权或者引用网页被确定没有存储在网站 102 上，则将该请求重新定向到入口网页之一。

[0034] RAM 210 与计算机总线 227 接口连接，以便在诸如操作系统应用程序的软件程序以及设备驱动器的运行期间为计算机 CPU 200 提供快速的 RAM 存储。更具体地讲，计算机 CPU 200 将计算机可执行处理步骤从固定盘驱动 111 或其它存储介质装载到 RAM 210 的字段中，以便执行软件程序。数据被存储在 RAM 210 中，在那里数据在运行期间被计算机 CPU 200 访问。

[0035] 如图 2 中所示，网关计算机 101 存储用于操作系统 221 的计算机可执行代码，以及应用程序 222，诸如文字处理、电子表格、演示文稿、游戏、或其它应用。虽然，能够使用上述实施方式来提供增强的跨站攻击防护，但是也可以将根据本公开的功能实施为动态链接库（“DLL”）或者插入其它应用程序的插件程序，所述其它应用程序如因特网网络浏览器，例如MICROSOFT® Internet Explorer网络浏览器。

[0036] 计算机 CPU 200 是高性能计算机处理器之一，包括INTEL®或AMD®处理器、POWERPC®处理器、MIPS®简化指令集计算机（“RISC”）处理器、SPARC®处理器、ACORN® RISC Machine（“ARM®”）体系结构处理器、HPALPHASERVER®处理器或大型机的专用计算机处理器。在另外的配置中，计算机 CPU 200 为不止一个的处理单元，包括存在于高性能工作站和服务器中的多 CPU 配置，或者存在于大型机中的多可升级 (scalable) 处理单元。

[0037] 操作系统 221 可以是MICROSOFT® WINDOWS NT® / WINDOWS® 2000 / WINDOWS® XP 工作站；MICROSOFT® WINDOWS VISTA® / WINDOWS NT® / WINDOWS® 2000 / WINDOWS® XP 服务器；多种 UNIX® 风格的操作系统，包括用于IBM®工作站和服务器的AIX®、用于SUN®工作站和服务器的SUNOS®、基于INTEL®CPU的工作站和服务器的LINUX®、用于HP®工作站和服务器的HP UX WORKLOAD MANAGER®、用于SGI®工作站和服务器的IRIX®、用于 Digital Equipment Corporation 的 VAX/VMS、用于基于 HP ALPHASERVER® 的计算机的OPENVMS®、用于基于POWERPC®的工作站和服务器的MAC OS® X；用于移动设备的SYMBIAN OS®、WINDOWS MOBILE®或WINDOWS CE®、PALM®、NOKIA® OS（“NOS”）、OSE®、或EPOC®，或者用

于计算机或嵌入式系统的专用操作系统。用于操作系统221的应用开发平台或框架可以是：BINARY RUNTIME ENVIRONMENT FOR WIRELESS®（“BREW®”）；Java Platform、Micro Edition（“Java ME”）或Java2 Platform、Micro Edition（“J2ME®”）；PYTHON、FLASH LITE®、或MICROSOFT®.NET Compact。

[0038] 虽然为了简洁目的而省略了网站102、以及计算机104和105的内部体系结构的描述，但是只要说出下面的内容就足够了：那些计算机的体系结构基本上类似于网关计算机101的体系结构。在替代的实施方式中，网关计算机101和服务器106的功能被组合到单一或组合的硬件环境中，所述内部体系结构被组合或复制。

[0039] 虽然图1和图2示出了执行被配置为实行增强的跨站攻击防护的程序代码、或程序或处理步骤的计算机系统的一个可能实施方式，但是其它类型的计算机也可以使用。

[0040] 关于跨站攻击，开发者使用SUN MICROSYSTEMS® JAVASCRIPT®语言，通过将脚本嵌入由用户网络浏览器解释的HTML页，来合法地增强基于网络的用户应用。网页中脚本的执行被浏览器沙盒化（sandboxed），这样所有的访问和引用（reference）都受到监控。沙盒（sandbox）创建了一种环境，其中对小程序能够请求或访问的系统资源做出了严格的限制，当可执行代码来自未知或非可信来源时使用沙盒，减少了运行非可信代码的用户的风险。对于脚本运行，同源策略规定了只允许脚本访问沙盒中的对象，特别是来源于相同网站的对象。按照同源策略的上下文中的理解，网站引用域名系统（“DNS”）域（例如www.website.com），这样来自那个网站或域的全部对象被视为来源于相同的来源。

[0041] 在JAVASCRIPT®语言对象模型中，示例对象包括网页或cookie。由于能够访问这些对象的脚本对它们具有有效的控制，因此例如，黑客能够重写网页或读取cookie并将其发送到不同的主机以便将汇款（money transfer）改写到黑客自己的账户上，或者将认证合法网络用户的cookie转发到黑客。对于同源策略，在用户和网站之间建立安全上下文，这样在特定安全上下文中运行的脚本能够从那个网站访问用户的网络浏览器中的对象。为了使脚本进入这个安全上下文，脚本被嵌入从网站请求的网页中。

[0042] 如果黑客能够将脚本嵌入合法网络用户从网站请求的网页中，则黑客能够控制合法网络用户的安全上下文。这样的恶意嵌入脚本被称为跨站脚本攻击，因为脚本可能来自不同的网站。

[0043] 为了安装跨站脚本攻击，黑客可以利用公共网络应用的弱点。例如，由于交互式网络应用接受用户输入以建立响应网页，所以黑客可以将脚本插入该输入中，该输入可能不会被特定网络应用详细地检查。在一个示例中，用户可以使用以下输入将请求提交到网页：

[0044] HTTP://WWW.WEBSITE.COM/INDEX.PHP ? NAME = JIM

[0045] 响应于该输入，网络应用可以用以下个性化网页来响应：

[0046] <HTML>

[0047] <BODY>

[0048] HELLO, JIM

[0049] …

[0050] 但是，黑客能够使用以下输入请求相同网页：

[0051] HTTP://WWW.WEBSITE.COM/INDEX.PHP ? NAME = JIM<SCRIPT>ALERT(" XSSSCRIPT")</SCRIPT>

[0052] 响应于这个输入,相同网络应用会生成以下内容 :

[0053] <HTML>

[0054] <BODY>

[0055] HELLO, JIM

[0056] <SCRIPT>ALERT(" XSS SCRIPT")</SCRIPT>

[0057] …

[0058] 基于插入文本到 URL 的输入部分中,产生在合法网络用户的安全上下文中运行脚本 (“XSS SCRIPT”) 的响应。这样的脚本运行的结果可能是严重的,并且可能包括 cookie 和会话盗窃、浏览器劫持、用户监视和数据盗窃、请求伪造、以及假冒交易。因为该输入被用户浏览器反射,所以这样的攻击被称为反射的跨站脚本攻击。并不总是这样的情况 :合法网络用户看到以他们名义发送的非法输入或与以他们名义发送的非法输入进行交互,因此合法网络用户可能没有机会在这个输入被发送到网站前检查该输入。

[0059] 作为跨站脚本攻击的危险的进一步的加剧,引入脚本的复杂度不必受到输入长度的限制。具体来讲,黑客还能够将引用引入不同的 URL 或网页,在其中接纳恶意链接的网站与脚本代码的来源不需要一致。黑客不仅可以通过网页,而且还可以通过电子邮件消息或其它形式的电子通信将恶意链接提供给合法网络用户。例如,当接收垃圾电子邮件消息时,用户会不知不觉地选择链接,并使用以下输入从上述示范网站请求网页 :

[0060] HTTP://WWW.WEBSITE.COM/INDEX.PHP ? NAME = JIM<SCRIPT

[0061] SRC =" HTTP://HACKER.NET/XSS.JS" >

[0062] 这样的输入会导致以下响应 :

[0063] <HTML>

[0064] <BODY>

[0065] HELLO, JIM

[0066] <SCRIPT SRC =" HTTP://HACKER.NET/XSS.JS" >

[0067] …

[0068] 类似的交互还可以用于跨站请求伪造攻击,虽然目的可能不同。在这样的攻击中,黑客利用会话的存在,其是合法网络用户执行一定动作的限时认证。当跨站脚本攻击试图将脚本引入合法网络用户的安全上下文中时,因为该请求可能启动伪造交易,所以请求本身足够用于请求伪造攻击。使用增强的跨站攻击防护方案,可以处理这两种攻击。由于到网络应用的输入来源于合法网络用户的网络浏览器,所以通过防止出现以该用户名义进行的非法输入而可能产生跨站攻击防护。

[0069] 图 3 是示出用于实施增强的跨站攻击防护的处理的流程图。简单来讲,该处理包括 :将网页存储在网站上,该网页被组织成不接受输入的入口网页和不是入口网页的保护的网页 ;从用户应用接收请求以接收所请求的网页,该请求包括指示引用网页的引用字符串以及标识数据 ;并确定所请求的网页是入口网页还是保护的网页。所述处理还包括 :如果所请求的网页被确定为保护的网页,则基于标识数据确定用户应用是否被授权,以及基于引用字符串确定引用网页是否存储在网站上 ;以及如果用户应用被确定为被授权并且引

用网页被确定为存储在网站上，则将所请求的网页传送到用户应用。而且，所述处理还包括：如果用户应用被确定为未被授权或者引用网页被确定没有存储在网站上，则将该请求重新定向到入口网页之一。

[0070] 更具体地讲，处理 300 开始 (S301)，此时网页在网站被组织成入口网页和保护的网页 (S302) 并存储在网站上时 (S304)。入口网页不接受输入，这样，到入口网页的输入或被网关过滤掉，或被丢弃，而保护的网页能够接受输入。对可能包括应用、小服务程序或脚本的保护的网页的访问经由通过入口网页的访问路径来提供。在图 1 的示范系统中，网页可以被组织和存储在网关计算机 101 和 / 或网站 102 上。

[0071] 在前进到保护的网页之前，对网站的访问在入口网页发生（或进入）。以这种方式，到保护的网页的输入被强制从合法网络用户的浏览器的合法入口开始，因此试图通过恶意链接的进行的跨站攻击被防止。入口网页的通常的候选者是登录页、主页、或入口扉页 (entry front)，以及典型地设定了书签的其它网页。

[0072] 保护的（或“普通的 (regular)”）网页是那些不是入口网页的网页。保护的网页能够但不必接受输入，并可以是不接受输入的网页。示例的保护的网页可以是在线银行交易页、在线银行菜单页、在线银行认证页、在线拍卖搜索结果页、在线拍卖登录页、在线拍卖认证页、在线拍卖投标入口页、在线拍卖投标验证页、在线零售商搜索结果页、在线零售商购物推车页、在线零售商登录页、在线零售商信用卡地址验证页、在线零售商确认页、网络邮件认证页、网络菜单页、网络邮件发送页、网络邮件搜索页、网络邮件读取页、搜索引擎搜索结果页、SAP® 入口认证页、或 SAP® 入口菜单页、或其它网页。

[0073] 在网站上将网页组织成入口网页或保护的网页可以手动进行，比如通过程序员和管理员，或者自动进行。例如，不接受输入的网页可以被自动分类作为入口网页，而所有其它网页或接受输入的网页被自动分类作为保护的网页。在一个具体示例中，存储在网站 102 上的网页通过存储在网关计算机 101 上的分类应用被自动组织成入口网页和保护的网页。

[0074] 首先简单涉及，图 4 示出了示范系统 400，包括目标网站 401、合法网络用户使用的计算机 402、以及黑客使用计算机 404。目标网站 401 存储网页 405，所述网页 405 被组织成不接受输入的入口网页 406a 到 406c、以及保护的网页 407a 到 407g。合法网络用户使用的计算机 402 将书签链接 409 存储到入口网页 406b。虽然存储在计算机 402 上的书签链接 410 表面上链接到保护的网页，但是该链接被重新定向到入口网页 406b 或 406c，这是因为直接进入 (direct entry) 或书签进入 (bookmarking) 保护的网页是不允许的。黑客使用的计算机 404 通过恶意跨站脚本输入将链接 411 存储到保护的网页 407b。

[0075] 返回图 3，用户应用可以在网站被授权 (S305)。授权可以通过唯一地标识用户应用，比如通过用户应用的唯一名称或地址，以及辨认或准许匹配该唯一标识符的请求来进行。授权还包括基于唯一标识符进行认证以建立用户应用的作者或来源，这可以通过基于具有用户名和网站所知的秘密密钥的消息授权代码来构建标识 cookie 来进行。或者，认证可以使用秘密密钥、使用会话 URL、使用 HTTP 认证、或用户应用端安全套接字层（“SSL”）来进行。

[0076] HTTP 认证允许网络浏览器或其它用户应用在进行请求时以用户标识符和口令的形式提供凭证 (credential)。这些凭证可以作为明文传递，或者它们可以被加密。用户应用可以是，例如，在用户设备上运行的浏览器应用。使用 HTTP 认证，用户应用请求需要认证

的网页，但是并不提供用户名和口令，比如通过输入地址或跟上到网页的链接。服务器以“401”响应代码作出响应以提供认证域 (realm)，并且客户端将该认证域展示给用户并针对用户名和口令进行提示，此时用户可以决定放弃进行认证。当用户名和口令被提供后，客户端重新发送相同的请求，但是包括了认证首标，而服务器接受该认证并将网页返回。如果用户名无效或口令不正确，则服务器将“401”响应代码返回，而用户应用再次提示用户。

[0077] 或者，SSL 是为用户应用提供安全访问以便在网络上进行通信的加密协议。SSL 通过以下方式工作：首先协商用户应用支持的算法，交换基于公共密钥加密的密钥和基于证书的认证，并执行基于对称密码的业务 (traffic) 加密。

[0078] 虽然这些以及其它的方案都可用，但是由于 cookie 在许多真实世界应用和入口中常用，所以在这里使用 cookie 描述认证。在一个示例实施方式中，当用户输入用户名和口令时 cookie 被生成，因此 cookie 与用户的身份电子地相关联。在用户完成认证协议之后，比如口令检查，网站可以发出 cookie。

[0079] 或者，在没有全面认证用户应用的情况下，“未认证的”cookie 可以产生并传送到用户应用，表示用户应用被授权遍历 (traverse) 保护的网页，但是未经认证。在这点上，网站可以被组织来在入口网页产生未认证的 cookie，以允许对一定保护的网页的访问，并跟踪用户经过一定保护的网页，随后在其它保护的网页被观看之后提供授权页，来执行用户应用的全面认证。

[0080] 基于授权用户应用，诸如 cookie 或口令的数据可以从网站传送到用户应用 (S306)。这个数据可以是标识数据，标识数据是被期望利用网站请求从用户应用传送回到网关的数据，或者该数据可以是授权数据，授权数据是由用户应用处理以产生标识数据的数据。在另一个示例实施方式中，没有数据从网站传送到用户应用。在图 1 的示范系统中，标识或授权数据被从网关计算机 101 传送到合法网络用户使用的计算机 104。

[0081] 标识数据可以是 cookie，cookie 是网络浏览器利用对网页的请求传送回到网站的一小段用来认证操作用户应用的用户的数据，其中 cookie 可以被网站修改。或者，授权数据可以是允许用户应用在客户端设备产生 cookie 的数据，其中产生的 cookie 作为标识数据被传送回到网站。cookie 被存储在用户的计算机上，并且如同源策略所规定的，与网站相关联，这样网站从用户接收其相关联的 cookie。网站可以与不止一个 cookie 相关联。

[0082] 从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据 (S307)。该请求可以在网关接收，比如网关计算机 101，或者在网站接收，比如网站 102。

[0083] 引用字符串可以是 HTTP 引用字符串，并且可以存储引用网页的 URL。HTTP 引用字符串是请求中的 HTTP 首标字段，含有引用所请求的网页的网页的 URL。网站开发者能够请求用户使能 (enable) 用户应用中的引用字符串，因为缺少引用字符串可以被检测到并用于将用户应用重新定向到通知用户使能引用字符串的网页。

[0084] 确定所请求的网页是入口网页还是保护的网页 (S309)。这样的确定可以通过参考存储在网关计算机 101 或网站 102 上的表格来进行，该表格将网页分类为入口网页或保护的网页。或者，可以检查所请求的网页本身中的元数据来确定该网页被标识为入口网页还是保护的网页。如果将网页组织成入口网页和保护的网页是自动执行的，类似的确定还可以基于相同的分类标准来自动进行。例如，如果网页接受输入，它们被自动分类为保护的网

页，网关计算机 101 可以通过确定所请求的网页是否接受输入来确定所请求的网页是否是保护的网页。

[0085] 如果确定所请求的网页不是保护的网页 (S310)，可以从请求中去除输入数据以产生剥离的请求 (S311)。对于入口网页的每个访问，采用查询 URL 或 POST 请求数据形式的输入被剥离，其中基于剥离的请求将入口网页传送到用户应用 (S312)，由此结束处理 300。

[0086] 其它输入数据，比如 HEAD、GET、PUT、DELETE、TRACE、OPTIONS、CONNECT 或其它请求数据也可以被剥离。在图 4 示例中，假设计算机 402 被授权，如果在合法网络用户使用的计算机 402 上选择到入口网页 406b 的链接 409，从该链接剥离所有输入，并且入口网页 406b 被传送到相关联的用户应用。在替代的实施方式中，不从请求中去除输入数据。

[0087] 如果确定所请求的网页是保护的网页 (S310)，则进一步基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站上 (S315)。在这点上，对于保护的网页的每个访问，网关验证已经设定认证用户的 cookie 以及请求的引用字符串来源于网站。cookie 可以是“未认证的”cookie。

[0088] 一组示例的用于反射的跨站脚本攻击的 HTTP 首标和增强的响应被示出如下：

[0089] GET/PROTECTED_PAGE.PHP ? NAME = <SCRIPT>ALERT(% 22XSS% 22)

[0090] <% 2FSCRIPT>HTTP/1.1

[0091] HOST :WWW.WEBSITE.COM

[0092] REFERER :HTTP://WWW.HACKER.NET/

[0093] MALICOUS_LINK.HTML

[0094] COOKIE :AUTH = USERNAME :9100ADA74E758C76D0CCB2595747C910

[0095] HTTP/1.1302FOUND

[0096] LOCATION :HTTP://WWW.WEBSITE.COM/

[0097] DEFAULT_ENTRY.HTML

[0098] 在这个示例中，通过黑客提供的输入，用户可能不注意地选择了请求网站上的敏感的保护的网页的恶意链接。网关计算机 101 或网站 102 检测引用字符串不是源自网站，并且将请求重新定向到默认的入口网页。即使已经由网络浏览器自动发送的 cookie 正确地认证了用户也进行重新定向。但是，如果请求具有标识 cookie 并含有适当的引用字符串，该请求不是跨站攻击，因此允许到保护的网页的访问。

[0099] 如果用户被确定为未被授权和 / 或引用网页被确定没有存储在网站上 (S316)，该请求被重新定向到入口网页之一 (S317)。在其它示例实施方式中，请求被重新定向到默认入口网页，或者不被重新定向。

[0100] 在图 4 的示范系统 400 中，虽然计算机 402 被假定为被授权，如果到保护的网页的链接 410 在合法网络用户使用的计算机 402 上被选择，则该请求被重新定向到入口网页 406b 或 406c 之一。而且，由于黑客使用的计算机 404 未被授权，所以，如果到保护的网页 407b 的链接 410 被合法网络用户不注意地选择，则该请求被重新定向到入口网页。

[0101] 回到图 3，如果用户被确定为被授权并且引用网页被确定存储在网站上 (S316)，该请求网页被传送到用户应用 (S319)。通过确定用户被授权以及引用网页存储在网站上，减小了发生跨站攻击的危险。使用用户应用反向导航控制在保护的网页之间进行导航 (S320)，并且处理 300 结束 (S314)。在替换的实施方式中，在保护的网页之间进行导航而不

使用用户应用导航控制，或者禁止 (disable) 使用用户应用导航控制的导航。

[0102] 通过处理 300 描述的增强的跨站攻击防护方案可以作为总体软件战略的一部分用来增加输入过滤，例如不允许在输入过滤算法中的缺陷 (flaw) 导致的不适当的输入。这种方案的使用支持了由过滤算法提供的保护，因为过滤算法开发使用蠕虫非常快速的扩展，并且过滤算法通常经由库共享。底层的库所导致的弱点的发现同时暴露多个网站，并且不能完全修复，直到所有网站都分别更新它们的代码为止。

[0103] 特别地，增强的跨站攻击防护方案不仅仅不允许存在于网站上的脚本，还禁止被检测为包括恶意特性的脚本，防止脚本将数据泄漏给黑客，通过将令牌 (token) 添加到 URL 来重写请求或响应，或者防止成功的脚本攻击偷取会话。如此，增强的跨站攻击防护方案减小了与设定系统和针对 (addressing) 每个请求相关联的成本，这是因为不需要超文本预处理器 (“PHP”) 包装和代理服务器，并且不需要将请求映射到 DNS 入口。这样做时，减轻了复制和负载平衡问题。

[0104] 诸如网关计算机 101 的网关可以在以任意语言编写的用户应用包括负载平衡应用之前进行部署。在网关对 cookie 进行的验证可以通过对 cookie 编排格式来实行，如下所示：

[0105] USERNAME|MAC(USERNAME,KEY)

[0106] 当以这种方式或类似的方式编排格式时，网关能够使用密钥、通过一种消息认证代码计算来验证 cookie 和用户的身份，而不重写该输出，这是因为网络应用的这个输出不仅仅是转发的。因此，对于每个请求，能够避免重写以及相应的延迟。

[0107] 图 5 示出了对示范在线银行应用 500 的入口网页和保护的网页的组织。简单来讲，在线银行应用 500 包括单个入口网页和通过该入口网页访问的多个保护的网页。

[0108] 更具体地讲，主页入口网页 501 提供用于登录到在线银行应用 500 的方式 (form)。用户应用不需要展示 cookie 或提供任何其它授权或标识数据来访问主页入口网页 501。在遍历主页入口网页之后，在线银行应用 500 通过输入接收认证保护的网页 (input-accepting authentication protected page)502 来认证用户应用。例如，输入接收认证保护的网页 502 可以验证提供的用户名和口令。

[0109] 当进行认证时，用户应用被重新定向到主菜单保护的网页 504，其提供由用户选择选项。主菜单保护的网页 504 提供的选项将用户应用链接到交易保护的网页 505a 到 505d，其可以接受输入。例如，这些交易可以包括汇款或股市定单。以及确认页。虽然单一交易可以包括不止一个步骤或网页，这些各个网页的保护的性质持续。选项还可以将用户应用链接到菜单保护的网页 506a 和 506b，其还可以接受输入。通过手动选择或自动重新定向，用户应用可以从任何保护的网页被重新定向到主页入口网页 501。

[0110] 图 6 示出了对示范在线拍卖应用 600 的入口网页和保护的网页的组织。简单来讲，在线拍卖应用 600 包括多个入口网页和用于实行浏览、搜索和投标的保护的网页。与在线银行应用 500 相似，主页入口网页 601 提供用于登陆到在线拍卖应用 600 的方式。由于主页入口网页 601 是入口网页，所以用户不需要展示 cookie 或提供任何其它认证或标识数据来访问这个网页。

[0111] 在成功地识别用户并在主页入口网页 601 输入搜索项 (search term) 之后，输入接受搜索结果保护的网页 602 被观看以显示搜索结果概要。由于搜索结果保护的网页 602

是保护的网页，所以不能在不访问入口网页比如主页入口网页 601 的情况下直接访问搜索结果保护的网页 602。还可以使用由入口网页提供的“未被认证的 cookie”来标识未被认证的用户，在不首先进行认证的情况下，访问搜索结果保护的网页 602。

[0112] 通过类别浏览入口网页 604a 到 604c，各种类别的项目可以被浏览而不需认证用户。类似其它入口网页，主页入口网页 601 和类别浏览入口网页 604a 到 604c 可以被书签标记 (bookmarked)。从输入接收搜索结果保护的网页 602 或类别浏览入口网页 604a 到 604c，在项目入口网页 605a 到 605e 上观看拍卖项目。由于项目入口网页 605a 到 605e 被组织成入口网页，所以它们能够被书签标记，被搜索引擎搜索，被转发给其他人，并直接被访问而不需要首先访问存储在网站上的另一个网页。而且，项目入口网页 605a 到 605e 不需要是静态的，并且能够包括变量部分来显示最高投标量或剩余拍卖时间。

[0113] 当通过项目入口网页 605 选择项目时，如果用户还没有被认证，则提供登录保护的网路 606 和输入接受认证保护的网页 607。一旦被认证，输入接受投标入口保护的网页 609 和输入接受投标验证保护的网页 610 被提供来接收投标。在没有首先访问入口网页的情况下，不允许对登录保护的网页 606、认证保护的网页 607、投标入口保护的网页 609 和投标验证保护的网页 610 的直接访问。

[0114] 在投标验证之后，用户应用被重新定向到项目入口网页 605。为了识别考虑中的项目，投标过程中涉及的各个网页接收项目标识符作为输入。如果保护的网页被配置来使用非标识的 (non-identification)cookie，则对不同网页的认证可以通过网关来实行。

[0115] 图 7 示出了对示范在线零售应用 700 的入口网页和保护的网页的组织。类似于在线拍卖应用 600，在线零售应用 700 还包括主页入口网页 701、输入接受搜索结果保护的网页 702、类别浏览入口网页 704a 到 704c、以及项目入口网页 705a 到 705e。通过使用未被认证的 cookie，用户可以被标识和授权来观看搜索结果保护的网页 702 和购物推车保护的网页 706，而不进行全面认证。当前进到结算 (check-out) 程序时，购物推车保护的网页 706 和输入接受登录保护的网页 707 强制对用户的认证。支付保护的网页 709 和确认保护的网页 710 类似于投标保护的网页，虽然在线零售上下文中可以涉及其它步骤。

[0116] 图 8 示出了对示范网络邮件应用 800 的入口网页和保护的网页的组织。网络邮件应用 800 提供电子邮件消息，包括具有可以包括恶意脚本的 HTML 内容的消息，的发送、读取、和搜索。简单来讲，类似于在线银行应用 500，网络邮件应用 800 包括单一入口网页和通过入口网页访问的多个保护的网页。

[0117] 更具体地讲，主页入口网页 801 提供登陆到网络邮件应用 800 的方式。用户应用不需要展示 cookie 或提供任何其它认证或标识数据来访问主页入口网页 801。在通过输入接受认证网页 802 成功地认证用户之后，网络邮件应用 800 将用户应用重新定向到主菜单保护的网页 804，其提供由用户选择选项。基于所选择的选项，用户应用可以进一步被定向到可以接受输入的邮件发送保护的网页 805a 和 805b、输入接受邮件搜索保护的网页 806、输入接受邮件读取保护的网页 807、或其它网页。

[0118] 图 9 示出了对示范搜索引擎应用 900 的入口网页和保护的网页的组织。简单来讲，搜索引擎应用 900 包括具有输入方式的输入接受主页入口网页 901 和输入接受搜索结果保护的网页 902。虽然搜索引擎应用 900 自己可能不存在威胁，然而它对黑客来说是很重要的目标，这是因为用户通常在这样的网页开始他们的因特网浏览会话。在这点上，搜索引擎应

用 900 可以是黑客用来放置恶意脚本的具有诱惑力的目标。

[0119] 因为搜索结果保护的网页 902 受到保护，所以搜索引擎应用 900 不允许书签搜索，或直接链接查询。在一个实施方式中，搜索引擎应用 900 唯一地进行识别和授权，但是不认证用户，由此通过使用未被认证的 cookie 来禁止对搜索结果保护的网页 902 的访问。

[0120] 图 10 示出了对示范 SAP® 入口应用 1000 的入口网页和保护的网页的组织。简单来讲，SAP® 入口应用 1000 包括入口扉页 (portal front entry page)1001 和保护的网页。通过输入接受认证保护的网页 1002 实行对保护的网页的访问，输入接受认证保护的网页 1002 本身通过入口扉页 1001 来访问。在一个示例实施方式中，使用客户端 SSL 证书来执行认证。当进行认证时，其它输入接受和非输入接受保护的网页 1004a 到 1004e 通过保护的主菜单网页 1003 来访问。特别地，用户应用在保护的网页之间进行导航期间保持被认证状态。

[0121] 图 11 是示出使用图 3 中绘出的示范处理的跨站脚本攻击的防护的浮动图。属于黑客的计算机 1101 将电子消息 1102 发送到合法网络用户使用的计算机 1104，电子消息 1102 包含了具有跨站脚本输入的恶意链接 1105。没不知道恶意链接 1105 的情况下，合法用户可以选择该链接 1105，其将请求 1106 发送到目标网站 1107。

[0122] 虽然合法用户可以被目标网站 1107 授权和认证，但是由于请求 1106 的引用网页的引用字符串被存储在属于黑客的计算机 1101 上，而没有存储在目标网站 1107 上，所以响应 1109 被产生，其将合法用户重新定向到入口网页，预先占据跨站脚本内容的反射。因此，增强的跨站攻击防护方案能够用来阻止跨站脚本和跨站请求伪造攻击。

[0123] 增强的跨站攻击防护方案可以部署在网络应用前，以处理请求，从而全面地保护网站免于遭受跨站攻击。由于没有执行响应重写，这个可升级的方案提供有效解决方案来防止跨站攻击，同时提供便利的部署。

[0124] 已经描述了许多实施方式。然而，应当理解在不脱离公开内容的精神和范围的情况下可以进行各种修改。因此，其它实施方式在后面权利要求书的范围之内。

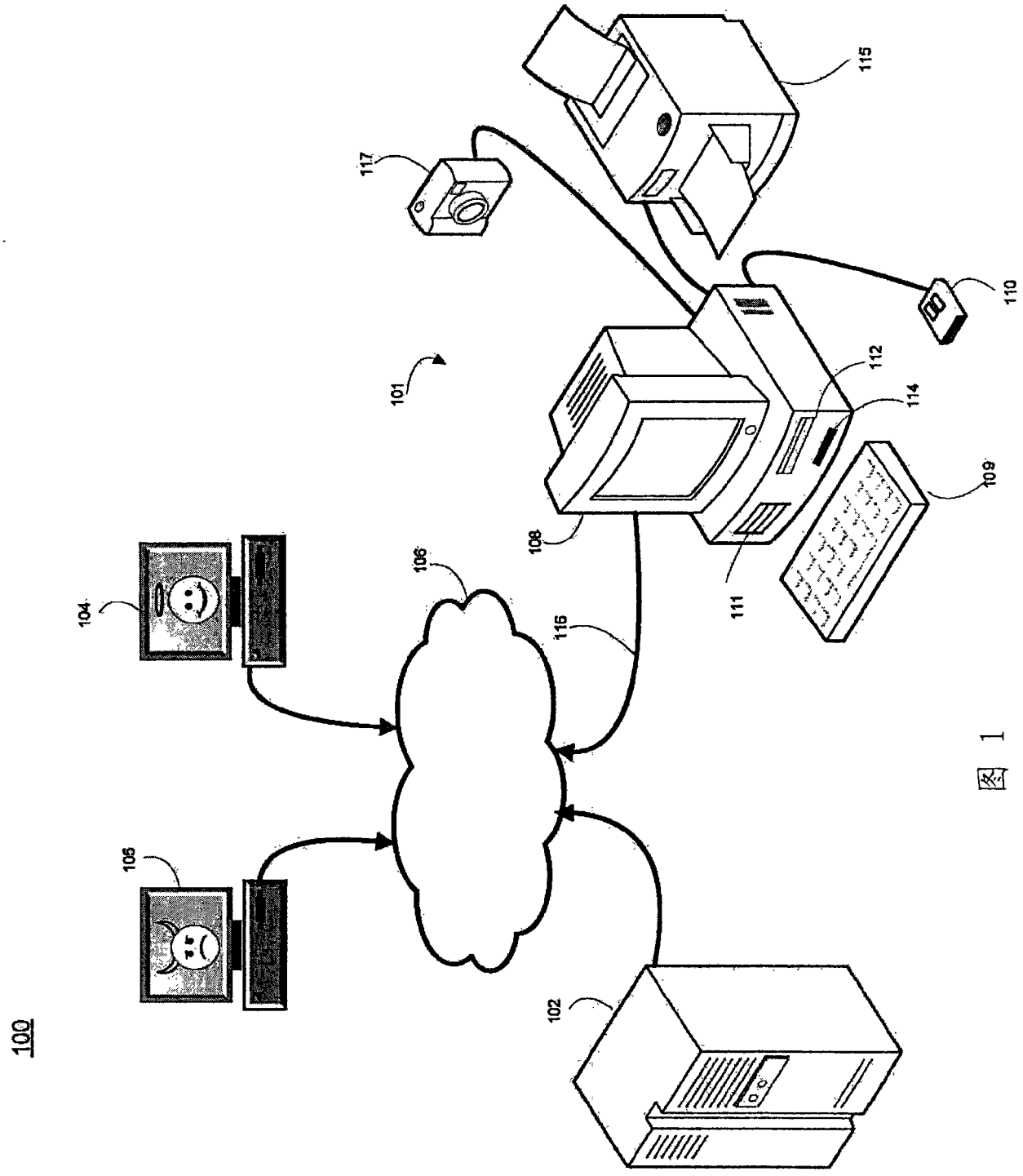


图 1

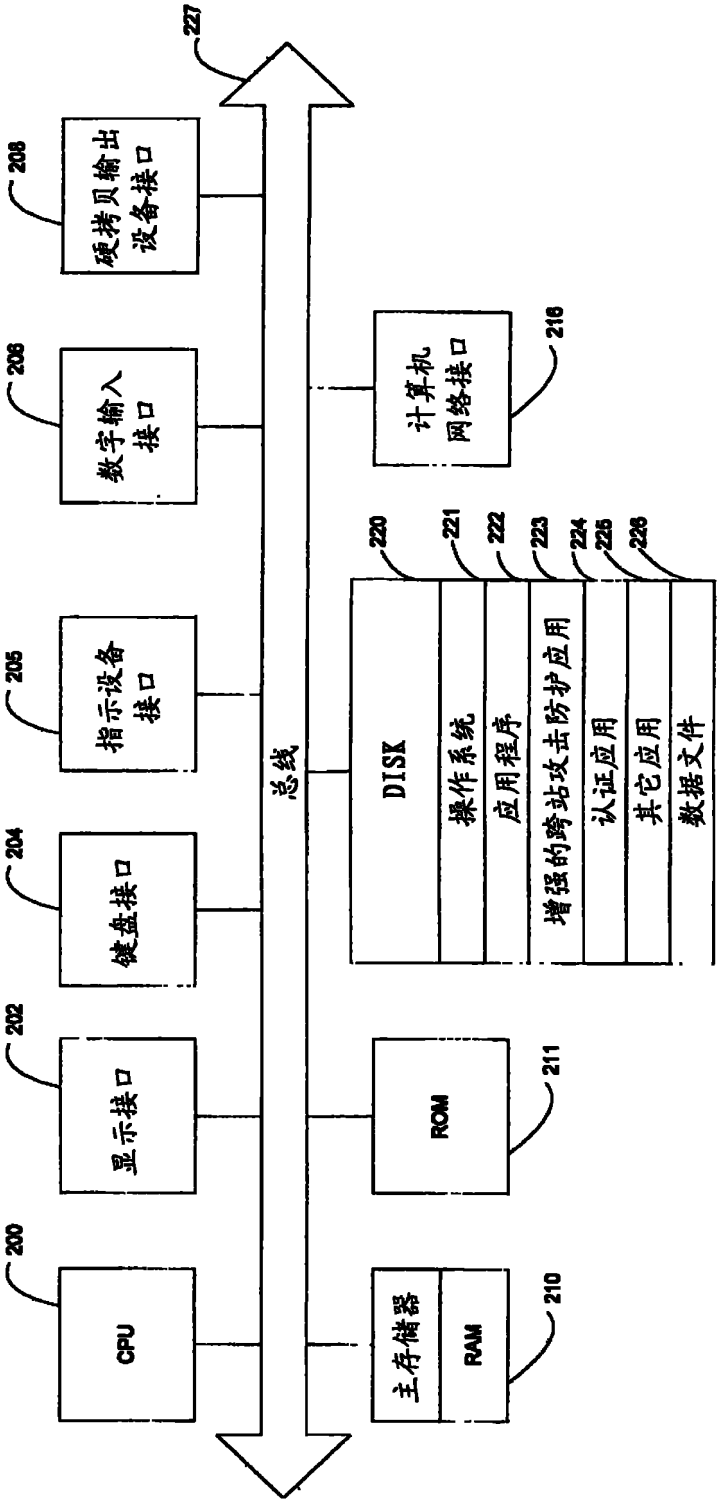

227
208
硬拷贝输出设备接口
206
数字输入接口
205
指示设备接口
204
键盘接口
202
显示接口
200
CPU
总线
计算机网络接口
216
220
221
222
223
224
225
226
DISK
操作系统
应用程序
增强的跨站攻击防护应用
认证应用
其它应用
数据文件
ROM
211
主存储器
RAM
210

图 2

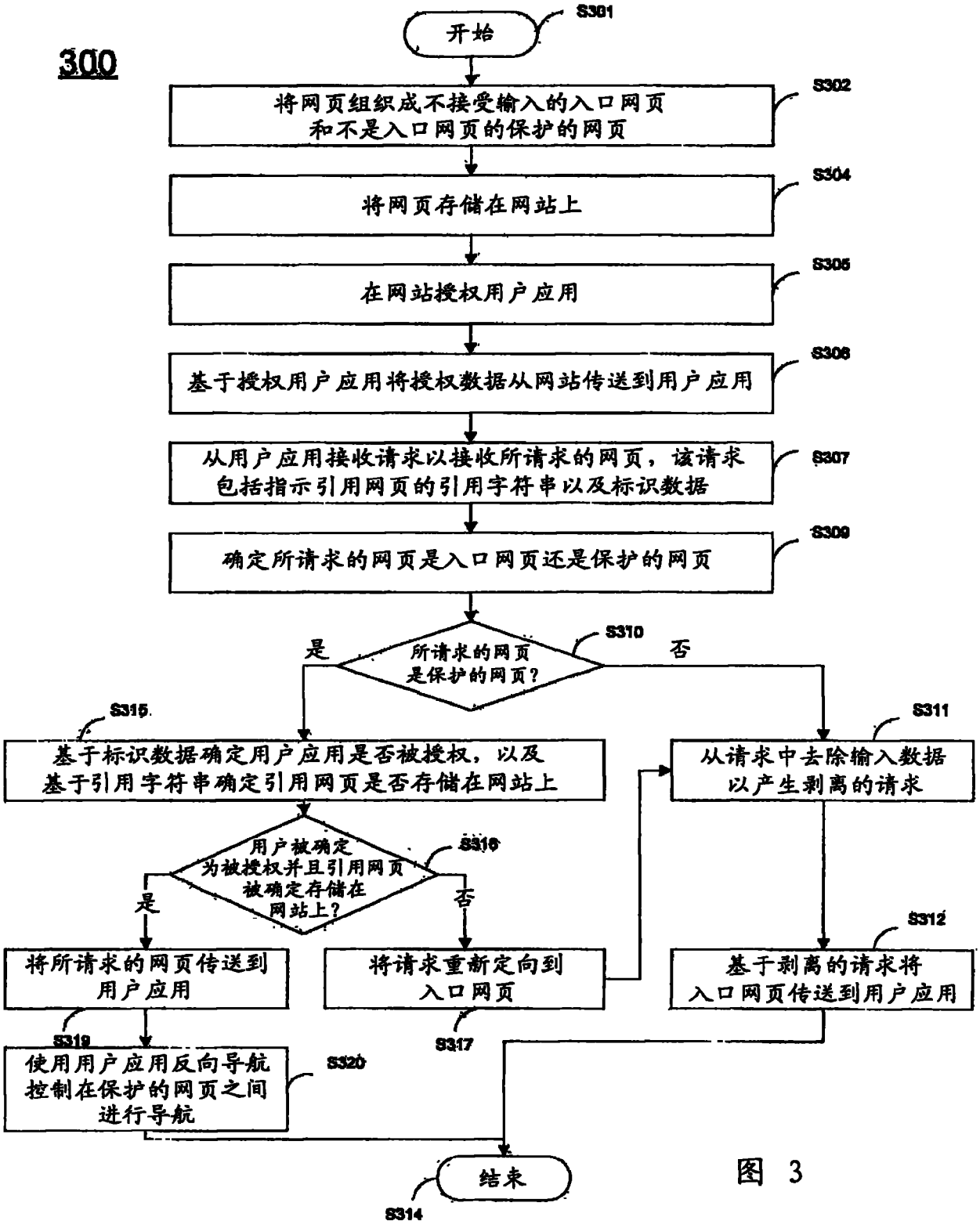

300
开始
S301
将网页组织成不接受输入的入口网页和不是入口网页的保护的网页
S302
将网页存储在网站上
S304
在网站授权用户应用
S305
基于授权用户应用将授权数据从网站传送到用户应用
S306
从用户应用接收请求以接收所请求的网页，该请求包括指示引用网页的引用字符串以及标识数据
S307
确定所请求的网页是入口网页还是保护的网页
S309
所请求的网页是保护的网页?
S310
是
否
基于标识数据确定用户应用是否被授权，以及基于引用字符串确定引用网页是否存储在网站上
S315
从请求中去除输入数据以产生剥离的请求
S311
用户被确定为被授权并且引用网页被确定存储在网站上?
S316
是
否
将所请求的网页传送到用户应用
将请求重新定向到入口网页
基于剥离的请求将入口网页传送到用户应用
S312
S319
S317
使用用户应用反向导航控制在保护的网页之间进行导航
S320
结束
S314

图 3

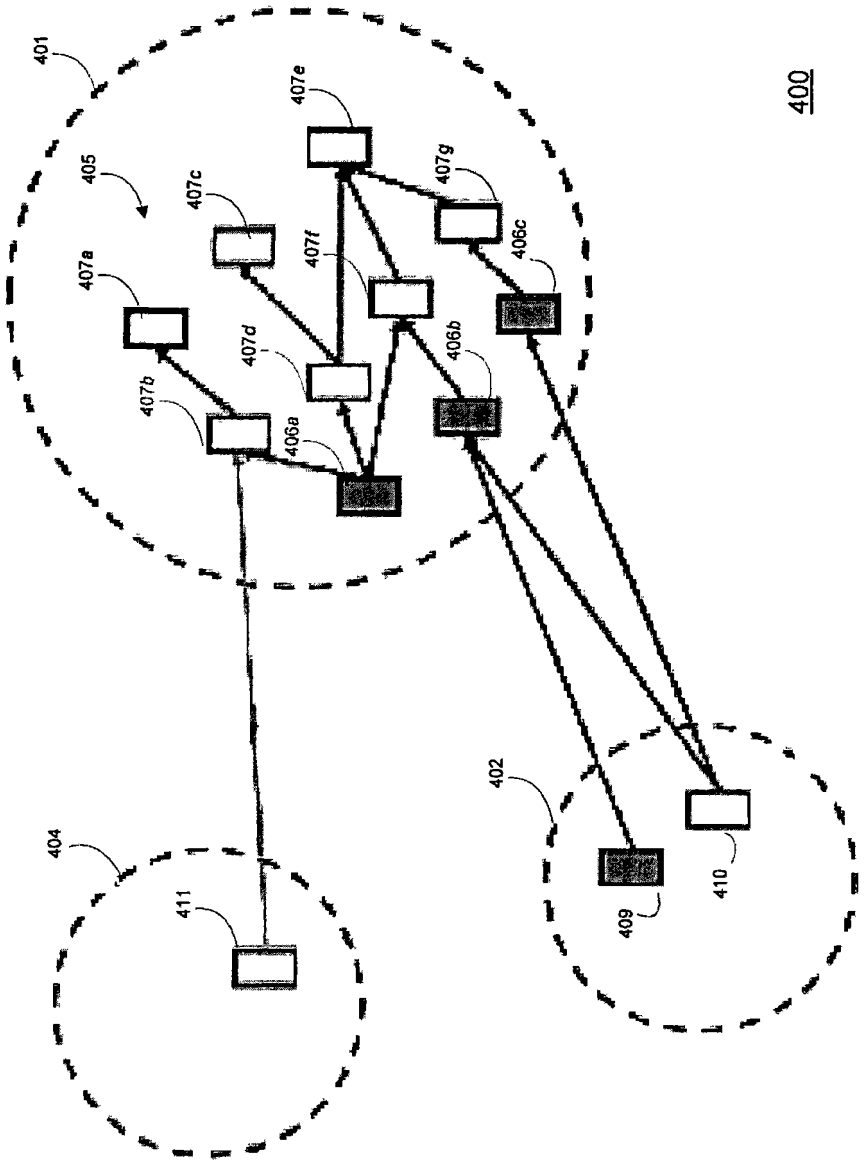

400
401
405
407a
407b
407c
407d
407e
407f
407g
406a
406b
406c
402
404
409
410
411

图 4

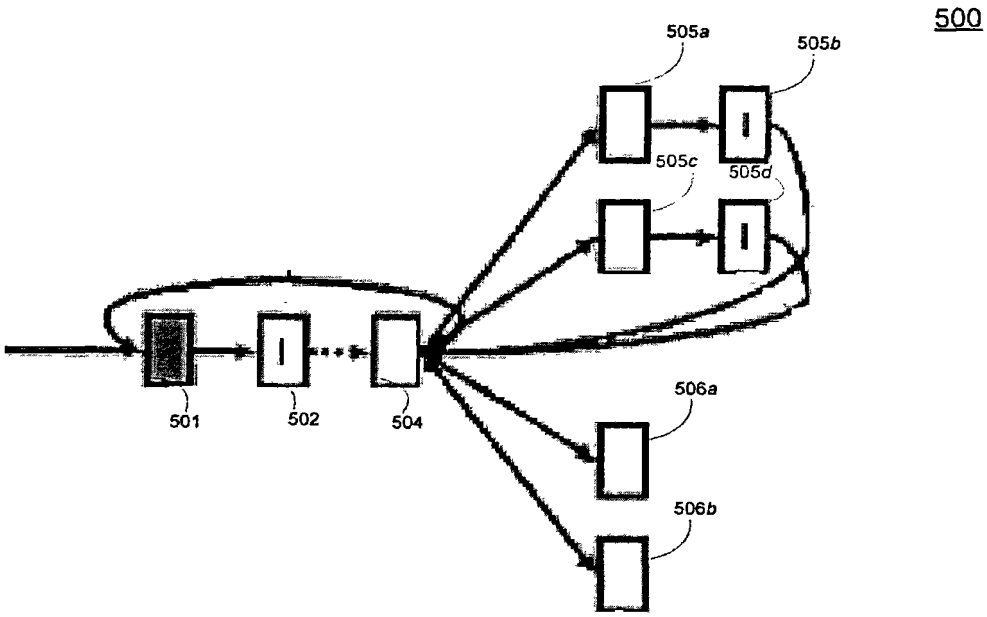

500
505a
505b
505c
505d
501
502
504
506a
506b

图 5

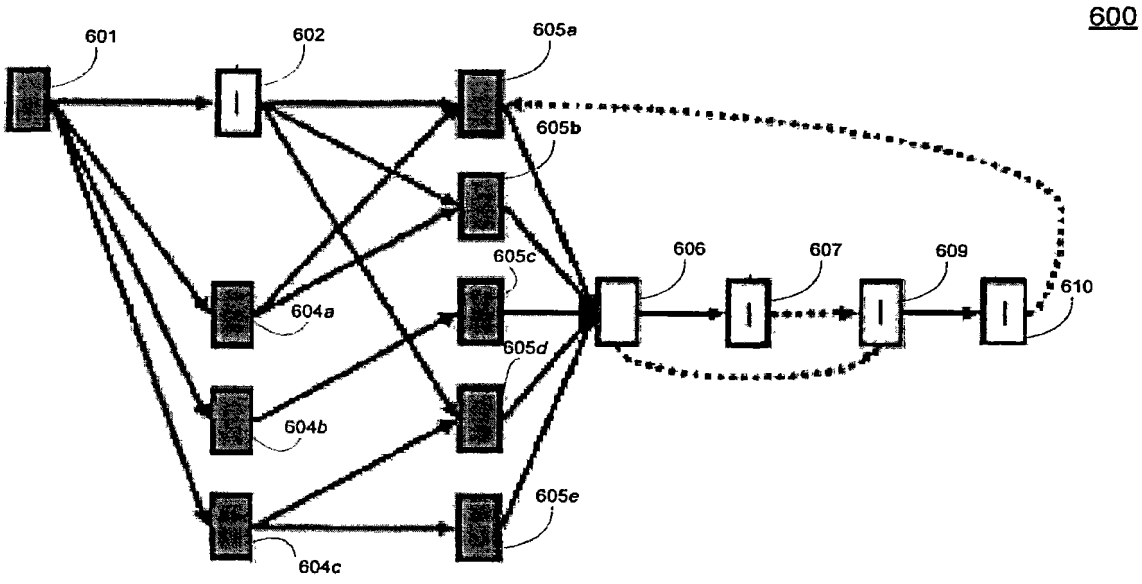

600
601
602
605a
605b
605c
605d
605e
604a
604b
604c
606
607
609
610

图 6

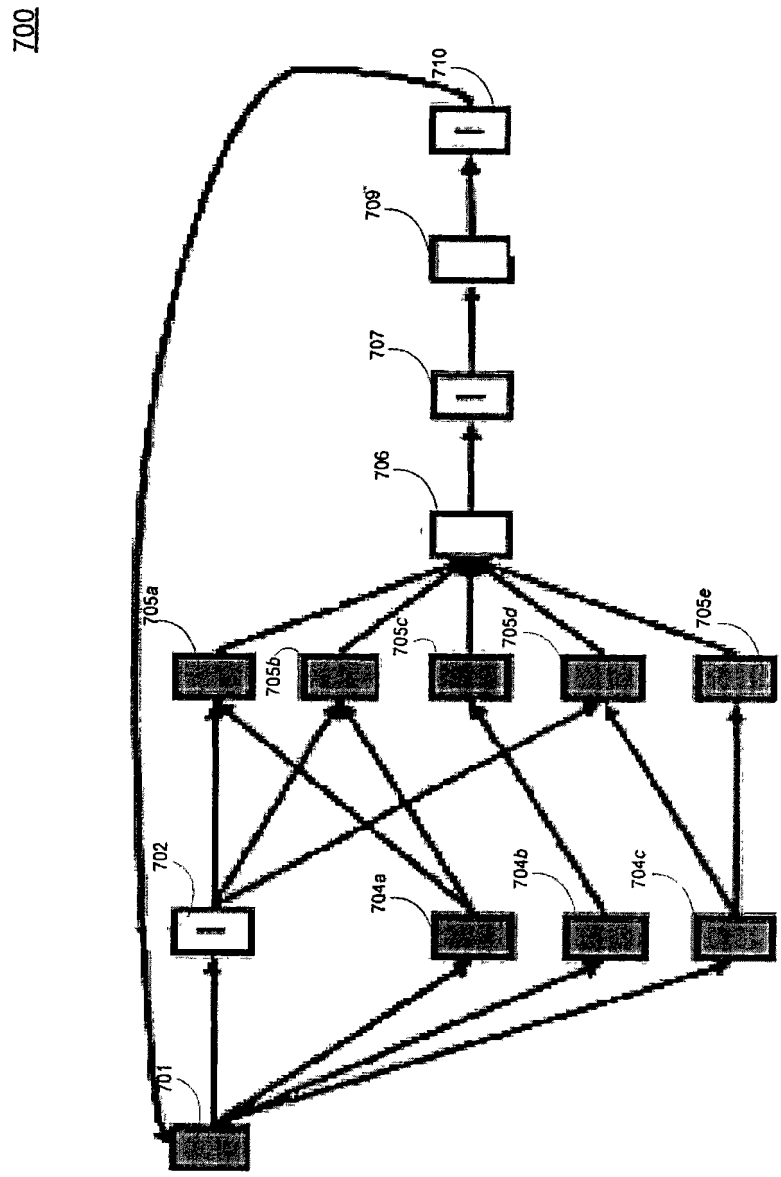

700
710
709
707
706
705a
705b
705c
705d
705e
702
704a
704b
704c
701

图 7

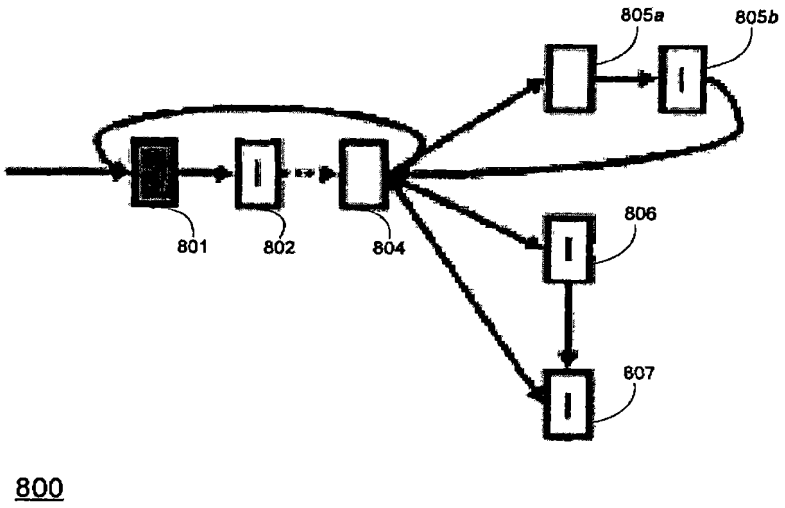


图 8

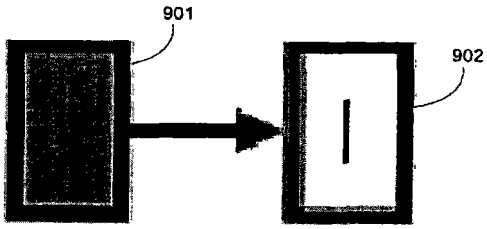


图 9

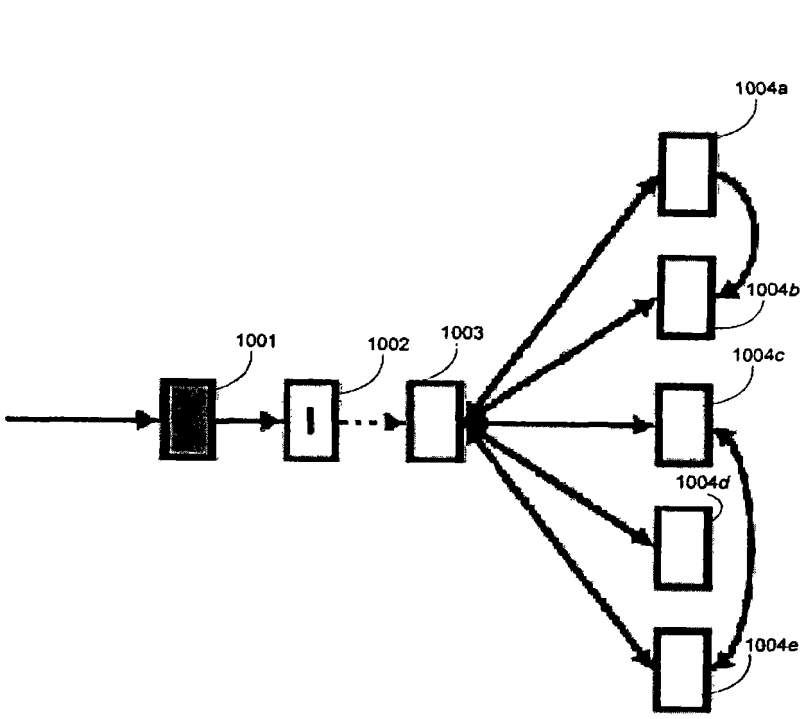


图 10

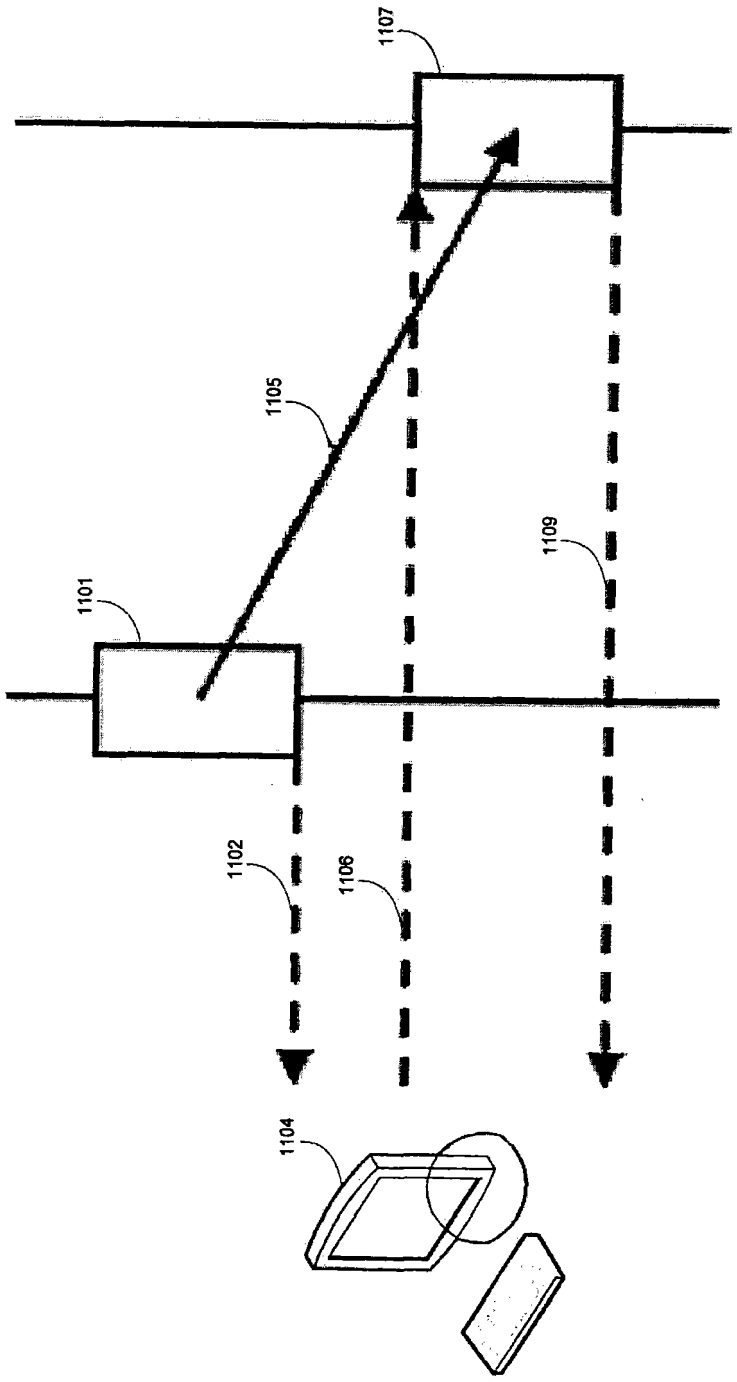


图 11