



(12) 发明专利

(10) 授权公告号 CN 101527717 B

(45) 授权公告日 2012.11.28

(21) 申请号 200910022057.0

CN 101159640 A, 2008.04.09,

(22) 申请日 2009.04.16

CN 101242267 A, 2008.08.13,

(73) 专利权人 西安西电捷通无线网络通信股份
有限公司

CN 101242268 A, 2008.08.13,

地址 710075 陕西省西安市高新区科技二路
68号西安软件园秦风阁A201

审查员 王飞

(72) 发明人 肖跃雷 曹军 葛莉 黄振海

(74) 专利代理机构 西安智邦专利商标代理有限
公司 61211

代理人 商宇科

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 12/24(2006.01)

G06F 21/00(2006.01)

(56) 对比文件

CN 101242267 A, 2008.08.13,
CN 101345766 A, 2009.01.14,
CN 101242266 A, 2008.08.13,
CN 101242401 A, 2008.08.13,

权利要求书 5 页 说明书 14 页 附图 4 页

(54) 发明名称

一种三元对等鉴别可信网络连接架构的实现
方法

(57) 摘要

本发明涉及一种三元对等鉴别可信网络连接
架构的实现方法,该方法包括以下步骤:1) 通过
定义接口建立三元对等鉴别可信网络连接架构;
2) 实现三元对等鉴别可信网络连接架构的可信
网络连接;本发明提供了一种建立终端可信、实
现终端的可信网络连接、实现终端间的可信认证
和实现对终端的可信管理的适合三元对等鉴别可
信网络连接架构的实现方法。

1. 一种三元对等鉴别可信网络连接架构的实现方法,其特征在于:该方法包括以下步骤:

1) 通过定义接口建立三元对等鉴别可信网络连接架构,其实现方式是:

1. 1) 可信网络传输接口 IF-TNT 的实现:

可信网络传输接口 IF-TNT 通过用户鉴别协议来实现网络访问请求者和访问控制器之间的用户鉴别;通过网络传输协议来实现访问请求者和访问控制器在可信网络连接 TNC 过程中的数据传输;通过访问控制协议来实现访问请求者和访问控制器之间的访问控制;所述用户鉴别协议的实现方式是:若访问请求者和访问控制器之间已实现过用户鉴别,且访问请求者和访问控制器之间的安全关联仍然有效,则网络访问请求者和网络访问控制者利用访问请求者和访问控制器之间的安全关联来实现访问请求者和访问控制器之间的用户鉴别;否则,网络访问请求者、网络访问控制者和鉴别策略服务者执行三元对等鉴别协议来实现访问请求者和访问控制器之间的用户鉴别,其中鉴别策略服务者充当可信第三方角色;所述网络传输协议实现方式为:采用与隧道扩展认证协议 EAP 封装传输机制相同的方式对用户鉴别协议数据和平台鉴别协议数据进行封装传输,其中用户鉴别协议数据封装在一个封装传输包中,而平台鉴别协议数据首先要封装成一个封装传输包并利用安全隧道进行保护,然后将上述安全隧道保护的封装传输包嵌套封装在一个封装传输包中;或者是采用相互独立的封装传输机制对用户鉴别协议数据和平台鉴别协议数据进行封装传输,其中用户鉴别协议数据独立封装在一个封装传输包中,平台鉴别协议数据独立封装在一个封装传输包中并利用安全隧道进行保护;

1. 2) 鉴别策略服务接口 IF-APS 的实现:

鉴别策略服务接口 IF-APS 是网络访问控制者和鉴别策略服务者之间的接口,该接口中定义了用户鉴别协议,用户鉴别协议数据是利用可信网络传输接口 IF-TNT 和鉴别策略服务接口 IF-APS 中定义的网络传输协议进行传输;所述网络传输协议是一个三方协议的封装包和解析包处理过程,该协议数据封装包在访问控制器处通过解析包,然后再封装成另一个协议数据封装包发送给另外一方;

1. 3) TNC 客户端—TNC 接入点接口 IF-TNCCAP 的实现:

TNC 客户端—TNC 接入点接口 IF-TNCCAP 通过网络连接管理机制来实现可信网络连接 TNC 客户端和 TNC 接入点之间的网络连接管理;通过平台鉴别协议来实现访问请求者和访问控制器之间的平台鉴别;通过平台鉴别协议管理机制来实现对平台鉴别过程中平台鉴别协议的管理;通过对完整性度量层消息的封装机制来实现完整性度量层消息的路由;所述网络连接管理机制的实现方法是:可信网络连接 TNC 客户端为每一对可信网络连接 TNC 客户端—TNC 接入点本地创建一个网络连接标识,用于标识每一个可信网络连接 TNC 过程;可信网络连接 TNC 接入点为每一对可信网络连接 TNC 客户端—TNC 接入点本地创建一个网络连接标识,用于标识每一个可信网络连接 TNC 过程;在一个可信网络连接 TNC 过程中,可信网络连接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者首先执行一次平台鉴别过程,若该次平台鉴别过程后通过进行平台修补,或者评估策略发生了改变,则可信网络连接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者通过重新执行一次平台鉴别过程,可信网络连接 TNC 客户端和可信网络连接 TNC 接入点保持上述创建的网络连接标识不变,直至该可信网络连接 TNC 过程被终止;所述平台鉴别协议的实现方法是由可信网络连

接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者执行的三元对等鉴别协议，其中可信网络连接 TNC 客户端和可信网络连接 TNC 接入点互相请求对方平台的完整性度量值，可信网络连接 TNC 客户端和可信网络连接 TNC 接入点仅验证对方平台的完整性度量值的平台签名，而平台身份证书的有效性验证和完整性度量值的评估由评估策略服务者来完成；或者是在一次平台鉴别过程中，可信网络连接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者可能通过执行多轮平台鉴别协议，其中，在每一轮平台鉴别协议中可信网络连接 TNC 客户端和可信网络连接 TNC 接入点互相发送请求对方平台的完整性度量参数，而向评估策略服务者发送的是已完成度量的完整性度量参数，本轮平台鉴别协议完成后，若请求度量的完整性度量参数与已完成度量的完整性度量参数不相同，则可信网络连接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者通过执行另外一轮平台鉴别协议，否则本次平台鉴别过程已成功完成；所述完整性度量层消息的封装机制为：由消息类型、完整性收集者标识和完整性度量层消息构成的封装格式进行封装；

1. 4) 评估策略服务接口 IF-EPS 的实现：

评估策略服务接口 IF-EPS 通过平台鉴别协议来实现访问请求者和访问控制器之间的平台鉴别；通过对完整性度量层消息的封装机制来实现完整性度量层消息的路由；通过评估策略动态分发机制来实现对访问请求者的评估策略的动态分发；所述评估策略动态分发机制是可信网络连接 TNC 接入点向评估策略服务者请求对访问请求者的评估策略，评估策略服务者返回对访问请求者的评估策略给可信网络连接 TNC 接入点；

1. 5) 完整性度量收集者接口 IF-IMC 的实现：

包括访问请求者中完整性度量收集者接口 IF-IMC 的具体实现和访问控制器中完整性度量收集者接口 IF-IMC 的具体实现，其中访问请求者中的完整性度量收集者接口 IF-IMC 和访问控制器中的完整性度量收集者接口 IF-IMC 通过定义功能函数来实现完整性握手；

所述访问请求者中的完整性度量收集者接口 IF-IMC 需定义的功能函数为：可信网络连接 TNC 客户端发现、装载访问请求者中的完整性收集者 IMC；可信网络连接 TNC 客户端初始化访问请求者中的完整性收集者 IMC；访问请求者中的完整性收集者 IMC 向可信网络连接 TNC 客户端报告所支持的消息类型；可信网络连接 TNC 客户端向访问请求者中的完整性收集者 IMC 通告网络连接状态；可信网络连接 TNC 客户端向访问请求者中的完整性收集者 IMC 通告请求度量的完整性度量参数；访问请求者中的完整性收集者 IMC 向可信网络连接 TNC 客户端发送完整性度量层消息；访问请求者中的完整性收集者 IMC 向可信网络连接 TNC 客户端提供完整性度量值中的平台配置寄存器 PCR 引用数据，包括引用的平台配置寄存器 PCR 值和对这些引用平台配置寄存器 PCR 值的平台签名；可信网络连接 TNC 客户端向访问请求者中的完整性收集者 IMC 通告该轮平台鉴别协议的该步骤消息将要发送，让访问请求者中的完整性收集者 IMC 停止收集完整性度量值；可信网络连接 TNC 客户端向访问请求者中的完整性收集者 IMC 发送已收到的完整性度量层消息；可信网络连接 TNC 客户端终止访问请求者中的完整性收集者 IMC；访问请求者中的 IMC 向可信网络连接 TNC 客户端请求重新执行完整性握手；

所述访问控制器中的完整性度量收集者接口 IF-IMC 需定义的功能函数为：可信网络连接 TNC 接入点发现、装载访问控制器中的完整性收集者 IMC；可信网络连接 TNC 接入点初始化访问控制器中的完整性收集者 IMC；访问控制器中的完整性收集者 IMC 向可信网络

连接 TNC 接入点报告所支持的消息类型 ; 可信网络连接 TNC 接入点向访问控制器中的完整性收集者 IMC 通告网络连接状态 ; 可信网络连接 TNC 接入点向访问控制器中的完整性收集者 IMC 通告请求度量的完整性度量参数 ; 访问控制器中的完整性收集者 IMC 向可信网络连接 TNC 接入点发送完整性度量层消息 ; 访问控制器中的完整性收集者 IMC 向可信网络连接 TNC 接入点提供完整性度量值中平台配置寄存器 PCR 引用数据 , 包括引用的平台配置寄存器 PCR 值和对这些引用平台配置寄存器 PCR 值的平台签名 ; 可信网络连接 TNC 接入点向访问控制器中的完整性收集者 IMC 通告该轮平台鉴别协议的该步骤消息将要发送 , 让访问控制器中的完整性收集者 IMC 停止收集完整性度量值 ; 可信网络连接 TNC 接入点向访问控制器中的完整性收集者 IMC 发送已收到的完整性度量层消息 ; 可信网络连接 TNC 接入点终止访问控制器中的完整性收集者 IMC ; 访问控制器中的完整性收集者 IMC 向可信网络连接 TNC 接入点请求重新执行完整性握手 ;

1.6) 完整性度量校验接口 IF-IMV 的实现 : 完整性度量校验接口 IF-IMV 通过定义功能函数来实现完整性握手 ;

所述完整性度量校验接口 IF-IMV 通过定义的功能函数为 : 评估策略服务者发现、装载策略管理器中的完整性校验者 IMV ; 评估策略服务者初始化策略管理器中的完整性校验者 IMV ; 策略管理器中的完整性校验者 IMV 向评估策略服务者报告所支持的消息类型 ; 评估策略服务者向策略管理器中的完整性校验者 IMV 通告本轮平台鉴别协议所通过设置的评估策略 ; 评估策略服务者向策略管理器中的完整性校验者 IMV 发送已收到的完整性度量层消息 ; 策略管理器中的完整性校验者 IMV 向评估策略服务者发送完整性度量层消息 ; 策略管理器中的完整性校验者 IMV 向评估策略服务者提供完整性度量值中平台配置寄存器 PCR 引用数据 , 包括引用的平台配置寄存器 PCR 值和对这些引用 PCR 值的平台签名 ; 策略管理器中的完整性校验者 IMV 向评估策略服务者提供组件级评估结果 ; 评估策略服务者终止策略管理器中的完整性校验者 IMV ;

1.7) 完整性度量接口 IF-IM 的实现 : 完整性度量接口 IF-IM 通过利用完整性收集者 IMC 和完整性校验者 IMV 之间所传输消息的封装方法来实现完整性收集者 IMC 和完整性校验者 IMV 之间的互通 ; 所述完整性度量接口 IF-IM 的封装方法为 : 与 TCG-TNC 架构中消息交换接口 IF-M 的封装方法相同 ;

2) 实现三元对等鉴别可信网络连接架构的可信网络连接 , 其步骤是 :

2.1) 网络访问请求者向网络访问控制者发送网络访问请求 ;

2.2) 网络访问请求者、网络访问控制者和鉴别策略服务者执行可信网络传输接口 IF-TNT 和鉴别策略服务接口 IF-APS 中定义的用户鉴别协议 , 其中用户鉴别协议数据是利用可信网络传输接口 IF-TNT 和鉴别策略服务接口 IF-APS 中定义的网络传输协议进行传输 ; 用户鉴别协议完成后 , 若网络访问控制者要求立即做出访问决策 , 则网络访问控制者根据用户鉴别结果做出访问决策并利用可信网络传输接口 IF-TNT 中定义的访问控制协议执行访问控制 , 否则向可信网络连接 TNC 接入点发送平台鉴别请求 ; 若网络访问请求者要求立即做出访问决策 , 则网络访问请求者根据用户鉴别结果做出访问决策并利用可信网络传输接口 IF-TNT 中定义的访问控制协议执行访问控制 , 否则向可信网络连接 TNC 客户端发送平台鉴别请求 ;

2.3) 当可信网络连接 TNC 接入点收到网络访问控制者发送的平台鉴别请求时 , 若可信

网络连接 TNC 接入点通过向评估策略服务者请求对访问请求者的评估策略，则利用评估策略服务接口 IF-EPS 中定义的评估策略动态分发机制进行该评估策略请求；

2.4) 当可信网络连接 TNC 接入点收到网络访问控制者发送的平台鉴别请求时，可信网络连接 TNC 接入点利用 TNC 客户端—TNC 接入点接口 IF-TNCCAP 中定义的平台鉴别协议启动平台鉴别过程；当可信网络连接 TNC 客户端收到网络访问请求者发送的平台鉴别请求时，若可信网络连接 TNC 接入点没有收到网络访问控制者发送的平台鉴别请求，则可信网络连接 TNC 客户端利用 TNC 客户端—TNC 接入点接口 IF-TNCCAP 中定义的平台鉴别协议启动平台鉴别过程；访问请求者、访问控制器和评估策略服务者执行平台鉴别过程；当可信网络连接 TNC 客户端收到 TNC 客户端—TNC 接入点接口 IF-TNCCAP 和评估策略服务接口 IF-EPS 中定义的平台鉴别协议消息时，通过检查可信网络连接 TNC 客户端是否已装载和初始化访问请求者中的完整性收集者 IMC，若可信网络连接 TNC 客户端还没有装载和初始化访问请求者中的完整性收集者 IMC，则利用访问请求者中完整性度量收集者接口 IF-IMC 定义的功能函数载装和初始化访问请求者中的 IMC；当可信网络连接 TNC 接入点收到 TNC 客户端—TNC 接入点接口 IF-TNCCAP 和评估策略服务接口 IF-EPS 中定义的平台鉴别协议消息时，通过检查可信网络连接 TNC 接入点是否已装载和初始化访问控制器中的完整性收集者 IMC，若可信网络连接 TNC 接入点还没有装载和初始化访问控制器中的完整性收集者 IMC，则利用访问控制器中完整性度量收集者接口 IF-IMC 定义的功能函数载装和初始化访问控制器中的完整性收集者 IMC；当评估策略服务者收到 TNC 客户端—TNC 接入点接口 IF-TNCCAP 和评估策略服务接口 IF-EPS 中定义的平台鉴别协议消息时，通过检查评估策略服务者是否已装载和初始化策略管理器中的完整性校验者 IMV，若评估策略服务者还没有装载和初始化策略管理器中的完整性校验者 IMV，则利用策略管理器中完整性度量校验接口 IF-IMV 定义的功能函数载装和初始化策略管理器中的完整性校验者 IMV；可信网络连接 TNC 客户端、可信网络连接 TNC 接入点和评估策略服务者可执行 TNC 客户端—TNC 接入点接口 IF-TNCCAP 和评估策略服务接口 IF-EPS 中定义的平台鉴别协议，其中平台鉴别协议数据利用可信网络传输接口 IF-TNT 和鉴别策略服务接口 IF-APS 中定义的网络传输协议进行传输，评估策略服务者通过为每一轮平台鉴别协议或每一次平台鉴别过程创建一个会话标识来实现区分；平台鉴别过程完成后，可信网络连接 TNC 客户端可根据平台鉴别过程中各轮平台鉴别协议中的平台鉴别结果做出访问决策并发送给网络访问请求者；可信网络连接 TNC 接入点可根据平台鉴别过程中各轮平台鉴别协议中的平台鉴别结果做出访问决策并发送给网络访问控制者，或者评估策略服务者可根据平台鉴别过程中各轮平台鉴别协议中的平台鉴别结果做出访问决策并发送给可信网络连接 TNC 接入点，然后可信网络连接 TNC 接入点发送给网络访问控制者；网络访问请求者和网络访问控制者利用可信网络传输接口 IF-TNT 中定义的访问控制方法执行访问控制；

2.5) 平台修补完成后，访问请求者中的完整性收集者 IMC 或访问控制器中的完整性收集者 IMC 利用访问请求者中的完整性度量收集者接口 IF-IMC 或访问控制器中的完整性度量收集者接口 IF-IMC 中定义的功能函数向可信网络连接 TNC 客户端或可信网络连接 TNC 接入点请求重新执行平台鉴别过程，或者评估策略发生了改变而要求重新执行平台鉴别过程，则根据网络连接状态和本地安全策略跳至步骤 2.1)、步骤 2.2) 或步骤 2.3)。

2. 根据权利要求 1 所述的三元对等鉴别可信网络连接架构的实现方法，其特征在于：

所述步骤 1.1) 中访问控制协议是基于三元对等鉴别的访问控制方法。

3. 根据权利要求 1 或 2 所述的三元对等鉴别可信网络连接架构的实现方法, 其特征在于 : 所述步骤 2) 中, 对于三元对等鉴别可信网络连接架构中的各个组件, 被装载或服务启用时被执行完整性校验, 以确定这些组件处于可信赖状态。

一种三元对等鉴别可信网络连接架构的实现方法

技术领域

[0001] 本发明涉及一种三元对等鉴别可信网络连接架构的实现方法。

背景技术

[0002] 随着信息化的发展,病毒、蠕虫等恶意软件的问题异常突出。目前已经出现了超过三万五千种的恶意软件,每年都有超过四千万的计算机被感染。要遏制住这类攻击,不仅通过解决安全的传输和数据输入时的检查,还要从源头即从每一台连接到网络的终端开始防御。而传统的安全防御技术已经无法防御种类繁多的恶意攻击。

[0003] 国际可信计算组织 (Trusted Computing Group, TCG) 针对这个问题,专门制定了一个基于可信计算技术的网络连接规范——可信网络连接 (Trusted Network Connect, TNC), 简记为 TCG-TNC, 其包括了开放的终端完整性架构和一套确保安全互操作的标准。这套标准可以在用户通过时保护一个网络,且由用户自定义保护到什么程度。TCG-TNC 本质上就是要从终端的完整性开始建立连接。首先,要创建一套在可信网络内部系统运行状况的策略。只有遵守网络设定策略的终端才能访问网络,网络将隔离和定位那些不遵守策略的设备。由于使用了可信平台模块 (Trusted Platform Module, TPM), 所以还可以阻挡 root kits 的攻击。root kits 是一种攻击脚本、经修改的系统程序,或者成套攻击脚本和工具,用于在一个目标系统中非法获取系统的最高控制权限。TCG-TNC 架构参见图 1。

[0004] 在图 1 中,特定厂家完整性收集者 (Integrity Measurement Collector, IMC)-完整性校验者 (Integrity Measurement Verifier, IMV) 消息交换接口 (Vendor-Specific IMC-IMV Messages, IF-M) 是完整性收集者和完整性校验者之间的接口,TNC 客户端-TNC 服务端接口 (TNC Client-TNC Server Interface, IF-TNCCS) 是 TNC 客户端和 TNC 服务端之间的接口,网络授权传输协议 (Network Authorization Transport Protocol, IF-T) 是网络访问请求者和网络访问授权者之间的接口,策略执行点接口 (Policy Enforcement Point Integrity, IF-PEP) 是策略执行点和网络访问授权者之间的接口,完整性度量收集者接口 (Integrity Measurement Collector Interface, IF-IMC) 是完整性收集者和 TNC 客户端之间的接口,完整性度量校验接口 (Integrity Measurement Verifier Interface, IF-IMV) 是完整性校验者和 TNC 服务端之间的接口。

[0005] 但是,由于图 1 所示的 TCG-TNC 架构中访问请求者不评估策略执行点的完整性,所以该架构存在策略执行点不可信赖的问题。为了解决这一问题,一种基于三元对等鉴别 (Tri-element Peer Authentication, TePA) 的 TNC 架构被提出。基于 TePA 的 TNC 架构参见图 2。

[0006] 在图 2 中,完整性度量接口 (Integrity Measurement Interface, IF-IM) 是完整性收集者和完整性校验者之间的接口, TNC 客户端-TNC 接入点接口 (TNCCClient-TNC Access Point Interface, IF-TNCCAP) 是 TNC 客户端和 TNC 接入点之间的接口,评估策略服务接口 (Evaluation Policy Service Interface) 是 TNC 接入点和评估策略服务者之间的接口,可信网络传输接口 (Trusted Network Transport Interface, IF-TNT) 是网络访问请

求者和网络访问控制者之间的接口,鉴别策略服务接口 (Authentication Policy Service Interface, IF-APS) 是网络访问控制者和鉴别策略服务器之间的接口,完整性度量收集者接口 (Integrity MeasurementCollector Interface, IF-IMC) 是完整性收集者和 TNC 客户端之间,以及完整性收集者和 TNC 接入点之间的接口,完整性度量校验接口 (Integrity MeasurementVerifier Interface, IF-IMV) 是完整性校验者和评估策略服务者之间的接口。

[0007] 为了具体实现图 1 所示的 TCG-TNC 架构,TCG 详细定义了 TCG-TNC 架构中各个接口的具体实现方法:在 IF-PEP 规范中定义远程用户拨号认证系统 (Remote Authentication Dial In User Service, RADIUS) 协议等;在 IF-T 规范中定义了绑定可扩展认证协议 (Extensible Authentication Protocol, EAP) 的隧道 EAP 封装传输方法等;在 IF-TNCCS 规范中定义了平台鉴别(包括平台凭证鉴别和完整性握手)的消息传输协议和连接管理等,包括如何路由 IMC 和 IMV 之间传输的消息;在 IF-M 规范中定义了 IMC 和 IMV 之间所传输消息的封装方法等,包括定义 IF-M 消息来描述组件的各个属性及其相关处理属性,如:产品信息属性和安全处理属性等;在 IF-IMC 规范中定义了 TNC 客户端和 IMC 之间的功能函数,用于支持平台鉴别过程;在 IF-IMV 规范中定义了 TNC 服务端和 IMV 之间的功能函数,也是用于支持平台鉴别过程。此外,在 TNC 过程中 TCG-TNC 架构的一些组件还可能通过可信平台服务接口 (Trusted Platform Service Interface, IF-PTS) 与可信平台服务 (Trusted Platform Service, PTS) 进行通信。PTS 负责管理完整性度量日志、创建快照和完整性报告等,并通过 IF-PTS 为 TCG-TNC 架构的一些组件提供服务。IF-PTS 是一个与架构类型无关的接口,即该 IF-PTS 可适用于图 1 和图 2 所示的 TNC 架构。

[0008] 同理,为了具体实现图 2 所示的基于 TePA 的 TNC 架构,需要通过详细定义基于 TePA 的 TNC 架构中各个接口的具体实现方法,然后基于上述接口的具体实现来实现基于 TePA 的 TNC 架构。但是,由于图 2 所示的基于 TePA 的 TNC 架构与图 1 所示的 TCG-TNC 架构存在着较大的差异性,所以基于 TePA 的 TNC 架构的具体实现方法也不同。

发明内容

[0009] 为了解决背景技术中存在的上述技术问题,本发明提供了一种建立终端可信、实现终端的可信网络连接、实现终端间的可信认证和实现对终端的可信管理的适合三元对等鉴别可信网络连接架构的实现方法。本发明的目的就是详细定义基于 TePA 的 TNC 架构中各个接口的具体实现方法,然后基于上述接口的具体实现来实现基于 TePA 的 TNC 架构。

[0010] 本发明的技术解决方案是:本发明提供了一种三元对等鉴别可信网络连接架构的实现方法,其特殊之处在于:该方法包括以下步骤:

[0011] 1) 通过定义接口建立三元对等鉴别可信网络连接架构,其具体实现方式是:

[0012] 1. 1) IF-TNT 的具体实现:

[0013] IF-TNT 通过用户鉴别协议来实现网络访问请求者和访问控制器之间的用户鉴别;通过网络传输协议来实现访问请求者和访问控制器在 TNC 过程中的数据传输;通过访问控制协议来实现访问请求者和访问控制器之间的访问控制;

[0014] 1. 2) IF-APS 的具体实现:

[0015] IF-APS 通过用户鉴别协议来实现网络访问请求者和访问控制器之间的用户鉴别;

通过网络传输协议来实现访问请求者和访问控制器在 TNC 过程中的数据传输；

[0016] 1.3) IF-TNCCAP 的具体实现：

[0017] IF-TNCCAP 通过网络连接管理机制来实现 TNC 客户端和 TNC 接入点之间的网络连接管理；通过平台鉴别协议来实现访问请求者和访问控制器之间的平台鉴别；通过平台鉴别协议管理机制来实现对平台鉴别过程中平台鉴别协议的管理；通过对完整性度量层消息的封装机制来实现完整性度量层消息的路由；

[0018] 1.4) IF-EPS 的具体实现：

[0019] IF-EPS 通过平台鉴别协议来实现访问请求者和访问控制器之间的平台鉴别；通过对完整性度量层消息的封装机制来实现完整性度量层消息的路由；通过评估策略动态分发机制来实现对访问请求者的评估策略的动态分发；

[0020] 1.5) IF-IMC 的具体实现：

[0021] 包括访问请求者中 IF-IMC 的具体实现和访问控制器中 IF-IMC 的具体实现，其中访问请求者中的 IF-IMC 和访问控制器中的 IF-IMC 通过定义功能函数来实现完整性握手；

[0022] 1.6) IF-IMV 的具体实现：IF-IMV 通过定义功能函数来实现完整性握手；

[0023] 1.7) IF-IM 的具体实现：IF-IM 通过利用 IMC 和 IMV 之间所传输消息的封装方法来实现 IMC 和 IMV 之间的互通；

[0024] 2) 实现三元对等鉴别可信网络连接架构的可信网络连接，其具体步骤是：

[0025] 2.1) 网络访问请求者向网络访问控制者发送网络访问请求；

[0026] 2.2) 网络访问请求者、网络访问控制者和鉴别策略服务者执行 IF-TNT 和 IF-APS 中定义的用户鉴别协议，其中用户鉴别协议数据是利用 IF-TNT 和 IF-APS 中定义的网络传输协议进行传输；用户鉴别协议完成后，若网络访问控制者要求立即做出访问决策，则网络访问控制者根据用户鉴别结果做出访问决策并利用 IF-TNT 中定义的访问控制协议执行访问控制，否则向 TNC 接入点发送平台鉴别请求；若网络访问请求者要求立即做出访问决策，则网络访问请求者根据用户鉴别结果做出访问决策并利用 IF-TNT 中定义的访问控制协议执行访问控制，否则向 TNC 客户端发送平台鉴别请求；

[0027] 2.3) 当 TNC 接入点收到网络访问控制者发送的平台鉴别请求时，若 TNC 接入点通过向评估策略服务者请求对访问请求者的评估策略，则利用 IF-EPS 中定义的评估策略动态分发机制进行该评估策略请求；

[0028] 2.4) 当 TNC 接入点收到网络访问控制者发送的平台鉴别请求时，TNC 接入点利用 IF-TNCCAP 中定义的平台鉴别协议启动平台鉴别过程；当 TNC 客户端收到网络访问请求者发送的平台鉴别请求时，若 TNC 接入点没有收到网络访问控制者发送的平台鉴别请求，则 TNC 客户端利用 IF-TNCCAP 中定义的平台鉴别协议启动平台鉴别过程；访问请求者、访问控制器和评估策略服务者执行平台鉴别过程；

[0029] 2.5) 平台修补完成后，访问请求者中的 IMC 或访问控制器中的 IMC 利用访问请求者中的 IF-IMC 或访问控制器中的 IF-IMC 中定义的功能函数向 TNC 客户端或 TNC 接入点请求重新执行平台鉴别过程，或者评估策略发生了改变而要求重新执行平台鉴别过程，则根据网络连接状态和本地安全策略跳至步骤 2.1)、步骤 2.2) 或步骤 2.3)。

[0030] 上述步骤 1.1) 和步骤 1.2) 中用户鉴别协议的实现方式是：若访问请求者和访问控制器之间已实现过用户鉴别，且访问请求者和访问控制器之间的安全关联仍然有效，则

网络访问请求者和网络访问控制者利用访问请求者和访问控制器之间的安全关联来实现访问请求者和访问控制器之间的用户鉴别；否则，网络访问请求者、网络访问控制者和鉴别策略服务者执行三元对等鉴别协议来实现访问访问请求者和访问控制器之间的用户鉴别，其中鉴别策略服务者充当可信第三方角色。

[0031] 上述步骤 1.1) 和步骤 1.2) 中网络传输协议实现方式为：采用与隧道 EAP 封装传输机制相同的方式对用户鉴别协议数据和平台鉴别协议数据进行封装传输，其中用户鉴别协议数据封装在一个封装传输包中，而平台鉴别协议数据首先要封装成一个封装传输包并利用安全隧道进行保护，然后将上述安全隧道保护的封装传输包嵌套封装在一个封装传输包中。

[0032] 上述步骤 1.1) 和步骤 1.2) 中网络传输协议实现方式为：采用相互独立的封装传输机制对用户鉴别协议数据和平台鉴别协议数据进行封装传输，其中用户鉴别协议数据独立封装在一个封装传输包中，平台鉴别协议数据独立封装在一个封装传输包中并利用安全隧道进行保护。

[0033] 上述步骤 1.1) 中访问控制协议是基于三元对等鉴别的访问控制方法。

[0034] 上述步骤 1.3) 中的网络连接管理机制的实现方法是：TNC 客户端为每一对 TNC 客户端——TNC 接入点本地创建一个网络连接标识，用于标识每一个 TNC 过程；TNC 接入点为每一对 TNC 客户端——TNC 接入点本地创建一个网络连接标识，用于标识每一个 TNC 过程；在一个 TNC 过程中，TNC 客户端、TNC 接入点和评估策略服务者首先执行一次平台鉴别过程，若该次平台鉴别过程后通过进行平台修补，或者评估策略发生了改变，则 TNC 客户端、TNC 接入点和评估策略服务者通过重新执行一次平台鉴别过程，TNC 客户端和 TNC 接入点保持上述创建的网络连接标识不变，直至该 TNC 过程被终止。

[0035] 上述步骤 1.3) 和步骤 1.4) 中的平台鉴别协议的实现方法是由 TNC 客户端、TNC 接入点和评估策略服务者执行的三元对等鉴别协议，其中 TNC 客户端和 TNC 接入点互相请求对方平台的完整性度量值，TNC 客户端和 TNC 接入点仅验证对方平台的完整性度量值的平台签名，而平台身份证件的有效性验证和完整性度量值的评估由评估策略服务者来完成。

[0036] 上述步骤 1.3) 中的平台鉴别协议管理机制的实现方法是：在一次平台鉴别过程中，TNC 客户端、TNC 接入点和评估策略服务者可能通过执行多轮平台鉴别协议，其中，在每一轮平台鉴别协议中 TNC 客户端和 TNC 接入点互相发送请求对方平台的完整性度量参数，而向评估策略服务者发送的是已完成度量的完整性度量参数，本轮平台鉴别完成后，若请求度量的完整性度量参数与已完成度量的完整性度量参数不相同，则 TNC 客户端、TNC 接入点和评估策略服务者通过执行另外一轮平台鉴别协议，否则本次平台鉴别过程已成功完成。

[0037] 上述步骤 1.3) 和步骤 1.4) 中的对完整性度量层消息的封装机制为：由消息类型、完整性收集者标识和完整性度量层消息构成的封装格式进行封装。

[0038] 上述步骤 1.4) 中的评估策略动态分发机制是 TNC 接入点向评估策略服务者请求对访问请求者的评估策略，评估策略服务者返回对访问请求者的评估策略给 TNC 接入点。

[0039] 上述步骤 1.5) 中的访问请求者中的 IF-IMC 需定义的功能函数为：TNC 客户端发现、装载访问请求者中的 IMC；TNC 客户端初始化访问请求者中的 IMC；访问请求者中的 IMC 向 TNC 客户端报告所支持的消息类型；TNC 客户端向访问请求者中的 IMC 通告网络连接状

态 ;TNC 客户端向访问请求者中的 IMC 通告请求度量的完整性度量参数 ; 访问请求者中的 IMC 向 TNC 客户端发送完整性度量层消息 ; 访问请求者中的 IMC 向 TNC 客户端提供完整性度量值中的 PCR 引用数据 , 包括引用的 PCR 值和对这些引用 PCR 值的平台签名 ;TNC 客户端向访问请求者中的 IMC 通告该轮平台鉴别协议的该步骤消息将要发送 , 让访问请求者中的 IMC 停止收集完整性度量值 ;TNC 客户端向访问请求者中的 IMC 发送已收到的完整性度量层消息 ;TNC 客户端终止访问请求者中的 IMC ; 访问请求者中的 IMC 向 TNC 客户端请求重新执行完整性握手。

[0040] 上述步骤 1.5) 中的访问控制器中的 IF-IMC 需定义的功能函数为 :TNC 接入点发现、装载访问控制器中的 IMC ;TNC 接入点初始化访问控制器中的 IMC ; 访问控制器中的 IMC 向 TNC 接入点报告所支持的消息类型 ;TNC 接入点向访问控制器中的 IMC 通告网络连接状态 ;TNC 接入点向访问控制器中的 IMC 通告请求度量的完整性度量参数 ; 访问控制器中的 IMC 向 TNC 接入点发送完整性度量层消息 ; 访问控制器中的 IMC 向 TNC 接入点提供完整性度量值中 PCR 引用数据 , 包括引用的 PCR 值和对这些引用 PCR 值的平台签名 ;TNC 接入点向访问控制器中的 IMC 通告该轮平台鉴别协议的该步骤消息将要发送 , 让访问控制器中的 IMC 停止收集完整性度量值 ;TNC 接入点向访问控制器中的 IMC 发送已收到的完整性度量层消息 ;TNC 接入点终止访问控制器中的 IMC ; 访问控制器中的 IMC 向 TNC 接入点请求重新执行完整性握手。

[0041] 上述步骤 1.6) 中的 IF-IMV 通过定义的功能函数为 : 评估策略服务者发现、装载策略管理器中的 IMV ; 评估策略服务者初始化策略管理器中的 IMV ; 策略管理器中的 IMV 向评估策略服务者报告所支持的消息类型 ; 评估策略服务者向策略管理器中的 IMV 通告本轮平台鉴别协议所通过设置的评估策略 ; 评估策略服务者向策略管理器中的 IMV 发送已收到的完整性度量层消息 ; 策略管理器中的 IMV 向评估策略服务者发送完整性度量层消息 ; 策略管理器中的 IMV 向评估策略服务者提供完整性度量值中 PCR 引用数据 , 包括引用的 PCR 值和对这些引用 PCR 值的平台签名 ; 策略管理器中的 IMV 向评估策略服务者提供组件级评估结果 ; 评估策略服务者终止策略管理器中的 IMV 。

[0042] 上述步骤 1.7) 中的 IF-IM 的封装方法为 : 与 TCG-TNC 架构中 IF-M 的封装方法相同。

[0043] 上述步骤 2.4) 中 , 当 TNC 客户端收到 IF-TNCCAP 和 IF-EPS 中定义的平台鉴别协议消息时 , 通过检查 TNC 客户端是否已装载和初始化访问请求者中的 IMC , 若 TNC 客户端还没有装载和初始化访问请求者中的 IMC , 则利用访问请求者中 IF-IMC 定义的功能函数载装和初始化访问请求者中的 IMC ; 当 TNC 接入点收到 IF-TNCCAP 和 IF-EPS 中定义的平台鉴别协议消息时 , 通过检查 TNC 接入点是否已装载和初始化访问控制器中的 IMC , 若 TNC 接入点还没有装载和初始化访问控制器中的 IMC , 则利用访问控制器中 IF-IMC 定义的功能函数载装和初始化访问控制器中的 IMC ; 当评估策略服务者收到 IF-TNCCAP 和 IF-EPS 中定义的平台鉴别协议消息时 , 通过检查评估策略服务者是否已装载和初始化策略管理器中的 IMV , 若评估策略服务者还没有装载和初始化策略管理器中的 IMV , 则利用策略管理器中 IF-IMV 定义的功能函数载装和初始化策略管理器中的 IMV 。

[0044] 上述步骤 2.4) 中 , TNC 客户端、TNC 接入点和评估策略服务者可执行 IF-TNCCAP 和 IF-EPS 中定义的平台鉴别协议 , 其中平台鉴别协议数据利用 IF-TNT 和 IF-APS 中定义的网

络传输协议进行传输,评估策略服务者通过为每一轮平台鉴别协议或每一次平台鉴别过程创建一个会话标识来实现区分。

[0045] 上述步骤 2.4) 中,平台鉴别过程完成后,TNC 客户端可根据平台鉴别过程中各轮平台鉴别协议中的组件级评估结果做出访问决策并发送给网络访问请求者;TNC 接入点可根据平台鉴别过程中各轮平台鉴别协议中的组件级评估结果做出访问决策并发送给网络访问控制者,或者评估策略服务者可根据平台鉴别过程中各轮平台鉴别协议中的组件级评估结果做出访问决策并发送给 TNC 接入点,然后 TNC 接入点发送给网络访问控制者;网络访问请求者和网络访问控制者利用 IF-TNT 中定义的访问控制方法执行访问控制。

[0046] 上述步骤 2) 中,对于三元对等鉴别可信网络连接架构中的各个组件,被装载或服务启用时被执行完整性校验,以确定这些组件处于可信状态。

[0047] 本发明的优点是:

[0048] 1、本发明可建立终端可信。本发明在建立终端可信的过程中,基于 TePA 的 TNC 架构中的访问请求者中的完整性收集者、TNC 客户端、TNC 接入点由终端来实现,而策略管理器中的完整性校验者和评估策略服务者可由终端来实现,也可由第三方服务提供者来实现,然后执行基于 TePA 的 TNC 架构中的平台鉴别过程来建立终端可信。

[0049] 2、本发明可实现终端的可信网络连接。本发明在终端的可信网络连接过程中,基于 TePA 的 TNC 架构中的访问请求者由接入网络的终端来实现,而访问控制器和策略管理器由网络服务提供者来实现,其中策略管理器的部分功能或所有功能还可以由第三方服务提供者来实现,然后执行基于 TePA 的 TNC 架构中的 TNC 过程来实现终端的可信网络连接。

[0050] 3、本发明可实现终端间的可信认证。本发明在终端间的可信认证中,基于 TePA 的 TNC 架构中的访问请求者由一个终端来实现,而访问控制器由另一个终端来实现,策略管理器可由网络服务提供者来实现,其中策略管理器的部分功能或所有功能还可以由第三方服务提供者来实现,若终端间已完成用户鉴别并生成了会话密钥,则执行基于 TePA 的 TNC 架构中的平台鉴别过程来实现终端间的可信认证,否则执行基于 TePA 的 TNC 架构中的 TNC 过程来实现终端间的可信认证。

[0051] 4、本发明可实现对终端的可信管理。本发明在对终端的可信管理过程中,基于 TePA 的 TNC 架构中的访问请求者由终端来实现,而访问控制器和策略管理器由网络服务提供者来实现,其中策略管理器的部分功能或所有功能还可以由第三方服务提供者来实现,若终端和网络服务提供者之间已完成用户鉴别并生成了会话密钥,则执行基于 TePA 的 TNC 架构中的平台鉴别过程来实现对终端的可信管理,否则执行基于 TePA 的 TNC 架构中的 TNC 过程来实现对终端的可信管理。

[0052] 5、本发明可广泛应用。本发明基于 TePA 的 TNC 架构的具体实现中的平台鉴别过程可采用一轮平台鉴别协议完成,也可以采用多轮平台鉴别协议完成,满足不同网络设备的需求。

[0053] 6、本发明有利于独立实现。本发明在基于 TePA 的 TNC 架构的具体实现中,策略管理器不参与网络连接管理,是一个独立的角色,有利于独立实现,从而使得策略管理器完全可以由可信第三方来实现;

附图说明

- [0054] 图 1 为现有技术中 TCG-TNC 架构示意图；
- [0055] 图 2 为现有技术中基于 TePA 的 TNC 架构示意图；
- [0056] 图 3 为本发明的访问请求者中 IF-IMC 的交互示意图；
- [0057] 图 4 为本发明的访问控制器中 IF-IMC 的交互示意图；
- [0058] 图 5 为本发明的策略管理器中 IF-IMV 的交互示意图。

具体实施方式

[0059] 本发明提供了一种三元对等鉴别可信网络连接架构的实现方法，该方法包括以下步骤：

[0060] 1) 通过定义接口建立三元对等鉴别可信网络连接架构，其具体实现方式是：

- [0061] 1. 1) IF-TNT 和 IF-APS 的具体实现方法：

[0062] IF-TNT 和 IF-APS 中定义的用户鉴别协议可以采用基于对称密钥和非对称密钥的三元对等鉴别协议，如：中国无线局域网标准中的 WAI 协议。

[0063] IF-TNT 和 IF-APS 中定义的网络传输协议可以为：协议数据封装包可以采用与 EAP 相同或类似的协议数据封装包，但该协议数据封装包的处理与 EAP 不一样，该协议数据封装包在访问控制器处通过解析包，然后再封装成另一个协议数据封装包发送给另外一方，不像 EAP 是一个点到点协议的封装包和解析包处理过程，而是一个三方协议的封装包和解析包处理过程，其中三方协议封装包可称为三元认证扩展协议封装包 (Tri-element Authentication Extensible Protocol, TAEP)；用户鉴别协议数据和平台鉴别协议数据可以采用与隧道 EAP 类似的封装方法进行封装，也可以采用相互独立的封装方法进行封装，对于前者，访问请求者和访问控制器将收到一个成功类型的协议数据封装包，如：TAEP-success 封装包，与整个 TNC 过程相对应，对于后者，访问请求者和访问控制器将收到两个成功类型的协议数据封装包，如：TAEP-success 封装包，分别与用户鉴别过程、平台鉴别过程相对应。

[0064] IF-TNT 和 IF-APS 中定义的访问控制协议可以采用基于三元对等鉴别的访问控制方法，如：中国无线局域网标准中所采用的访问控制方法。

- [0065] 1. 2) IF-TNCCAP 和 IF-EPS 的具体实现方法：

[0066] IF-TNCCAP 中定义的网络连接管理机制可以为：TNC 客户端本地生成与 TNC 接入点的网络连接标识，TNC 接入点本地生成与 TNC 客户端的网络连接标识，网络连接标识用 ConnectionID 表示；TNC 客户端和 TNC 接入点为每一个 ConnectionID 设置一些网络连接状态，如：创建、完整性握手、允许、禁止、隔离和终止连接。在一个 TNC 过程中，TNC 客户端、TNC 接入点和评估策略服务者首先执行一次平台鉴别过程，若本次平台鉴别过程后需要进行平台修补，或者评估策略发生了改变，则 TNC 客户端、TNC 接入点和评估策略服务者需要重新执行一次平台鉴别过程，TNC 客户端和 TNC 接入点保持上述创建的 ConnectionID 不变，但网络连接状态可以设置为不同状态，直至该 TNC 过程被终止。

[0067] IF-TNCCAP 中定义的平台鉴别协议管理机制可以为：在一次平台鉴别过程中，TNC 客户端、TNC 接入点和评估策略服务者可能需要执行多轮平台鉴别协议，其中，在每一轮平台鉴别协议中 TNC 客户端和 TNC 接入点互相发送请求对方平台的完整性度量参数，而向评估策略服务者发送的是已完成度量的完整性度量参数，本轮平台鉴别协议完成后，若请求

度量的完整性度量参数与已完成度量的完整性度量参数不相同，则 TNC 客户端、TNC 接入点和评估策略服务者需要执行另外一轮平台鉴别协议，否则本次平台鉴别过程已成功完成。

[0068] IF-EPS 中定义的评估策略动态分发机制可以为：评估策略服务者为每一级别用户、每一级别服务设置对应的评估策略，TNC 接入点可以将访问请求者的用户身份、或者访问请求者所请求的服务、或者访问请求者的用户身份和所请求的服务发送给评估策略服务者，然后评估策略服务者依据本地的设置向 TNC 接入点返回对访问请求者的评估策略。

[0069] IF-TNCCAP 和 IF-EPS 中定义的对完整性度量层消息的封装机制可为（消息类型 + 完整性收集者标识 + 完整性度量层消息表）列表，该消息类型可由组件类型和厂家标识构成：

[0070]

消息类型	完整性收集者标识	完整性度量层消息 1	完整性度量层消息 2
消息类型	完整性收集者标识	完整性度量层消息 1	完整性度量层消息 2
.....

[0071] IF-TNCCAP 和 IF-APS 中定义的平台鉴别协议是由 TNC 客户端、TNC 接入点和评估策略服务者执行的三元对等鉴别协议，其中 TNC 客户端和 TNC 接入点互相请求对方平台的完整性度量值，TNC 客户端和 TNC 接入点仅验证对方平台的完整性度量值的平台签名，而平台身份证件的有效性验证和完整性度量值的评估由评估策略服务者来完成。

[0072] 1.3) 访问请求者中 IF-IMC 的具体实现方法：

[0073] 访问请求者中 IF-IMC 的功能函数为：

[0074] 1.3.1) 发现、装载访问请求者中的 IMC 的函数，它与特定平台相关，可以利用不同的方法实现；

[0075] 1.3.2) TNC_IMC_Initialize{imcID, minVersion, maxVersion, *pOutActualVersion}，用于初始化 IMC，由访问请求者中的 IMC 实现，其中 imcID 为 TNC 客户端为该 IMC 分配的完整性收集者标识，minVersion 和 maxVersion 是 TNC 客户端支持的应用接口函数版本号，*pOutActualVersion 是实际使用的应用接口函数版本号；

[0076] 1.3.3) TNC_TNCC_ReportMessageTypes{imcID, supportedTypes, typeCount}，用于访问请求者中的 IMC 向 TNC 客户端通告所支持的消息类型，由 TNC 客户端实现，其中 supportedTypes 为访问请求者所支持的各个消息类型，typeCount 为访问请求者所支持的消息类型的数目；

[0077] 1.3.4) TNC_IMC_NotifyConnectionChange{imcID, connectionID, newState}，用于 TNC 客户端向访问请求者中的 IMC 通告网络连接状态，由 IMC 实现，其中 connectionID 为 TNC 客户端创建的网络连接标识，newState 为网络连接状态；

[0078] 1.3.5) TNC_IMC_RequestMeasurementInfo{imcID, connectionID, MeasurementInfo}，用于 TNC 客户端向访问请求者中的 IMC 通知请求度量的完整性度量参数，由 IMC 实现，其中 MeasurementInfo 为请求度量的完整性度量参数；

[0079] 1.3.6) TNC_TNCC_SendMessage{imcID, connectionID, message, messageLength, messageType}，用于访问请求者中的 IMC 向 TNC 客户端发送完整性度量层消息，由 TNC

客户端实现,其中 messgae 为完整性度量层消息, messageLength 为 message 的长度, messageType 为 message 的消息类型 ;

[0080] 1. 3. 7) TNC_TNCC_ProvidePCRsIndex{imcID, connectionID, PCRsIndex} ,用于访问请求者中的 IMC 向 TNC 客户端提供完整性度量值中的 PCR 引用数据 (可信平台评估层组件可知的),由 TNC 客户端实现,其中 PCRsIndex 为完整性度量值中的 PCR 引用数据 ;

[0081] 1. 3. 8) TNC_IMC_PAIEnding{imcID, connectionID} ,用于 TNC 客户端向访问请求者中的 IMC 通告该轮平台鉴别协议的该步骤消息将要发送,让访问请求者中的 IMC 停止收集完整性度量值,由 IMC 实现 ;

[0082] 1. 3. 9) TNC_IMC_ReceiveMessage{imcID, connectionID, messgae, messageLength, messageType} ,用于 TNC 客户端向访问请求者中的 IMC 发送已收到的完整性度量层消息,由 IMC 实现 ;

[0083] 1. 3. 10) TNC_IMC_Terminate{imcID} ,用于 TNC 客户端终止访问请求者中的 IMC,由 IMC 实现 ;

[0084] 1. 3. 11) TNC_TNCC_RequestHandshakeRetry{imcID, connectionID, reason} , 用于访问请求者中的 IMC 向 TNC 客户端请求重新执行完整性握手,由 TNC 客户端实现,其中 reason 为请求重新执行完整性握手的原因。

[0085] 在平台鉴别过程中,访问请求者中 IF-IMC 的交互示意图,参见图 3。在图 3 中, IF-IMC 中的虚线功能函数调用箭头表示可选的,而实线功能函数调用箭头表示必备的,完整性握手过程中的平台鉴别协议可以是任意轮的 (不局限于 2 轮),直至做出访问决策为止,且访问请求者和访问控制器都可以发起平台鉴别协议。

[0086] 1. 4) 访问控制器中 IF-IMC 的具体实现方法

[0087] 访问控制器中 IF-IMC 的功能函数为 :

[0088] 1. 4. 1) 发现、装载访问控制器中的 IMC 的函数,它与特定平台相关,可以利用不同的方法实现 ;

[0089] 1. 4. 2) TNC_IMC_Initialize{imcID, minVersion, maxVersion, *pOutActualVersion} ,用于初始化 IMC,由访问控制器中的 IMC 实现,其中 imcID 为 TNC 接入点为该 IMC 分配的完整性收集者标识, minVersion 和 maxVersion 是 TNC 接入点支持的应用接口函数版本号,*pOutActualVersion 是实际使用的应用接口函数版本号 ;

[0090] 1. 4. 3) TNC_TNCAP_ReportMessageTypes{imcID, supportedTypes, typeCount} ,用于访问控制器中的 IMC 向 TNC 接入点通告所支持的消息类型,由 TNC 接入点实现,其中 supportedTypes 为访问控制器所支持的各个消息类型, typeCount 为访问控制器所支持的消息类型的数目 ;

[0091] 1. 4. 4) TNC_IMC_NotifyConnectionChange{imcID, connectionID, newState} , 用于 TNC 接入点向访问控制器中的 IMC 通告网络连接状态,由 IMC 实现,其中 connectionID 为 TNC 接入点创建的网络连接标识, newState 为网络连接状态 ;

[0092] 1. 4. 5) TNC_IMC_RequestMeasurementInfo{imcID, connectionID, MeasurementInfo} ,用于 TNC 接入点向访问控制器中的 IMC 通知请求度量的完整性度量参数,由 IMC 实现,其中 MeasurementInfo 为请求度量的完整性度量参数 ;

[0093] 1. 4. 6) TNC_TNCAP_SendMessage{imcID, connectionID, messgae, messageLength,

messageType} , 用于访问控制器中的 IMC 向 TNC 接入点发送完整性度量层消息, 由 TNC 接入点实现, 其中 message 为完整性度量层消息, messageLength 为 message 的长度, messageType 为 message 的消息类型;

[0094] 1.4.7) TNC_TNCAP_ProvidePCRsIndex {imcID, connectionID, PCRsIndex} , 用于访问控制器中的 IMC 向 TNC 接入点提供完整性度量值中的 PCR 引用数据 (可信平台评估层组件可知的), 由 TNC 接入点实现, 其中 PCRsIndex 为完整性度量值中的 PCR 引用数据;

[0095] 1.4.8) TNC_IMC_PAIEnding {imcID, connectionID} , 用于 TNC 接入点向访问控制器中的 IMC 通告该轮平台鉴别协议的该步骤消息将要发送, 让访问控制器中的 IMC 停止收集完整性度量值, 由 IMC 实现;

[0096] 1.4.9) TNC_IMC_ReceiveMessage {imcID, connectionID, message, messageLength, messageType} , 用于 TNC 接入点向访问控制器中的 IMC 发送已收到的完整性度量层消息, 由 IMC 实现;

[0097] 1.4.10) TNC_IMC_Terminate {imcID} , 用于 TNC 接入点终止访问控制器中的 IMC, 由 IMC 实现;

[0098] 1.4.11) TNC_TNCAP_RequestHandshakeRetry {imcID, connectionID, reason} , 用于访问控制器中的 IMC 向 TNC 接入点请求重新执行完整性握手, 由 TNC 接入点实现, 其中 reason 为请求重新执行完整性握手的原因。

[0099] 在平台鉴别过程中, 访问控制器中 IF-IMC 的交互示意图, 参见图 4。在图 4 中, IF-IMC 中的虚线功能函数调用箭头表示可选的, 而实线功能函数调用箭头表示必备的, 完整性握手过程中的平台鉴别协议可以是任意轮的 (不局限于 2 轮), 直至做出访问决策为止, 且访问请求者和访问控制器都可以发起平台鉴别协议。

[0100] 1.5) IF-IMV 的具体实现方法:

[0101] 策略管理器中 IF-IMV 的功能函数为:

[0102] 1.5.1) 发现、装载策略管理器中的 IMV 的功能函数, 它与特定平台相关, 可以利用不同的方法实现;

[0103] 1.5.2) TNC_IMV_Initialize {imvID, minVersion, maxVersion, *pOutActualVersion} , 用于评估策略服务者初始化策略管理器中的 IMV, 由策略管理器中的 IMV 实现, 其中 imvID 为评估策略服务者为该策略管理器中的 IMV 分配的完整性校验者标识, minVersion 和 maxVersion 是评估策略服务者支持的应用接口函数版本号, *pOutActualVersion 是实际使用的应用接口函数版本号;

[0104] 1.5.3) TNC_EPS_ReportMessageTypes {imvID, supportedTypes, typeCount} , 用于策略管理器中的 IMV 向评估策略服务者通告所支持的消息类型, 由评估策略服务者实现, 其中 supportedTypes 为策略管理器中的 IMV 所支持的各个消息类型, typeCount 为策略管理器中的 IMV 所支持的消息类型的数目;

[0105] 1.5.4) TNC_IMV_SetAttributePolicy {imvID, PAIBindingID, AttributePolicy} , 用于评估策略服务者向策略管理器中的 IMV 通告本轮平台鉴别协议所通过设置的评估策略, 由策略管理器中的 IMV 实现, 其中 PAIBindingID 为评估策略服务者为本轮平台鉴别协议创建的平台鉴别协议绑定标识, 目的是使评估策略服务者可以管理所执行的各个平台鉴别协议, 如: 由平台鉴别协议中访问控制器的平台鉴别校验挑战 N_{AC-PM} 和访问请求者的平台

鉴别请求挑战 N_{AR} 共同导出的一个随机数, AttributePolic 为所通过设置的评估策略;

[0106] 1.5.5) TNC_IMV_ReceiveMessage {imvID, PAIBindingID, messgae, messageLength, messageType}, 用于评估策略服务者向策略管理器中的 IMV 发送已收到的完整性度量层消息, 由策略管理器中的 IMV 实现, 其中 messgae 为完整性度量层消息, messageLength 为 message 的长度, messageType 为 message 的消息类型;

[0107] 1.5.6) TNC_EPS_SendMessage {imvID, PAIBindingID, messgae, messageLength, messageType}, 用于策略管理器中的 IMV 向评估策略服务者发送完整性度量层消息, 由评估策略服务者实现;

[0108] 1.5.7) TNC_EPS_ProvideRecommendation {imvID, PAIBindingID, recommendation, evaluation}, 用于策略管理器中的 IMV 向评估策略服务者提供组件级评估结果(可信平台评估层组件可知的), 由评估策略服务者实现, 其中 recommendation 为组件级评估结果中的行为推荐, evaluation 为组件级评估结果中的评定结果;

[0109] 1.5.8) TNC_EPS_ProvidePCRsIndex {imvID, PAIBindingID, PCRsIndex}, 用于策略管理器中的 IMV 向评估策略服务者提供完整性度量值中的 PCR 引用数据(可信平台评估层组件可知的), 由评估策略服务者实现, 其中 PCRsIndex 为完整性度量值中的 PCR 引用数据;

[0110] 1.5.9) TNC_IMV_Terminate {imvID}, 用于评估策略服务者终止的策略管理器中的 IMV, 由策略管理器中的 IMV 实现;

[0111] 在平台鉴别过程中, 策略管理器中 IF-IMV 的交互示意图, 参见图 5。在图 5 中, IF-IMV 中的虚线功能函数调用箭头表示可选的, 而实线功能函数调用箭头表示必备的, 完整性握手过程中的平台鉴别协议可以是任意轮的(不局限于 2 轮), 直至做出访问决策为止, 且访问请求者和访问控制器都可以发起平台鉴别协议。

[0112] 1.6) IF-IM 的具体实现方法:

[0113] 除了使用 TNC_IMC_RequestMeasurementInfo 来完成 TCG-TNC 架构中的请求完整性度量属性功能(使用完整性度量层消息来完成, 即使用 IF-M 消息来完成)外, 其他与 TCG-TNC 架构中 IF-M 相同。

[0114] 2) 实现三元对等鉴别可信网络连接架构的可信网络连接, 其具体步骤是:

[0115] 2.1) 网络访问请求者向网络访问控制者发送网络访问请求;

[0116] 2.2) 网络访问请求者、网络访问控制者和鉴别策略服务者执行用户鉴别协议, 如: 中国无线局域网标准中 WAI 协议, 其中用户鉴别协议数据采用 TAEP 包封装传输。用户鉴别协议完成后, 若网络访问控制者要求立即做出访问决策, 则网络访问控制者根据用户鉴别结果做出访问决策并采用基于三元等鉴别的访问控制方法(如: 中国无线局域网标准中所采用的访问控制方法)执行访问控制, 否则向 TNC 接入点发送平台鉴别请求; 若网络访问请求者要求立即做出访问决策, 则网络访问请求者根据用户鉴别结果做出访问决策并采用基于三元等鉴别的访问控制方法(如: 中国无线局域网标准中所采用的访问控制方法)执行访问控制, 否则向 TNC 客户端发送平台鉴别请求。在装载 TNC 接入点, 或 TNC 接入点的服务启动时, 访问控制器中的 PTS 可以扫描 TNC 接入点的文件代码和内存代码, 以保证其可信赖性。在装载 TNC 客户端, 或 TNC 客户端的服务启动时, 访问请求者中的 PTS 可以扫描 TNC 客户端的文件代码和内存代码, 以保证其可信赖性。

[0117] 2.3) 当 TNC 接入点收到网络访问控制者发送的平台鉴别请求时,若 TNC 接入点通过向评估策略服务者请求对访问请求者的评估策略,则基于访问请求者的用户级别和访问请求者所请求的服务级别向评估策略服务者发送评估策略请求,然后评估策略服务者下发相应的评估策略。在装载评估策略服务者,或评估策略服务者的服务启动时,策略管理器中的 PTS 可以扫描评估策略服务者的文件代码和内存代码,以保证其可信赖性。在请求评估策略过程中,由于涉及到可信赖性,所以 TNC 接入点可以利用访问控制器中的 IF-PTS 向 PTS 请求扫描网络访问控制者的文件代码和内存代码,以保证其可信赖性;评估策略服务者可以利用策略管理器中的 IF-PTS 请求扫描鉴别策略服务者的文件代码和内存代码,以保证其可信赖性。

[0118] 2.4) 平台鉴别过程

[0119] 2.4.1) 当 TNC 接入点收到网络访问控制者发送的平台鉴别请求,或者通过执行另一轮平台鉴别协议时,TNC 接入点启动平台鉴别过程,并构造平台鉴别协议中的消息 1 发送给 TNC 客户端;

[0120] 2.4.2) 若 TNC 客户端收到的平台鉴别协议中的消息 1 为首轮平台鉴别协议消息(若 TNC 客户端此时还没有装载和初始化访问请求者中的 IMC,则利用访问请求者中的 IMC 平台绑定方法、TNC_IMC_Initialize 和 TNC_TNCC_ReportMessageTypes 来实现访问请求者中 IMC 的装载和初始化),则 TNC 客户端本地创建 ConnectionID,并可以调用 TNC_IMC_NotifyConnectionChange 向访问请求者中的 IMC 通告网络连接状态为 CREATE,接着可以调用 TNC_IMC_NotifyConnectionChange 向访问请求者中的 IMC 通告网络连接状态为 HANDSHAKE,表示访问请求者中的 IMC 与策略管理器中的 IMV 之间的完整性握手过程开始,然后调用 TNC_IMC_RequestMeasurementInfo 向访问请求者中的 IMC 通告请求度量的完整性度量参数,否则直接调用 TNC_IMC_RequestMeasurementInfo 向访问请求者中的 IMC 通告请求度量的完整性度量参数,访问请求者中的 IMC 收到请求度量的完整性度量参数后利用访问请求者中的 IF-PTS 请求 PTS 执行度量,并生成对访问请求者的完整性度量值;

[0121] 2.4.3) 访问请求者中的 IMC 调用 TNC_TNCC_SendMessage 向 TNC 客户端发送对访问请求者的完整性度量值,还可以调用 TNC_TNCC_ProvidePCRsIndex 向 TNC 客户端提供可信平台评估层组件可知的 PCR 引用数据;

[0122] 2.4.4) 当该轮平台鉴别协议的该步骤消息将要发送,则 TNC 客户端首先调用 TNC_IMC_PAIEnding 向访问请求者中的 IMC 通告让访问请求者中的 IMC 停止收集完整性度量值;

[0123] 2.4.5) 当 TNC 客户端收到 TNC 接入点发送的平台鉴别协议中的消息 1,即步骤 2.4.1) ~ 步骤 2.4.4) 存在时, TNC 客户端构造平台鉴别协议中的消息 2 发送给 TNC 接入点;当 TNC 客户端没有收到 TNC 接入点发送的平台鉴别协议中的消息 1,即步骤 2.4.1) ~ 步骤 2.4.4) 不存在时,若 TNC 客户端收到网络访问请求者发送的平台鉴别请求,或者通过执行另一轮平台鉴别协议,则 TNC 客户端启动平台鉴别过程,并构造平台鉴别协议中的消息 2 发送给 TNC 接入点;

[0124] 2.4.6) 若 TNC 接入点收到的平台鉴别协议中的消息 2 为首轮平台鉴别协议消息(若 TNC 接入点此时还没有装载和初始化访问控制器中的 IMC,则利用访问控制器中的 IMC 平台绑定方法、TNC_IMC_Initialize 和 TNC_TNCC_ReportMessageTypes 来实现访问

控制器中 IMC 的装载和初始化), 则 TNC 接入点本地创建 ConnectionID , 并可以调用 TNC_IMC_NotifyConnectionChange 向访问控制器中的 IMC 通告网络连接状态为 CREATE , 接着可以调用 TNC_IMC_NotifyConnectionChange 向访问控制器中的 IMC 通告网络连接状态为 HANDSHAKE , 表示访问控制器中的 IMC 与策略管理器中的 IMV 之间的完整性握手过程开始 , 然后调用 TNC_IMC_RequestMeasurementInfo 向访问控制器中的 IMC 通告请求度量的完整性度量参数 , 否则直接调用 TNC_IMC_RequestMeasurementInfo 向访问控制器中的 IMC 通告请求度量的完整性度量参数 , 访问控制器中的 IMC 收到请求度量的完整性度量参数后利用访问控制器中的 IF-PTS 请求 PTS 执行度量 , 并生成对访问控制器的完整性度量值 ;

[0125] 2.4.7) 访问控制器中的 IMC 调用 TNC_TNCAP_SendMessage 向 TNC 接入点发送对访问控制器的完整性度量值 , 还可以调用 TNC_TNCAP_ProvidePCRsIndex 向 TNC 接入点提供可信平台评估层组件可知的 PCR 引用数据 ;

[0126] 2.4.8) 当该轮平台鉴别协议的该步骤消息将要发送 , 则 TNC 接入点首先调用 TNC_IMC_PAIEnding 向访问控制器中的 IMC 通告让访问控制器中的 IMC 停止收集完整性度量值 ;

[0127] 2.4.9) TNC 接入点构造平台鉴别协议中的消息 3 发送给评估策略服务者 ;

[0128] 2.4.10) 评估策略服务者收到 TNC 接入点发送的平台鉴别协议中的消息 3 后 , 首先调用 TNC_IMV_SetAttributePolicy 向策略管理器中的 IMV 通告本轮平台鉴别协议所通过设置的评估策略 , 然后调用 TNC_IMV_ReceiveMessage 来向策略管理器中的 IMV 发送已收到的完整性度量层消息 ;

[0129] 2.4.11) 策略管理器中的 IMV 收到步骤 2.4.10) 中发送的消息后 , 将这些消息发给与策略管理器中的 IMV 相连接的 PTS , 若 PTS 解析这些信息出错 , 则生成组件级错误信息并发送给策略管理器中的 IMV , 否则 PTS 解析这些消息并在后台 (TCG-TNC 架构定义的) 参照完整性清单数据库的协助下生成组件级评估结果和平台修补信息 ;

[0130] 2.4.12) 策略管理器中的 IMV 调用 TNC_EPS_SendMessage 向评估策略服务者发送步骤 2.4.11) 中生成的完整性度量层消息。

[0131] 2.4.13) 策略管理器中的 IMV 可以调用 TNC_EPS_ProvideRecommendation 向评估策略服务者提供组件级评估结果 (可信平台评估层组件可知的) ;

[0132] 2.4.14) 策略管理器中的 IMV 可以调用 TNC_EPS_ProvidePCRsIndex 向评估策略服务者提供完整性度量值中的 PCR 引用数据 (可信平台评估层组件可知的) ;

[0133] 2.4.15) 评估策略服务者构造平台鉴别协议中的消息 4 并发送给 TNC 接入点 ; 2.4.16) TNC 接入点收到评估策略服务者发送的平台鉴别协议中的消息 4 后 , 首先调用 TNC_IMC_ReceiveMessage 向访问控制器中的 IMC 发送已收到的完整性度量层消息 , 若对访问请求者的评估已完成 , 则根据对访问请求者的完整性度量值的组件级评估结果生成访问控制器的访问决策 , 否则表明 TNC 接入点通过执行另一轮平台鉴别协议 , 即 : 该轮平台鉴别协议结束后重新从步骤 2.4.1) 开始执行 , 然后 TNC 接入点构造平台鉴别协议中的消息 5 发送给 TNC 客户端 ;

[0134] 2.4.17) TNC 客户端收到步骤 2.4.16) 中发送的平台鉴别协议中的消息 5 后 , 首先调用 TNC_IMC_ReceiveMessage 向访问请求者中的 IMC 发送已收到的完整性度量层消息 , 若收到访问控制器的访问决策 (表示对访问请求者的平台鉴别已经完成) , 则可以调用 TNC_

IMC_NotifyConnectionChange 向访问请求者中的 IMC 通告访问控制器的访问决策（也就是网络连接状态），若对访问控制器的评估已完成，则根据对访问控制器的完整性度量值的组件级评估结果生成访问请求者的访问决策，否则表明 TNC 客户端通过执行另一轮平台鉴别协议，即：该轮平台鉴别协议结束后重新从步骤 2.4.5) 开始执行，然后 TNC 客户端构造平台鉴别协议中的消息 6 发送给 TNC 接入点；

[0135] 2.4.18) TNC 接入点收到步骤 2.4.17) 中发送的平台鉴别协议中的消息 6 后，可以调用 TNC_IMC_NotifyConnectionChange 向访问控制器中的 IMC 通告访问请求者的访问决策（也就是网络连接状态）。

[0136] 2.5) 平台修补完成后，访问请求者中的 IMC 调用 TNC_TNCC_RequestHandshakeRetry 向 TNC 客户端请求重新执行完整性握手，访问控制器中的 IMC 调用 TNC_TNCAP_RequestHandshakeRetry 向 TNC 接入点请求重新执行完整性握手，或者评估策略发生了改变，从而通过重新执行平台鉴别过程，则根据网络连接状态和本地安全策略跳至步骤 2.1)、步骤 2.2) 或步骤 2.4)。

[0137] 上述步骤 2.4) 描述了一个完整的平台鉴别过程，其中的平台鉴别协议可以为上面所述的 IF-TNCCAP 和 IF-PTS 的具体实现方法中的平台鉴别协议，若应用于单向平台鉴别，则可以选用步骤 2.4) 中的一些子步骤来实现。

[0138] 在上述步骤 2.4) 中，为了保证 TNC 客户端、TNC 接入点和评估策略服务者的可信赖性，在装载 TNC 客户端，或 TNC 客户端的服务启动时，访问请求者中的 PTS 可以扫描 TNC 客户端的文件代码和内存代码，在装载 TNC 接入点，或 TNC 接入点的服务启动时，访问控制器中的 PTS 可以扫描 TNC 接入点的文件代码和内存代码，在装载评估策略服务者，或评估策略服务者的服务启动时，策略管理器中的 PTS 可以扫描评估策略服务者的文件代码和内存代码。

[0139] 在上述步骤 2.4) 中，为了保证访问请求者中的 IMC、访问控制器中的 IMC 和策略管理器中的 IMV 的可信赖性，在装载访问请求者中的 IMC，或访问请求者中的 IMC 的服务启动时，TNC 客户端可以利用访问请求者中的 IF-PTS 向访问请求者中的 PTS 请求扫描访问请求者中的 IMC 的文件代码和内存代码，在装载访问控制器中的 IMC，或访问控制器中的 IMC 的服务启动时，TNC 接入点可以利用访问控制器中的 IF-PTS 向访问控制器中的 PTS 请求扫描访问控制器中的 IMC 的文件代码和内存代码，在装载策略管理器中的 IMV，或策略管理器中的 IMV 的服务启动时，评估策略服务者可以利用策略管理器中的 IF-PTS 向策略管理器中的 PTS 请求扫描策略管理器中的 IMV 的文件代码和内存代码。

[0140] 在上述步骤 2.4) 中，为了保证网络访问请求者、网络访问控制者和鉴别策略服务者的可信赖性，在装载网络访问请求者，或网络访问请求者的服务启动时，TNC 客户端可以利用访问请求者中的 IF-PTS 向访问请求者中的 PTS 请求扫描网络访问请求者的文件代码和内存代码，在装载网络访问控制者，或网络访问控制者的服务启动时，TNC 接入点可以利用访问控制器中的 IF-PTS 向访问控制器中的 PTS 请求扫描网络访问控制者的文件代码和内存代码，在装载鉴别策略服务者，或鉴别策略服务者的服务启动时，评估策略服务者可以利用策略管理器中的 IF-PTS 向策略管理器中的 PTS 请求扫描鉴别策略服务者的文件代码和内存代码。

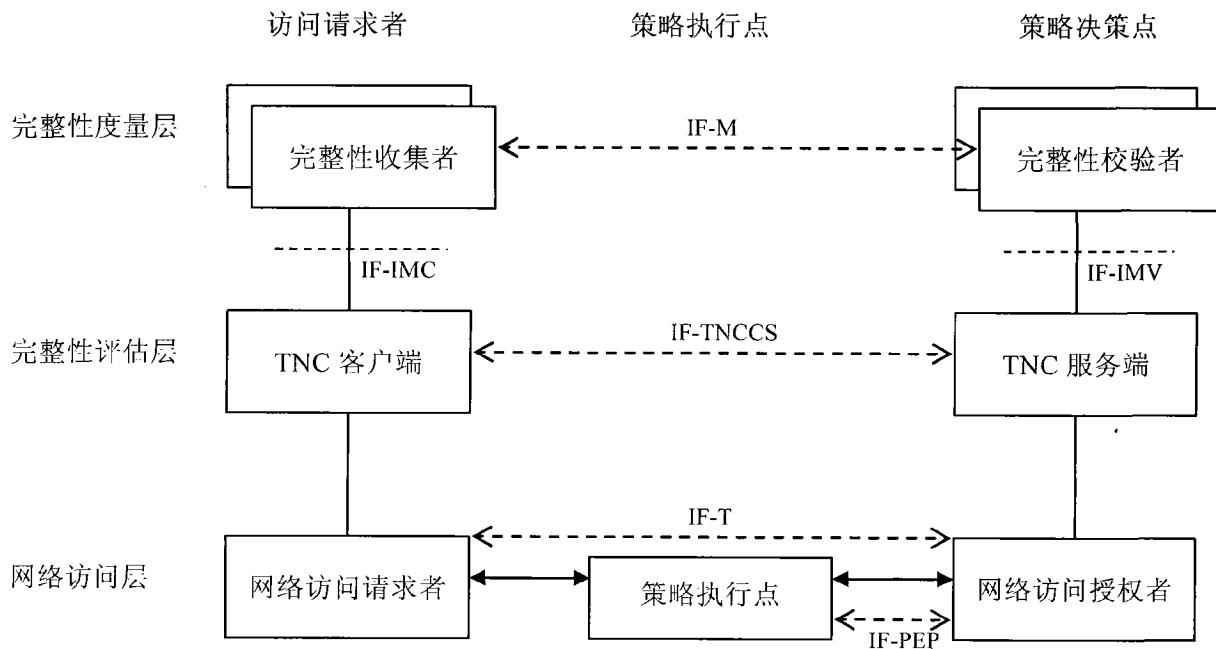


图 1

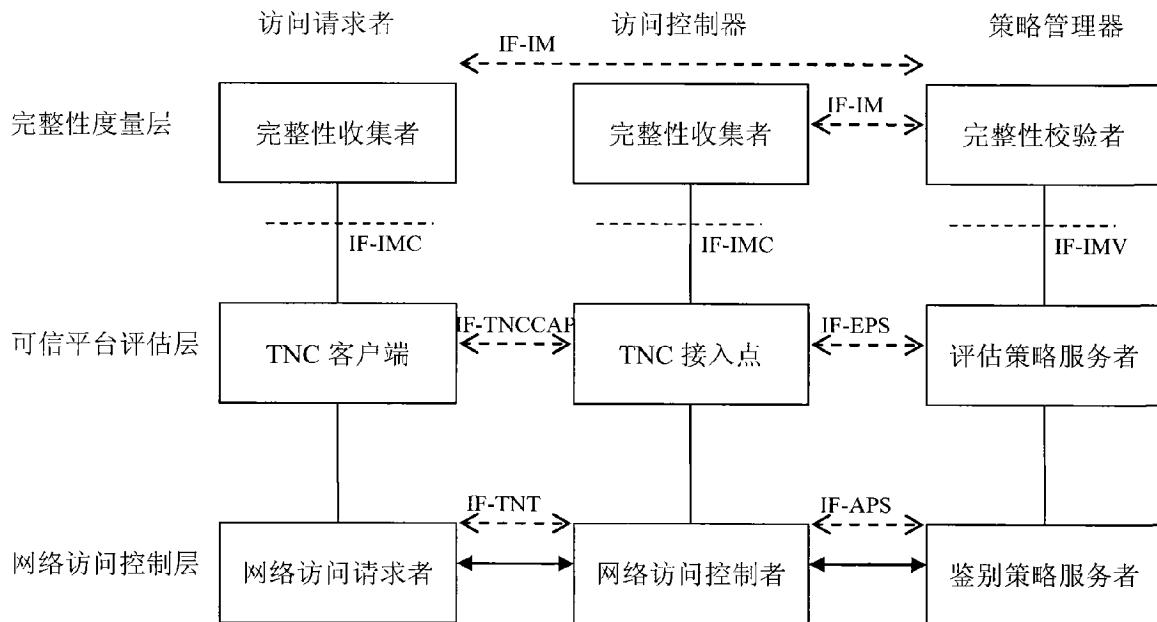


图 2

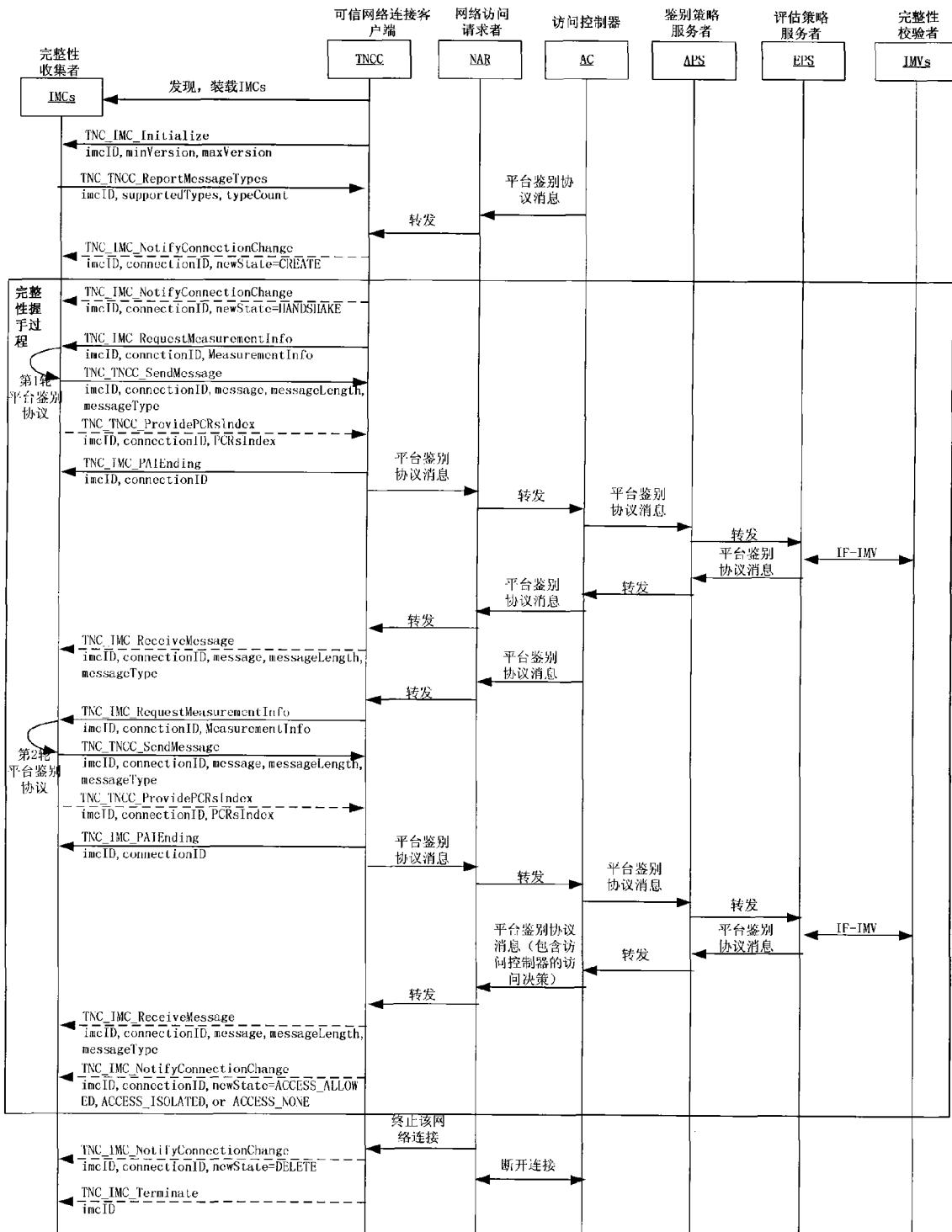


图 3

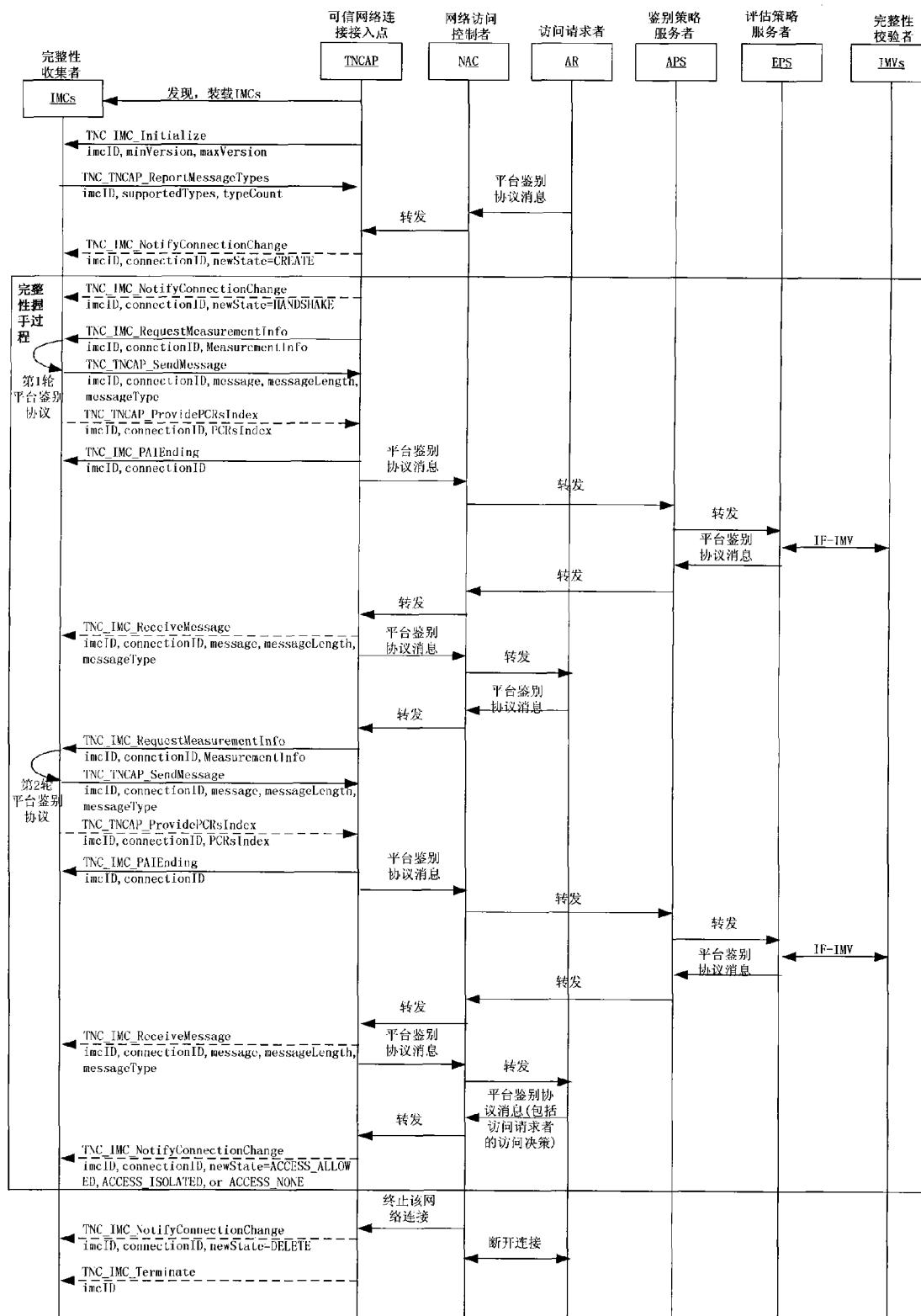


图 4

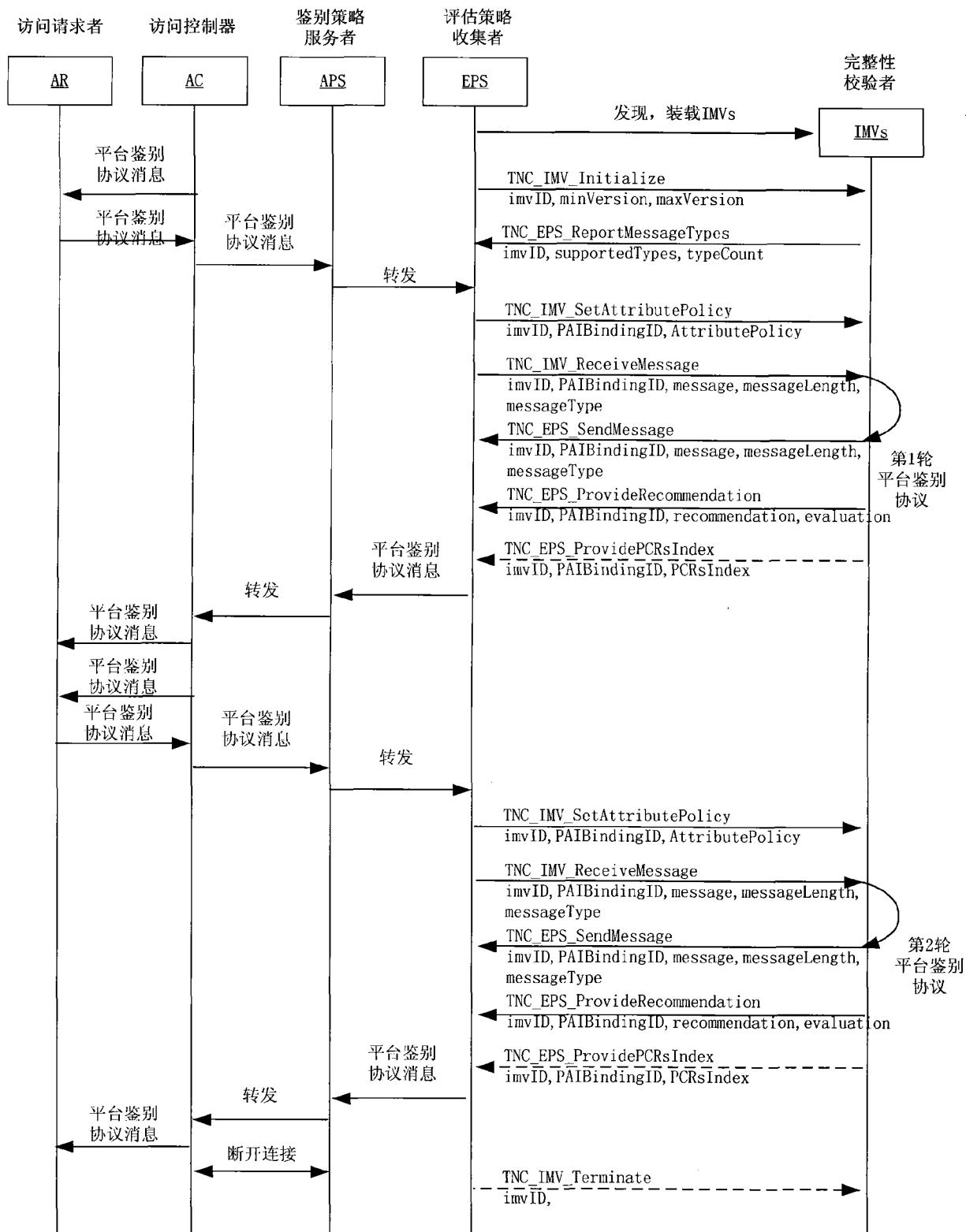


图 5