(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 101800983 A
(43)申请公布日 2010.08.11

(21)申请号 201010017649.6

(22)申请日 2010.01.12

(71)申请人 南京烽火星空通信发展有限公司
地址 210019 江苏省南京市建邺区云龙山路88号烽火大厦A座20层

(72)发明人 刘国俭 王娜

(74)专利代理机构 南京苏科专利代理有限责任公司 32102
代理人 何朝旭

(51)Int.Cl.
H04W 12/06(2009.01)
H04W 12/08(2009.01)
H04W 60/00(2009.01)
H04W 88/02(2009.01)

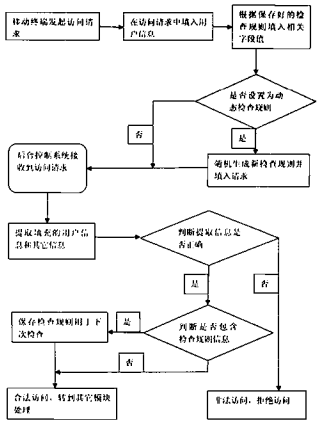
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种可配置的移动终端的访问控制方法

(57)摘要

本发明涉及一种控制移动终端访问信息系统的控制方法，属于通信安全技术领域。该方法在由移动终端和后台访问控制系统构成的无线网络中，通过在后台访问控制系统注册移动终端信息，形成移动终端注册信息；在后台访问控制系统设置需要进行检查的注册移动终端信息，并建立检查规则；将检查规则同步发送到对应的移动终端；移动终端在发出访问请求时，根据检查规则添加相应的移动终端信息；后台访问控制系统接收到访问请求后，从中提取需检查的移动终端信息，按检查规则与移动终端注册信息逐一比对，从而决定是否允许访问。采用本发明后，可以对访问请求进行精确识别控制，有效减少非法及伪造访问，确保信息系统安全。



CN 101800983 A

1. 一种可配置的移动终端的访问控制方法，在由移动终端和后台访问控制系统构成的无线网络中，访问控制步骤如下：

A、在后台访问控制系统注册移动终端信息，形成移动终端注册信息；

B、在后台访问控制系统设置需要进行检查的移动终端注册信息，建立检查规则并存储；

C、后台访问控制系统将检查规则同步发送到对应的移动终端保存；

D、移动终端在向后台访问控制系统发出访问请求时，根据保存的检查规则，在访问请求中自动添加相应的移动终端信息；

E、后台访问控制系统接收到移动终端发送的访问请求后，从中提取需检查的移动终端信息，按存储的检查规则，与移动终端注册信息逐一比对检查；

F、如存在与发送来的移动终端信息相同的移动终端注册信息，则确认该请求合法，允许访问；否则确认该请求非法，拒绝访问。

2. 根据权利要求 1 所述的可配置的移动终端访问控制方法，其特征在于：在所述步骤 D 中，移动终端在向后台访问控制系统发出访问请求时，还随机生成新检查规则，取代原保存的检查规则，并将新检查规则加入访问请求一并发送给后台访问控制系统；

所述步骤 F 之后，后台访问控制系统还从接收到移动终端发送的访问请求中提取新的检查规则，取代原存储的检查规则，用于下一次检查。

3. 根据权利要求 2 所述的可配置的移动终端访问控制方法，其特征在于：所述步骤 A 中，移动终端注册信息包含用户自定义信息；所述步骤 C 中，后台访问控制系统还同步发送自定义信息的字段值到相应移动终端上保存；所述步骤 D 中，移动终端还从后台访问控制系统同步得到的相应自定义信息字段值中添加到访问请求中。

4. 根据权利要求 2 所述的可配置的移动终端访问控制方法，其特征在于：所述步骤 C 中，后台访问控制系统还发送动态设置要求信息到移动终端；所述步骤 D 中，移动终端根据动态设置要求信息，随机生成新检查规则。

5. 根据权利要求 3 或 4 所述的可配置的移动终端访问控制方法，其特征在于：所述步骤 F 中，后台访问控制系统拒绝存在多余字段移动终端信息的访问请求。

一种可配置的移动终端的访问控制方法

技术领域

[0001] 本发明涉及一种控制移动终端访问信息系统的控制方法，尤其是一种基于移动终端信息的访问控制方法，属于通信安全技术领域。

背景技术

[0002] 随着信息科技的发展，办公信息化软件、ERP 软件、CRM 软件等得到了广泛的应用。并且随着信息化系统的不断广泛应用并作为工作中的重要支撑平台，能够随时随地访问内部信息系统成了新的应用需求。而移动通信技术的不断发展使得将有线网络环境下的信息化系统扩展到无线网络中成为可能，借助移动通信网络的可移动性、快捷性，可以把已有的信息系统延伸到无线网络环境中，并利用手机、PDA 等移动终端来与现有的信息系统随时随地进行访问。

[0003] 在使用手机等终端设备通过移动网络访问信息系统时，有可能使原本只开放给内部使用的信息系统暴露出来，因此需要考虑阻止非法访问入侵，并要求有效降低服务器的负荷来提供更多的负载能力。同时，由于手机等终端访问具有便捷性和广泛性，因此需要更加精准的访问控制方法来控制访问请求。

[0004] 公开号为 CN101163336 的中国专利提供了“一种手机终端访问权限认证的实现方法”。该发明提供了一种通过三元访问控制策略对手机终端的终端类型，终端号码和目标 URL 进行组合访问控制的方法。但是此发明不能有效的防御恶意访问，例如在手机模拟器上或者 PC 上模拟终端类型，终端号码来伪造访问请求从而实现对目标 URL 的非法访问。而针对特定的移动信息化系统，需要更为精准的认证方法来控制访问请求从而确保系统安全和信息安全。

发明内容

[0005] 本发明的目的在于：提供一种可配置的移动终端访问控制方法，该方法不仅便于实施，并且能够和其它信息化系统集成用于防范非法访问，从而有效保护系统安全和降低系统负荷。

[0006] 为了达到以上目的，本发明可配置的移动终端访问控制方法在由移动终端和后台访问控制系统构成的无线网络中，访问控制步骤如下：

[0007] A、在后台访问控制系统注册移动终端信息，形成移动终端注册信息，所述移动终端信息包括但不限于终端用户信息（例如用户名）、终端自身信息（例如：手机号码、电子序列号 --ESN、国际移动通讯设备识别号 --IMSI、终端操作系统型号、终端制造商，以及其他有关信息（例如终端所带蓝牙的物理地址等）。

[0008] B、在后台访问控制系统设置需要进行检查的移动终端注册信息（例如手机号码、ESN、蓝牙物理地址信息），建立检查规则并存储（例如可以设置手机号码、蓝牙物理地址为必须按序检查的信息）。

[0009] C、后台访问控制系统将检查规则同步发送到对应的移动终端保存。

[0010] D、移动终端在向后台访问控制系统发出访问请求时，根据保存的检查规则，在访问请求中自动添加相应的移动终端信息（例如，在访问请求中按序添加手机号码、蓝牙物理地址信息）。

[0011] E、后台访问控制系统接收到移动终端发送的访问请求后，从中提取需检查的移动终端信息，按存储的检查规则，与移动终端注册信息逐一比对（例如将手机号码和蓝牙物理地址与与已经注册的相应信息进行对比）检查。

[0012] F、如存在与发送来的移动终端信息相同的移动终端注册信息，则确认该访问请求合法，允许访问；否则确认该请求非法，拒绝访问；必要时将该请求转到其它模块进行处理。

[0013] 至此，后台访问控制系统可以根据设定好的检查规则对移动终端的访问请求进行检查。由于发起请求的过程对用户透明，用户不能修改填充到请求中的物理信息，因此可以有效防止非法或者伪造的访问请求。在此基础上，为了更进一步特绝非法或者伪造的访问请求，本发明进一步的完善为：

[0014] 在上述步骤 D 中，移动终端在向后台访问控制系统发出访问请求时，还随机生成新检查规则，取代原保存的检查规则，并将新检查规则加入访问请求一并发送给后台访问控制系统。

[0015] 在上述步骤 F 之后，后台访问控制系统还从接收到移动终端发送的访问请求中提取新的检查规则，取代原存储的检查规则，用于下一次检查。

[0016] 这样，原先固定不变的静态检查规则成为了不断更新的动态检查规则，由于随机产生的检查规则每次都不尽相同，既每次后台访问控制系统都以新的检查规则进行检查，从而使得伪造访问请求的难度进一步大大增加，从而可以更改好的抵御伪造的非法访问请求。

[0017] 综上所述，采用本发明的可配置的移动终端访问控制方法，可以通过对对用户注册的移动终端信息的认证，达到对访问请求的精确识别控制，有效减少非法访问，确保信息系统安全。并且本发明还提供了可以进行动态配置，对访问请求进行检查的检查规则，从而进一步杜绝了通过伪造信息非法访问的可能，有效保护了信息安全。

附图说明

[0018] 下面结合附图对本发明作进一步的说明。

[0019] 图 1 为本发明后台访问控制系统注册终端信息和设置检查规则示意图。

[0020] 图 2 为作为本发明实施例一的移动终端和后台访问控制系统交互示意图。

[0021] 图 3 为作为本发明实施例二的设置动态检查后移动终端和后台访问控制系统交互示意图。

具体实施方式

[0022] 实施例一

[0023] 本实施例可配置的移动终端访问控制方法在由移动终端和后台访问控制系统构成的无线网络中，后台访问控制系统注册移动终端信息、设置检查规则的具体过程（访问控制）如下：

[0024] A、在后台访问控制系统注册移动终端信息，形成移动终端注册信息。

[0025] 后台访问控制系统提供一个管理界面进行移动终端信息注册，注册信息包括用户信息，以及该用户对应的移动终端的信息。例如：注册用户名为张三，其对应的移动终端信息包括手机号码 137XXX45678、手机操作系统为 SYMBIAN、电子序列号为 12345678、国际移动通讯设备识别号为 1234567890。此外，还可以添加用户自定义信息，例如自定义信息一为“ABCD”。最终依这些注册信息形成该移动终端注册信息。

[0026] B、在后台访问控制系统设置需要进行检查的移动终端注册信息，建立检查规则并存储。

[0027] 信息注册完后，后台访问控制系统设置需要检查的注册好的移动终端注册信息。例如设置手机号码、电子序列号和自定义信息一为需要进行检查的信息字段。接着，根据设置好的需要检查的字段生成检查规则，检查规则包括检查顺序、注册信息数量等，并存储到后台访问控制系统的存储单元。

[0028] C、后台访问控制系统将检查规则同步发送到对应的移动终端保存。

[0029] 后台访问控制系统在建立检查规则后，按照预定格式同步发送到该移动终端保存，用于该移动终端以后与后台访问控制系统的交互。

[0030] 对于存在用户自定义信息（即需要检查的信息字段）的移动终端，后台访问控制系统还同步发送自定义信息的字段值到该移动终端上保存，便于以后使用。（以上过程参见图 1）

[0031] D、移动终端在向后台访问控制系统发出访问请求时，根据保存的检查规则，在访问请求中添加相应的移动终端信息。

[0032] 移动终端通过客户端程序向后台访问控制系统发起访问请求时，根据从后台访问控制系统获得并保存的检查规则，在发送请求中自动从该移动终端获取添加填入需要的信息（例如填入检查规则中需要检查的手机号码、电子序列号等）。如检查规则中存在用户自定义信息的检查，则从后台访问控制系统同步得到的相应自定义信息字段值添加到访问请求中。同时，发起的访问请求中应包含用户信息（例如用户名）。该客户端程序发起请求的过程对用户透明，用户不能够修改填充到请求中的物理信息。

[0033] E、后台访问控制系统接收到移动终端发送的访问请求后，从中提取需检查的移动终端信息，按存储的检查规则，与移动终端注册信息逐一比对检查。

[0034] 后台访问控制控制系统在接收到访问请求后，首先从访问请求中提取用户信息和其它信息，同时按照已经存储的检查规则对提取到的信息进行检查。例如首先检查用户名张三，该用户存在后，则根据提取到的其它信息与存储的该移动终端注册信息进行对比检查。按照前面举例，检查手机号码、电子序列号以及用户自定义信息一的字段值。

[0035] F、如存在与发送来的移动终端信息相同的移动终端注册信息，则确认该请求合法，允许访问；否则确认该请求非法，拒绝访问。

[0036] 只有对比结果完全相同，才认为合法，允许访问。只要有一个检查字段信息不符，则拒绝该访问请求。包括需要检查的字段信息都与移动终端注册信息一致，但是提取到多余的字段信息，也认为该访问请求非法，拒绝此访问请求。（以上过程参见图 2）

[0037] 后台访问控制系统的检查结果为合法，则把此访问请求转到其它模块进行下一步处理，否则直接拒绝该访问请求。

[0038] 实施例二

[0039] 本实施例的移动终端访问控制过程如图 3 所示，后台访问控制系统进一步可以动态设置检查规则，用于终端和后台访问控制系统交互，与实施例一相比，有如下主要改变：

[0040] 在后台访问控制系统完成终端信息注册并第一次设定检查规则之，进入步骤 C 时，后台访问控制系统将检查规则同步发送到对应的移动终端保存，同时还发送动态设置要求信息，此信息会和设定好的检查规则一起同步到移动终端。

[0041] 在上述步骤 D 中，移动终端在向后台访问控制系统发出访问请求时，还根据动态设置要求信息，随机生成新检查规则，取代原保存的检查规则，并将新检查规则加入访问请求一并发送给后台访问控制系统。例如当前检查规则是手机号码、电子序列号以及自定义信息一，移动终端需要在访问请求中填入对应的字段值，同时移动终端根据动态设置要求信息，随机生成新的检查规则，例如新的检查规则为只检查自定义信息一，并把此检查规则填入访问请求，并将此检查规则保存到移动终端上，用于下一次请求。

[0042] 后台访问控制系统在接收到终端请求之后，首先按照已经存储的检查规则对该访问请求进行检查，如果检查通过，则提取其中包含的新的检查规则，取代原先存储的检查规则，用于下一次检查。

[0043] 移动终端在下一次访问请求中，会根据前一次随机生成的并保存的新的检查规则填入相应的待检查信息，同时再次生成更新的检查规则并保存。而后台访问控制系统则根据当前存储的检查规则对访问请求进行检查，同时提取出更新的检查规则并存储用于再下一次检查。

[0044] 本实施例通过设置动态检查规则，终端访问请求中包含的检查信息每次都不相同。例如后台访问控制系统有 10 个注册好的检查字段，通过设置动态检查规则，即使检查字段的值被泄露用于伪造访问请求，由于有了动态检查规则的屏障，伪造合法访问请求的难度会进一步大大增加。

[0045] 总之，通过以上各步骤和判断识别，本发明可以达到了对移动终端访问进行访问验证和控制的目的。与现有技术相比，本发明通过验证用户信息，绑定用户所对应的终端的物理信息以及自定义信息，达到了精确控制终端访问认证和访问请求的目的，同时通过设置动态检查规则，使得伪造访问请求的难度增加，从而可以有效的减少非法访问，确保信息安全。

[0046] 上述具体实施例不构成对本发明保护范围的限制。除上述实施例外，本发明还可以有其他实施方式。凡采用等同替换或等效变换形成的技术方案，均落在本发明要求的保护范围。

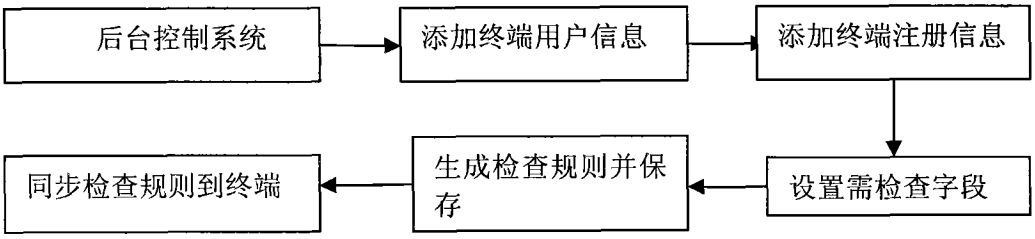

后台控制系统
添加终端用户信息
添加终端注册信息
设置需检查字段
生成检查规则并保存
同步检查规则到终端

图 1

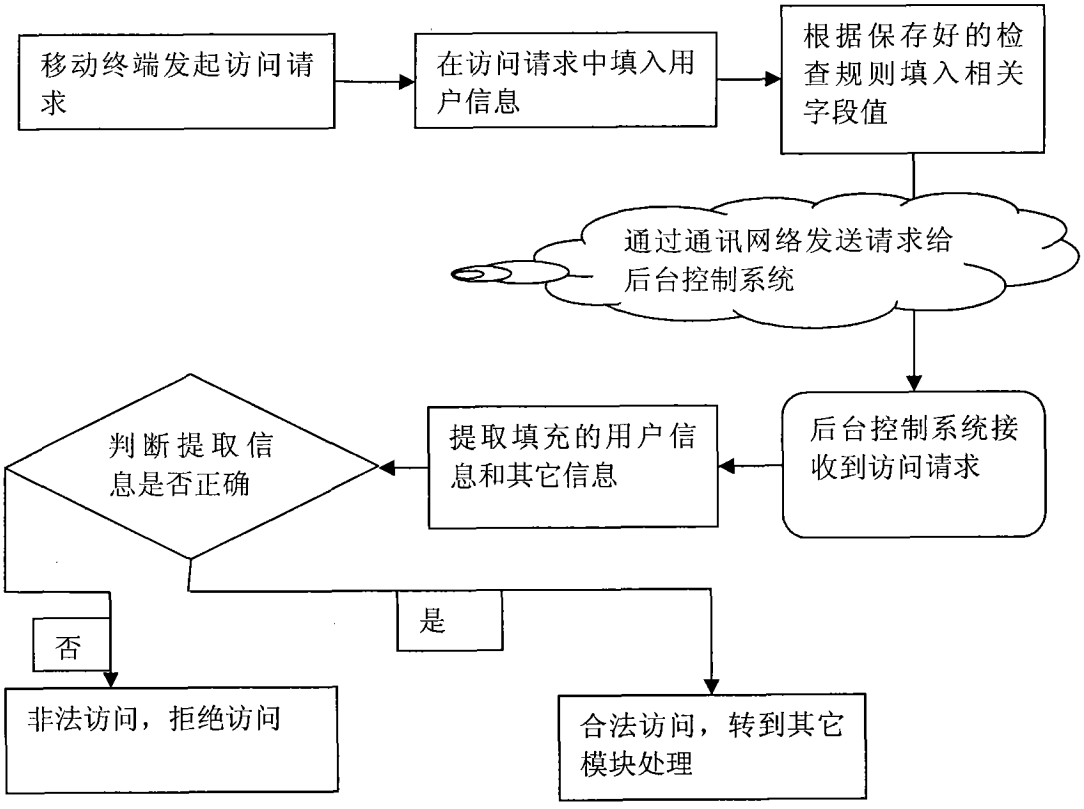

移动终端发起访问请求
在访问请求中填入用户信息
根据保存好的检查规则填入相关字段值
通过通讯网络发送请求给后台控制系统
后台控制系统接收到访问请求
提取填充的用户信息和其它信息
判断提取信息是否正确
否
是
非法访问，拒绝访问
合法访问，转到其它模块处理

图 2

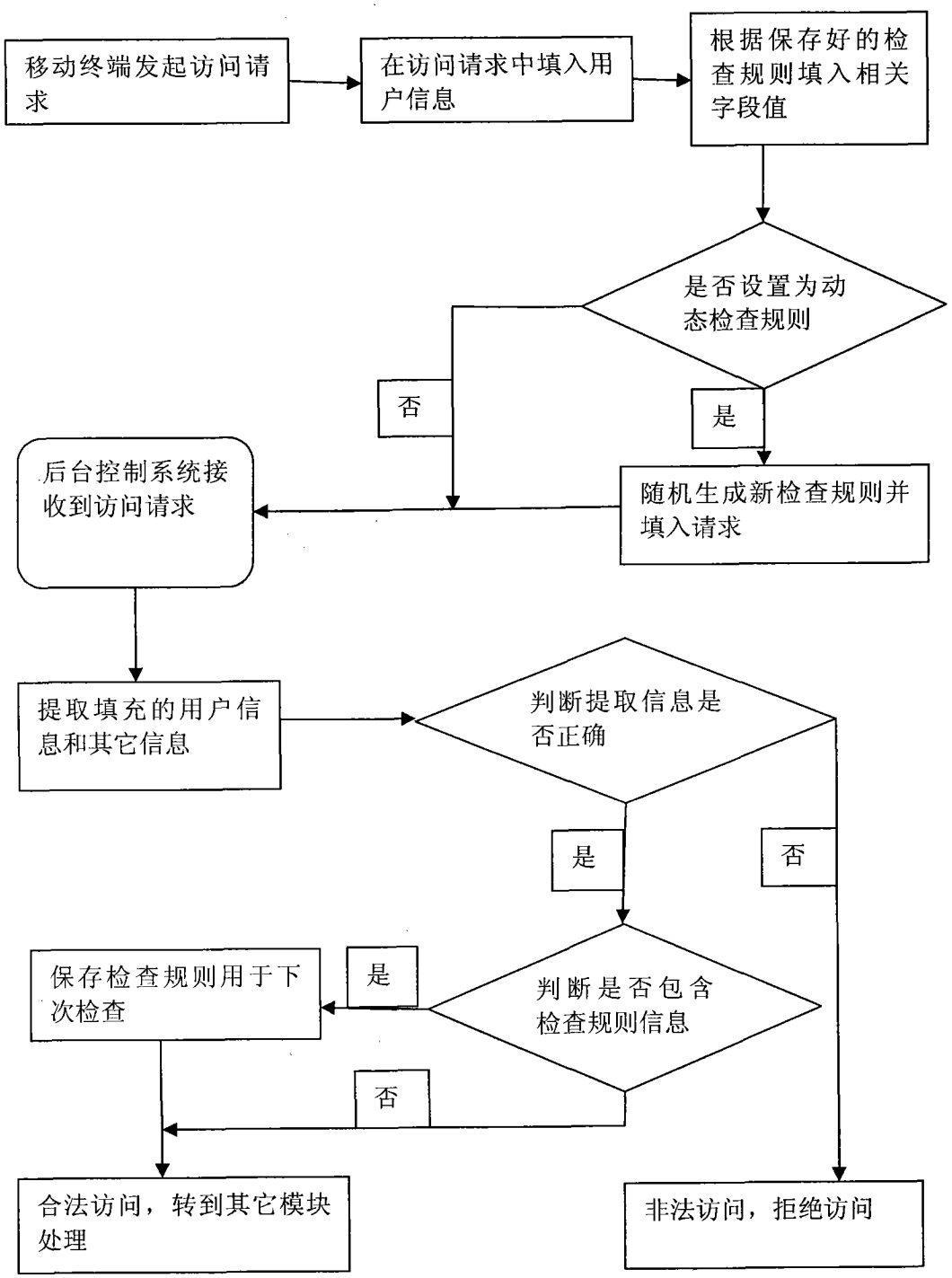

移动终端发起访问请求
在访问请求中填入用户信息
根据保存好的检查规则填入相关字段值
是否设置为动态检查规则
否
是
后台控制系统接收到访问请求
随机生成新检查规则并填入请求
提取填充的用户信息和其它信息
判断提取信息是否正确
是
否
保存检查规则用于下次检查
是
判断是否包含检查规则信息
否
合法访问，转到其它模块处理
非法访问，拒绝访问

图 3