(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 109379193 B
(45)授权公告日 2021.06.29

(21)申请号 201811486989.6
(22)申请日 2018.12.06
(65)同一申请的已公布的文献号
申请公布号 CN 109379193 A
(43)申请公布日 2019.02.22
(73)专利权人 佛山科学技术学院
地址 528000 广东省佛山市南海区狮山镇仙溪水库西路佛山科学技术学院
(72)发明人 郑永旭 马莉 陈健聪 郑浩文 钟声远 蔡坚生 庄义炎
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 谢泳祥
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102739659 A,2012.10.17
CN 103179134 A,2013.06.26
CN 101060404 A,2007.10.24
CN 101252437 A,2008.08.27
US 7215781 B2,2007.05.08
US 2011196965 A1,2011.08.11

审查员 孙铭君

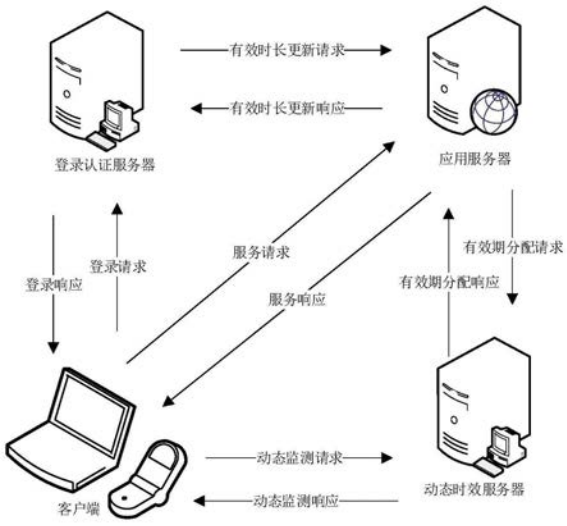
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种动态防重放攻击认证方法及装置

(57)摘要

本发明公开了一种动态防重放攻击认证方法及装置，通过采用多个安全等级的分级控制，统一在一个独立的有效期分配服务器中进行动态的有效期时间分配，且生成时间戳也在另一个独立的服务器中，保证了校验的准确性；确保用户的合法服务请求不被重放攻击的同时，也动态的确保了用户的合法服务请求的有效期得到了保障，确保了用户体验，保证了校验的准确性；确保用户的合法服务请求不被重放攻击的同时，也动态的确保了用户的合法服务请求的有效期得到了保障，提升了用户体验，保证了客户端与服务器端登录的安全性与稳定性。



CN 109379193 B

1.一种动态防重放攻击认证方法,其特征在于,所述方法包括以下步骤:

步骤1,客户端向登录认证服务器发送登录请求;

步骤2,登录认证服务器发送有效时长更新请求给应用服务器;

步骤3,应用服务器向动态时效服务器发送有效期分配请求;

步骤4,动态时效服务器发送有效期分配响应给应用服务器;

步骤5,应用服务器发送有效时长更新响应给登录认证服务器;

步骤6,登录认证服务器发送登录响应给客户端;

步骤7,客户端发送服务请求到应用服务器,同时发送动态监测请求给动态时效服务器,动态监测请求为判断开始计算登录成功的维持的持续时间;

步骤8,动态时效服务器发送认证判断请求给登录认证服务器,认证判断请求为判断应用服务器是否已经开始对客户端进行服务响应;

步骤9,登录认证服务器发送认证判断响应给动态时效服务器,认证判断响应为开始通过循环通过步骤4循环进行有效期的重新分配;

步骤10,动态时效服务器发送动态监测响应给客户端,动态监测响应为应用服务器开始从动态时效服务器中读取有效期;

步骤11,应用服务器对客户端服务请求的有效性进行判断并进行服务响应;

在步骤1中,登录请求包括,用户名字符串、密码字符串和客户端的安全等级,密码字符串为密码经过SHA256算法加密形成的字符串,客户端的安全等级包括:移动设备的安全等级为1级;平板电脑等级为2级;家庭台式电脑等级为3级;公共场所使用的终端机为3级;

在步骤4中,有效期分配响应为通过公式$T_{ava}=\sqrt{\frac{T_{now}{}^2-t_x{}^2}{2\sigma^2}}-t_y-\Delta t$计算有效期$T_{ava}$,式子中,$T_{now}$为当前时间,Δt为当前时间与时间戳的时间差,$t_x$为登录时间增量,$t_x$初始值为1,登录成功的维持的持续时间每增加10秒则t_x增加0.1;t_y为时间戳的时间;σ为客户端的安全等级,即客户端的安全等级包括:移动设备的安全等级为1级,σ=1,风险等级最低;平板电脑等级为2级,σ=2;家庭台式电脑等级为3级;公共场所使用的终端机为3级,σ=3。

2.根据权利要求1所述的一种动态防重放攻击认证方法,其特征在于,在步骤2中,有效时长更新请求为登录认证服务器生成,包括标识当前时间的时间戳和请求认证的用户名。

3.根据权利要求2所述的一种动态防重放攻击认证方法,其特征在于,在步骤3中,有效期分配请求为应用服务器传递的用户名和客户端的安全等级、当前时间与时间戳的时间差,当前时间与时间戳的时间差用于证明用户是否已经登录的认证凭据的正确性的判定结果。

4.根据权利要求2所述的一种动态防重放攻击认证方法,其特征在于,在步骤5中,有效时长更新响应为应用服务器根据存储的认证信息的正确性进行判断生成判定结果,认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串,判定结果用于证明用户是否已经登录。

5.根据权利要求1所述的一种动态防重放攻击认证方法,其特征在于,在步骤6中,登录响应为在登录认证服务器生成的认证凭据,该认证凭据包括标识当前时间的时间戳,还包括用于认证的校验码,以标识用户是否登录成功。

6.根据权利要求1所述的一种动态防重放攻击认证方法，其特征在于，在步骤7中，动态监测请求为判断开始计算登录成功的维持的持续时间，从应用服务器进行第一次的服务响应的时间开始计算，计算登录时间增量t_x，t_x初始值为1，登录成功的维持的持续时间每增加10秒则t_x增加0.1。

7.根据权利要求1所述的一种动态防重放攻击认证方法，其特征在于，在步骤11中，应用服务器对客户端服务请求的有效性进行判断并进行服务响应为，应用服务器动态时效服务器中实时的读取有效期，这样保证了在登录认证服务器中不断的调整动态时效服务器分配的有效期的值，通过判断认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串的正确性，若服务请求在有效期内认证成功，则应用服务器进行服务响应。

一种动态防重放攻击认证方法及装置

技术领域

[0001] 本公开涉及信息安全技术领域,具体涉及一种动态防重放攻击认证方法及装置。

背景技术

[0002] 在现有的重放攻击防御技术中,为避免服务器遭受重放攻击,一般采用基于时间判断的防御机制,而为了保证不同服务器直接能识别接收到的消息是否过期,一般采用基于时间戳的方法,而基于时间戳的方法包括在客户端生成时间戳、在服务器端生成时间戳和由登录认证服务器生产时间戳三种方式,虽然在服务器端生成时间戳和由登录认证服务器生产时间戳都能提升安全性防御重放攻击,但是由于有效期是固定的时间,虽然在通过单向数据链时提升安全性,在校验认证凭证时无论采用哪一种方式的有效期依然是以这个时间戳比较,如果重放攻击的频率小于有效期则依然存在安全隐患,而且有效期过短会产生其他的问题,例如一段时间不操作,session的访问有效期很快就过期了,由于有效期的时间过短,导致了要反复的输入密码重新进行登录验证等访问操作不便的用户体验问题。

发明内容

[0003] 本公开提供一种动态防重放攻击认证方法及装置,通过采用多个安全等级的分级控制,统一在一个独立的有效期分配服务器中进行动态的有效期时间分配,且生成时间戳也在另一个独立的服务器中,保证了校验的准确性;确保用户的合法服务请求不被重放攻击的同时,也动态的确保了用户的合法服务请求的有效期得到了保障,确保了用户体验。

[0004] 为了实现上述目的,根据本公开的一方面,提供一种动态防重放攻击认证方法,所述方法包括以下步骤:

[0005] 步骤1,客户端向登录认证服务器发送登录请求;

[0006] 步骤2,登录认证服务器发送有效时长更新请求给应用服务器;

[0007] 步骤3,应用服务器向动态时效服务器发送有效期分配请求;

[0008] 步骤4,动态时效服务器发送有效期分配响应给应用服务器;

[0009] 步骤5,应用服务器发送有效时长更新响应给登录认证服务器;

[0010] 步骤6,登录认证服务器发送登录响应给客户端;

[0011] 步骤7,客户端发送服务请求到应用服务器,同时发送动态监测请求给动态时效服务器;

[0012] 步骤8,动态时效服务器发送认证判断请求给登录认证服务器;

[0013] 步骤9,登录认证服务器发送认证判断响应给动态时效服务器;

[0014] 步骤10,动态时效服务器发送动态监测响应给客户端;

[0015] 步骤11,应用服务器对客户端服务请求的有效性进行判断并进行服务响应。

[0016] 进一步地,在步骤1中,登录请求包括,用户名字符串、密码字符串和客户端的安全等级,密码字符串为密码经过SHA256算法加密形成的字符串,客户端的安全等级包括:移动设备的安全等级为1级,风险等级最低;平板电脑等级为2级;家庭台式电脑等级为3级;公共

场所使用的终端机为3级，风险等级最高，获取客户端的安全等级方式为人工选择、管理员指定登录IP或自动识别任意一种方法。

[0017] 进一步地，在步骤2中，有效时长更新请求为登录认证服务器生成，包括标识当前时间的时间戳和请求认证的用户名。

[0018] 进一步地，在步骤3中，有效期分配请求为应用服务器传递的用户名和客户端的安全等级、当前时间与时间戳的时间差，当前时间与时间戳的时间差用于证明用户是否已经登录的认证凭据的正确性的判定结果。

[0019] 进一步地，在步骤4中，有效期分配响应为通过公式$T_{\text{ava}}=\sqrt{\frac{T_{now}{}^{2}-t_{x}{}^{2}}{2\sigma^{2}}}-t_{y}-\Delta t$计算有效期$T_{ava}$，式子中，$T_{now}$为当前时间，Δt为当前时间与时间戳的时间差，$t_x$为登录时间增量，$t_x$初始值为1，登录成功的维持的持续时间每增加10秒则t_x增加0.1；t_y为时间戳的时间；σ为客户端的安全等级，即客户端的安全等级包括：移动设备的安全等级为1级，σ＝1，风险等级最低；平板电脑等级为2级，σ＝2；家庭台式电脑等级为3级；公共场所使用的终端机为3级，σ＝3。

[0020] 进一步地，在步骤5中，有效时长更新响应为应用服务器根据存储的认证信息的正确性进行判断生成判定结果，认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串，判定结果用于证明用户是否已经登录。

[0021] 进一步地，在步骤6中，登录响应为在登录认证服务器生成的认证凭据，该认证凭据包括标识当前时间的时间戳，还包括用于认证的校验码，以标识用户是否登录成功。

[0022] 进一步地，在步骤7中，动态监测请求为判断开始计算登录成功的维持的持续时间，从应用服务器进行第一次的服务响应的时间开始计算，计算登录时间增量t_x，t_x初始值为1，登录成功的维持的持续时间每增加10秒则t_x增加0.1。

[0023] 进一步地，在步骤8中，认证判断请求为判断应用服务器是否已经开始对客户端进行服务响应。

[0024] 进一步地，在步骤9中，认证判断响应为开始通过循环通过步骤4循环进行有效期的重新分配。

[0025] 进一步地，在步骤10中，动态监测响应为应用服务器开始从动态时效服务器中读取有效期。

[0026] 进一步地，在步骤11中，应用服务器对客户端服务请求的有效性进行判断并进行服务响应为，应用服务器动态时效服务器中实时的读取有效期，这样保证了在登录认证服务器中不断的调整动态时效服务器分配的有效期的值，通过判断认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串的正确性，若服务请求在有效期内认证成功，则应用服务器进行服务响应。这样即使窃听者通过统计出了当前的服务的有效期值，但是有效期值一直在变化，从而无法推导出最新的效期值，无法确定重放攻击的频率，导致服务器的访问有效期很容易就过期了，从而避免了重放攻击。

[0027] 本发明还提供了一种动态防重放攻击认证装置，所述装置包括：存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序运行在以下装置的单元中：

[0028] 登录请求单元，用于客户端向登录认证服务器发送登录请求；

[0029] 有效时长更新请求单元，用于登录认证服务器发送有效时长更新请求给应用服务器；

[0030] 有效期分配请求单元，用于应用服务器向动态时效服务器发送有效期分配请求；

[0031] 有效期分配响应单元，用于动态时效服务器发送有效期分配响应给应用服务器；

[0032] 有效时长更新响应单元，用于应用服务器发送有效时长更新响应给登录认证服务器；

[0033] 登录响应单元，用于登录认证服务器发送登录响应给客户端；

[0034] 服务与动态监测请求单元，用于客户端发送服务请求到应用服务器，同时发送动态监测请求给动态时效服务器；

[0035] 认证判断请求单元，用于动态时效服务器发送认证判断请求给登录认证服务器；

[0036] 认证判断响应单元，用于登录认证服务器发送认证判断响应给动态时效服务器；

[0037] 动态监测响应单元，用于动态时效服务器发送动态监测响应给客户端；

[0038] 服务响应单元，用于应用服务器对客户端服务请求的有效性进行判断并进行服务响应。

[0039] 本公开的有益效果为：本发明提供一种动态防重放攻击认证方法及装置，保证了校验的准确性；确保用户的合法服务请求不被重放攻击的同时，也动态的确保了用户的合法服务请求的有效期得到了保障，提升了用户体验，保证了客户端与服务器端登录的安全性与稳定性。

附图说明

[0040] 通过对结合附图所示出的实施方式进行详细说明，本公开的上述以及其他特征将更加明显，本公开附图中相同的参考标号表示相同或相似的元素，显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图，在附图中：

[0041] 图1所示为一种动态防重放攻击认证方法的流程图；

[0042] 图2所示为一种动态防重放攻击认证装置图。

具体实施方式

[0043] 以下将结合实施例和附图对本公开的构思、具体结构及产生的技术效果进行清楚、完整的描述，以充分地理解本公开的目的、方案和效果。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0044] 如图1所示为根据本公开的一种动态防重放攻击认证方法的流程图，下面结合图1来阐述根据本公开的实施方式的一种动态防重放攻击认证方法。

[0045] 本公开提出一种动态防重放攻击认证方法，具体包括以下步骤：

[0046] 步骤1，客户端向登录认证服务器发送登录请求；

[0047] 步骤2，登录认证服务器发送有效时长更新请求给应用服务器；

[0048] 步骤3，应用服务器向动态时效服务器发送有效期分配请求；

[0049] 步骤4，动态时效服务器发送有效期分配响应给应用服务器；

[0050] 步骤5，应用服务器发送有效时长更新响应给登录认证服务器；

[0051] 步骤6，登录认证服务器发送登录响应给客户端；

[0052] 步骤7，客户端发送服务请求到应用服务器，同时发送动态监测请求给动态时效服务器；

[0053] 步骤8，动态时效服务器发送认证判断请求给登录认证服务器；

[0054] 步骤9，登录认证服务器发送认证判断响应给动态时效服务器；

[0055] 步骤10，动态时效服务器发送动态监测响应给客户端；

[0056] 步骤11，应用服务器对客户端服务请求的有效性进行判断并进行服务响应。

[0057] 进一步地，在步骤1中，登录请求包括，用户名字符串、密码字符串和客户端的安全等级，密码字符串为密码经过SHA256算法加密形成的字符串，客户端的安全等级包括：移动设备的安全等级为1级，风险等级最低；平板电脑等级为2级；家庭台式电脑等级为3级；公共场所使用的终端机为3级，风险等级最高，获取客户端的安全等级方式为人工选择、管理员指定登录IP或自动识别任意一种方法。

[0058] 进一步地，在步骤2中，有效时长更新请求为登录认证服务器生成，包括标识当前时间的时间戳和请求认证的用户名。

[0059] 进一步地，在步骤3中，有效期分配请求为应用服务器传递的用户名和客户端的安全等级、当前时间与时间戳的时间差，当前时间与时间戳的时间差用于证明用户是否已经登录的认证凭据的正确性的判定结果。

[0060] 进一步地，在步骤4中，有效期分配响应为通过公式$T_{\text{ava}}=\sqrt{\frac{T_{now}{}^{2}-t_{x}{}^{2}}{2\sigma^{2}}}-t_{y}-\Delta t$计算有效期$T_{ava}$，式子中，$T_{now}$为当前时间，Δt为当前时间与时间戳的时间差，$t_x$为登录时间增量，$t_x$初始值为1，登录成功的维持的持续时间每增加10秒则t_x增加0.1；t_y为时间戳的时间；σ为客户端的安全等级，即客户端的安全等级包括：移动设备的安全等级为1级，σ＝1，风险等级最低；平板电脑等级为2级，σ＝2；家庭台式电脑等级为3级；公共场所使用的终端机为3级，σ＝3。

[0061] 进一步地，在步骤5中，有效时长更新响应为应用服务器根据存储的认证信息的正确性进行判断生成判定结果，认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串，判定结果用于证明用户是否已经登录。

[0062] 进一步地，在步骤6中，登录响应为在登录认证服务器生成的认证凭据，该认证凭据包括标识当前时间的时间戳，还包括用于认证的校验码，以标识用户是否登录成功。

[0063] 进一步地，在步骤7中，动态监测请求为判断开始计算登录成功的维持的持续时间，从应用服务器进行第一次的服务响应的时间开始计算，计算登录时间增量t_x，t_x初始值为1，登录成功的维持的持续时间每增加10秒则t_x增加0.1。

[0064] 进一步地，在步骤8中，认证判断请求为判断应用服务器是否已经开始对客户端进行服务响应。

[0065] 进一步地，在步骤9中，认证判断响应为开始通过循环通过步骤4循环进行有效期的重新分配。

[0066] 进一步地，在步骤10中，动态监测响应为应用服务器开始从动态时效服务器中读取有效期。

[0067] 进一步地，在步骤11中，应用服务器对客户端服务请求的有效性进行判断并进行

服务响应为，应用服务器动态时效服务器中实时的读取有效期，这样保证了在登录认证服务器中不断的调整动态时效服务器分配的有效期的值，通过判断认证信息为用户名字符串、密码字符串经过SHA256算法解密形成的字符串的正确性，若服务请求在有效期内认证成功，则应用服务器进行服务响应。这样即使窃听者通过统计出了当前的服务的有效期值，但是有效期值一直在变化，从而无法推导出最新的效期值，无法确定重放攻击的频率，导致服务器的访问有效期很容易就过期了，从而避免了重放攻击。

[0068] 本公开的实施例提供的一种动态防重放攻击认证装置，如图2所示为本公开的一种动态防重放攻击认证装置图，该实施例的一种动态防重放攻击认证装置包括：处理器、存储器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述一种动态防重放攻击认证装置实施例中的步骤。

[0069] 所述装置包括：存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序运行在以下装置的单元中：

[0070] 登录请求单元，用于客户端向登录认证服务器发送登录请求；

[0071] 有效时长更新请求单元，用于登录认证服务器发送有效时长更新请求给应用服务器

[0072] 有效期分配请求单元，用于应用服务器向动态时效服务器发送有效期分配请求；

[0073] 有效期分配响应单元，用于动态时效服务器发送有效期分配响应给应用服务器；

[0074] 有效时长更新响应单元，用于应用服务器发送有效时长更新响应给登录认证服务器；

[0075] 登录响应单元，用于登录认证服务器发送登录响应给客户端；

[0076] 服务与动态监测请求单元，用于客户端发送服务请求到应用服务器，同时发送动态监测请求给动态时效服务器；

[0077] 认证判断请求单元，用于动态时效服务器发送认证判断请求给登录认证服务器；

[0078] 认证判断响应单元，用于登录认证服务器发送认证判断响应给动态时效服务器；

[0079] 动态监测响应单元，用于动态时效服务器发送动态监测响应给客户端；

[0080] 服务响应单元，用于应用服务器对客户端服务请求的有效性进行判断并进行服务响应。

[0081] 所述一种动态防重放攻击认证装置可以运行于桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备中。所述一种动态防重放攻击认证装置，可运行的装置可包括，但不仅限于，处理器、存储器。本领域技术人员可以理解，所述例子仅仅是一种动态防重放攻击认证装置的示例，并不构成对一种动态防重放攻击认证装置的限定，可以包括比例子更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述一种动态防重放攻击认证装置还可以包括输入输出设备、网络接入设备、总线等。

[0082] 所称处理器可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等，所述处理器是所述一种动态防重放攻击认证装置运行装置的控制中心，利用各种接口

和线路连接整个一种动态防重放攻击认证装置可运行装置的各个部分。

[0083] 所述存储器可用于存储所述计算机程序和/或模块，所述处理器通过运行或执行存储在所述存储器内的计算机程序和/或模块，以及调用存储在存储器内的数据，实现所述一种动态防重放攻击认证装置的各种功能。所述存储器可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等；存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本等)等。此外，存储器可以包括高速随机存取存储器，还可以包括非易失性存储器，例如硬盘、内存、插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0084] 尽管本公开的描述已经相当详尽且特别对几个所述实施例进行了描述，但其并非旨在局限于任何这些细节或实施例或任何特殊实施例，而是应当将其视作是通过参考所附权利要求考虑到现有技术为这些权利要求提供广义的可能性解释，从而有效地涵盖本公开的预定范围。此外，上文以发明人可预见的实施例对本公开进行描述，其目的是为了提供有用的描述，而那些目前尚未预见的对本公开的非实质性改动仍可代表本公开的等效改动。

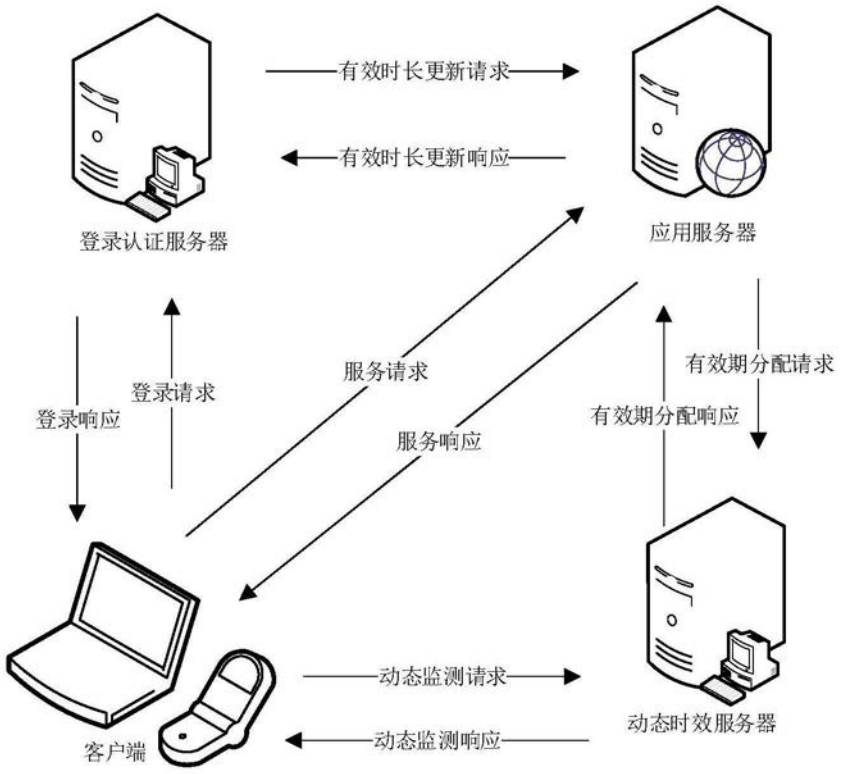

有效时长更新请求
有效时长更新响应
登录认证服务器
应用服务器
登录响应
登录请求
服务请求
服务响应
有效期分配请求
有效期分配响应
客户端
动态监测请求
动态监测响应
动态时效服务器

图1

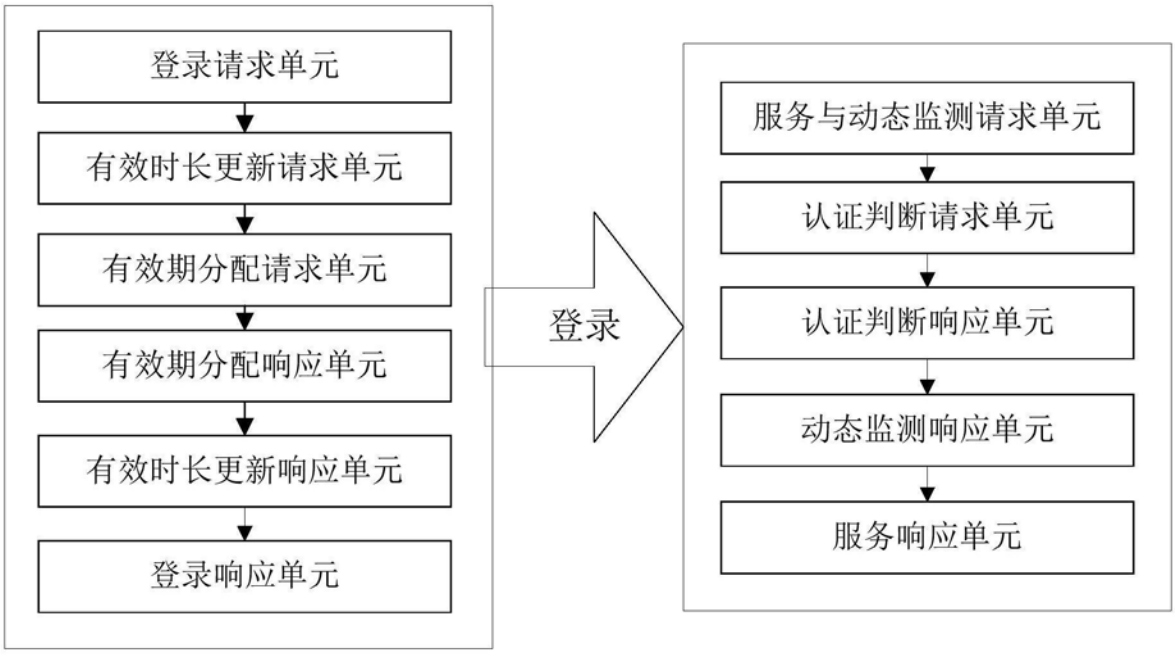

登录请求单元
有效时长更新请求单元
有效期分配请求单元
有效期分配响应单元
有效时长更新响应单元
登录响应单元
登录
服务与动态监测请求单元
认证判断请求单元
认证判断响应单元
动态监测响应单元
服务响应单元

图2