(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
2006 年8 月31 日 (31.08.2006)

PCT

(10) 国际公布号
WO 2006/089473 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2005/002129

(22) 国际申请日: 2005 年12 月8 日 (08.12.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200510051117.3
2005 年2 月28 日 (28.02.2005) CN

(71) 申请人 (对除美国外的所有指定国): 联想 (北京) 有限公司(LENOVO (BEIJING) LIMITED) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 韦卫(WEI, Wei) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。 曲亚东(QU, Yadong) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。 陈军(CHEN, Jun) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

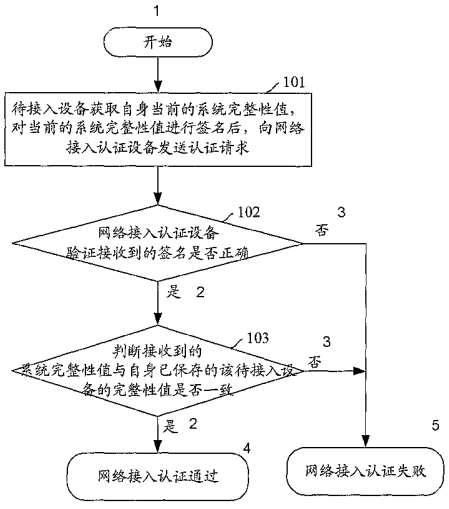
(74) 代理人: 中科专利商标代理有限责任公司(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.); 中国北京市海淀区王庄路1号清华同方科技大厦B座15层, Beijing 100083 (CN)。

(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, AT, AU, AZ, BA, BB, BG,

[见续页]

(54) Title: A METHOD FOR REALIZING NETWORK ACCESS AUTHENTICATION

(54) 发明名称: 一种实现网络接入认证的方法



101 THE DEVICE WAITING TO ACCESS TAKE THE CURRENT SYSTEM INTEGRITY ITSELF, AND AFTER SIGNING THE CURRENT SYSTEM INTEGRITY VALUE, SEND THE AUTHENTICATION REQUEST TO THE NETWORK ACCESS DEVICE
102 THE NETWORK ACCESS DEVICE AUTHENTICATE WHETHER THE SIGNATURE RECEIVED IS RIGHT
103 JUDGE WHETHER THE CURRENT SYSTEM INTEGRITY VALUE RECEIVED AND THE SYSTEM INTEGRITY VALUE STORED BY ITSELF OF THE DEVICE WAITING TO ACCESS ARE IDENTICAL
1 START
2 YES
3 NO
4 THE NETWORK ACCESS IS AUTHENTICATED
5 THE NETWORK ACCESS AUTHENTICATION IS FAILED

(57) Abstract: A method for realizing network access authentication, includes: the network access authentication device prestoring the system integrity value of the access device and the corresponding relation between each device waiting to access and the system integrity value. When the access device need to access the network, it takes the current system integrity itself, and sends the current system integrity value to the network access authentication device; The network access authentication device judges whether the received current system integrity value of the device waiting to access and the system integrity value stored by itself of the device waiting to access are identical, and in the case of the received current system integrity value of the device waiting to access and the system integrity value stored by itself of the device waiting to access being identical, it judges that the network access is authenticated. In this case, the network access device could determine the real state of the device waiting to access, and ensure the device accessing to the network is real secure, thereby ensure the security of the network.

[见续页]

WO 2006/089473 A1

BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：

一种实现网络接入认证的方法，其中网络接入认证设备内预先保存待接入设备的系统完整性值，以及每个待接入设备与其系统完整性值的对应关系。当待接入设备需要接入网络时，其获取自身当前的系统完整性值，将当前的系统完整性值发送给网络接入认证设备；网络接入认证设备判断接收到的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的完整性值是否一致，以及在接收到的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的完整性值一致的情况下判断通过网络接入认证。这样，使网络接入认证设备能够确认当前待接入设备的真正状态，确保了接入网络的设备是真正安全的，进而保证了网络的安全。

一种实现网络接入认证的方法

技术领域

本发明涉及网络接入认证技术和可信计算技术领域，特别是指一种实现网络接入认证的方法。

背景技术

目前，网络接入认证设备对待接入网络的设备进行的认证处理主要基于以下技术协议实现：

（1）口令字认证协议；

（2）基于与共享密钥和挑战应答协议；

（3）基于动态一次口令协议；

（4）基于公钥体制的认证协议。

上述所有认证处理的思路都是：网络接入认证设备通过判断待接入的设备是否拥有认证协议需要的口令和/或密钥来确认是否允许该待接入设备接入。上述认证处理的目的就是为了保证接入网络的是一个安全的设备，而不是一个攻击者。但是，如果待接入设备自身已受到了攻击，如已被植入木马病毒程序，那么，当该设备接入网络时，其内的木马病毒程序是可以监听认证过程的，并且，通过监听可以窃取该接入设备的关键信息，用其他设备假冒该待接入设备，或利用该待接入设备对网络发起攻击。

由此可以看出，仅验证待接入设备的口令和/或密钥是无法保证待接入设备是否真正是安全的，进而无法保证网络的安全。

发明内容

有鉴于此，本发明的主要目的在于提供一种实现网络接入认证的方法，使网络接入认证设备能够确认当前待接入设备的真正状态，以确保接入网络的设备是真正安全的。

为达到上述目的，本发明的技术方案是这样实现的：

一种实现网络接入认证的方法，网络接入认证设备预先保存待接入设备已计算出的其自身的系统完整性值，以及每个待接入设备与其自身的系统完整性值的对应关系，该方法包括以下步骤：

a、待接入设备获取自身当前的系统完整性值，向网络接入认证设备发送包括包含当前的系统完整性值的信息的认证请求；

b、网络接入认证设备根据接收到的认证请求以及所述对应关系，判断接收到的认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值是否一致，并在接收到的认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值一致的情况下判断网络接入认证通过。

较佳地，所述当前的系统完整性值是基本系统完整性值；

步骤 a 所述待接入设备获取自身当前的系统完整性值包括：

所述待接入设备启动时，计算自身的当前的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中直接取出该基本系统完整性值作为当前的系统完整性值。

较佳地，所述当前的系统完整性值是基本系统完整性值和用于网络接入的模块一起计算出的完整性值；

步骤 a 所述待接入设备获取自身当前的系统完整性值包括：所述待接入设备启动时，计算自身的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中取出基本系统完整性值，与用于网络接入的模块一起进行完整性计算，以获取该计算出的值，作为自身当前的系统完整性值。

较佳地，所述用于网络接入的模块包括链路层网络驱动模块、网络层和传输层协议软件模块和网络接入应用软件模块。

较佳地，所述待接入设备是计算机，所述计算自身的基本系统完整性值的过程包括以下步骤：

i、计算机电源开启后，计算系统 ROM，以及 BIOS 或 EFI 的固件代码以及硬件配置参数的完整性值，并将其存储在安全存储部件中；

ii、在 BIOS 或 EFI 启动后，计算系统所有已经配置完成的参数信息、主引导扇区和系统引导分区的完整性值，并将其存储在安全存储部件中；

iii、在 BIOS 或 EFI 装入引导操作系统之前，计算操作系统装入代码的完整性值，并将其存储在安全存储部件中；

iv、在操作系统装入代码后，计算操作系统内核、系统启动文件、系统配置

文件和驱动软件的完整性值，并将其存储在安全存储部件中；

v、在操作系统启动后，计算应用软件的完整性值，并将其存储在安全存储部件中；

vi、根据步骤 i 至步骤 vi 所述的所有完整性值，计算基本系统完整性值。

较佳地，所述已经配置完成的参数信息包括：CPU 微码软件，系统各类功能的使能（enable 或 disable）状态配置，各类认证口令，磁盘配置参数，外设配置参数，安全功能配置参数。

较佳地，安全存储部件为安全芯片 TPM、具有安全保护功能的硬盘、USB-key 或 smart-card。

较佳地，步骤 b 进一步包括：对接收到的信息的可信性进行验证。

较佳地，待接入设备预先生成公私钥，且该公私钥经可信第三方签署；

步骤 a 在所述待接入设备发送认证请求之前包括：应用所述私钥对当前的系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名以及所述公钥；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用接收到的公钥验证接收到的签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

较佳地，待接入设备预先生成公私钥，且该公私钥经可信第三方签署，网络接入认证设备中预先存储有所述公钥；

步骤 a 所述待接入设备发送认证请求之前，进一步包括：应用所述私钥对当前的系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用预先存储的公钥验证接收到的签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

较佳地，待接入设备预先生成公私钥，该公私钥未经可信第三方签署；

步骤 a 所述待接入设备发送认证请求之前，进一步包括：应用所述私钥对当前的系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名、匿名身份证书以

及所述公钥；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用接收到的匿名身份证书验证发送方身份合法后，应用接收到的公钥验证签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

较佳地，待接入设备和网络接入认证设备中预先存储有对称密钥；

步骤 a 所述待接入设备发送认证请求之前进一步包括：应用所述对称密钥对当前的系统完整性值进行加密，所述认证请求中的信息是经对称密钥加密后的当前系统完整性值；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用自身已保存的对称密钥对接收到的信息进行解密，以及在解密成功的情况下判断接收到的信息可信，在解密未成功的情况下判断接收到的信息不可信。

较佳地，该方法进一步包括：待接入设备中预先保存有网络接入认证设备的系统完整性值；

待接入设备获取网络接入认证设备当前的系统完整性值，验证所获取网络接入认证设备的当前系统完整性值与自身已保存的该网络接入认证设备的系统完整性值一致后，再执行步骤 a。

较佳地，所述网络接入认证设备由一个服务器构成，或者，由防火墙、交换机或路由器与认证服务器共同构成。

较佳地，该方法进一步包括：在接收到的认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值不一致的情况下，网络接入认证设备向待接入设备发送指示该待接入设备当前不安全的告警提示。

较佳地，所述网络接入认证设备和待接入设备之间交互的信息由 SSL 协议、TLS 协议、IPv6 协议、或 IPSec 的 IKE 协议承载。

较佳地，所述网络接入认证设备和待接入设备之间交互的信息由 SSL 协议或 TLS 协议承载时，步骤 a 所述待接入设备在接收到来自 server 的 ServerHello 信息后，将包含完整性值的信息随握手协议发送给网络接入认证设备，或者，步骤 a 所述待接入设备在发送的 ClientHello 中包含所述包含完整性值的信息；所述网络接入认证设备和待接入设备之间交互的信息由 IPv6 协议或 IPSec 的 IKE 协议承载时，步骤 a 所述待接入设备发送 HDR, SA 时将包含完整性值的信

息随握手协议发送给网络接入认证设备。

应用本发明，其关键是网络接入认证设备内预先保存待接入设备的系统完整性值，以及该待接入设备与其系统完整性值的对应关系。当待接入设备需要接入网络时，其获取自身当前的系统完整性值，将当前的系统完整性值发送给网络接入认证设备；网络接入认证设备判断接收到的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的完整性值是否一致，如果一致，则通过网络接入认证，否则网络接入认证失败。这样，使网络接入认证设备能够确认当前待接入设备的真正状态，确保了接入网络的设备是真正安全的，进而保证了网络的安全。

附图说明

图 1 所示为应用本发明的一实施例的实现流程示意图；

图 2 所示为应用本发明的待接入设备计算自身的基本系统完整性值的流程示意图。

具体实施方式

下面结合附图及具体实施例对本发明再做进一步地详细说明。

本发明的思路是：网络接入认证设备内预先保存待接入设备的系统完整性值，以及每个待接入设备与其系统完整性值的对应关系。当待接入设备需要接入网络时，其获取自身当前的系统完整性值，将当前的系统完整性值发送给网络接入认证设备；网络接入认证设备判断接收到的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的完整性值是否一致，如果一致，则网络接入认证通过，否则网络接入认证失败。

图 1 所示为应用本发明的一实施例的实现流程示意图。网络接入认证设备预先保存待接入设备已计算出的其自身的系统完整性值，以及每个待接入设备与其自身的系统完整性值的对应关系，且待接入设备预先生成有公私钥，该公私钥已经可信第三方签署。

步骤 101，待接入设备获取自身当前的系统完整性值，应用上述私钥对当前的系统完整性值进行签名；之后，向网络接入认证设备发送认证请求，该认证请求中包括：当前的系统完整性值，当前的系统完整性值的签名以及所述公钥；

步骤 102，网络接入认证设备接收到来自待接入设备的信息后，应用接收到的公钥验证接收到的签名是否正确，如果签名正确，则表示接收到的信息可信，

执行步骤 103；如果签名不正确则表示接收到的信息不可信，网络接入认证失败。

步骤 103，网络接入认证设备根据接收到的认证请求以及所述对应关系，获取该待接入设备的系统完整性值，判断该接收到的待接入设备的当前系统完整性值与自身已保存的该待接入设备所对应的系统完整性值是否一致，如果一致，则网络接入认证通过，否则网络接入认证失败。

如果网络接入认证失败，网络接入认证设备可以进一步向待接入设备发送指示该待接入设备当前不安全的告警提示，如提示待接入设备存在安全漏洞，或提示待接入设备已受到攻击等。

至此，网络接入认证设备完成了对待接入设备的接入认证。

上述当前的系统完整性值可以为基本系统完整性值，也可以为基本系统完整性值和用于网络接入的模块一起计算出的完整性值。

如果当前的系统完整性值是基本系统完整性值，则步骤 101 所述待接入设备获取自身当前的系统完整性值的方法为：待接入设备每次启动时，计算自身当前的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中直接取出该基本系统完整性值作为当前的系统完整性值。

如果当前的系统完整性值是基本系统完整性值和用于网络接入的模块一起计算出的完整性值，则步骤 101 所述待接入设备获取自身当前的系统完整性值的方法为：待接入设备每次启动时，计算自身当前的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中取出基本系统完整性值，与用于网络接入的模块一起进行计算，将计算出的值作为自身当前的系统完整性值。所述用于网络接入的模块包括链路层网络驱动模块、网络层和传输层协议软件模块和网络接入应用软件模块。

参见图 2，图 2 所示为应用本发明的待接入设备计算自身的基本系统完整性值的流程示意图。在本实施例中，待接入设备为计算机。

步骤 201，计算机每次电源开启后，由 CPU 计算系统 ROM，以及基本输入输出系统（BIOS）或可扩展固件界面（EFI）的固件代码以及硬件配置参数的完整性值，并将其存储在安全存储部件中。

步骤 202，在 BIOS 或 EFI 启动后，计算系统所有已经配置完成的参数信息、主引导扇区和系统引导分区的完整性值，并将其存储在安全存储部件中；所述已

经配置完成的参数信息包括：CPU 微码软件，系统各类功能的使能（enable 或 disable）状态配置，各类认证口令，磁盘配置参数，外设配置参数以及安全功能配置参数等。

步骤 203，在 BIOS 或 EFI 装入引导操作系统之前，计算操作系统装入代码的完整性值，并将其存储在安全存储部件中。

步骤 204，在操作系统装入代码后，计算操作系统内核、系统启动文件、系统配置文件和驱动软件的完整性值，并将其存储在安全存储部件中。

步骤 205，在操作系统启动后，计算应用软件的完整性值，并将其存储在安全存储部件中。

步骤 206，根据步骤 201 至步骤 205 所述的所有完整性值，计算基本系统完整性值。

上述安全存储部件为安全芯片（TPM，Trusted Platform Module）、或具有安全保护功能的硬盘、或 USB-key，或 smart-card。

图 1 所示流程仅为一实施例而已，当然还可以有多种实现方式，比如：

待接入设备预先生成公私钥，且该公私钥经可信第三方签署后，已将公钥预先存储在了网络接入认证设备中；此时，步骤 101 中所述向网络接入认证设备发送的认证请求中只需包含当前的系统完整性值，以及当前的系统完整性值的签名即可；其它实现步骤不变。

再比如：待接入设备预先生成了公私钥，但该公私钥未经可信第三方签署；此时，步骤 101 中所述向网络接入认证设备发送的认证请求中需包含当前的系统完整性值，当前的系统完整性值的签名、匿名身份证书以及所述公钥；网络接入认证设备接收到来自待接入设备的信息后，首先应用接收到的匿名身份证书验证发送方身份是否合法，如合法，再应用接收到的公钥验证签名是否准确，并继续执行后续步骤，如果验证发送方的身份不合法，则网络接入认证失败，并结束。

再比如：待接入设备和网络接入认证设备之间传送的信息不使用公私钥保护，而使用对称密钥的方式保护，即不需要待接入设备生成公私钥，而是待接入设备和网络接入认证设备中预先存储有对称密钥；此时，待接入设备应用对称密钥对当前的系统完整性值进行加密后，将加密后的当前系统完整性值包含在认证请求信息中发送给网络接入认证设备，网络接入认证设备则对接收到的信息进行解密，解密成功后，进行完整性判断操作。

上述待接入设备无论采用公私钥的方式还是对称密钥的方式保护当前的系统完整性值，都是为了保证网络接入认证设备所接收到的系统完整性值是可信的，是传输途中未被更改过的。

当然，待接入设备也可以直接将自身当前的系统完整性值以文明的方式传送给网络接入认证设备，而不对所传输出的系统完整性值进行保护，该传送方式不安全，在此并不推荐。

上述计算系统完整性值的操作是由待接入设备内的完整性信息采集模块执行的，上述签名或加密操作，是由待接入设备内的签名加密模块完成的。网络接入认证设备所执行的验证操作是由其内的认证模块完成的。

为了进一步保证网络接入认证的安全可信性，待接入设备也可以对网络接入认证设备进行完整性验证，以确认该网络接入认证设备是否为安全可信的。此时待接入设备内还具有用于执行的验证操作的验证模块，网络接入认证设备还具有用于计算系统完整性值的完整性信息采集模块以及执行签名或加密操作的签名加密模块。

具体实现过程与网络接入认证设备验证待接入设备的过程一致，即：

待接入设备中预先保存网络接入认证设备的系统完整性值；待接入设备接收来自网络接入认证设备的当前系统完整性值后，验证所接收的当前系统完整性值与自身已保存的该网络接入认证设备的系统完整性值是否一致，如果一致，再执行图 1 所述流程，如果不一致，则直接结束。

网络接入认证设备将自身的当前系统完整性值传送给待接入设备时，也可以采用上述公私钥或对称密钥的方式加以保护，以确保所传送的信息在传输途中的安全。具体应用公私钥或对称密钥的方式与上述方式相同，在此不再重复描述。

以上所述网络接入认证设备由一个服务器构成，或者，由防火墙、交换机或路由器与认证服务器共同构成。当网络接入认证设备由一个服务器构成时，该服务器完成接收信息、验证信息可信以及验证完整性的操作；当网络接入认证设备由防火墙、交换机或路由器与认证服务器共同构成时，由防火墙、交换机或路由器将接收到来自待接入设备的信息传送给服务器，由服务器执行验证信息可信以及验证完整性的操作，之后，服务器将验证结果返回给防火墙或路由器，由防火墙或路由器将验证结果信息返回给待接入设备。

上述网络接入认证设备和待接入设备之间交互的信息由安全套接字（SSL，Secure Socket Layer）协议、传输层安全（TLS，Transport Layer Security）

协议、IPv6 协议、或 IP 安全协议（IPSec，Internet protocol Security）中的密钥交换（IKE，Internet Key Exchange）协议承载。下面再进一步说明当网络接入认证设备和待接入设备之间由上述协议承载时，待接入设备发送完整性值的时机。对于待接入设备的具体发送方式，以及网络接入认证设备的认证方式，均与上述方式相同，下面不再详细说明。

当网络接入认证设备和待接入设备之间为 SSL 或 TLS 协议时，所述待接入设备为客户端（client），所述网络接入认证设备为 server。此时，当 client 接收到来自 server 的 ServerHello 后，将已计算出的完整性值随握手协议发送给 server，由 server 验证接收到的完整性值与预先存储的是否一致，如果一致，则继续握手协议，否则停止握手协议。或者，client 将已计算出的完整性值随 ClientHello 发送给 server；在 server 接收到来自 client 的 ClientHello 后验证收到的完整性值与预先存储的是否一致，如果一致，则继续握手协议，否则停止握手协议。

当网络接入认证设备和待接入设备之间为 IPv6 或 IPSec 的 IKE 协议时，所述待接入设备作为发起方（Initiator），所述网络接入认证设备作为响应方（Responder）。在 Initiator 发送 HDR, SA 时将完整性值随握手协议发送给网络接入认证设备，由网络接入认证设备则验证接收到的完整性值与预先存储的是否一致，如果一致，则表明认证成功，并继续后续操作，否则停止握手协议。

如果是单独发送包含完整性值的报文，则该报文中至少包含完整性值的标识信息、长度信息以及具体的完整性值信息。如果是随现有的报文一起发送完整性值，则在现有的报文中增加多个字段，以承载完整性值的标识信息、长度信息以及具体的完整性值信息，或应用现有报文中的保留字段承载完整性值的标识信息、长度信息以及具体的完整性值信息。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求

1、一种实现网络接入认证的方法，其特征在于，网络接入认证设备预先保存待接入设备已计算出的其自身的系统完整性值，以及每个待接入设备与其自身的系统完整性值的对应关系，该方法包括以下步骤：

a、待接入设备获取自身当前的系统完整性值，向网络接入认证设备发送包括包含当前的系统完整性值的信息的认证请求；

b、网络接入认证设备根据接收到的认证请求以及所述对应关系，判断接收到的认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值是否一致，并在接收到的认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值一致的情况下，判断网络接入认证通过。

2、根据权利要求 1 所述的方法，其特征在于，

所述当前的系统完整性值是基本系统完整性值；

步骤 a 所述待接入设备获取自身当前的系统完整性值包括：

所述待接入设备启动时，计算自身的当前的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中直接取出该基本系统完整性值作为当前的系统完整性值。

3、根据权利要求 1 所述的方法，其特征在于，

所述当前的系统完整性值是基本系统完整性值和用于网络接入的模块一起计算出的完整性值；

步骤 a 所述待接入设备获取自身当前的系统完整性值包括：所述待接入设备启动时，计算自身的基本系统完整性值，保存该当前的基本系统完整性值于安全存储部件中；当需要接入网络时，待接入设备从安全存储部件中取出基本系统完整性值，与用于网络接入的模块一起进行完整性计算，以获取该计算出的值，作为自身当前的系统完整性值。

4、根据权利要求 3 所述的方法，其特征在于，所述用于网络接入的模块包括链路层网络驱动模块、网络层和传输层协议软件模块和网络接入应用软件模块。

5、根据权利要求 2 或 3 所述的方法，其特征在于，所述待接入设备是计算机，

所述计算自身的基本系统完整性值的步骤包括以下步骤：

i、计算机电源开启后，计算系统 ROM，以及 BIOS 或 EFI 固件代码以及硬件配置参数的完整性值，并将其存储在安全存储部件中；

ii、在 BIOS 或 EFI 启动后，计算系统所有已经配置完成的参数信息、主引导扇区和系统引导分区的完整性值，并将其存储在安全存储部件中；

iii、在 BIOS 或 EFI 装入引导操作系统之前，计算操作系统装入代码的完整性值，并将其存储在安全存储部件中；

iv、在操作系统装入代码后，计算操作系统内核、系统启动文件、系统配置文件和驱动软件的完整性值，并将其存储在安全存储部件中；

v、在操作系统启动后，计算应用软件的完整性值，并将其存储在安全存储部件中；

vi、根据步骤 i 至步骤 vi 所述的所有完整性值，计算基本系统完整性值。

6、根据权利要求 5 所述的方法，其特征在于，所述已经配置完成的参数信息包括：CPU 微码软件，系统各类功能的使能（enable 或 disable）状态配置，各类认证口令，磁盘配置参数，外设配置参数，安全功能配置参数。

7、根据权利要求 2 或 3 所述的方法，其特征在于，安全存储部件为安全芯片 TPM、具有安全保护功能的硬盘、USB-key 或 smart-card。

8、根据权利要求 1 所述的方法，其特征在于，步骤 b 进一步包括：对接收到的信息的可信性进行验证。

9、根据权利要求 8 所述的方法，其特征在于，

待接入设备预先生成公私钥，且该公私钥经可信第三方签署；

步骤 a 在所述待接入设备发送认证请求之前包括：应用所述私钥对当前的系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名以及所述公钥；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用接收到的公钥验证接收到的签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

10、根据权利要求 8 所述的方法，其特征在于，待接入设备预先生成公私钥，且该公私钥经可信第三方签署，网络接入认证设备中预先存储有所述公钥；

步骤 a 所述待接入设备发送认证请求之前，进一步包括：应用所述私钥对当前的

系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用预先存储的公钥验证接收到的签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

11、根据权利要求 8 所述的方法，其特征在于，待接入设备预先生成公私钥，该公私钥未经可信第三方签署；

步骤 a 所述待接入设备发送认证请求之前，进一步包括：应用所述私钥对当前的系统完整性值进行签名；所述认证请求中的信息是当前的系统完整性值的明文，且该认证请求中进一步包括：当前的系统完整性值的签名、匿名身份证书以及所述公钥；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用接收到的匿名身份证书验证发送方身份合法后，应用接收到的公钥验证签名是否正确，以及在签名正确的情况下判断接收到的信息可信，在签名不正确的情况下判断接收到的信息不可信。

12、根据权利要求 8 所述的方法，其特征在于，待接入设备和网络接入认证设备中预先存储有对称密钥；

步骤 a 所述待接入设备发送认证请求之前进一步包括：应用所述对称密钥对当前的系统完整性值进行加密，所述认证请求中的信息是经对称密钥加密后的当前系统完整性值；

所述对接收到的信息的可信性进行验证包括：网络接入认证设备应用自身已保存的对称密钥对接收到的信息进行解密，以及在解密成功的情况下判断接收到的信息可信，在解密未成功的情况下判断接收到的信息不可信。

13、根据权利要求 1 或 8 所述的方法，其特征在于，该方法进一步包括：待接入设备中预先保存有网络接入认证设备的系统完整性值；

待接入设备获取网络接入认证设备当前的系统完整性值，验证所获取网络接入认证设备的当前系统完整性值与自身已保存的该网络接入认证设备的系统完整性值一致后，再执行步骤 a。

14、根据权利要求 1 所述的方法，其特征在于，所述网络接入认证设备由一个服务器构成，或者，由防火墙、交换机或路由器与认证服务器共同构成。

15、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：在接收到的

认证请求中的该待接入设备当前的系统完整性值与自身已保存的该待接入设备的系统完整性值不一致的情况下，网络接入认证设备向待接入设备发送指示该待接入设备当前不安全的告警提示。

16、根据权利要求 1 或 8 所述的方法，其特征在于，

所述网络接入认证设备和待接入设备之间交互的信息由 SSL 协议或 TLS 协议承载时，步骤 a 所述待接入设备在接收到来自 server 的 ServerHello 信息后，将包含完整性值的信息随握手协议发送给网络接入认证设备，或者，步骤 a 所述待接入设备在发送的 ClientHello 中包含所述包含完整性值的信息；

所述网络接入认证设备和待接入设备之间交互的信息由 IPv6 协议或 IPSec 的 IKE 协议承载时，步骤 a 所述待接入设备发送 HDR, SA 时将包含完整性值的信息随握手协议发送给网络接入认证设备。

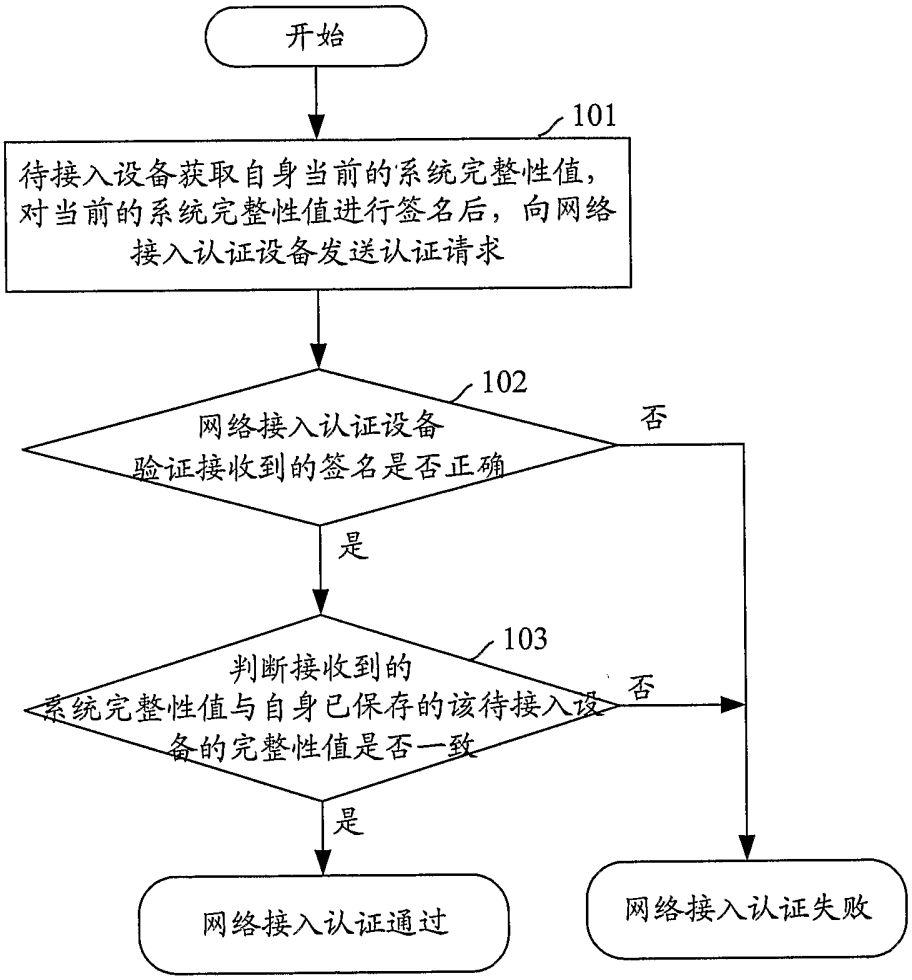

开始
101
待接入设备获取自身当前的系统完整性值，对当前的系统完整性值进行签名后，向网络接入认证设备发送认证请求
102
网络接入认证设备验证接收到的签名是否正确
否
是
103
判断接收到的系统完整性值与自身已保存的该待接入设备的完整性值是否一致
否
是
网络接入认证通过
网络接入认证失败

图 1

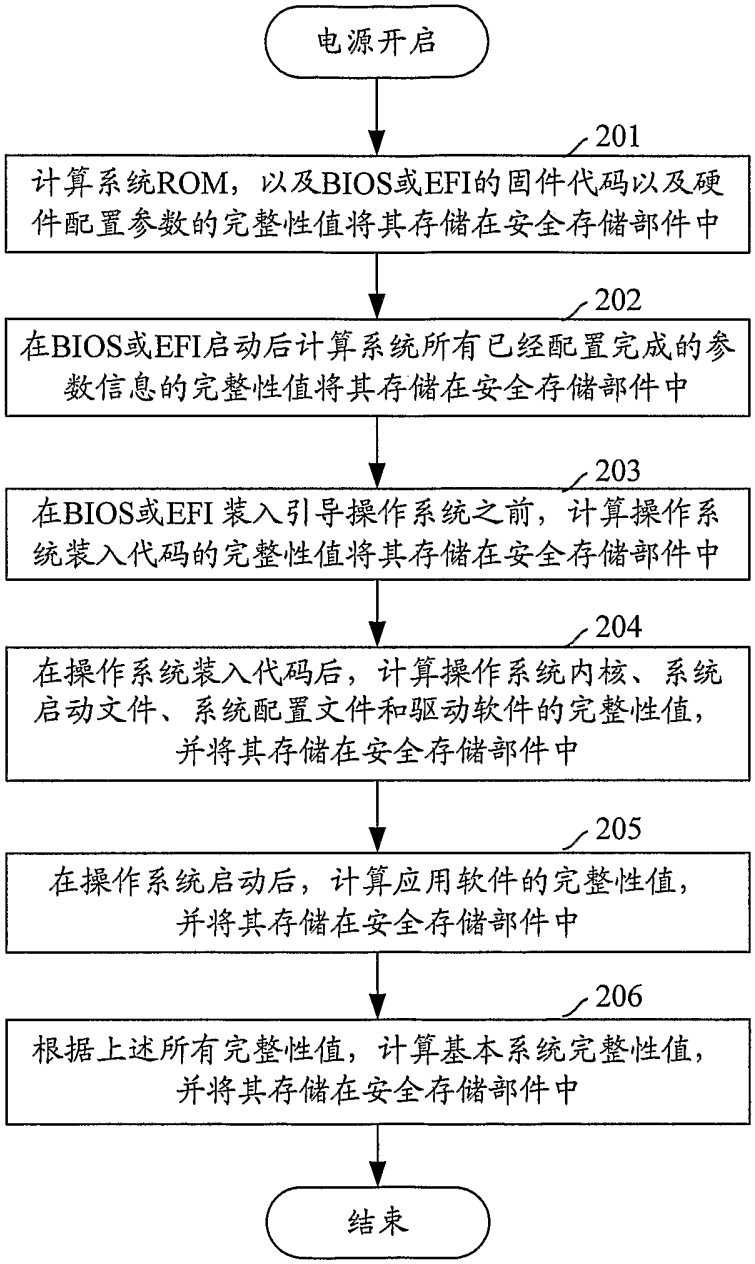

电源开启
201
计算系统ROM，以及BIOS或EFI的固件代码以及硬件配置参数的完整性值将其存储在安全存储部件中
202
在BIOS或EFI启动后计算系统所有已经配置完成的参数信息的完整性值将其存储在安全存储部件中
203
在BIOS或EFI 装入引导操作系统之前，计算操作系统装入代码的完整性值将其存储在安全存储部件中
204
在操作系统装入代码后，计算操作系统内核、系统启动文件、系统配置文件和驱动软件的完整性值，并将其存储在安全存储部件中
205
在操作系统启动后，计算应用软件的完整性值，并将其存储在安全存储部件中
206
根据上述所有完整性值，计算基本系统完整性值，并将其存储在安全存储部件中
结束

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/002129

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

H04L9(2006.01)

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)

WPI, EPODOC, PAJ, CNPAT,CNKI:access,system,integrity,authenticat+,identificat+,certificat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO2004044687 A2 (MILLIPORE CORP) 27.May.2004 (27.05.2004) the whole documnet	1-16
A	WO03090402 A1 (INT BUSINESS MACHINES CORP) 30.Oct.2003 (30.10.2003) the whole documnet	1-16
A	US2004128518 A1 (CAVERS F M) 01.Jul.2004 (01.07.2004) the whole documnet	1-16
A	US2004250121 A1 (MILLAR K) 19.Dec.2004 (09.12.2004) the whole documnet	1-16

☐ 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
06.Mar.2006 (06.03.2006)	16 · MAR 2006 (16 · 03 · 2006)
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 LIU Bin Telephone No. (86-10)62084534

Form PCT/ISA /210 (second sheet) (April 2005)

TERNATIONAL SEARCH REPORT

Information patent family members

Search request No.
PCT/CN2005/002129

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO2004044687 A2	27.05.2004	AU2003291326 A1	03.06.2004
		US2004093526 A1	13.05.2004
		EP1561155 A	10.08.2005
WO03090402 A1	30.10.2003	US2003200454 A	23.10.2003
		US6715085 B	30.03.2004
		CA2481569 A	30.10.2003
		AU2003223671 A	03.11.2003
		US2004083375 A	29.04.2004
		US2004088559 A	06.05.2004
		EP1500225 A	26.01.2005
		CN1647443 A	27.07.2005
		JP2005523537T T	04.08.2005
US2004128518 A1	01.07.2004	CA2431076 A	29.11.2003
US2004250121 A1	09.12.2004	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/002129

CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i
H04L 9/00 (2006.01) i

国际检索报告

国际申请号
PCT/CN2005/002129

A. 主题的分类

参见附加页

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)

H04L9(2006.01)

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））

WPI, EPODOC, PAJ, CNPAT,CNKI: access,system,integrity,authenticat+,identificat+,certificat+,接入,认证,识别,系统,完整性,

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
A	WO2004044687 A2　（米利波尔公司） 27.5 月 2004 (27.05.2004)　全文	1-16
A	WO03090402 A1　（国际商业机器公司） 30.10 月 2003 (30.10.2003)　全文	1-16
A	US2004128518 A1　（CAVERS F M） 01.7 月 2004 (01.07.2004)　全文	1-16
A	US2004250121 A1　（MILLAR K） 09.12 月 2004 (09.12.2004)　全文	1-16

☐ 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
06.3 月 2006（06.03.2006）	16 · 3月 2006 (16 · 03 · 2006)
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 刘斌 电话号码：(86-10)62084534

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/002129

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO2004044687 A2	27.05.2004	AU2003291326 A1	03.06.2004
		US2004093526 A1	13.05.2004
		EP1561155 A	10.08.2005
WO03090402 A1	30.10.2003	US2003200454 A	23.10.2003
		US6715085 B	30.03.2004
		CA2481569 A	30.10.2003
		AU2003223671 A	03.11.2003
		US2004083375 A	29.04.2004
		US2004088559 A	06.05.2004
		EP1500225 A	26.01.2005
		CN1647443 A	27.07.2005
		JP2005523537T T	04.08.2005
US2004128518 A1	01.07.2004	CA2431076 A	29.11.2003
US2004250121 A1	09.12.2004	无	

国际检索报告	国际申请号 PCT/CN2005/002129

主题的分类

H04L 9/32 (2006.01) i
H04L 9/00 (2006.01) i