



(12) 发明专利

(10) 授权公告号 CN 101997685 B

(45) 授权公告日 2013. 05. 29

(21) 申请号 200910171267. 6

CN 101075875 A, 2007. 11. 21,

(22) 申请日 2009. 08. 27

审查员 罗啸

(73) 专利权人 阿里巴巴集团控股有限公司

地址 英属开曼群岛大开曼岛

(72) 发明人 彭卫 孔勇伟

(74) 专利代理机构 北京同达信恒知识产权代理

有限公司 11291

代理人 郭润湘

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

(56) 对比文件

CN 101179387 A, 2008. 05. 14,

US 2003/0188193 A1, 2003. 10. 02,

US 7404204 B2, 2008. 07. 22,

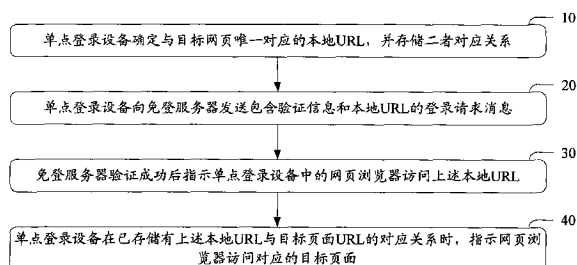
权利要求书3页 说明书10页 附图5页

(54) 发明名称

单点登录方法、单点登录系统以及相关设备

(57) 摘要

本申请公开了一种单点登录方法、单点登录系统以及相关装置,用以解决现有技术中非法用户冒充合法用户访问目标页面的问题。该方法包括:客户端处理单元向网页服务单元发送注册请求;网页服务单元确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,以及将包含所述本地 URL 的注册响应发送给客户端处理单元;客户端处理单元接收到注册响应后向免登服务器发送包含验证信息和所述本地 URL 的登录请求;单点登录设备接收免登服务器基于登录请求中的验证信息对用户身份验证成功后发送的指示,指示网页浏览器向网页服务单元发送访问本地 URL 的请求消息;网页服务单元根据所述请求消息,指示网页浏览器访问对应的目标页面 URL。



1. 一种单点登录方法,其特征在于,包括:

单点登录设备中的客户端处理单元向网页服务单元发送注册请求;

网页服务单元确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,并存储所述本地 URL 与目标网页 URL 的对应关系,以及将包含所述本地 URL 的注册响应发送给客户端处理单元;

客户端处理单元接收到注册响应后向免登服务器发送包含验证信息和所述本地 URL 的登录请求;

单点登录设备接收免登服务器基于登录请求中的验证信息对用户身份验证成功后发送的指示,指示单点登录设备中的网页浏览器向网页服务单元发送访问本地 URL 的请求消息;

网页服务单元根据所述请求消息,在确定存储有请求访问的本地 URL 与目标页面 URL 的对应关系时,指示网页浏览器访问对应的目标页面 URL。

2. 如权利要求 1 所述的方法,其特征在于,所述验证信息为客户端处理单元接收到注册响应后,按照预先与免登服务器约定的方法,根据用户输入的用户标识、密码、以及注册响应中包含的本地 URL 确定出的。

3. 如权利要求 1 所述的方法,其特征在于,所述验证信息为网页服务单元接收到注册请求后,按照与免登服务器约定的方法,根据确定出的与目标网页唯一对应的本地 URL、注册请求包含的用户标识和密码确定出的;

网页服务单元在确定出验证信息后,将该验证信息包含在注册响应中发送给客户端。

4. 如权利要求 3 所述的方法,其特征在于,网页服务单元根据所述本地 URL、注册请求包含的用户标识和密码、以及当前时间信息,来确定验证信息;

网页服务单元发送给客户端的注册响应还包括所述时间信息;

客户端处理单元向免登服务器发送的登录请求还包括所述时间信息;

免登服务器根据登录请求中包含的验证信息进行验证,具体包括:

免登服务器查找登录请求中包含的用户标识对应的密码,并

根据该用户标识、查找到的密码、登录请求包含的本地 URL 和时间信息,获得服务器端验证信息,以及

判断登录请求中包含的验证信息和获得的服务器端验证信息是否一致,在一致时,确定验证成功;否则,验证失败。

5. 如权利要求 4 所述的方法,其特征在于,网页服务单元按照与免登服务器约定的方法,根据本地 URL、注册请求包含的用户标识和密码、以及当前时间信息,获得验证信息,具体包括:

网页服务单元获得包含所述本地 URL、用户标识、密码、以及当前时间信息的字符串,并按照与免登服务器约定的加密方法对获得的字符串加密,以及

求取加密后的字符串的哈希反列;

网页服务单元将求取的哈希反列作为验证信息。

6. 如权利要求 1 至 3 中任一权利要求所述的方法,其特征在于,免登服务器根据登录请求中包含的验证信息,对用户身份进行验证,具体包括:

免登服务器查找登录请求中包含的用户标识对应的密码,并

根据该用户标识、查找到的密码和登录请求包含的本地 URL, 获得服务器端验证信息, 以及

判断登录请求中包含的验证信息和获得的服务器端验证信息是否一致, 在一致时, 确定验证成功; 否则, 验证失败。

7. 如权利要求 1 所述的方法, 其特征在于, 注册请求中包含的密码为客户端处理单元按照与免登服务器约定的加密方法, 对用户输入的密码加密后获得的;

免登服务器根据登录请求中包含的用户标识查找到的密码为按照约定的加密方法, 对用户在该免登服务器中注册时输入的密码加密后获得的。

8. 如权利要求 1 所述的方法, 其特征在于, 免登服务器对用户身份验证成功后, 指示单点登录设备中的网页浏览器请求本地 URL 时, 还包括按照与单点登录设备中的网页服务单元约定的加密方法, 对分配给用户的认证凭据加密, 并在指示单点登录设备中的网页浏览器访问本地 URL 的指示消息中携带加密后的认证凭据的步骤; 以及

网页服务单元在确定出存储有网页浏览器访问的本地 URL 与目标页面 URL 的对应关系后, 还包括: 对网页浏览器发送的访问网页的请求消息中携带的已加密的认证凭据解密, 并在指示网页浏览器访问对应的目标页面 URL 的指示消息中携带解密后的认证凭据。

9. 如权利要求 1 至 3 中任一权利要求所述的方法, 其特征在于, 网页服务单元在确定出存储有网页浏览器访问的本地 URL 与目标页面 URL 的对应关系, 并指示网页浏览器访问对应的目标页面 URL 后, 还包括:

网页服务单元清除存储的所述本地 URL 与目标页面 URL 的对应关系。

10. 如权利要求 1 所述的方法, 其特征在于, 所述网页服务单元与客户端处理单元位于同一单点登录设备内, 或所述网页服务单元独立于单点登录设备。

11. 一种单点登录方法, 其特征在于, 包括:

免登服务器接收到单点登录设备发来的登录请求后, 查找登录请求中包含的用户标识对应的密码, 以及

根据用户标识、查找到的密码、登录请求中包含的本地 URL, 获得服务器端验证信息, 以及

在确定出登录请求包含的验证信息和服务器端验证信息一致后, 指示所述单点登录设备中的网页浏览器访问所述本地 URL, 其中, 所述本地 URL 与用户要访问的目标页面 URL 唯一对应。

12. 一种单点登录设备, 其特征在于, 包括:

客户端处理单元, 用于向网页服务单元发送注册请求, 以及在接收到对应的注册响应后向免登服务器发送包含验证信息和注册响应中包含的本地 URL 的登录请求;

网页服务单元, 用于接收注册请求, 确定与注册请求包含的目标网页 URL 唯一对应的本地 URL, 并存储所述本地 URL 与目标网页 URL 的对应关系, 向客户端处理单元发送包含所述本地 URL 的注册响应, 以及根据该单点登录设备中的网页浏览器发来的访问网页请求, 在确定存储有网页请求中的本地 URL 与目标页面 URL 的对应关系时, 指示所述网页浏览器访问对应的目标页面 URL。

13. 一种免登服务器, 其特征在于, 包括:

接收单元, 用于接收单点登录设备发来的登录请求;

查找单元,用于查找登录请求中包含的用户标识对应的密码;

确定单元,用于按照与单点登录设备约定的方法,根据登录请求包含的用户标识和本地 URL,以及查找单元查找到的密码,获得服务器端验证信息;

判断单元,用于判断确定单元获得的服务器端验证信息与所述登录请求中包含的验证信息是否一致;

指示单元,用于在判断单元判断出服务器端验证信息与登录请求中包含的验证信息一致时,指示所述单点登录设备中的网页浏览器访问登录请求中包含的本地 URL,其中所述本地 URL 与用户要访问的目标页面 URL 唯一对应。

14. 一种单点登录系统,其特征在于,包括单点登录设备和免登服务器,其中,

单点登录设备,用于确定与目标 URL 唯一对应的本地 URL,向免登服务器发送包含验证信息和所述本地 URL 的登录请求,以及在根据免登服务器的指示,确定出存储有免登服务器指示请求的本地 URL 和目标页面 URL 的对应关系时,向网络侧提供目标 URL 对应页面的网页服务器发送访问目标页面 URL 的请求消息;

免登服务器,用于接收登录请求,以及在根据登录请求中包含的验证信息,对用户身份验证成功后,指示单点登录设备访问登录请求中包含的 URL。

单点登录方法、单点登录系统以及相关设备

技术领域

[0001] 本申请涉及计算机网络技术领域,尤其涉及一种单点登录方法、一种单点登录设备、一种免登服务器和一种单点登录系统。

背景技术

[0002] 随着信息技术和网络技术的迅猛发展,各种网络应用系统越来越多,例如网络邮箱、专业论坛、公告板系统(BBS,Bulletin Board System)等。用户在使用其中的每个网络应用系统之前,都必须按照事先约定的用户名和密码进行登录,为此用户必须记住登录每个网络系统所需的用户名和密码,对用户而言,操作非常不便。

[0003] 为了解决上述问题,单点登录(SSO,Single Sign-on)技术应运而生。SSO技术可以为用户访问多个网络应用系统提供便利,用户在登录第一个网络应用系统时,会被客户端引导到免登服务器进行登录;免登服务器根据用户提供的用户名、密码(或客户端对用户密码加密后获得的验证信息)等登录信息进行身份验证,如果通过身份验证,返回给用户一个认证凭据 ticket;用户在后续访问其他网络应用系统时会携带该 ticket,其他网络应用系统在接收到用户的访问请求后会根据该 ticket 到免登服务器中验证 ticket 的合法性,如果该 ticket 是合法的,用户就可以无需再次登录而直接访问其他应用系统。

[0004] 附图1为用户在第一次登录网络应用系统,以及在免登服务器进行验证过程的示意图。

[0005] 步骤101、步骤102,用户通过客户端、网页浏览器向免登服务器发送单点登录请求消息,该消息中包含用户标识UID、第一签名信息以及想要访问的目标网页的统一资源定位符(URL,Uniform Resource Locator),其中第一签名信息是客户端对UID、密码和目标网页的URL进行加密处理后获得的;

[0006] 步骤103,免登服务器接收到单点登录请求后,根据单点登录请求中包含的UID查找到UID对应的密码,并根据事先与客户端预定的加密方法,对UID、查找到的密码和单点登录请求中包含的目标网页的URL进行加密,获得第二签名信息,并对第一签名信息与第二签名信息进行比对,在二者一致时,为用户分配 ticket,并进入步骤104;

[0007] 步骤104,将分配的 ticket 发送给网页浏览器,指示网页浏览器跳转到单点登录请求消息中包含的目标网页的URL中;

[0008] 步骤105,页面浏览器向目标应用系统发送请求消息,该消息包含所请求的目标网页的URL以及 ticket;

[0009] 步骤106,目标网页对应的网络应用系统对 ticket 进行身份验证;

[0010] 步骤107,目标网络应用系统在步骤106身份验证成功后,向用户返回所请求的目标网页的页面内容。

[0011] 如果上述步骤102发送的单点登录请求消息被其他恶意用户采用黑客软件截取到,那么其他用户就可以向免登服务器发送请求,在验证成功后冒充该用户访问目标网络应用系统。

[0012] 为了避免上述问题,免登服务器向用户下发 ticket 时确定了该 ticket 的有效时间,例如 5 分钟等,在超出有效时间后,使用该 ticket 将无法请求到目标应用系统的页面内容。然而,即使设定了较短的 ticket 有效时间,仍然难以避免恶意用户在较短的时间内冒充合法用户访问目标网络应用系统。

发明内容

[0013] 本申请实施例提供一种单点登录方法,用以解决在现有单点登录技术中,非法用户冒充合法用户访问目标页面的问题。

[0014] 对应地,本申请实施例还提供了一种单点登录设备、免登服务器和一种单点登录系统。

[0015] 本申请实施例提供的技术方案如下:

[0016] 一种单点登录方法,包括:

[0017] 单点登录设备中的客户端处理单元向网页服务单元发送注册请求;

[0018] 网页服务单元确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,并存储所述本地 URL 与目标网页 URL 的对应关系,以及将包含所述本地 URL 的注册响应发送给客户端处理单元;

[0019] 客户端处理单元接收到注册响应后向免登服务器发送包含验证信息和所述本地 URL 的登录请求;

[0020] 单点登录设备接收免登服务器基于登录请求中的验证信息对用户身份验证成功后发送的指示,指示单点登录设备中的网页浏览器向网页服务单元发送访问本地 URL 的请求消息;

[0021] 网页服务单元根据所述请求消息,在确定存储有请求访问的本地 URL 与目标页面 URL 的对应关系时,指示网页浏览器访问对应的目标页面 URL。

[0022] 一种单点登录方法,包括:

[0023] 免登服务器接收到单点登录设备发来的登录请求后,查找登录请求中包含的用户标识对应的密码,以及

[0024] 根据用户标识、查找到的密码、登录请求中包含的本地 URL,获得服务器端验证信息,以及

[0025] 在确定出登录请求包含的验证信息和服务器端验证信息一致后,指示所述单点登录设备中的网页浏览器访问所述本地 URL,其中,所述本地 URL 与用户要访问的目标页面 URL 唯一对应。

[0026] 一种单点登录设备,包括:

[0027] 客户端处理单元,用于向网页服务单元发送注册请求,以及在接收到对应的注册响应后向免登服务器发送包含验证信息和注册响应中包含的本地 URL 的登录请求;

[0028] 网页服务单元,用于接收注册请求,确定与注册请求包含的目标网页 URL 唯一对应的本地 URL,并存储所述本地 URL 与目标网页 URL 的对应关系,向客户端处理单元发送包含所述本地 URL 的注册响应,以及根据该单点登录设备中的网页浏览器发来的访问网页请求,在确定存储有网页请求中的本地 URL 与目标页面 URL 的对应关系时,指示所述网页浏览器访问对应的目标页面 URL。

- [0029] 一种免登服务器,包括:
- [0030] 接收单元,用于接收单点登录设备发来的登录请求;
- [0031] 查找单元,用于查找登录请求中包含的用户标识对应的密码;
- [0032] 确定单元,用于按照与单点登录设备约定的方法,根据登录请求包含的用户标识和本地 URL,以及查找单元查找到的密码,获得服务器端验证信息;
- [0033] 判断单元,用于判断确定单元获得的服务器端验证信息与所述登录请求中包含的验证信息是否一致;
- [0034] 指示单元,用于在判断单元判断出服务器端验证信息与登录请求中包含的验证信息一致时,指示与所述单点登录设备中的网页浏览器请求登录请求中包含的本地 URL,其中所述本地 URL 与用户要访问的目标页面 URL 唯一对应。
- [0035] 一种单点登录系统,包括单点登录设备和免登服务器,其中,
- [0036] 单点登录设备,用于确定与目标 URL 唯一对应的本地 URL,向免登服务器发送包含验证信息和所述本地 URL 的登录请求,以及在根据免登服务器的指示,确定出存储有免登服务器指示请求的本地 URL 和目标页面 URL 的对应关系时,向网络侧提供目标 URL 对应页面的网页服务器发送访问目标页面 URL 的请求消息;
- [0037] 免登服务器,用于接收登录请求,以及在根据登录请求中包含的验证信息,对用户身份验证成功后,指示单点登录设备访问登录请求中包含的 URL。
- [0038] 本申请实施例通过客户端在登录请求消息不再携带目标网页 URL,而是携带预先确定的与目标网页 URL 唯一对应的本地 URL,免登服务器在验证通过后,将指示与客户端位于同一计算机的网页浏览器请求登录请求包含的本地 URL,与客户端位于同一计算机的本地网页服务器在判断出已存储有网页浏览器请求的本地 URL 与目标页面的对应关系时,指示所述网页浏览器请求对应的目标页面,避免了携带目标网页 URL 的登录请求被非法用户获取而造成的非法用户冒充合法用户访问目标页面的问题。

附图说明

- [0039] 图 1 为现有单点登录技术中验证过程的示意图;
- [0040] 图 2 为本申请实施例的主要实现原理流程图;
- [0041] 图 3 为本申请实施例一提出的单点登录方法的流程图;
- [0042] 图 4 为本申请实施例二提出的单点登录方法的流程图;
- [0043] 图 5 为本申请实施例三提出的单点登录方法的流程图;
- [0044] 图 6 为本申请实施例提出的单点登录设备的结构示意图;
- [0045] 图 7 为本申请实施例提出的免登服务器的结构示意图。

具体实施方式

[0046] 在现有单点登录方案中,当单点登录客户端向免登服务器发送的携带有用户标识 UID、签名信息以及想要访问的目标网页 URL 的登录请求消息被非法用户截取后,非法用户就可以在冒充用户向免登服务器请求验证后,获得认证凭据 ticket,从而可以访问目标页面,因此存在安全隐患。

[0047] 本申请实施例提出了在登录请求消息不再携带目标网页 URL,而是携带预先确定

的与目标网页 URL 唯一对应的本地 URL,免登服务器在验证通过后,将指示发出登录请求消息的用户跳转到本地 URL,这样合法用户就可以根据预先存储的本地 URL 和目标网页 URL 的对应关系获取目标网页 URL,并通过目标网页 URL 访问目标网页;而非法用户由于本地并不存在与所述本地 URL 对应的目标网页 URL,因此无法继续访问目标页面,从而避免了现有单点登录技术的上述安全问题。

[0048] 下面结合各个附图对本申请实施例技术方案的主要实现原理、具体实施方式及其对应能够达到的有益效果进行详细地阐述。

[0049] 如图 2 所示,本申请实施例的主要实现原理流程如下:

[0050] 步骤 10,单点登录设备在向免登服务器发送登录请求前,确定与目标网页唯一对应的本地 URL,并在提供所述本地 URL 的单点登录设备中的网页服务单元中存储该本地 URL 与目标网页 URL 的对应关系;

[0051] 步骤 20,单点登录设备向免登服务器发送登录请求消息,该登录请求消息中包含验证信息和步骤 10 确定出的本地 URL;

[0052] 步骤 30,免登服务器根据登录请求消息中包含的验证信息,验证成功后,指示单点登录设备中的网页浏览器向单点登录设备中的网页服务单元发送访问登录请求消息中包含的本地 URL 的请求消息;

[0053] 步骤 40,所述网页服务单元在确定出已存储有网页浏览器请求的本地 URL 与目标页面 URL 的对应关系时,指示网页浏览器访问对应的目标页面。

[0054] 下面将依据本申请上述发明原理,详细介绍一个实施例来对本申请方法的主要实现原理进行详细的阐述和说明。

[0055] 实施例一、

[0056] 请参照附图 3,为本实施例提出的单点登录方法的流程图,单点登录系统包括位于用户侧的单点登录设备以及位于网络侧的免登服务器,其中单点登录设备中包含客户端处理单元、网页服务单元和网页浏览器,其中客户端处理单元用于接收用户输入的用户名、密码、需要登录的目标页面 URL,以及向免登服务器发送登录请求;该客户端处理单元可以是一个独立的软件产品,也可以是在现有的浏览器的基础上加以改进形成的浏览器形式的软件产品。网页服务单元可以由现有的网页服务器来实现,网页服务器是用于提供本地网页 URL,响应网页浏览器的 URL 访问请求的软件产品的统称,例如广泛应用与 UNIX 平台的 Apache 系列产品;网页浏览器是用于根据用户或其他应用程序的指示,访问指定的 URL 的软件产品的统称,例如微软公司的 Internet Explorer 系列产品。用户在进行单点登录前,应预先通过客户端处理单元在免登服务器中注册用户标识以及对应的密码。

[0057] 步骤 301,用户在单点登录设备的客户端处理单元中输入用户标识、对应的密码以及需要登录的目标网页的 URL 后,客户端处理单元向与自身位于同一单点登录设备中的网页服务单元发送包含目标网页 URL 的注册请求,例如目标网页 URL 为 http://www.targetweb.com/item_detail=23445;

[0058] 步骤 302,网页服务单元接收到注册请求后,按照预定的规则,确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,例如确定本地 URL 的规则为“<http://127.0.0.1:8808/auth?sid=>”+与注册请求中包含的目标网页 URL 唯一对应的标识,为上述目标网页 URLhttp://www.targetweb.com/item_detail=23445 确定出的本

地 URL 为 <http://127.0.0.1:8808/auth?sid=123456> ;并在自身存储上述目标网页 URL 与确定出的本地 URL 的对应关系 ;

[0059] 步骤 303, 网页服务单元将包含步骤 302 中确定出的本地 URL 的注册响应发送给客户端处理单元 ;

[0060] 步骤 304, 客户端处理单元接收到网页服务单元发来的注册响应后, 从注册响应中获取本地 URL, 按照预先与免登服务器约定的方法, 根据用户输入的用户标识、密码、注册响应中包含的本地 URL, 确定第一验证信息, 例如, 客户端处理单元首先获得包含该本地 URL、用户标识、密码的字符串, 并按照预先与免登服务器约定的加密方法, 例如 MD5 算法等, 对获得的字符串加密, 为了提高验证信息的安全性, 还可以求取加密后的字符串的哈希反列, 将求取的哈希反列作为第一验证信息。为了进一步提高验证信息的安全性, 使每次登录同一目标网页时的验证信息都不同, 在确定验证信息时, 不仅可以根据本地 URL、用户标识、密码, 还可以在此基础上加入当前的时间信息。

[0061] 步骤 305, 客户端处理单元确定出第一验证信息后, 向免登服务器发送包含用户标识、第一验证信息以及注册响应中包含的本地 URL 的登录请求 ;

[0062] 步骤 306, 免登服务器接收到步骤 305 中客户端处理单元发来的登录请求后, 查找自身预先存储的与登录请求中包含的用户标识对应的密码, 并按照预先与客户端处理单元约定的确定验证信息的方法, 例如 MD5 算法等, 根据用户标识、查找到的密码、登录请求包含的本地 URL, 获得第二验证信息 ;

[0063] 步骤 307, 免登服务器对步骤 305 中单点登录设备中客户端处理单元发来的登录请求中包含的第一验证信息, 以及步骤 306 中确定出的第二验证信息进行比较, 在第一验证信息与第二验证信息一致时, 确定验证成功, 进入步骤 308, 否则确定验证失败, 丢弃该登录请求或返回登录失败信息 ;

[0064] 步骤 308, 免登服务器在验证成功后, 指示用户侧单点登录设备中的网页浏览器访问步骤 306 中接收到的登录请求中包含的本地 URL。与现有技术类似, 免登服务器在验证成功后指示网页浏览器访问登录请求中包含的本地 URL 时, 可以在指示消息中携带认证凭据。具体的携带方式可以为将认证凭据作为登录请求中包含的本地 URL 的参数, 将携带参数的本地 URL 指示给网页浏览器。为了提高安全性, 还可以按照与网页服务器约定的加密方式, 对认证凭据加密, 例如携带加密后的认证凭据的本地 URL 为 “<http://127.0.0.1/dosth?sid=123456&ticket=JDFU324o329jdcvjcv0374023842--8324-83207230432084>”, 其中 ticket 后的新增部分 “JDFU324o329jdcvjcv0374023842--8324-83207230432084” 为加密后的认证凭据 ;

[0065] 步骤 309, 单点登录设备中的网页浏览器根据步骤 308 中免登服务器的指示, 向同一单点登录设备中的网页服务单元发送访问上述本地 URL 的请求消息 ;

[0066] 步骤 310, 单点登录设备中的网页服务单元在接收到网页浏览器发送的访问本地 URL 的请求消息后, 判断自身存储的本地 URL 与目标页面 URL 的对应关系中, 是否存在与网页浏览器发送的访问请求消息中的本地 URL 对应的目标页面 URL。若存在, 说明步骤 305 中的登录请求包含的本地 URL 是预先通过注册过程确定出的, 即登录请求是由该单点登录设备中的客户端处理单元发出的, 进入步骤 311, 否则不进行后续处理 ;

[0067] 步骤 311, 网页服务单元指示网页浏览器向目标网页 URL 对应的网页服务器发送

访问请求消息。网页服务单元在指示消息中可以携带认证凭据,该认证凭据是根据预先与免登服务器预定的加密方法,对步骤 310 中网页浏览器的访问请求消息中携带的本地 URL 解密后获得的。

[0068] 在步骤 301 至步骤 303 的注册交互过程中,由于客户端处理单元与网页服务单元是位于同一单点登录设备中的,因此交互过程中的消息不会被网络中的其他非法用户获取到。

[0069] 本实施例中,网页服务单元也可独立于单点登录设备,例如,在单点登录设备之外单独设置一台或一组服务器。只要确保该网页服务单元与单点登录设备之间交互的通信安全,例如,网页服务单元与单点登录设置之间通过专线连接等,即可提高单点登录过程的安全性。

[0070] 本实施例在用户向免登服务器发送登录请求前,预先确定与用户请求的目标页面 URL 对应的本地 URL,登录请求中携带的不再是目标页面 URL,而是本地 URL,因此即使该登录请求消息被其他非法用户截获,由于非法用户所使用的计算机中并没有与本地 URL 对应的目标网页 URL,因此非法用户也无法在验证成功后冒充该用户访问目标页面 URL,从而避免了登录请求被非法用户截获所可能造成的非法用户冒充合法用户登录目标页面的问题。

[0071] 实施例二、

[0072] 在实施例一中,是由单点登录设备中的客户端处理单元确定第一验证信息的,在本实施例中由单点登录设备中的网页服务单元来实现确定第一验证信息的功能,客户端处理单元发送给网页服务单元的注册请求不仅应包含目标网页 URL,还应该包含用户输入的用户标识和密码,网页服务单元在确定出第一验证信息后,将第一验证信息告知客户端处理单元,由客户端处理单元在发送给免登服务器的登录请求中携带第一验证信息,具体过程请参照附图 4 所示。

[0073] 步骤 401,用户在单点登录设备中的客户端处理单元中输入用户标识、对应的密码以及需要登录的目标网页的 URL 后,客户端处理单元向同一单点登录设备中的网页服务单元发送包含目标网页 URL、用户输入的用户标识和用户标识对应的密码的注册请求,例如目标网页 URL 为 `http://www.targetweb.com/item_detail = 23445`;

[0074] 步骤 402,网页服务单元接收到注册请求后,按照预定的规则,确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,例如确定出的本地 URL 为 `http://127.0.0.1:8808/auth?sid = 123456`;并保存上述目标网页 URL 与确定出的本地 URL 的对应关系;

[0075] 步骤 403,网页服务单元在确定出目标网页 URL 对应的本地 URL 后,按照预先与免登服务器约定的方法,根据用户输入的用户标识、密码、注册响应中包含的本地 URL,确定第一验证信息,进入步骤 404;

[0076] 步骤 404,网页服务单元向客户端发送注册响应,注册响应中包含步骤 403 中确定出的本地 URL 和第一验证信息;

[0077] 步骤 405,客户端处理单元在接收到注册响应后,向网络侧的免登服务器发送登录请求,登录请求中包含用户输入的用户标识、以及注册响应中包含的本地 URL 和第一验证信息;

[0078] 步骤 406,免登服务器接收到步骤 405 中单点登录设备中的客户端处理单元发来

的登录请求后,从登录请求中获得用户标识,从存储的用户标识和密码的对应关系中查找该用户标识对应的密码,并按照预先与单点登录设备中的网页服务单元约定的确定验证信息的方法,根据该用户标识、查找到的密码和登录请求中包含的 URL,确定第二验证信息;

[0079] 步骤 407,免登服务器对步骤 405 中单点登录设备中的客户端处理单元发来的登录请求中包含的第一验证信息和步骤 406 中确定出的第二验证信息进行比较,在二者一致时,确定验证成功,进入步骤 408,否则,丢弃该登录请求或告知用户验证失败;

[0080] 步骤 408,免登服务器在验证成功后,指示用户侧单点登录设备中的网页浏览器访问步骤 406 中接收到的登录请求中包含的本地 URL,与步骤 308 类似,免登服务器可以将认证凭据作为登录请求中包含的本地 URL 的参数;

[0081] 步骤 409,网页浏览器根据步骤 408 中免登服务器的指示,向同一单点登录设备中的网页服务单元发送访问上述本地 URL 的请求消息;

[0082] 步骤 410,单点登录设备中的网页服务单元在接收到网页浏览器发送的访问本地 URL 的请求消息后,判断在自身存储的本地 URL 与目标页面 URL 的对应关系中,是否存在与网页浏览器发送的访问请求消息中的本地 URL 对应的目标页面 URL。若存在,说明步骤 405 中的登录请求包含的本地 URL 是预先通过注册过程确定出的,即登录请求是由该单点登录设备中的客户端处理单元发出的,进入步骤 411,否则不进行后续处理;

[0083] 步骤 411,网页服务单元指示网页浏览器向目标网页 URL 对应的网页服务器发送访问请求消息。网页服务单元在指示消息中可以携带认证凭据,该认证凭据是根据预先与免登服务器预定的加密方法,对步骤 410 中网页浏览器的访问请求消息中携带的本地 URL 解密后获得的。

[0084] 同理,在本实施例中,网页服务单元也可独立于单点登录设备,例如,在单点登录设备之外单独设置一台或一组服务器。只要确保该网页服务单元与单点登录设备之间交互的通信安全,例如,网页服务单元与单点登录设备之间通过专线连接等,即可提高单点登录过程的安全性。

[0085] 实施例三、

[0086] 在实施例一或实施例二中,第一验证信息、或第二验证信息是由客户端处理单元、网页服务单元或免登服务器按照约定的方法,根据用户标识、密码、本地 URL 确定的,在本实施例中,确定验证信息时不仅根据上述三种信息,还包括确定第一验证信息时的时间信息,这样即使使用同一台计算机,在不同时间访问同一目标网页时,确定出的验证信息也是不同的,以免使用同一台计算机的其他非法用户冒充合法用户来访问该目标网页。具体过程请参照附图 5 所示。

[0087] 步骤 501,用户在单点登录设备中的客户端处理单元中输入用户标识、对应的密码以及需要登录的目标网页的 URL 后,客户端处理单元向同一单点登录设备中的网页服务单元发送包含目标网页 URL、用户输入的用户标识和用户标识对应的密码的注册请求,例如目标网页 URL 为 `http://www.targetweb.com/item_detail = 23445`;

[0088] 步骤 502,网页服务单元接收到注册请求后,按照预定的规则,确定与注册请求中包含的目标网页 URL 唯一对应的本地 URL,例如确定出的本地 URL 为 `http://127.0.0.1:8808/auth? sid = 123456`;并保存上述目标网页 URL 与确定出的本地

URL 的对应关系；

[0089] 步骤 503, 网页服务单元在确定出目标网页 URL 对应的本地 URL 后, 按照预先与免登服务器约定的方法, 根据用户输入的用户标识、密码、注册响应中包含的本地 URL 以及当前时间信息, 确定第一验证信息, 进入步骤 504；

[0090] 步骤 504, 网页服务单元向客户端发送注册响应, 注册响应中包含步骤 503 中确定出的本地 URL、第一验证信息和该网页服务单元在确定第一验证信息时的时间信息；

[0091] 步骤 505, 客户端处理单元在接收到注册响应后, 向网络侧的免登服务器发送登录请求, 登录请求中包含用户输入的用户标识、以及注册响应中包含的本地 URL、第一验证信息和时间信息；

[0092] 步骤 506, 免登服务器接收到步骤 505 中单点登录设备中的客户端处理单元发来的登录请求后, 从登录请求中获得用户标识, 从存储的用户标识和密码的对应关系中查找到该用户标识对应的密码, 并按照预先与单点登录设备中的网页服务单元约定的确定验证信息的方法, 根据该用户标识、查找到的密码、登录请求中包含的 URL 和时间信息, 确定第二验证信息；

[0093] 步骤 507, 免登服务器对步骤 505 中单点登录设备中的客户端处理单元发来的登录请求中包含的第一验证信息和步骤 506 中确定出的第二验证信息进行比较, 在二者一致时, 确定验证成功, 进入步骤 508, 否则, 丢弃该登录请求或告知用户验证失败；

[0094] 步骤 508, 免登服务器在验证成功后, 指示用户侧单点登录设备中的网页浏览器访问步骤 506 中接收到的请求登录请求中包含的本地 URL, 与步骤 308 类似, 免登服务器可以将认证凭据作为登录请求中包含的网页 URL 的参数；

[0095] 步骤 509, 网页浏览器根据步骤 508 中免登服务器的指示, 向同一单点登录设备中的网页服务单元发送访问上述本地 URL 的请求消息；

[0096] 步骤 510, 单点登录设备中的网页服务单元在接收到网页浏览器发送的访问本地 URL 的请求消息后, 判断在自身存储的本地 URL 与目标页面 URL 的对应关系中, 是否存在与网页浏览器发送访问请求消息中的本地 URL 对应的目标页面 URL。若存在, 说明步骤 505 中的登录请求包含的本地 URL 是预先通过注册过程确定出的, 即登录请求是由该单点登录设备中的客户端处理单元发出的, 进入步骤 511, 否则不进行后续处理；

[0097] 步骤 511, 网页服务单元指示网页浏览器向目标网页 URL 对应的网页服务器发送访问请求消息。网页服务单元在指示消息中可以携带认证凭据, 该认证凭据是根据预先与免登服务器预定的加密方法, 对步骤 510 中网页浏览器的访问请求消息中携带的本地 URL 解密后获得的。

[0098] 其中, 为了提高安全性, 步骤 501 中单点登录设备中的客户端处理单元发送的注册请求中所包含的密码可以为客户端处理单元按照与免登服务器约定的加密方法, 对用户输入的密码加密后获得的；同样, 免登服务器根据登录请求中包含的用户标识查找到的密码为按照约定的加密方法, 对用户在该免登服务器中注册时输入的密码加密后获得的。

[0099] 在步骤 503 中, 单点登录设备中的网页服务单元根据用户输入的用户标识、密码、注册响应中包含的本地 URL 以及当前时间信息, 确定第一验证信息的过程与步骤 304 中客户端确定第一验证信息的过程类似：网页服务单元首先获得包含该本地 URL、用户标识、密码和当前时间的字符串, 并按照预先与免登服务器约定的加密方法, 例如 MD5 算法, 对获得

的字符串加密,为了提高验证信息的安全性,还可以求取加密后的字符串的哈希反列,将求取的哈希反列作为第一验证信息。

[0100] 在上述步骤 506 中,免登服务器按照与步骤 503 中确定第一验证信息类似的方法,根据用户标识、查找到的密码、登录请求包含的本地 URL 和时间信息,获得第二验证信息。

[0101] 与实施例一相类似,在步骤 503 中,网页服务单元确定第一验证信息的功能也可以由同一单点登录设备中的客户端处理单元来实现。

[0102] 与实施例一相类似,为了保证认证凭据传输的安全性,免登服务器在验证成功后,按照预先与单点登录设备中的网页服务单元约定的加密方法,对分配给用户的认证凭据加密,并在指示单点登录设备中的网页浏览器访问本地 URL 的指示消息中携带加密后的认证凭据的,例如,将加密后的认证凭据作为请求的本地 URL 的参数,网页服务单元在判断出已存在网页浏览器请求的本地 URL 与目标页面 URL 的对应关系时,按照约定的加密方法对网页浏览器发送的网页请求消息中携带的已加密的认证凭据解密,并在指示网页浏览器访问的目标页面的指示消息中携带解密后的认证凭据。

[0103] 在步骤 510 中,网页服务单元在确定出登录请求是由与网页浏览器位于同一单点登录设备中的客户端处理单元发出的后,还可以清除本地 URL 与目标页面 URL 的对应关系,这样可以节省存储空间。

[0104] 相应地,请参照附图 6,为本申请提出的一种单点登录设备的结构示意图,该单点登录设备包括客户端处理单元 601、网页服务单元 602 和网页浏览器 603,其中,

[0105] 客户端处理单元 601,用于向网页服务单元 602 发送注册请求,以及在接收到对应的注册响应后向网络侧的免登服务器发送包含验证信息和注册响应中包含的本地 URL 的登录请求;

[0106] 网页服务单元 602,用于接收注册请求,确定与注册请求包含的目标网页 URL 唯一对应的本地 URL,并存储所述本地 URL 与目标网页 URL 的对应关系,向客户端处理单元 601 发送包含所述本地 URL 的注册响应,以及根据网页浏览器 603 发来的访问网页的请求消息,在确定存储有网页请求消息中的本地 URL 与目标页面 URL 的对应关系时,指示网页浏览器 603 访问对应的目标页面 URL;

[0107] 网页浏览器 603,用于根据网络侧的免登服务器基于登录请求中的验证信息对用户身份验证成功后发送的指示,向网页服务器 602 发送的包含本地 URL 的访问网页的请求消息,以及根据网页服务单元 602 的指示,向目标 URL 对应的网页服务器发送访问请求消息。

[0108] 上述单点登录设备可以位于用户的同一台计算机中,其组成部分也可以彼此独立位于多台计算机内或具有数据处理功能的设备内。

[0109] 对应地,本申请还提供了一种网络侧的免登服务器,请参照附图 7,该免登服务器包括接收单元 701、查找单元 702、确定单元 703、判断单元 704 和指示单元 705,其中,

[0110] 接收单元 701,用于接收上述单点登录设备发来的登录请求;

[0111] 查找单元 702,用于查找登录请求中包含的用户标识对应的密码;

[0112] 确定单元 703,用于按照与单点登录设备约定的方法,根据登录请求包含的用户标识和本地 URL,以及查找单元查找到的密码,获得服务器端验证信息;

[0113] 判断单元 704,用于判断确定单元 703 获得的服务器端验证信息与所述登录请求

中包含的验证信息是否一致；

[0114] 指示单元 705,用于在判断单元 704 判断出服务器端验证信息与登录请求中包含的验证信息一致时,指示与所述单点登录设备中的网页浏览器请求登录请求中包含的本地 URL,其中所述本地 URL 与用户要访问的目标页面 URL 唯一对应。

[0115] 为了描述的方便,描述以上系统时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和 / 或硬件中实现。

[0116] 显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

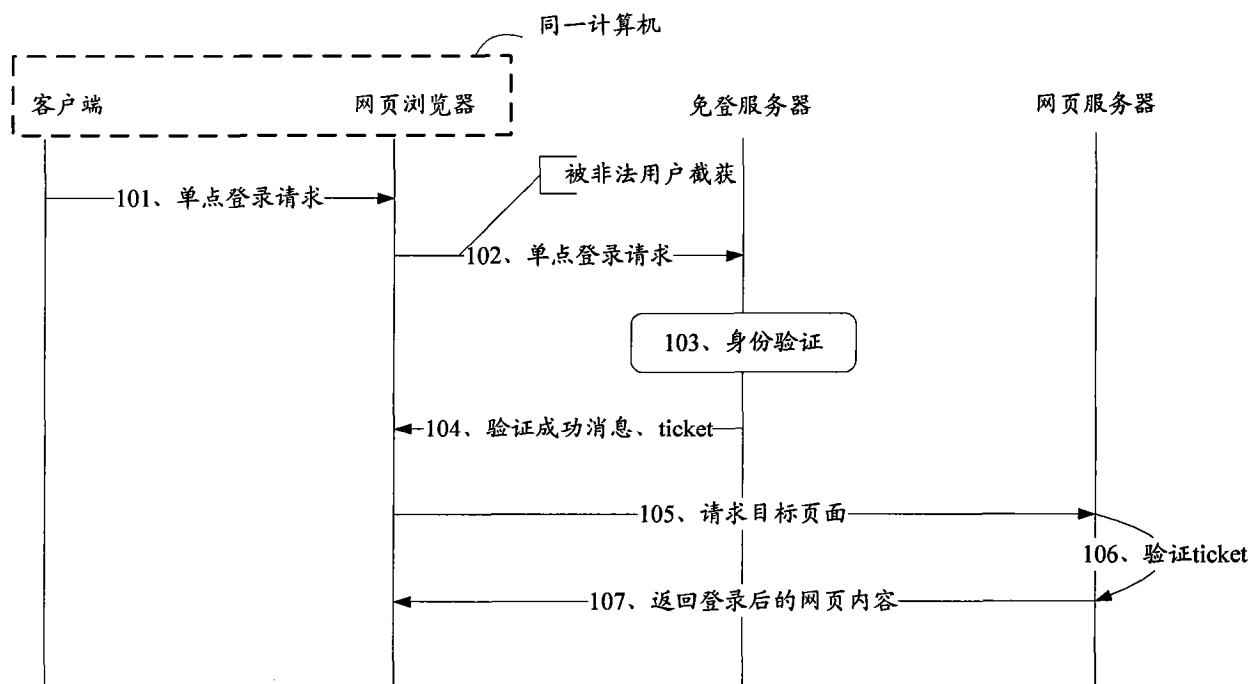


图 1

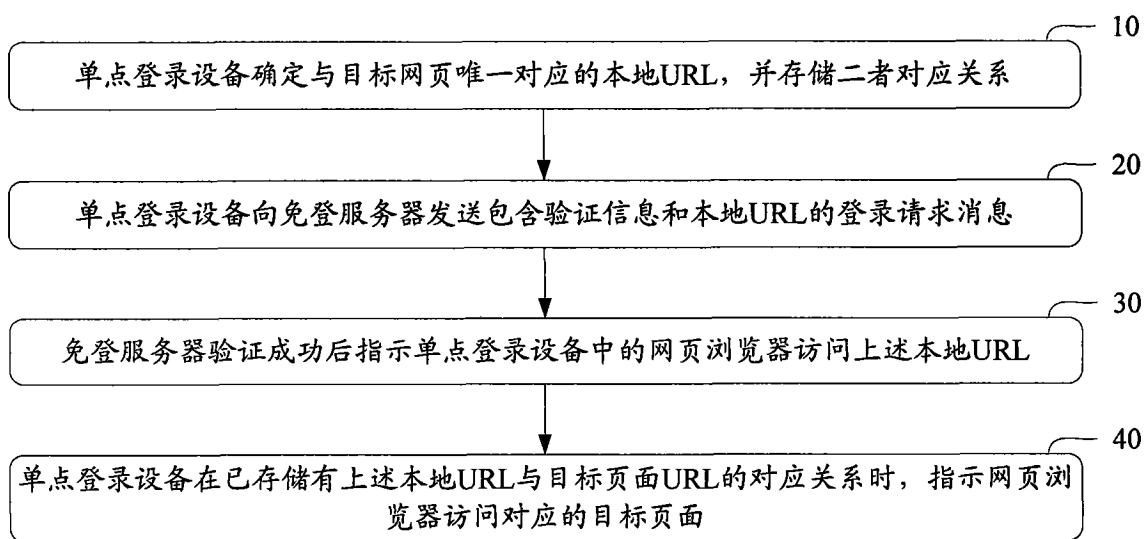


图 2

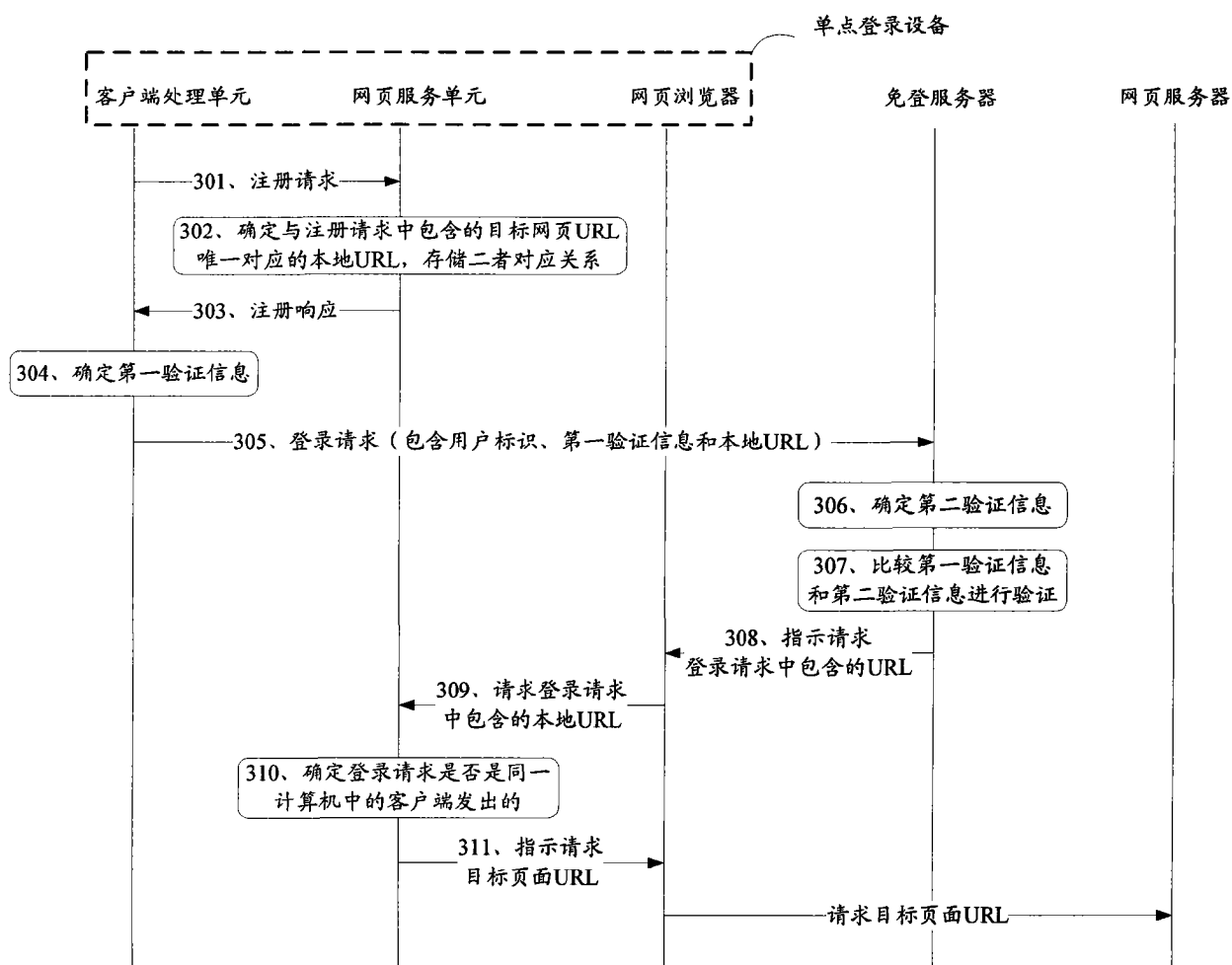


图 3

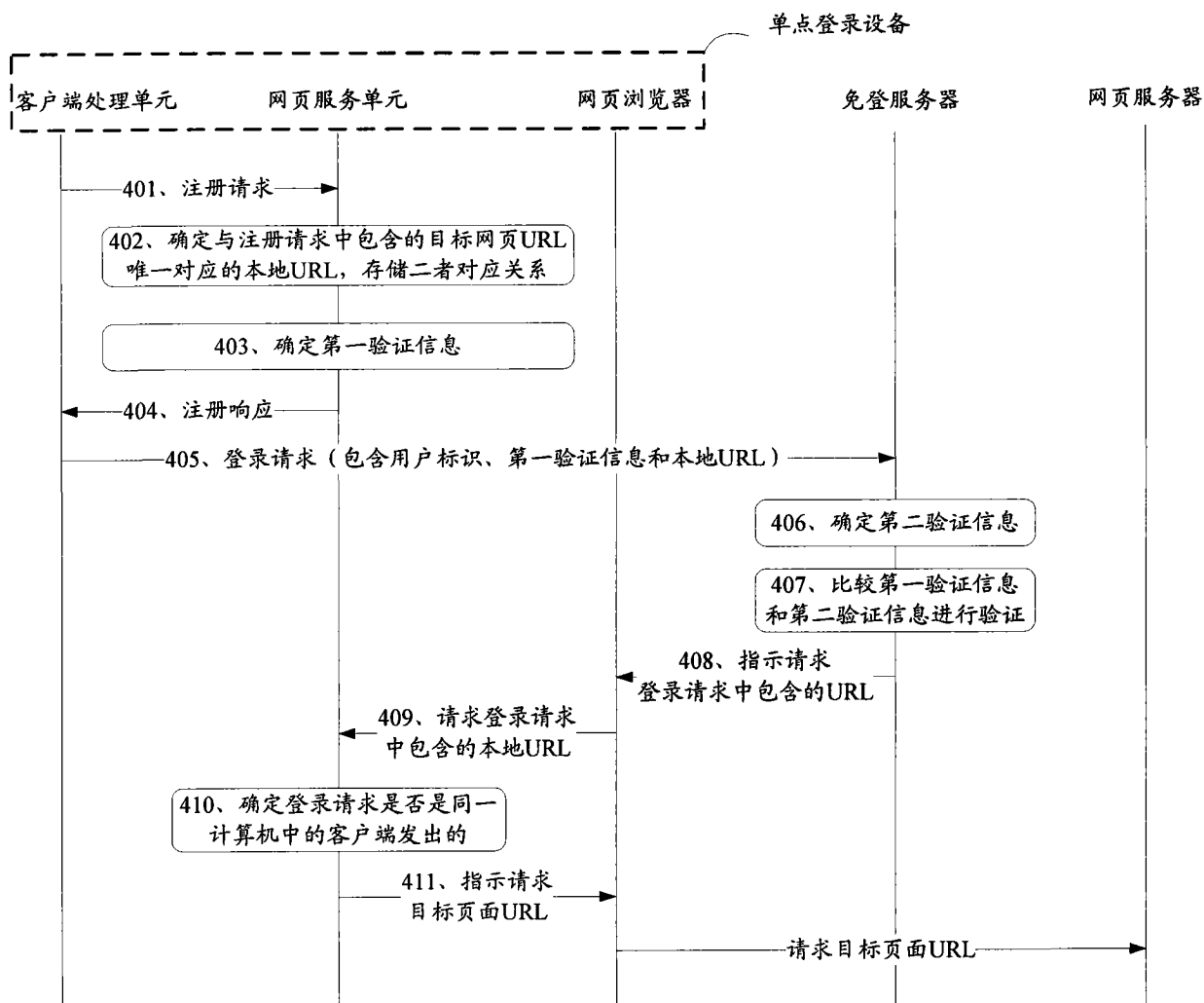


图 4

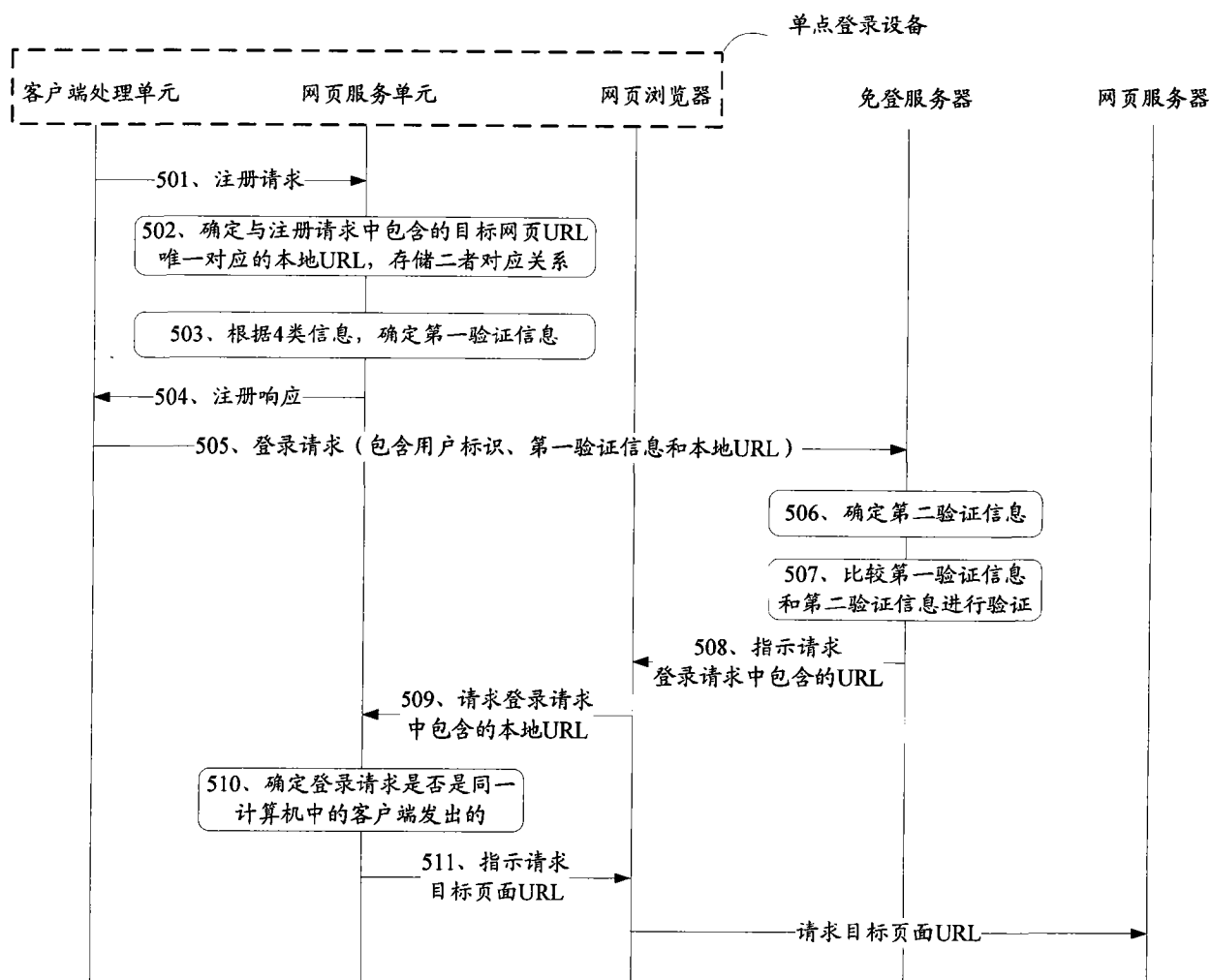


图 5

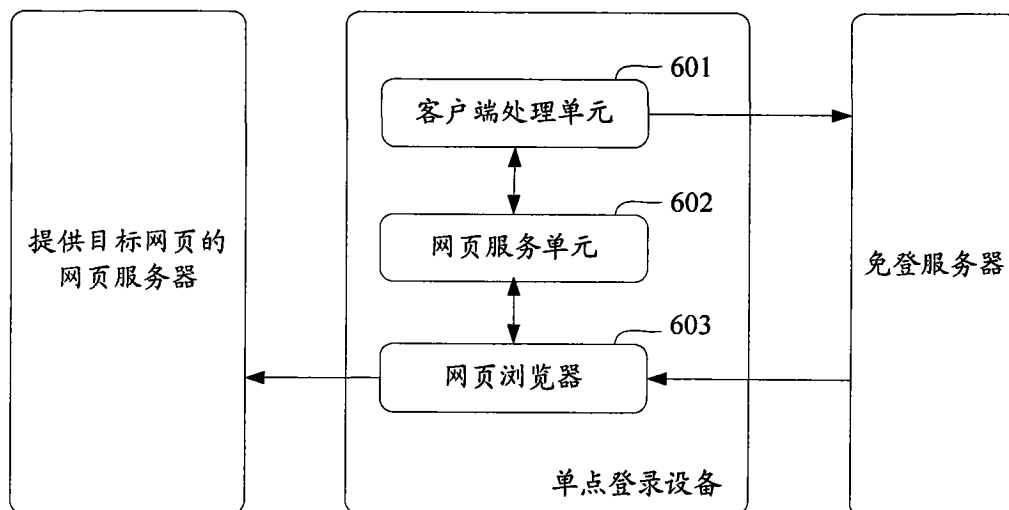


图 6

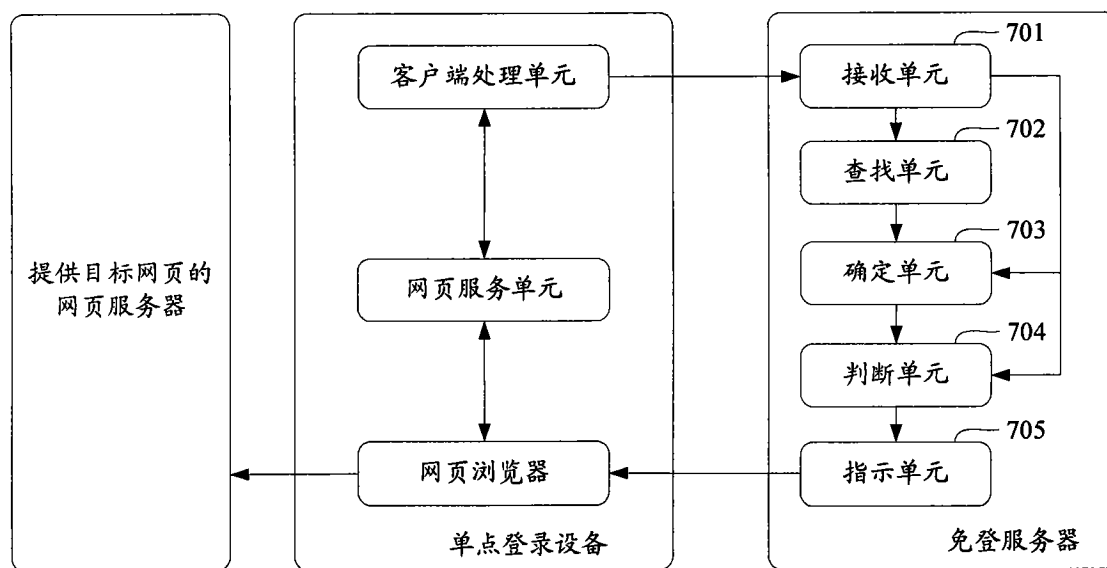


图 7