(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
2010 年 4 月 1 日 (01.04.2010)

PCT

(10) 国际公布号
WO 2010/034209 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2009/072555

(22) 国际申请日: 2009 年 6 月 30 日 (30.06.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810168480.7 2008 年 9 月 28 日 (28.09.2008) CN

(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **任兰芳 (REN, Lanfang)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 **尹瀚 (YIN, Han)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 **贾科 (JIA, Ke)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100140 (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, 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, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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, SYSTEM AND DEVICE FOR REVALUATING SECURITY STATE

(54) 发明名称 : 一种安全状态重评估的方法、系统及装置

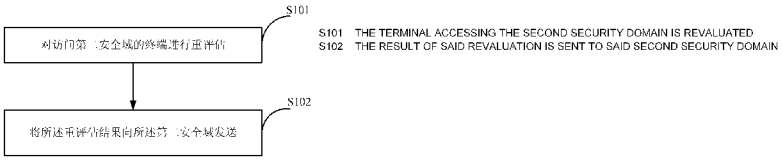

图 1 / Fig. 1

(57) Abstract: The present invention provides a method, a system and a device for revaluating security state. Said method includes: the terminal accessing the second security domain is revaluated; the result of said revaluation is sent to said second security domain. By means of the revaluation after the terminal accessed the relying security domain (RSD), the present invention ensures that the security state of the terminal accessing the network always meets the requirement of security policy of the current network in the whole connection process of the terminal and would not threaten the network security to a certain extent.

(57) 摘要:

本发明公开了一种安全状态重评估的方法、系统及装置。所述方法包括：对访问第二安全域的终端进行重评估；将所述重评估的结果向所述第二安全域发送。通过对终端接入依赖安全域（RSD）之后的重评估，本发明保证了接入网络的终端的安全状态在终端的整个连接过程中始终满足当前网络的安全策略要求，并且不会对网络的安全造成一定的威胁。

WO 2010/034209 A1

一种安全状态重评估的方法、系统及装置

技术领域

本发明涉及通信技术领域，特别是涉及一种安全状态重评估的方法、系统及装置。

背景技术

随着因特网的飞速发展和普遍应用，病毒技术也迅速发展，当病毒大规模爆发时，网络中传输的大量数据流量会因病毒而产生垃圾数据，造成资源浪费，严重影响了网络效率和安全，对用户的终端和业务产生了不利的影响和安全威胁，而且用户终端的病毒侵入很容易，终端会存在系统漏洞或病毒库过期等安全隐患。对终端进行安全控制，通过严格的终端安全评估，可以保证网络的安全。

随着移动技术的发展以及移动终端的普及，越来越多的用户希望可以随时接入网络享受各种各样的服务，此时，不仅需要对终端进行网络初始接入时候的安全防护以及高效安全评估，而且需要在终端整个通信的过程中保证该终端不会对网络造成一定的威胁，这就需要在网络侧根据一定的策略定期对终端进行安全状态的重评估。

现有技术中，当一个 ASD（Asserting Security Domain，断言安全域）的终端跨域访问 RSD（Relying Security Domain，依赖安全域）时，RSD 需要对该终端进行安全状态评估。RSD 不直接对终端进行安全状态信息的收集与评估，而是在接收到终端的接入请求之后，RSD 向终端的 ASD 发送终端安全状态断言请求，在接收到终端 ASD 的安全状态断言之后，根据这一结果对终端的接入请求做出响应。只有满足 RSD 安全策略要求的终端才允许访问 RSD。当终端得到 RSD 的允许接入响应之后，终端就可以与 RSD 之间进行通信或者享受某项服务。

在实现本发明过程中，发明人发现现有技术中至少存在如下问题：

在终端与 RSD 之间进行通信之后，RSD 不再对终端的安全状态进行重

评估或是其它的任何关注，在终端与 RSD 的整个通信过程中，RSD 也不会对终端的安全状态进行重评估。

发明内容

本发明实施例提供一种安全状态重评估的方法、系统及装置，以根据重评估的结果及时调整对终端的合适的控制。

为了达到上述目的，本发明实施例提出了一种安全状态重评估的方法，包括：

对访问第二安全域的终端进行重评估；

将所述重评估结果向所述第二安全域发送。

本发明实施例还提出了一种安全状态重评估的系统，包括：

第一安全域，用于对访问第二安全域的终端进行重评估，并向所述第二安全域发送所述重评估结果；

第二安全域，用于根据所述重评估结果对所述终端的访问做出相应的控制。

本发明实施例还提出了一种安全状态重评估的装置，包括：

重评估模块，用于对访问第二安全域的终端进行重评估；

发送模块，用于将所述重评估结果向所述第二安全域发送。

本发明实施例还提出了一种安全状态重评估的装置，包括：

接收模块，用于接收来自第一安全域发送的重评估的结果；

控制模块，用于根据所述重评估的结果对终端的访问做出相应的控制。

与现有技术相比，本发明实施例具有以下优点：

通过对终端接入 RSD 一段时间之后的重评估，保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例一提出的一种安全状态重评估的方法流程图；

图 2 为本发明实施例二提出的一种安全状态重评估的方法流程图；

图 3 为本发明实施例二提出的 RSD 对终端请求接入网络时的初始评估的执行流程图；

图 4 为本发明实施例二提出的 RSD 对终端进行重评估的执行流程图；

图 5 为本发明实施例二提出的另一种 RSD 对终端进行重评估的执行流程图；

图 6 为本发明实施例二提出的另一种 RSD 对终端进行重评估的执行流程图；

图 7 为本发明实施例三提出的一种安全状态重评估的系统结构图；

图 8 为本发明实施例四提出的一种安全状态重评估的装置结构图；

图 9 为本发明实施例五提出的一种安全状态重评估的装置结构图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例一提出的一种安全状态重评估的方法，如图 1 所示，可以包括：

步骤 S101，对访问第二安全域的终端进行重评估；

步骤 S102，将所述重评估结果向所述第二安全域发送。

具体的，在将所述重评估结果向所述第二安全域发送之后，第二安全域

还可以接收该重评估结果，并根据该重评估结果对该终端的访问做出相应控制。进一步的，该方法还可以包括：

步骤 S103，第二安全域接收该重评估结果，并根据该重评估结果对该终端的访问做出相应控制。

从安全的角度来看，一个网络中的所有系统实际上由多个安全域构成，每一个安全域简称域。第二安全域和第一安全域可以是安全域或者网络中的服务器，可以是认证服务器，也可以是评估服务器等设备，在本发明的所有实施例中，第二安全域以依赖安全域 RSD 为例，第一安全域以断言安全域 ASD 为例。而终端可以是智能终端、手机、PDA（Personal Digital Assistant，个人数据处理机）、普通 PC（personal computer，个人电脑）、笔记本以及 AP（Access Point，接入点）等支持 TNC（Trusted Network Connect，可信网络连接）评估的设备。

重评估正在跨域通信的终端的触发条件可以包括：ASD 向 RSD 发送终端安全状态重评估结果的断言触发条件；和/或所述 RSD 向该终端的 ASD 发送重评估请求或订阅重评估结果信息的触发条件。该 ASD 向该 RSD 发送终端安全状态重评估结果的断言触发条件包括：该终端 ASD 的自身安全策略配置发生改变、该终端 ASD 的安全策略配置规定需要周期性的对终端进行安全状态评估、该终端请求 ASD 重新对该终端进行安全状态评估中的一种或几种。该 RSD 向该终端的 ASD 发送重评估请求或订阅重评估结果信息的触发条件包括：该 RSD 发现该终端发生了可疑行为、该 RSD 自身的安全策略发生改变，要求对所述终端进行重评估、该 RSD 向该 ASD 订阅关于所述终端安全状态重评估结果信息，要求一旦所述评估结果发生变化，该 ASD 向该 RSD 及时发送所述评估结果信息，或者规定固定的重评估周期中的一种或几种。

该根据重评估的结果对该终端进行合适的控制包括：如果初始接入评估时，所述终端的安全状态只是部分符合第二安全域的安全策略要求，所述终

端只能部分接入所述第二安全域，而重评估的结果显示所述终端的安全状态完全符合所述第二安全域策略要求，所述第二安全域继续保持与所述终端的通信，并将所述终端的接入状态改为完全接入所述第二安全域；或

如果初始接入评估时，所述终端的安全状态完全符合所述第二安全域安全策略要求，所述重评估结果显示所述终端的安全状态只是部分符合所述第二安全域要求，所述第二安全域允许所述终端接入以继续保持与所述终端的通信，此时的接入是部分接入所述第二安全域；

如果初始接入评估时，所述终端的安全状态完全符合所述第二安全域安全策略要求，所述重评估结果说明所述终端安全状态不符合所述第二安全域安全策略要求，所述第二安全域中止与该所述终端当前的所有连接；或

所述第二安全域根据所述终端重评估结果对所述允许接入的终端进行角色映射，将不属于所述第二安全域的终端映射为所述第二安全域域内的终端。

可见，本发明实施例中，通过对终端接入 RSD 一段时间之后的重评估，保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。

本发明实施例二提出的一种安全状态重评估的方法，如图 2 所示，包括：

步骤 S201，RSD 对终端请求接入网络时进行初始评估，并判断 ASD 提供的安全状态断言是否满足 RSD 安全策略要求，当 ASD 提供的安全状态断言满足 RSD 安全策略要求时，在完成对终端请求接入网络时的初始评估并建立终端与 RSD 之间的通信之后，当 ASD 向 RSD 发送终端安全状态重评估结果的断言时，转到步骤 S202，当 RSD 向终端的 ASD 发送重评估请求或者订阅重评估结果信息时，转到步骤 S203，当 ASD 提供的安全状态断言不能满足 RSD 安全策略要求时，转到步骤 S204。

步骤 S202，当终端完成初始评估，并与 RSD 建立通信一段时间之后，ASD 向 RSD 发送终端安全状态重评估结果的断言，RSD 会及时对该终端进

行重评估，并根据重评估的结果及时调整对终端的合适的控制。该终端与RSD之间建立通信具体为跨域通信，具体是ASD域与RSD域之间的跨域通信。

具体的，在 RSD 完成对终端的初始评估，并与该终端开始通信之后，该终端的安全状态断言的提供方的ASD会向RSD发送终端安全状态重评估结果的断言，RSD根据该结果及时调整对终端的合适的控制。此外，该终端的安全状态断言的提供方的 ASD 还可以将该安全状态重评估结果的断言发送给该终端，使得该终端向 RSD 转发该安全状态重评估结果的断言，RSD根据该结果及时调整对终端的合适的控制。

该终端的安全状态断言的提供方的ASD向RSD发送终端安全状态重评估结果的断言的触发条件包括但不限于以下场景，终端 ASD 的自身安全策略配置发生改变、或是终端 ASD 的安全策略配置规定需要周期性的对终端进行安全状态评估、或是终端请求 ASD 重新对其进行安全状态评估。在上述触发条件的驱使下，ASD会对该终端的安全状态重新进行评估并产生相应的重评估结果，并将该一重评估结果主动发送给RSD。

步骤S203，当终端初始评估完成，并与RSD建立通信一段时间之后，当RSD向终端的ASD发送重评估请求或者订阅重评估结果信息，要求ASD对终端安全状态进行重评估并发送针对该终端重评估结果的断言时，RSD可以及时对该终端进行重评估，并根据重评估的结果及时调整对终端的合适的控制。

具体的，在 RSD 完成对终端的初始评估，并与该终端开始通信之后，RSD向终端的ASD发送重评估请求或者订阅重评估结果信息，要求ASD对终端安全状态进行重评估并发送针对终端重评估结果的断言时，RSD可以根据该结果及时调整对终端的合适的控制。

该RSD向终端的ASD发送重评估请求或者订阅重评估结果信息，要求ASD 对终端安全状态进行重评估并发送针对终端重评估结果的断言的触发

条件包括但不限于以下场景，RSD 发现该终端发生了某些可疑行为、或是RSD 自身的安全策略发生改变，要求对终端进行重评估、或是 RSD 向 ASD 订阅关于终端安全状态重评估结果信息，要求一旦其评估结果发生变化，ASD 就向 RSD 及时发送这一信息，或者规定固定的重评估周期或频率。

在上述步骤 S202 和步骤 S203 中，并没有先后的顺序关系，只是发送重评估请求的对象不同，在步骤 S202 中为接入请求，具体为 ASD 向 RSD 发送终端安全状态重评估结果的断言，在步骤 S203 中为服务请求，具体为 RSD 向终端的 ASD 发送重评估请求或者订阅重评估结果信息。本实施例中，该进行重评估的网络包括但不限于固网、无线网以及其它融合网络。

步骤 S204，当 ASD 提供的安全状态断言不满足 RSD 安全策略要求时，该 RSD 不会直接做出拒绝接入的响应，而是向该 ASD 请求其它的安全状态断言，该 RSD 会根据该 ASD 重新提供的其它安全状态断言对终端的请求做出响应。

具体的，在步骤 S201 中，该 RSD 对终端请求接入网络时的初始评估的执行流程如图 3 所示，包括：

步骤 S301，终端向 RSD 的服务器发起接入请求。

步骤 S302，RSD 确定该终端安全状态断言的提供方的 ASD，并向该 ASD 发送终端安全状态断言请求。

该安全状态断言是指对终端安全状态信息、安全评估结果以及与终端相关的安全事件元数据的一种声明，根据该安全状态断言可以判断出该终端是否是安全的。

步骤 S303，ASD 接收到 RSD 的终端断言请求之后，识别该终端断言请求是对应哪个终端的，并响应 RSD 所请求的该终端的安全状态断言。

步骤 S304，RSD 根据该终端的安全状态断言对该终端的 ASD 发来的安全状态进行评估。

步骤 S305，根据上述评估结果，RSD 做出是否允许该终端接入的响应。

步骤 S306，完成初始评估过程，该允许接入的终端就可以与 RSD 之间建立连接进行通信。

当终端的 ASD 提供的安全状态断言不能满足 RSD 的要求时，RSD 可以重新请求新的或者其它类型的安全状态断言。这时的重评估，可以通过 ASD 与 RSD 之间预先协商确定，要求 ASD 提供最新的或者特定的安全状态断言相关信息，以完成初始评估过程。

具体的，在步骤 S202 中，该 RSD 会及时对该终端进行重评估，并根据重评估的结果及时调整对终端的合适的控制，其执行流程如图 4 所示，包括：

步骤 S401，终端初始评估完成，并与 RSD 之间开始通信。

具体的，RSD 完成对终端请求接入的初始安全状态评估，对于允许接入的终端，该终端可以与 RSD 之间进行通信。对于允许接入该 RSD 的终端，可以是完全允许接入该 RSD，即，终端可以访问该 RSD 内的所有资源，也可以是部分允许接入，即，终端只能访问该 RSD 内的部分资源。如果终端的安全状态完全符合 RSD 的策略要求，则允许终端完全接入 RSD，如果终端的部分安全状态符合 RSD 策略要求，则 RSD 可能只允许终端部分接入。

步骤 S402，终端接入 RSD 并与 RSD 进行通信一段时间之后，该终端可以向 ASD 发起重评估请求，请求 ASD 对终端执行重评估过程。

具体的，当终端的 ASD 自身安全策略发生改变，或者终端 ASD 的策略规定需要对终端进行周期性的重评估，或者 ASD 接收到终端发送的上述重评估请求时，ASD 就会对终端进行安全状态信息的重评估，并产生相应的重评估结果。

步骤 S403，ASD 将当前的重评估结果断言发送给 RSD。

此外，ASD 还可以将当前的重评估结果断言发送该终端，使得该终端向 RSD 转发该安全状态重评估结果的断言。

步骤 S404，RSD 根据该重评估结果，及时调整对终端的合适的控制。

具体的，当 ASD 发来的重评估结果为允许接入时，可以继续终端与 RSD

之间的通信，当终端安全状态断言不能满足 RSD 的要求时，也可以结束终端与 RSD 之间的通信。当不能满足 RSD 的要求时，RSD 可以重新请求新的或者其它类型的安全状态断言。

根据 ASD 发来的重评估结果，及时调整对终端的合适的控制包括但不限于：

如果初始接入评估时，终端的安全状态只是部分符合 RSD 安全策略要求，终端只能部分接入 RSD，而重评估的结果显示终端的安全状态完全符合 RSD 策略要求，那么此时 RSD 将继续保持与终端的通信，并将终端的接入状态改为完全接入 RSD，可以享受 RSD 的所有服务；

如果初始接入评估时，终端的安全状态完全符合 RSD 安全策略要求，而重评估结果显示终端的安全状态只是部分符合 RSD 要求，RSD 也允许终端接入继续保持与终端的通信，但是此时的接入只能是部分接入，这时 RSD 就会限制终端的某些服务；

如果初始接入评估时，终端的安全状态完全符合 RSD 安全策略要求，而重评估结果说明终端安全状态不再符合 RSD 安全策略要求，此时 RSD 就会中止的与该终端当前的所有连接不再为其提供服务；这种情况下，RSD 可能会将该终端划分到一定的隔离区域，也可能会通知 ASD 进行修复。

此外，RSD 可以根据终端重评估的结果对允许接入的终端进行角色映射，将原本不属于自己的终端映射为该 RSD 域内的终端，使得终端能够访问与本域内其角色相对应的所有网络资源。

具体的，在步骤 S203 中，该 RSD 及时对该终端进行重评估，并根据重评估的结果及时调整对终端的合适的控制的执行流程如图 5 所示，包括：

步骤 S501，终端初始评估完成，并与 RSD 之间开始通信。

具体的，RSD 完成对终端请求接入的初始安全状态评估，对于允许接入的终端，该终端可以与 RSD 之间进行通信。对于允许接入该 RSD 的终端，可以是完全允许接入该 RSD，即，终端可以访问该 RSD 内的所有资源，也

可以是部分允许接入，即，终端只能访问该 RSD 内的部分资源。如果终端的安全状态完全符合 RSD 的策略要求，则允许终端完全接入 RSD，如果终端的部分安全状态符合 RSD 策略要求，则 RSD 可能只允许终端部分接入。

步骤 S502，终端接入 RSD 并与 RSD 进行通信一段时间之后，RSD 向 ASD 发送重评估请求，请求 ASD 将针对终端的重评估结果发送给 RSD。

具体的， RSD 发现该终端发生了某些可疑行为，或者 RSD 自身的安全策略发生改变，要求对终端进行重评估，这时，RSD 向 ASD 发送重评估请求，请求 ASD 将针对终端的重评估结果发送给 RSD；另外，RSD 也可以主动向 ASD 订阅关于终端安全状态重评估结果信息，要求一旦其评估结果发生变化，ASD 就向 RSD 及时发送这一信息，或者规定固定的重评估周期或频率。

步骤 S503，ASD 对终端进行安全状态信息的重评估，并产生相应的重评估结果。

步骤 S504，ASD 将当前的重评估结果断言发送给 RSD。此外，ASD 还可以将当前的重评估结果断言发送该终端，使得该终端向 RSD 转发该安全状态重评估结果的断言。

步骤 S505， RSD 根据 ASD 发来的重评估结果，及时调整对终端的合适的控制。

具体的，当 ASD 发来的重评估结果为允许接入时，可以继续终端与 RSD 之间的通信，当终端安全状态断言不能满足 RSD 的要求时，也可以结束终端与 RSD 之间的通信。当不能满足 RSD 的要求时，RSD 可以重新请求新的或者其它类型的安全状态断言。

根据 ASD 发来的重评估结果，及时调整对终端的合适的控制包括但不限于：如果初始接入评估时，终端的安全状态只是部分符合 RSD 安全策略要求，终端只能部分接入 RSD，而重评估的结果显示终端的安全状态完全符合 RSD 策略要求，那么此时 RSD 将继续保持与终端的通信，并将终端的接

入状态改为完全接入 RSD，可以享受 RSD 的所有服务；

如果初始接入评估时，终端的安全状态完全符合 RSD 安全策略要求，而重评估结果显示终端的安全状态只是部分符合 RSD 要求，RSD 也允许终端接入继续保持与终端的通信，但是此时的接入只能是部分接入，这时 RSD 就会限制终端的某些服务；

如果初始接入评估时，终端的安全状态完全符合 RSD 安全策略要求，而重评估结果说明终端安全状态不再符合 RSD 安全策略要求，此时 RSD 就会中止的与该终端当前的所有连接不再为其提供服务；这种情况下，RSD 可能会将该终端划分到一定的隔离区域，也可能会通知 ASD 进行修复。

此外，RSD 可以根据终端重评估的结果对允许接入的终端进行角色映射，将原本不属于自己的终端映射为该 RSD 域内的终端，使得终端能够访问与本域内其角色相对应的所有网络资源。

具体的，在步骤 S204 中，该 RSD 不直接拒绝接入响应，向 ASD 请求其它的安全状态断言的执行流程如图 6 所示，包括：

步骤 S601，终端向 RSD 的服务器发起接入请求。

步骤 S602，RSD 确定该终端安全状态断言的提供方的 ASD，并向该 ASD 发送终端安全状态断言请求。

步骤 S603，ASD 接收到 RSD 的终端断言请求之后，识别该终端断言请求是对应哪个终端的，并响应 RSD 所请求的该终端的安全状态断言。

步骤 S604，RSD 根据该终端的安全状态断言对该终端的 ASD 发来的安全状态进行评估，判定该终端的安全状态断言不满足该 RSD 的安全策略要求。

步骤 S605，该 RSD 向该终端安全状态断言的提供方的 ASD 发送该终端的其它安全状态的断言请求。

步骤 S606，ASD 接收到 RSD 的其它安全状态的断言请求之后，响应 RSD 所请求的该终端的其它安全状态断言。

步骤 S607，根据上述重评估的结果，RSD 做出是否允许该终端接入的响应。

步骤 S608，完成重评估过程，该允许接入的终端就可以与 RSD 之间建立连接进行通信。

当终端的 ASD 提供的其它安全状态断言仍不能满足该 RSD 的要求时，可以拒绝该终端的接入请求了。

上述实施例中，均可以适用于任意两个网络设备，该两个网络设备可以是属于不同安全域（或者是属于同一个安全域，或者属于不同网络、或者是同一网络）之间对同一终端通过安全状态评估进行合适的控制。本实施例也适用于企业网、电信网以及移动网等各种网络对终端安全状态评估的合适的控制。本发明所有实施例中，终端不一定是访问两个不同的安全域，而可以是同一个网络、同一个安全域或者不同网络之间的共享安全评估信息。

可见，本实施例中，通过对终端接入 RSD 一段时间之后的重评估，保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。而且当终端的 ASD 在初次提供的安全状态断言不满足 RSD 要求时，RSD 也可以重新请求其它的断言，从而提高了网络的效率。

本发明实施例三提出的一种安全状态重评估的系统，如图 7 所示，包括：

ASD 71，用于对访问 RSD 72 的终端 73 进行重评估，并向 RSD 72 发送该重评估的结果；

RSD 72，用于根据 ASD 71 发送的重评估的结果对该终端 73 的访问做出相应的控制。

终端 73，用于与该 RSD 72 进行通信，该终端 73 为支持可信网络连接评估的设备，其类型包括智能终端、手机、个人数据处理机、个人电脑、笔记本以及接入点中的一种或几种。

可见，本发明实施例中，通过对终端接入 RSD 一段时间之后的重评估，

保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。

本发明实施例四提出的一种安全状态重评估的装置，该网络装置部署在第一安全域内，如图 8 所示，包括：

重评估模块 81，用于对访问 RSD 的终端进行重评估；

发送模块 82，用于将重评估模块 81 重评估的结果向 RSD 发送，以使该 RSD 对终端的访问做出合适的控制。

进一步的，该重评估模块 81 包括：

接收单元 811，用于接收终端发起的重评估请求，以对该终端执行重评估过程。

发送单元 812，用于在接收单元 811 对该终端执行重评估过程之后，向 RSD 发送终端安全状态重评估结果的断言。该重评估结果的断言的触发条件包括所述终端 ASD 的自身安全策略配置发生改变；所述终端 ASD 的安全策略配置规定需要周期性的对终端进行安全状态评估；所述终端请求 ASD 重新对所述终端进行安全状态评估中的一种或几种。

可见，本发明实施例中，通过对终端接入 RSD 一段时间之后的重评估，保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。

本发明实施例五提出的一种安全状态重评估的装置，该装置为 RSD 9，并且该网络装置部署在第二安全域内，如图 9 所示，包括：

接收模块 91，用于接收来自 ASD 发送的重评估的结果；

控制模块 92，用于根据接收模块 91 接收的重评估的结果对该终端的访问做出合适的控制。

进一步的，该装置还包括：

发送模块 93，用于向终端的 ASD 发送重评估请求或订阅重评估结果信息，该重评估请求或订阅重评估结果信息。该触发条件包括所述 RSD 发现

所述终端发生了可疑行为；所述 RSD 自身的安全策略发生改变，要求对所述终端进行重评估；所述 RSD 向所述 ASD 订阅关于所述终端安全状态重评估结果信息，要求一旦所述评估结果发生变化，所述 ASD 向所述 RSD 及时发送所述评估结果信息，或者规定固定的重评估周期中的一种或几种。

可见，本发明实施例中，通过对终端接入 RSD 一段时间之后的重评估，保证进入网络的终端安全状态在终端整个连接的过程中始终满足当前网络的安全策略要求，不会对网络的安全造成一定的威胁。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以可借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视本发明的保护范围。

权利要求书

1、一种安全状态重评估的方法，其特征在于，处于第一安全域的终端访问第二安全域，包括：

对访问第二安全域的终端进行重评估；

将所述重评估结果向所述第二安全域发送。

2、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

根据所述终端的第一安全域的自身安全策略配置发生改变的触发条件，对所述访问第二安全域的终端重评估。

3、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

根据所述终端的第一安全域的安全策略配置规定需要周期性的对所述终端进行安全状态评估的触发条件，对访问第二安全域的终端重评估。

4、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

根据所述终端请求第一安全域重新对所述终端进行安全状态评估的触发条件，对访问第二安全域的终端重评估。

5、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

根据所述第二安全域发现所述终端发生了可疑行为的触发条件，对访问第二安全域的终端重评估。

6、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

根据所述第二安全域自身的安全策略发生改变，要求对所述终端进行重评估的触发条件，对访问第二安全域的终端重评估。

7、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的

终端进行重评估包括：

根据所述第二安全域向所述第一安全域订阅关于所述终端安全状态重评估结果信息，要求一旦所述评估结果发生变化，所述第一安全域向所述第二安全域及时发送所述评估结果信息，或者规定固定的重评估周期的触发条件，对访问第二安全域的终端重评估。

8、如权利要求 1 所述的方法，其特征在于，在所述对访问第二安全域的终端进行重评估之后，还包括：

所述第二安全域接收所述重评估结果，根据所述重评估结果对所述终端的访问做出相应控制。

9、如权利要求 8 所述的方法，其特征在于，所述对终端的访问做出相应的控制包括：

如果初始接入评估时，所述终端的安全状态只是部分符合第二安全域的安全策略要求，所述终端只能部分接入所述第二安全域，而重评估的结果显示所述终端的安全状态完全符合所述第二安全域策略要求，所述第二安全域继续保持与所述终端的通信，将所述终端的接入状态改为完全接入所述第二安全域；或

如果初始接入评估时，所述终端的安全状态完全符合所述第二安全域安全策略要求，所述重评估结果显示所述终端的安全状态只是部分符合所述第二安全域要求，所述第二安全域允许所述终端接入以继续保持与所述终端的通信，此时的接入是部分接入所述第二安全域；或

如果初始接入评估时，所述终端的安全状态完全符合所述第二安全域安全策略要求，所述重评估结果说明所述终端安全状态不符合所述第二安全域安全策略要求，所述第二安全域中止与该所述终端当前的所有连接；或

所述第二安全域根据所述终端重评估结果对所述允许接入的终端进行角色映射，将不属于所述第二安全域的终端映射为所述第二安全域域内的终端，允许该终端访问对应的资源。

10、如权利要求 1 所述的方法，其特征在于，在所述对访问第二安全域的终端进行重评估之前，还包括：

第二安全域对所述终端请求接入网络时进行初始评估；

判断第一安全域提供的安全状态断言是否满足所述第二安全域的安全策略要求；

当所述第一安全域提供的所述安全状态断言不满足所述第二安全域的安全策略要求时，根据所述第一安全域提供的其它安全状态断言进行重评估。

11、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

第一安全域接收所述终端发起的重评估请求，以对所述终端执行重评估过程；

所述第一安全域将所述重评估的结果断言向所述第二安全域发送。

12、如权利要求 1 所述的方法，其特征在于，所述对访问第二安全域的终端进行重评估包括：

第二安全域向第一安全域发送重评估请求，以使所述第一安全域对所述终端进行安全状态信息的重评估，生成重评估结果；

所述第二安全域接收所述第一安全域生成的重评估结果断言。

13、如权利要求 1 所述的方法，其特征在于，所述将重评估结果向所述第二安全域发送包括：

第一安全域直接向第二安全域发送所述重评估的结果；和/或

所述第一安全域向所述终端发送所述重评估的结果，以使所述终端将所述重评估的结果转发给所述第二安全域。

14、一种网络系统，其特征在于，包括：

第一安全域，用于对访问第二安全域的终端进行重评估，向所述第二安全域发送所述重评估结果；

第二安全域，用于根据所述重评估结果对所述终端的访问做出相应的控制。

15、如权利要求 14 所述的系统，其特征在于，还包括：

终端，用于与所述第二安全域进行通信，所述终端为支持可信网络连接评估的设备，其类型包括智能终端、或手机、或个人数据处理机、或个人电脑、或笔记本。

16、一种网络装置，其特征在于，该网络装置部署在第一安全域内，包括：

重评估模块，用于对访问第二安全域的终端进行重评估；

发送模块，用于将所述重评估结果向所述第二安全域发送。

17、如权利要求 16 所述的装置，其特征在于，所述重评估模块包括：

接收单元，用于接收所述终端发起的重评估请求，以对所述终端执行重评估过程；

发送单元，用于在执行所述重评估过程之后，向第二安全域发送所述终端安全状态重评估结果的断言。

18、一种网络装置，其特征在于，该网络装置部署在第二安全域内，包括：

接收模块，用于接收来自第一安全域发送的重评估结果；

控制模块，用于根据所述重评估结果对终端的访问做出相应的控制。

19、如权利要求 18 所述的装置，其特征在于，还包括：

发送模块，用于向所述终端的第一安全域发送重评估请求或订阅重评估结果信息。

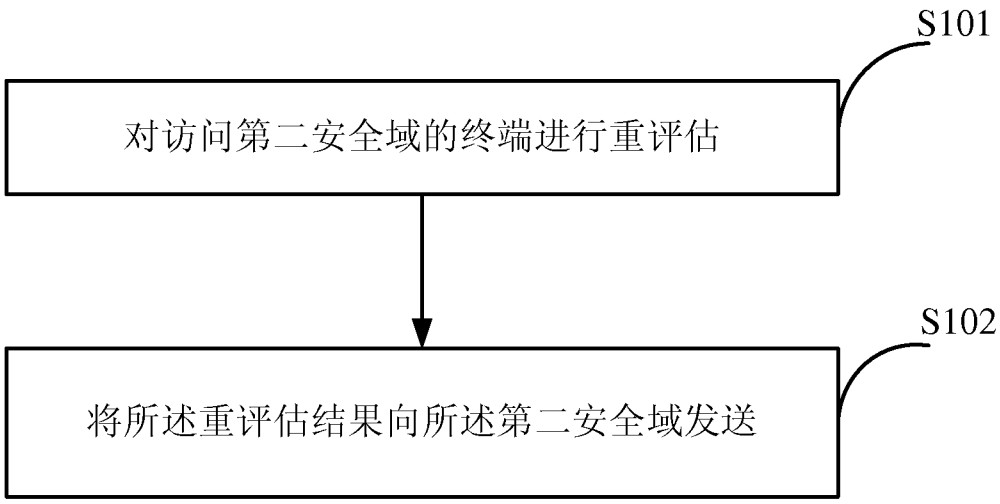

图 1

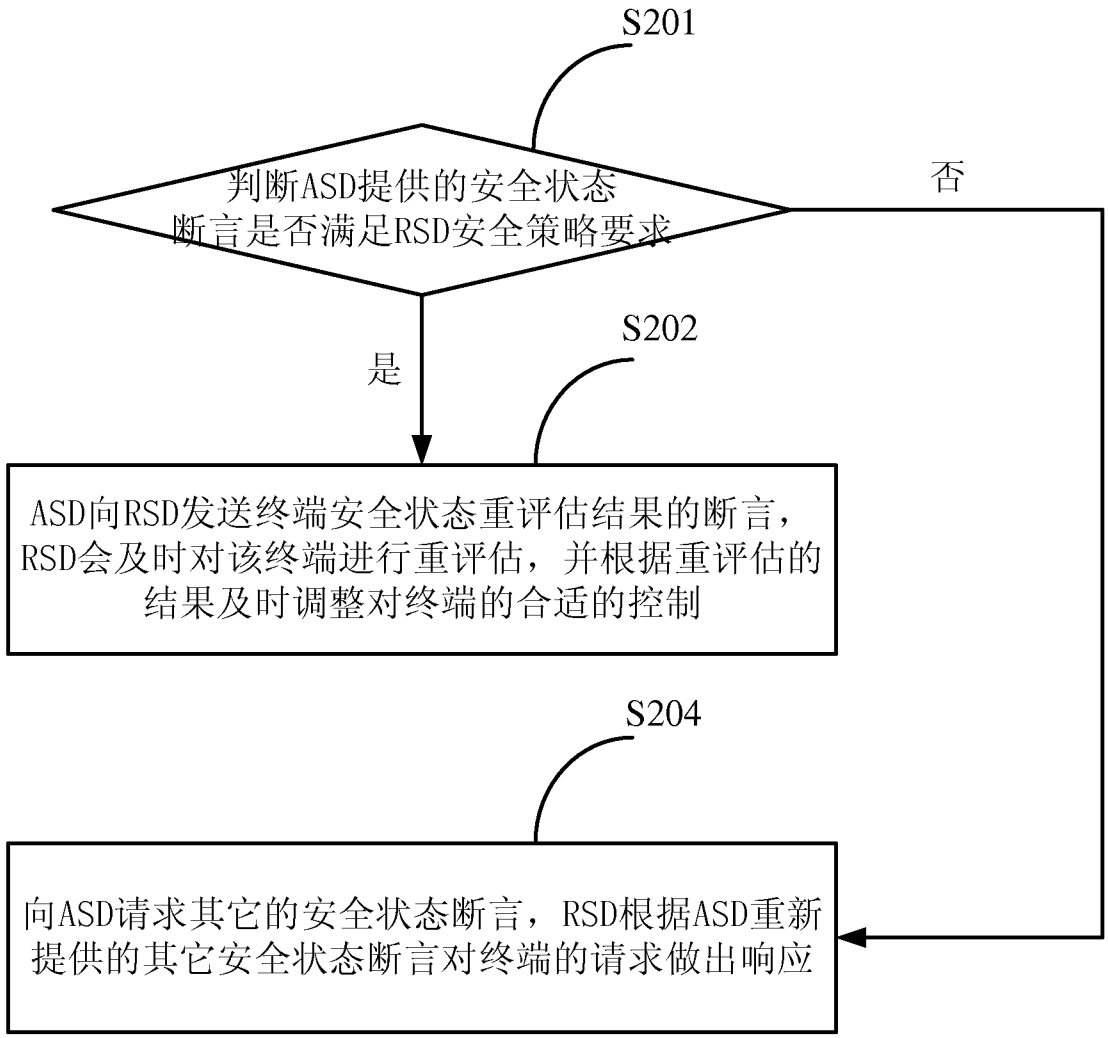
S201
判断ASD提供的安全状态断言是否满足RSD安全策略要求
否
是
S202
ASD向RSD发送终端安全状态重评估结果的断言，RSD会及时对该终端进行重评估，并根据重评估的结果及时调整对终端的合适的控制
S204
向ASD请求其它的安全状态断言，RSD根据ASD重新提供的其它安全状态断言对终端的请求做出响应

图 2

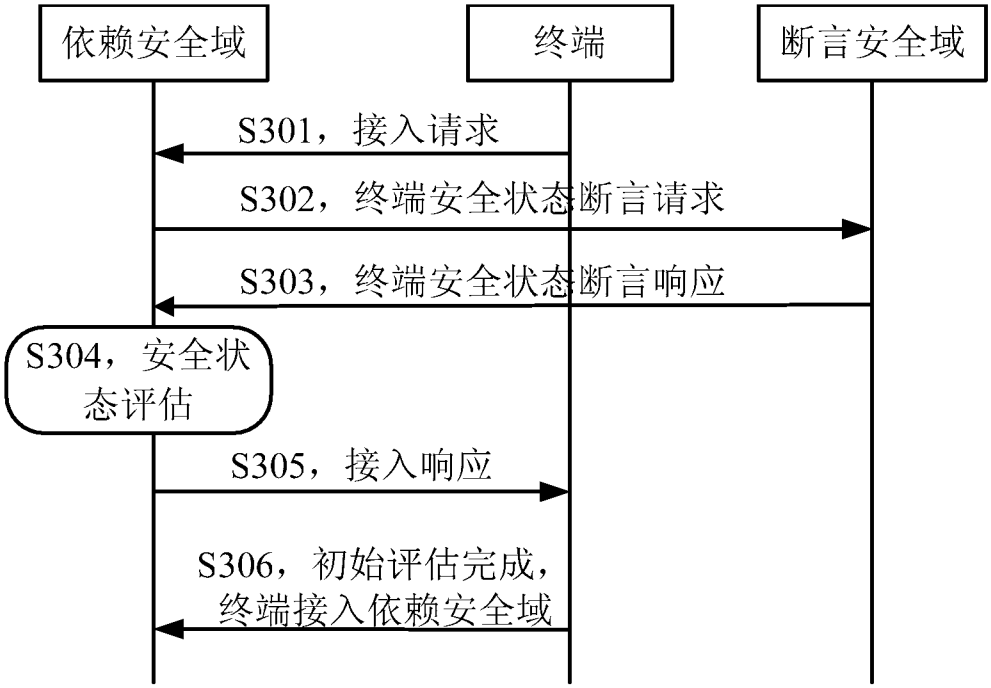
依赖安全域
终端
断言安全域
S301，接入请求
S302，终端安全状态断言请求
S303，终端安全状态断言响应
S304，安全状态评估
S305，接入响应
S306，初始评估完成，终端接入依赖安全域

图 3

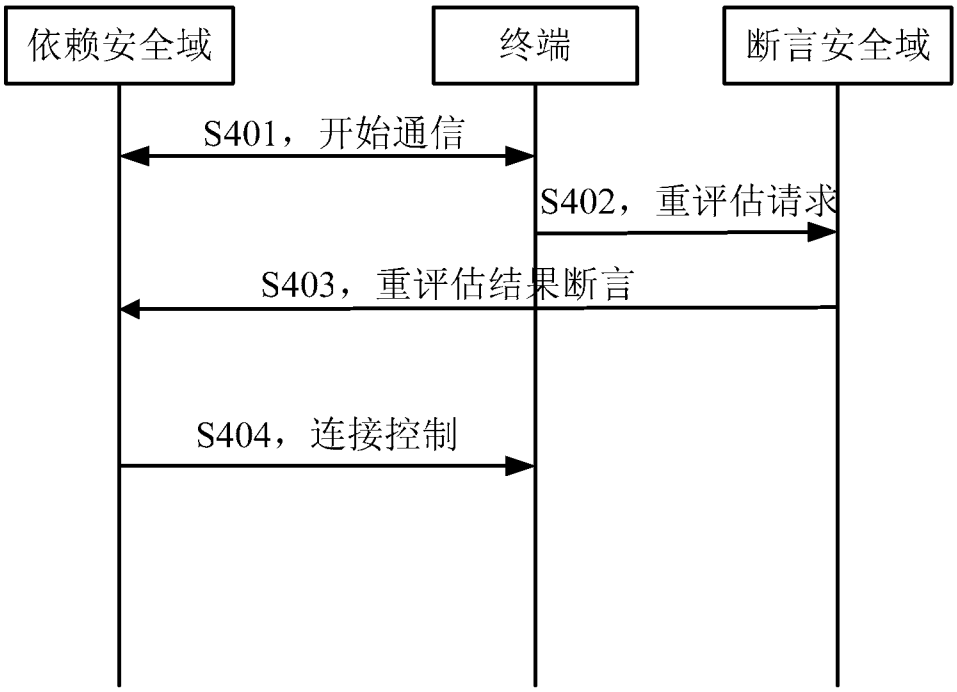
依赖安全域
终端
断言安全域
S401，开始通信
S402，重评估请求
S403，重评估结果断言
S404，连接控制

图 4

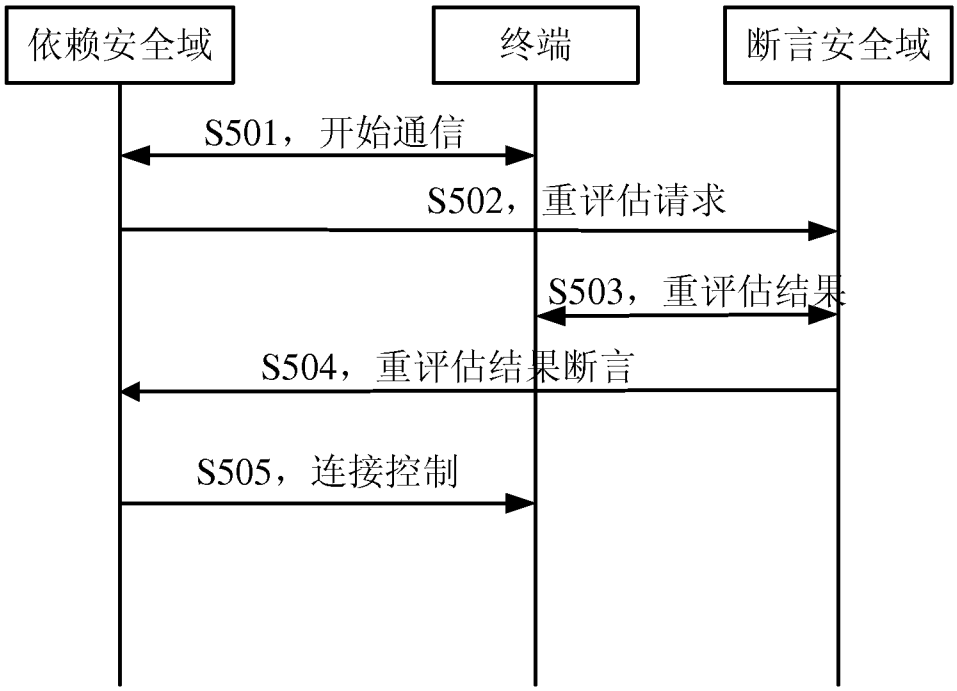
依赖安全域
终端
断言安全域
S501，开始通信
S502，重评估请求
S503，重评估结果
S504，重评估结果断言
S505，连接控制

图 5

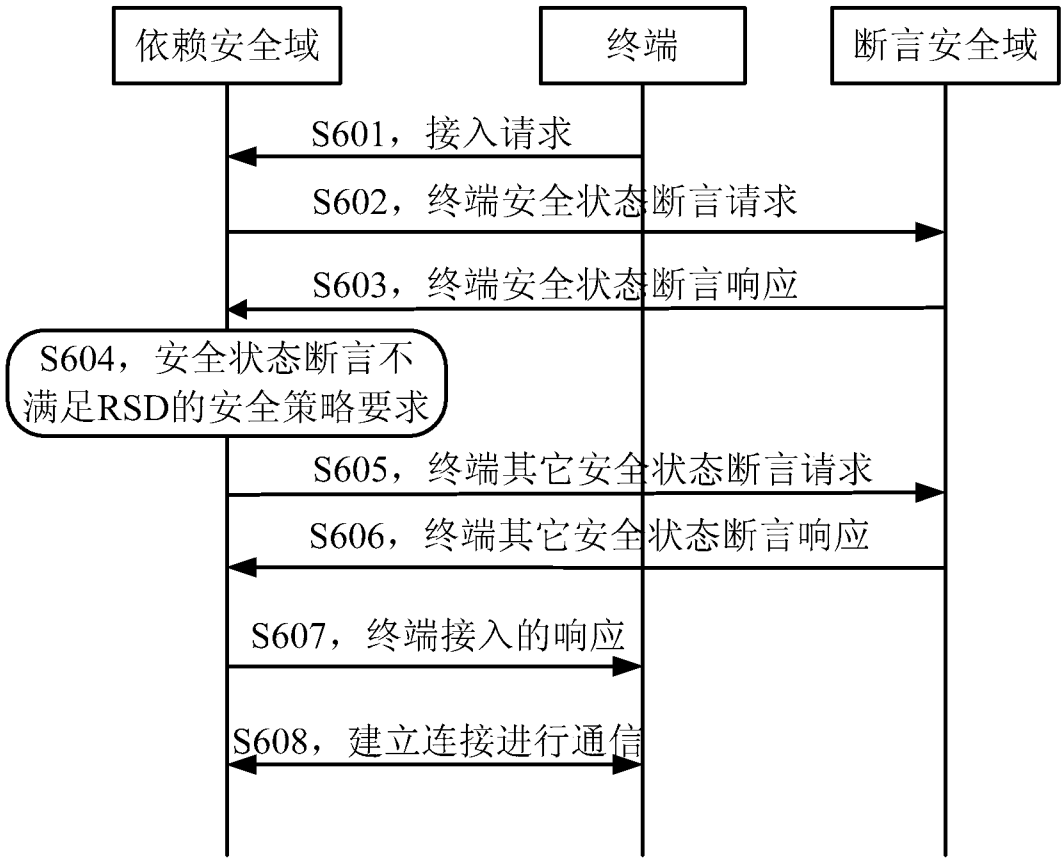
依赖安全域
终端
断言安全域
S601，接入请求
S602，终端安全状态断言请求
S603，终端安全状态断言响应
S604，安全状态断言不满足RSD的安全策略要求
S605，终端其它安全状态断言请求
S606，终端其它安全状态断言响应
S607，终端接入的响应
S608，建立连接进行通信

图 6

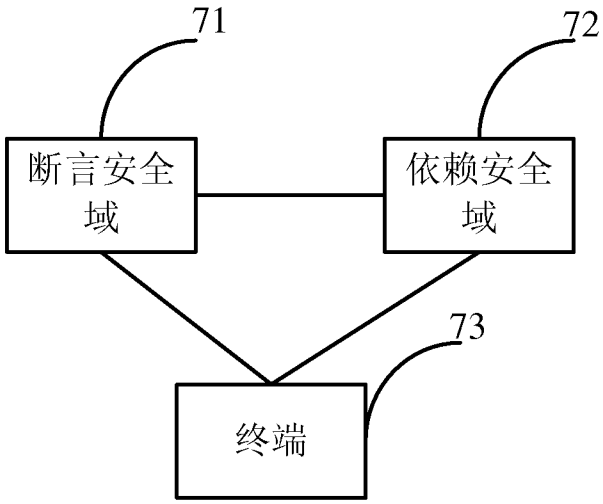

图 7

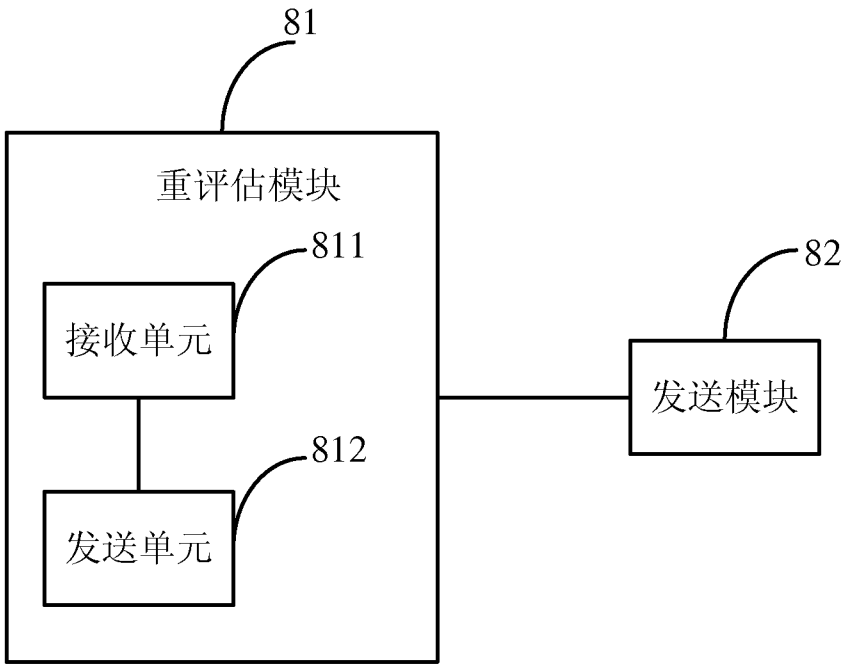

图 8

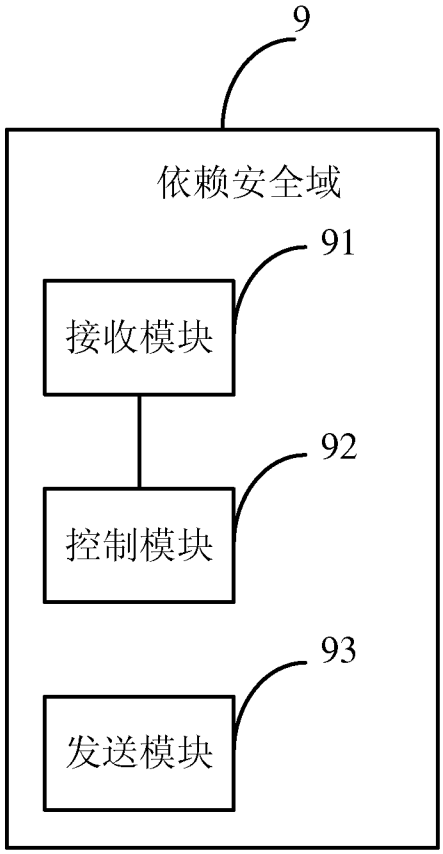

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072555

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)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:H04L,H04Q,H04W,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)

CNPAT,WPI,PAJ,EPODOC,IEEE,CNKI,3GPP:ASD,RSD,security,domain,revaluat+,policy,validate,verify,authenticat+, profile,assert+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1656773A(TELEFONAKTIEBOLAGET L. M. ERICSSON) 17 Aug. 2005 (17.08.2005) Description page 23 line 24- page 31 line 28, figs. 3,10-11	1-19
A	CN101242272A(UNIV. NANJING POSTS & TELECOM) 13 Aug. 2008 (13.08.2008) The whole document	1-19
A	US2004/0267551A1(YADAV,Satyendra) 30 Dec. 2004 (30.12.2004) The whole document	1-19

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 Aug. 2009(25.08.2009)	**17 Sep. 2009 (17.09.2009)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZUO, Zimei Telephone No. (86-10)62413506

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/072555

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1656773A	17.08.2005	WO03100544A2	04.12.2003
		AU2003245887A1	12.12.2003
		EP1508236A2	23.02.2005
		KR20040105259A	14.12.2004
		JP2005535006T	17.11.2005
		US2006053296A1	09.03.2006
		AU2003245887A8	27.10.2005
		EP1508236B1	11.07.2007
		DE60314871E	23.08.2007
		DE60314871T2	13.03.2008
CN101242272A	13.08.2008	None	
US2004/0267551A1	30.12.2004	None	

国际检索报告

国际申请号
PCT/CN2009/072555

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类表(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:H04L,H04Q,H04W,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）)

CNPAT,WPI,PAJ,EPODOC,IEEE,CNKI,3GPP:安全,域,评估,重,再,策略,验证,鉴权,认证,简档,声称,断言,ASD,RSD,security,domain,revaluat+,policy,validate,verify,authenticat+,profile,assert+

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
X	CN1656773A(艾利森电话股份有限公司) 17.8 月 2005（17.08.2005） 说明书第 23 页第 24 行-第 31 页第 28 行、图 3, 10-11	1-19
A	CN101242272A(南京邮电大学) 13.8 月 2008（13.08.2008） 全文	1-19
A	US2004/0267551A1(YADAV,Satyendra) 30.12 月 2004（30.12.2004） 全文	1-19

☐ 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

"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	国际检索报告邮寄日期
25.8 月 2009(25.08.2009)	**17.9 月 2009 (17.09.2009)**
中华人民共和国国家知识产权局(ISA/CN) 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 左子湄 电话号码：(86-10) **62413506**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/072555

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1656773A	17.08.2005	WO03100544A2	04.12.2003
		AU2003245887A1	12.12.2003
		EP1508236A2	23.02.2005
		KR20040105259A	14.12.2004
		JP2005535006T	17.11.2005
		US2006053296A1	09.03.2006
		AU2003245887A8	27.10.2005
		EP1508236B1	11.07.2007
		DE60314871E	23.08.2007
		DE60314871T2	13.03.2008
CN101242272A	13.08.2008	无	
US2004/0267551A1	30.12.2004	无	