(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 693**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.11.2008 PCT/CN2008/073069**

(87) Fecha y número de publicación internacional: **28.05.2009 WO09065350**

(96) Fecha de presentación y número de la solicitud europea: **14.11.2008 E 08853076 (1)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2222014**

(54) Título: **Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos**

(30) Prioridad:

16.11.2007 CN 200710019094

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

CHINA IWNCOMM CO., LTD. (100.0%)
A201 QIN FENG GE XI'AN SOFTWARE PARK NO. 68 KE JI 2ND ROAD XI'AN HI-TECH INDU
XI'AN, SHAANXI 710075, CN

(72) Inventor/es:

XIAO, YUELEI;
CAO, JUN;
LAI, XIAOLONG y
HUANG, ZHENHAI

(74) Agente/Representante:

ZEA CHECA, Bernabé

DESCRIPCIÓN

Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos

La presente solicitud reivindica el beneficio de la solicitud de patente china No. 200710019094.7 presentada ante la Oficina de Propiedad Intelectual China el 16 de noviembre de 2007, titulada "Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos", que se incorpora aquí como referencia en su totalidad.

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un campo de la tecnología de la seguridad de la red, en particular, a un sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos.

ANTECEDENTES DE LA INVENCIÓN

Junto con el desarrollo de la información, los problemas de software malicioso, tales como virus y gusanos son bastante importantes. En la actualidad, hay más de 35.000 tipos de software malicioso, y más de 40 millones de ordenadores se infectan cada año. Con el fin de proteger los ordenadores de este tipo de ataques, se requiere no sólo tratar una seguridad de transmisión y una comprobación de entrada de datos, sino que también debe iniciarse una defensa desde una fuente, es decir, cada terminal conectado a la red. Sin embargo, la tecnología de defensa de seguridad convencional no ha defendido contra una amplia variedad de ataques maliciosos.

Para abordar este problema, el *Trusted Computing Group* internacional (TCG) formuló especialmente una norma de conexión de red basada tecnología informática confiable de conexión de red confiable (TNC), que se denomina TCG-TNC. La TCG-TNC incluye una arquitectura de integridad terminal abierta y un conjunto de normas para garantizar una operación mutua segura. Este conjunto de normas puede proteger una red en caso de necesidad de un usuario, y el usuario puede definir el alcance de la protección. La TCG-TNC comienza sustancialmente a establecer una conexión en base a la integridad del terminal. En primer lugar, es necesario crear un conjunto de políticas sobre el estado de funcionamiento en el sistema interior de red confiable. Sólo los terminales que cumplan con las políticas creadas por la red pueden acceder a la red. La red aísla y localiza los dispositivos que no cumplan con las políticas. Debido a la utilización de un módulo se plataforma confiable TPM, puede bloquearse un ataque de los sistemas raíz. Los sistemas raíz son un tipo de script y herramientas de ataque, un programa de sistema modificado, o un conjunto de scripts y herramientas de ataque, que se utiliza para obtener ilegalmente la autorización de control más alta del sistema en un sistema de destino.

La figura 1 ilustra la arquitectura existente TCG-TNC que tiene tres entidades lógicas, es decir, un solicitante de acceso AR, un punto de aplicación de políticas PEP y un punto de decisión de políticas PDP, que pueden estar distribuidos en cualquier posición en la red. La arquitectura TCG-TNC puede dividirse en tres capas en una dirección longitudinal, es decir, en una capa de acceso de red, una capa de evaluación de integridad y una capa medición de integridad. La capa de acceso de red tiene tres componentes, es decir, un solicitante de acceso a la red NAR, un ejecutor de políticas PE y un autorizador de acceso a la red NAA, y una interfaz de protocolos de transporte de autorización de la red IF-T y una interfaz de puntos de aplicación de políticas IF-PEP. La capa de acceso a la red está adaptada para soportar la tecnología de conexión de red convencional, y la capa de evaluación de integridad está adaptada para evaluar la integridad de todas las entidades que solicitan acceso a la red. La capa de evaluación de integridad tiene dos interfaces importantes: una interfaz de colector de medición de integridad IF-IMC y una interfaz de medición de verificador de integridad IF-IMV. Adicionalmente, tiene, además, una interfaz TNC cliente-servidor IF-TNCCS entre el TCN cliente y el TNC servidor. La capa de medición de integridad tiene dos componentes, es decir, un colector de medición de integridad IMC y un verificador de medición de integridad IMV, que están adaptados para recoger y verificar la información relacionada con la integridad de la solicitante de acceso. Un proceso de transmisión de información completa mediante una conexión de red confiable en la arquitectura TCG-TNC existente es el siguiente: antes de establecer una conexión de red, es necesario que el TNC cliente TNCC prepare la información de medición de integridad de la plataforma necesaria para enviar la información al colector de medición de integridad IMC. En un terminal que tiene un módulo de plataforma confiable, la etapa anterior es para el cifrado de la información de la plataforma requerida por la política de red para almacenar la información de cifrado en cada registro de configuración de la plataforma, personalización previa, por el TNC servidor TNCS, un requisito de verificación de la plataforma para proporcionar integridad al verificador medición de integridad IMV. Los procesos específicos de la realización de un control de acceso a la red con la arquitectura TCG-TNC existentes son tal como sigue:

1) iniciar una solicitud de acceso por el solicitante de acceso a la red NAR al aplicador de políticas PE;
2) transmitir la descripción de solicitud de acceso por el aplicador de políticas PE al autorizador de acceso a la red NAA;

3) después de recibir la descripción de la solicitud de acceso del solicitante de acceso a la red NAR, el autorizador de acceso a la red NAA ejecuta un protocolo de autenticación de usuario con el solicitante de acceso a la red NAR, y transmitir, mediante el autorizador de acceso a la red NAA, la petición e información de acceso para indicar una autenticación de usuario satisfactoria al TNC servidor TNCS en caso de autenticación de usuario satisfactoria;

4) después de recibir la petición y la información de acceso para indicar una autenticación de usuario satisfactoria transmitida por el autorizador de acceso a la red NAA, el TNC servidor TNCS comienza a ejecutar una autenticación bidireccional de credenciales de la plataforma con el TNC cliente TNCC, por ejemplo, una clave de identidad de certificación AIK para verificar una plataforma;

5) cuando la autenticación de credenciales de la plataforma es satisfactoria, el TNC cliente TNCC informa al colector de medición de integridad IMC que se ha iniciado una nueva conexión a la red y se requiere un protocolo de acuerdo de integridad. El colector de medición de integridad IMC devuelve la información de la integridad de la plataforma requerida a través de la interfaz del colector de medición de la integridad IF-IMC. El TNC servidor TNCS envía la información de la integridad de la plataforma al verificador de integridad IMV a través de la interfaz del verificador de medición de integridad IF-IMV;

6) en el proceso de protocolo de acuerdo de integridad, es necesario que el TNC cliente TNCC y el TNC servidor TNCS cambien datos una vez o muchas veces, hasta que el TNC servidor TNCS satisface;

7) después de completar el protocolo de integridad de acuerdo por el TNC cliente TNCC, el TNC servidor TNCS transmitirá una información de recomendación al autorizador de acceso a la red NAA para solicitar una autorización de acceso; y el punto de aplicación de políticas PEP todavía puede no permitir un acceso del solicitante de acceso AR si existen otras consideraciones sobre seguridad; y

8) el autorizador de acceso a la red NAA transfiere una decisión de acceso al ejecutor de políticas PE que finalmente realiza la decisión de controlar el acceso del solicitante de acceso AR.

Recientemente, el producto de arquitectura TCG-TNC no se encuentra suficientemente desarrollado, y algunas tecnologías importantes de la arquitectura TCG-TNC se encuentran todavía en fases de investigación y estandarización. Dado que no existe un canal de seguridad predefinido entre el punto de aplicación de políticas PEP y el punto de decisión de políticas PDP que puede manejar una gran cantidad de puntos de aplicación de políticas PEP, el punto de decisión de políticas PDP debe configurar una gran cantidad de canales de seguridad, de modo que la gestión se vuelve compleja. Por lo tanto, la capacidad de expansión de la arquitectura TCG-TNC saliente es pobre. Además, dado que se llevará a cabo la protección de salvaguardia para los datos sobre la capa de acceso a la red, un pasaje de seguridad entre el solicitante de acceso AR y el punto de decisión de políticas PDP, es decir, debe establecerse una negociación de claves de sesión entre ellos; sin embargo, también es necesaria una protección de datos entre el solicitante de acceso AR y el punto de aplicación de políticas PEP y, por lo tanto, se llevará a cabo una vez más una negociación de claves de sesión entre el solicitante de acceso AR y el punto de decisión de políticas PEP, lo cual hace que el proceso de negociación de claves resulte complejo. Mientras tanto, la clave maestra negociada por el solicitante de acceso AR y el punto de decisión de políticas PDP se transfiere al punto de aplicación de políticas PEP por el punto de decisión de políticas PDP, y la transmisión de una clave en la red introduce nuevos puntos de ataque de seguridad, reduciendo así la seguridad. Además, se utiliza la misma clave maestra para las dos negociaciones de claves de sesión y, por lo tanto, se reduce la seguridad de toda la arquitectura conexión a la red confiable. Además, el solicitante de acceso no puede verificar la validez del certificado AIK del punto de decisión de políticas PDP. En el proceso de autenticación de credenciales de la plataforma, el solicitante de acceso AR y el punto de decisión de políticas PDP utilizan una clave privada AIK y un certificado para realizar una autenticación bidireccional de credenciales de la plataforma, y ambas partes tienen que verificar la validez del certificado AIK. Si el punto de decisión de políticas PDP es un proveedor de servicios de Internet del solicitante de acceso AR, el solicitante de acceso AR no tiene acceso a la red hasta que se conecta a la red confiable, es decir, no se puede verificar la validez del certificado AIK del punto de decisión de políticas PDP, que es inseguro. Finalmente, la evaluación de la integridad de la plataforma no es punto a punto. En la arquitectura TCG-TNC, el punto de decisión de políticas PDP lleva a cabo la evaluación de la integridad de la plataforma al solicitante de acceso AR, pero el solicitante de acceso AR no realiza la evaluación de la integridad de la plataforma del punto de decisión de políticas PDP, lo cual es injusto e inseguro para el solicitante de acceso AR. Además, el punto de aplicación de políticas PEP puede saber si la plataforma del solicitante de acceso AR es confiable en base a la política de ejecución del punto de decisión de políticas PDP, pero el solicitante de acceso AR no puede determinar si la plataforma del punto de decisión de políticas PDP es confiable, de manera que el solicitante de acceso AR puede estar conectado a un dispositivo no confiable (por ejemplo, un dispositivo de software malicioso existente, etc.) y, por lo tanto, es inseguro. Además, la cadena confiable del solicitante de acceso AR de la red confiable puede interrumpirse en el punto de aplicación de políticas PEP, pero la confianza entre pares es necesaria en la red ad hoc.

La "Arquitectura de Conexión de Red Confiable TCG TNC para Interoperabilidad, Versión de Especificación 1.1, Revisión 2" define una arquitectura de Conexión de Red Confiable (TNC) para el control y autorización de acceso a la red interoperable. El TNC se aprovechará y se integrará con mecanismos de control de acceso de red existentes,

tales como 802.1 × [18] u otros. Las especificaciones TNC también definirán interfaces de interoperabilidad para permitir el intercambio de nuevos tipos de atributos en el contexto de las soluciones de control de acceso de la red. Esos atributos incluirán información sobre cumplimiento de punto final, certificación de estado de software, así como información relacionada con el intercambio de autenticación de la plataforma. Los mecanismos de certificación de estado de software y Autenticación de la Plataforma se basarán en los principios y características de informática confiable, tal como se define por el *Trusted Computing Group* (TCG).

US 20050138417 describe un sistema y un método de control de acceso a una red confiable. El sistema de control de acceso a la red confiable incluye un ordenador remoto que ejecuta un asesor. Un primer dispositivo de control de acceso a la red confiable se conecta al ordenador remoto mediante una red. Un director está conectado al primer dispositivo de control de acceso a la red confiable y controla el primer dispositivo de control de acceso a la red confiable. En una realización, un controlador de acceso remoto está conectado al primer dispositivo de control de acceso a la red confiable. Un segundo dispositivo de control de acceso a la red confiable está conectado al controlador de acceso remoto. En otra realización, una red protegida está conectada al primer dispositivo de control de acceso a la red confiable.

DESCRIPCIÓN DE LA INVENCIÓN

El objeto de la invención es disponer un sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, que resuelve el problema técnico de la pobre capacidad de expansión de TCG-TNC existente que se describe en la información sobre el estado de la técnica, que puede resolver, además, los problemas técnicos de que el proceso de negociación de claves es complejo, la seguridad es relativamente baja, el solicitante de acceso puede no ser capaz de verificar la validez del certificado AIK y la evaluación integridad de la plataforma puede no ser punto a punto.

La solución técnica de la invención es la siguiente:

Un sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, que comprende un solicitante de acceso AR, un controlador de acceso AC y un gestor de políticas PM, en el que
el PM está adaptado para verificar la validez de certificados AIK de claves de identidad de certificación del AR y el AC comprueba la confiabilidad de la plataforma del AR y el AC; el AR está conectado al AC a través de una interfaz de protocolo a través de la red, el AC está conectado al PM a través de una interfaz de protocolo a través de la red y el AR está conectado al PM a través del AC a través de la red;
la interfaz de protocolo que conecta el AR con el AC comprende: una interfaz de transporte de red confiable IF-TNT y una interfaz IF-TNACCS entre el TNAC cliente y el TNAC servidor, en el que la IF-TNT es la interfaz de intercambio de información entre el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC en la capa de control de acceso a la red; y la IF-TNACCS es una interfaz de intercambio de información entre el TNAC cliente y el TNAC servidor en la capa de evaluación de plataforma confiable;
la interfaz de protocolo entre el AC y el PM comprende: una interfaz de servicio de políticas de autenticación IF-APS, una interfaz de servicio de políticas de evaluación IF-EPS y una interfaz de medición de confiabilidad IF-TM, en el que la IF-APS es una interfaz de intercambio de información entre el controlador de acceso a la red NAC y el servidor de políticas de autenticación APS en la capa de control de acceso a la red; la IF-EPS es una interfaz de intercambio de información entre un TNC servidor y un servidor de políticas de evaluación EPS en la capa de evaluación de la plataforma confiable; y la IF-TM es una interfaz entre el colector de medición de confiabilidad y el verificador de medición de confiabilidad en la capa de medición de la confiabilidad;
la interfaz de protocolo que conecta el AR con el PM que comprende un interfaz de la medida confiabilidad IF-TM, en el que la IF-TM es una interfaz entre el colector de medición de la confiabilidad y el verificador de medición de la confiabilidad en la capa de medición confiabilidad.

Opcionalmente, el AR comprende un solicitante de acceso a la red NAR, un TNAC cliente TNACC y un colector de medición de la confiabilidad TMC_1 del solicitante de acceso, el NAR está conectado al TNACC de manera que se transportan datos; y el TNACC está conectado al colector de medición de la confiabilidad TMC_1 del AR a través de la interfaz del colector de medición de confiabilidad IF-TMC;
el AC comprende el NAC, el TNAC servidor TNACS y el colector de medición de la confiabilidad TMC_2 del AC, el NAC está relacionado con el TNACS de manera que se transportan datos, y el TNACS está conectado al TMC_2 del AC a través de IF-TMC;
el PM comprende el APS, el EPS y el verificador de medición de la confiabilidad TMV, el APS está conectado al EPS de manera que se transportan datos, y el EPS está conectado al TMV a través de la interfaz de verificación de medición de la confiabilidad IF-TMV;
el NAR está conectado al NAC a través de la interfaz de transporte de la red confiable IF-TNT, y el NAC está relacionado con el APS a través de la IF-APS;
el TNACC está conectado al TNACS través de la interfaz IF-TNACCS entre el TNAC cliente y el TNAC servidor, y el TNACS está conectado al EPS a través de la IF-EPS;

el TMC_1 del AR está conectado al TMV a través de la IF-TM, y el TMC_2 del AC está conectado al TMV a través de la IF-TM.

Opcionalmente, el AR y el AC son entidades lógicas que tienen un módulo de plataforma confiable TPM.

Opcionalmente, el TMC_1 del AR es un componente para recoger la información de la confiabilidad de la plataforma AR, el TMC_2 del AC es el componente para recoger de información de confiabilidad de la plataforma del AC, y el TMV es un componente para realizar la verificación de la confiabilidad de la plataforma al AR y el AC.

En comparación con las tecnologías existentes, la invención tiene las siguientes ventajas:

La invención define la confiabilidad como cada atributo de estado de la plataforma que se utiliza para medir y evaluar si una plataforma es confiable, por ejemplo, la integridad y, de este modo, extiende la descripción de la confiabilidad de la plataforma. En la invención, se lleva a cabo la negociación de claves entre el solicitante de acceso y el controlador de acceso, y los datos en el proceso de evaluación de la plataforma confiable y los datos de servicio que están sometidos a un control de acceso de la red confiable TNAC están protegidos por seguridad directamente sin necesidad de una segunda negociación de claves de sesión. Por lo tanto, el proceso de negociación de claves puede simplificarse y la seguridad del control de acceso a la red confiable TNAC puede mejorarse. Además, no es necesario transferir en la red la clave maestra generada en el proceso de autenticación de la invención, de manera que puede garantizarse la seguridad de la clave. En segundo lugar, la invención puede mejorar la seguridad del proceso de evaluación de la plataforma confiable, simplificar la gestión de claves del control de acceso a la red confiable TNAC y el mecanismo de verificación de la medición de la confiabilidad. Se utiliza un método de autenticación entre pares de tres elementos, es decir, un método de autenticación bidireccional basado en un tercero, en la capa de evaluación de la plataforma confiable para implementar respectivamente la identificación y la verificación de los certificados AIK y la confiabilidad de la plataforma del solicitante de acceso y el control de acceso de manera concentrada, de tal manera que se aumenta no sólo la seguridad del proceso de evaluación de la plataforma confiable, sino que también la gestión de claves de la arquitectura TNAC de control de la red confiable y el mecanismo de verificación de la confiabilidad se simplifican. Además, la invención no sólo utiliza una autenticación entre pares de tres elementos en la capa de control de acceso a la red para implementar la autenticación de usuario bidireccional, sino que también utiliza el método en la capa de evaluación de la plataforma confiable para implementar la evaluación bidireccional de la plataforma confiable. Por lo tanto, la invención mejora la seguridad de toda la arquitectura de control de acceso a la red confiable TNAC. En la aplicación práctica, un gestor de políticas necesita gestionar una gran cantidad de controladores de acceso. La invención puede eliminar el requisito de una fuerte relevancia de seguridad entre el controlador de acceso y el gestor de políticas. Por lo tanto, la invención aumenta aún más la capacidad de expansión del control de acceso a la red confiable TNAC. En la invención, dado que se implementa la evaluación bidireccional de la plataforma confiable entre el solicitante de acceso y el controlador de acceso, se elimina el problema de que la cadena confiable se interrumpa durante el acceso del controlador de acceso del dispositivo. Finalmente, en la invención, el controlador de acceso realiza un control de múltiples niveles a los puertos controlados mediante el uso de un control de múltiples niveles, controlando estrictamente de esta manera el derecho de acceso del solicitante de acceso, mejorando la seguridad y el rendimiento de la arquitectura del control de acceso de la red confiable y expandiendo la descripción del módulo de la plataforma confiable. En la arquitectura TCG-TNC existente, el módulo de la plataforma confiable TPM es el chip seguro en la placa principal, y en la invención, el módulo de la plataforma confiable TPM puede ser un módulo de software abstracto que sea responsable de la implementación de una evaluación de plataforma confiable. Por ejemplo, el módulo de plataforma confiable TPM implementado por software explora cada componente de la plataforma, y luego genera resultados de exploración segura para enviarlos a la plataforma homóloga, y la plataforma homóloga evalúa los resultados de la exploración segura, de manera que se implementa la evaluación de la plataforma confiable.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es una vista esquemática de la arquitectura básica TCG-TNC existente.
La figura 2 es una vista esquemática de la arquitectura básica TNAC de acuerdo con la invención.
La figura 3 es una vista esquemática de una transferencia de información completa del control de acceso a la red confiable TNAC de acuerdo con la invención.

Los signos de referencia del dibujo se explican como sigue:

PEP: punto de aplicación de políticas; PE: aplicador de políticas; PDP: punto de decisión de políticas; NAA: autorizador de acceso a la red; AR: solicitante de acceso; AC: controlador de acceso; PM: gestor de políticas; TMC_1: colector de medición de confiabilidad del solicitante de acceso AR; TMC_2: colector de medición de confiabilidad del controlador de acceso AC; TMV: verificador de medición de confiabilidad; TNACC: TNAC cliente; TNACS: TNAC servidor; EPS: servidor de políticas de

evaluación; NAR: solicitante de acceso a la red; NAC: controlador de acceso a la red; APS: servidor de políticas de autenticación; IF-TNT: interfaz de transporte de red confiable que define una interfaz de información entre el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC; IF-APS: política de autenticación de interfaz de servicios que define un intercambio de información de la interfaz entre el controlador de acceso a red NAC y el servidor de políticas de autenticación APS; IF-TNACCS: interfaz TNAC cliente - TNAC servidor que es la interfaz de protocolo entre el TNAC cliente TNACC y el TNAC servidor TNACS; IF-EPS: interfaz de servicio de políticas de evaluación que define una interfaz de intercambio de información entre el TNAC servidor TNACS y el servidor de políticas de evaluación EPS; IF-TMC: interfaz de colector de medición de confiabilidad que es una interfaz de protocolo entre el TNAC cliente TNACC y el colector de medición de confiabilidad TMC_1 del solicitante de acceso AR, que es también una interfaz de protocolo entre el TNAC servidor TNACS y el colector de medición de confiabilidad TMC_2 del controlador de acceso AC; IF-TMV: interfaz de verificador de medición de confiabilidad que es una interfaz de protocolo entre el servidor de políticas de evaluación EPS y el verificador de medición de confiabilidad TMV; IF-TM: interfaz de medición de la confiabilidad que es una interfaz de protocolo entre el colector de medición de confiabilidad TMC_1 del solicitante de acceso AR y el verificador de medición de confiabilidad TMV, que es también una interfaz de protocolo entre el colector de medición confiabilidad TMC_2 del controlador de acceso AC y el verificador de medición confiabilidad TMV.

DESCRIPCIÓN DE LAS REALIZACIONES PREFERIDAS

La invención es un sistema de control de conexión a una red basado en una tecnología informática confiable, y es un sistema de control de acceso a una red confiable TNAC basado en autenticación entre pares de tres elementos. La invención se dispone principalmente para el problema existente de la arquitectura TNC en el actual sistema de TCG.

La confiabilidad en la invención significa cada atributo de estado de la plataforma que se utiliza para medir y evaluar si una plataforma es confiable, por ejemplo, la integridad.

En la invención, el módulo de plataforma confiable TPM puede ser un módulo de plataforma confiable TPM de la arquitectura TNC en el sistema TCG, o un módulo de software abstracto responsable de implementar una evaluación de plataforma segura. Por ejemplo, el módulo de plataforma confiable TPM implementado por software explora cada componente de la plataforma, y luego genera un resultado de exploración segura para enviar el resultado a una plataforma homóloga. La plataforma homóloga evalúa los resultados de la exploración segura, aplicando, de esta manera, una evaluación de plataforma confiable.

Haciendo referencia a la figura 2, la invención consiste principalmente en tres entidades lógicas, es decir, un solicitante de acceso AR, un controlador de acceso AC y un gestor de políticas PM, que pueden estar distribuidos en cualquier posición en la red. El solicitante de acceso AR también se refiere a un solicitante, una estación de usuario, etc.; el controlador de acceso AC también se refiere a un controlador de acceso de autenticación, una estación de base, una unidad de servicio de acceso, etc.; el gestor de políticas PM también se denomina servidor de autenticación, servidor confiable, servidor oculto, etc. El solicitante de acceso AR está conectado al controlador de acceso AC a través de una interfaz de protocolo a través de la red, el controlador de acceso AC está conectado al gestor de políticas PM a través de una interfaz de protocolo a través de la red, y el gestor de políticas PM está conectado al solicitante de acceso AR a través del controlador de acceso AC a través de la red. El solicitante de acceso AR solicita acceder a una red de protección y puede juzgar si es necesario acceder a la red de protección. El controlador de acceso AC controla el acceso del solicitante de acceso AR a la red de protección. El gestor de políticas PM gestiona el solicitante de acceso AR y el controlador de acceso AC, y formula y distribuye políticas de control de acceso a la red para el solicitante de acceso AR y el controlador de acceso AC. En una capa de control de acceso a la red, el solicitante de acceso AR, el controlador de acceso AC y el gestor de políticas PM ejecutan un protocolo de autenticación entre pares de tres elementos, es decir, un protocolo de autenticación de usuario bidireccional basado en un gestor de políticas PM de un tercero confiable, para poner en práctica la autenticación de usuario bidireccional entre el solicitante de acceso AR y el controlador de acceso AC. En la capa de evaluación de la plataforma confiable, la solicitante de acceso AR, el controlador de acceso AC y el gestor de políticas PM ejecutan un protocolo de autenticación entre pares de tres elementos, es decir, un protocolo de evaluación bidireccional de la plataforma confiable basado en un gestor de políticas PM de un tercero confiable, para implementar la evaluación de la plataforma bidireccional confiable entre el solicitante de acceso AR y el controlador de acceso AC. El gestor de políticas PM está adaptado para verificar la validez de los certificados AIK del solicitante de acceso AR y el controlador de acceso AC y comprueba la confiabilidad de la plataforma del solicitante de acceso AR y el controlador de acceso AC. Durante la verificación de la confiabilidad de la plataforma del solicitante de acceso AR y el controlador de acceso AC, se utilizará un colector de medición de confiabilidad y un verificador de medición de confiabilidad en la capa de medición de confiabilidad. El solicitante de acceso AR se compone principalmente de un solicitante de acceso a la red NAR, un TNAC cliente TNACC y un colector de medición de confiabilidad TMC_1 del solicitante de acceso. El solicitante de acceso a la red NAR está conectado al TNAC cliente TNACC de manera que

se transportan datos para reenviar mensajes por el TNAC cliente TNACC. El TNAC cliente TNACC está conectado al colector de medición de confiabilidad TMC_1 del solicitante de acceso AR a través de una interfaz del colector de medición de confiabilidad IF-TMC para implementar la comunicación entre el colector de medición de confiabilidad TMC_1 del solicitante de acceso AR y el verificador de medición confiabilidad TMV.

El controlador de acceso AC consiste principalmente en un controlador de acceso a la red NAC, un TNAC servidor TNACS, un colector de medición de confiabilidad TMC_2 del controlador de acceso AC. El controlador de acceso a la red NAC está conectado al TNAC servidor TNACS de manera que se transportan datos para reenviar mensajes por el TNAC servidor TNACS. El TNAC servidor TNACS está conectado al colector de medición de confiabilidad TMC_2 del colector de acceso AC a través de una interfaz de colector de medición de confiabilidad IF-TMC para implementar una comunicación entre el colector de medición confiabilidad TMC_2 del controlador de acceso AC y el verificador de medición de confiabilidad TMV. Debe indicarse que la interfaz de protocolo que conecta el AR con el AC incluye una interfaz de transporte de red confiable IF-TNT y una interfaz IF-TNACCS entre el TNAC cliente y el TNAC servidor.

El gestor de políticas PM consiste principalmente en un servidor de políticas de autenticación APS, un servidor de políticas de evaluación EPS, un verificador de medición de confiabilidad TMV. El servidor de políticas de autenticación APS está conectado al servidor de políticas de evaluación EPS de manera que se transportan datos para reenviar mensajes por el servidor de políticas de evaluación EPS. El servidor de política de evaluación EPS está conectado al verificador de medición de confiabilidad TMV a través de una interfaz de verificador de medición de confiabilidad IF-TMV para implementar una comunicación entre el verificador de medición de confiabilidad TMV y el colector de medición de confiabilidad TMC_1 del solicitante de acceso AR y el colector de medición de confiabilidad TMC_2 del controlador de acceso AC.

El solicitante de acceso a la red NAR, el controlador de acceso a la red NAC y el servidor de políticas de autenticación APS constituyen una capa de control de acceso a la red. El solicitante de acceso a la red NAR está conectado al controlador de acceso a la red NAC a través de una interfaz de transporte de red confiable IF-TNT, que es la interfaz de intercambio de información entre el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC en la capa de control de acceso a la red; y el controlador de acceso a la red NAC está conectado al servidor de políticas de autenticación APS a través de la interfaz de servicio de políticas de autenticación IF-APS. En la capa de control de acceso a la red, el solicitante de acceso a la red NAR, el controlador de acceso a la red NAC y el servidor de políticas de autenticación APS ejecutan un protocolo de autenticación entre pares de tres elementos, es decir, un protocolo de autenticación de usuario bidireccional basado en un servidor de políticas de autenticación de terceros confiables APS. La capa de control de acceso a la red es responsable de implementar lo siguiente: una autenticación de usuario bidireccional y una negociación de claves entre el solicitante de acceso AR y el controlador de acceso AC, un control de múltiples niveles para el puerto controlado en base al resultado de la autenticación del usuario y el resultado de la evaluación de la plataforma confiable para implementar un control de acceso mutuo entre el solicitante de acceso AR y el controlador de acceso AC. La capa de control de acceso a la red puede utilizar un método de control de acceso basado en una autenticación entre pares de tres elementos, en la cual se añade una función de control de puertos de múltiples niveles en base a la tecnología de control de acceso a la red utilizada en la norma WLAN china.

Debe indicarse que la información intercambiada entre el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC en la capa de control de acceso a la red incluye información de gestión de control, el protocolo de autenticación entre pares de tres elementos, el protocolo de negociación de claves de sesión y el protocolo de transferencia de la red en la capa de control de acceso a la red, etc. La información de gestión de control incluye un comando de negociación y control de la política de acceso, tal como un conjunto de negociación y acceso, un conjunto de autenticación y un conjunto de cifrado, para enviar diversos tipos de comandos de control; y el protocolo de transferencia de la red incluye principalmente el paquete de datos del protocolo de autenticación entre pares de tres elementos y la transmisión secreta de datos en la capa superior.

El TNAC cliente TNACC, el TNAC servidor TNACS y el servidor de políticas de evaluación EPS constituyen la capa de evaluación de la plataforma confiable. El TNAC cliente TNACC está conectado al TNAC servidor TNACS a través de la interfaz TNAC cliente-TNAC servidor IF-TNACCS que es la interfaz de intercambio de información entre el TNAC cliente y el TNAC servidor en la capa de evaluación de la plataforma confiable; y el TNAC servidor TNACS está conectado al servidor de políticas de evaluación EPS a través de la interfaz de servicio de políticas de evaluación IF-EPS. La capa de evaluación de la plataforma confiable está adaptada para poner en práctica la evaluación de la plataforma confiable entre el solicitante de acceso AR y el controlador de acceso AC, incluyendo la autenticación de credenciales de la plataforma y la verificación de la medición de la confiabilidad de la plataforma. El gestor de políticas PM está adaptado para verificar la validez de los certificados AIK del solicitante de acceso AR y el controlador de acceso AC, y comprobar la confiabilidad de la plataforma del solicitante de acceso AR y el controlador de acceso AC. En la capa de evaluación de la plataforma confiable, el TNAC cliente TNACC, el TNAC servidor TNACS y el servidor de políticas de evaluación EPS ejecutan el protocolo de autenticación entre pares de tres

elementos, es decir, el protocolo de evaluación bidireccional de la plataforma confiable basado en un servidor de políticas de evaluación de terceros confiables EPS.

Debe indicarse que la información que se intercambia entre el TNAC cliente y el TNAC servidor en la capa de evaluación de la plataforma confiable incluye información de gestión de sesiones y el protocolo de autenticación entre pares de tres elementos en la capa de evaluación de la plataforma confiable; la información de gestión de sesiones incluye la política de evaluación de la plataforma confiable de negociación, por ejemplo: la negociación de la extracción del valor del registro de configuración de la plataforma PCRs para probar la medición de la confiabilidad per se para la plataforma homóloga, y negociar el lenguaje de descripción estándar del informe de la confiabilidad y la información de comandos de control, etc.

El colector de medición de confiabilidad TMC_1 del solicitante de acceso AR, el colector de medición de confiabilidad TMC_2 del controlador de acceso AC y el verificador medición de confiabilidad TMV constituyen la capa de medición de confiabilidad. El colector de medición de confiabilidad TMC_1 del solicitante de acceso AR está conectado al verificador de medición de confiabilidad TMV a través de una interfaz de medición de confiabilidad IF-TM, y el colector de medición confiabilidad TMC_2 del controlador de acceso AC está conectado al verificador de medición de confiabilidad TMV a través de una interfaz de medición de confiabilidad IF-TM. La capa de medición de confiabilidad está adaptada para recoger y verificar información relacionada con la medición de la confiabilidad de la plataforma del solicitante de acceso AR y el controlador de acceso AC.

Debe indicarse que la información intercambiada entre el controlador de acceso a la red NAC y el servidor de políticas de autenticación APS en la capa de control de acceso a la red incluye el protocolo de autenticación entre pares de tres elementos y el protocolo de transferencia de la red en la capa de control de acceso a la red. La información intercambiada entre el servidor TNC y el servidor de políticas de evaluación EPS en la capa de evaluación de la plataforma confiable incluye un protocolo de autenticación entre pares de tres elementos y el protocolo de distribución de políticas de evaluación de la plataforma confiable en la capa de evaluación de la plataforma confiable. La IF-TM es una interfaz entre el colector de medición de confiabilidad y el verificador de medición de confiabilidad en la capa de medición de la confiabilidad que está adaptada para definir la interfaz de protocolo de operación mutua entre el colector de medición de confiabilidad y el verificador de medición de confiabilidad producido por varios fabricantes. El NAR está conectado al TNACC de manera que transporta datos, el cual está adaptado para reenviar mensajes por el TNAC cliente TNACC; y el TNACC está conectado al colector de medición de confiabilidad TMC_1 del AR a través de una interfaz del colector de medición de confiabilidad IF-TMC para implementar la comunicación entre el colector de medición de confiabilidad TMC_1 del solicitante de acceso AR y el verificador de medición confiabilidad TMV.

Haciendo referencia a la figura 3, las etapas específicas de la implementación del control de acceso a una red confiable TNAC basado en autenticación entre pares de tres elementos de acuerdo con la invención son las siguientes:

1) inicializar el colector de medición de confiabilidad TMC y el verificador medición de confiabilidad en la capa de medición de confiabilidad, que prácticamente puede comprender las siguientes sub-etapas:
1.1) inicializar el colector de medición confiabilidad TMC de la capa de medición de confiabilidad por el TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, e inicializar el verificador de medición de confiabilidad TMV de la capa de medición de confiabilidad por el servidor de políticas de evaluación del gestor de políticas.
1.2) almacenar, mediante los módulos de plataforma confiable TPMs del solicitante de acceso AR y el controlador de acceso AC, la información de confiabilidad requerida por la política de red en registros de configuración de la plataforma PCRs, en el que la información de confiabilidad requiere llevar a cabo un proceso de cifrado que se almacena en los registros de la configuración de la plataforma PCR cuando la información de confiabilidad es integridad.
1.3) recoger la información de la confiabilidad de la plataforma del solicitante de acceso AR por el TNAC cliente TNACC del solicitante de acceso AR utilizando el colector de medición de confiabilidad TMC_1 del solicitante de acceso, y recoger la información de confiabilidad de la plataforma del controlador de acceso AC por el TNAC cliente TNACC del controlador de acceso AC utilizando el colector de medición de confiabilidad TMC_2 del controlador de acceso.
1.4) formular y distribuir, por el gestor de políticas PM, la política de control de acceso a la red que incluye la política para determinar si el solicitante de acceso AR añade la red a conectarse y la política de control de acceso a la red del controlador de acceso AC al solicitante el acceso AR, y aplicar, mediante el gestor de políticas PM, la formulación y la distribución la política de control de acceso a la red del solicitante de acceso AR y el controlador de acceso AC en base a la norma de protección del grado de seguridad de la información de estado.

1.5) preparar una tabla de parámetros PCRs para solicitar una interverification entre el solicitante de acceso AR y el control de acceso AC por el TNAC cliente TNACC y el TNAC servidor TNACS en base a la política de control de acceso a la red distribuida por el gestor de políticas, respectivamente.
2) ejecutar un protocolo de autenticación entre pares de tres elementos en base a un tercero que es el gestor de políticas en la capa de control de acceso a la red, el solicitante de acceso, el controlador de acceso y el gestor de políticas para implementar la autenticación bidireccional de usuario entre el solicitante de acceso y el controlador de acceso;

En particular, la etapa comprende lo siguiente:

2.1) iniciar una solicitud de acceso al controlador de acceso a la red NAC por el solicitante de acceso a la red NAR.
2.2) después de recibir la petición de acceso desde el solicitante de acceso a la red NAR, iniciar el proceso de autenticación de usuario por el controlador de acceso a la red NAC para ejecutar el protocolo de autenticación entre pares de tres elementos, es decir, el protocolo de autenticación bidireccional basado en el tercero, entre el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC y el servidor de políticas de autenticación APS que actúa como tercero en la capa de control de acceso a la red, aplicando de este modo la autenticación de usuario bidireccional entre el solicitante de acceso AR y el controlador de acceso AC y generando los resultados de la autenticación de usuario del solicitante de acceso AR y el controlador de acceso AC. Si la autenticación de usuario bidireccional es satisfactoria, el solicitante de acceso AR y el controlador de acceso AC generarán una clave maestra entre ellos durante la autenticación de usuario.
2.3) realizar, por parte del solicitante de acceso AR y el controlador de acceso AC, una negociación de claves de sesión utilizando la clave maestra generada durante la autenticación de usuario en caso de una autenticación de usuario satisfactoria, y después enviar la información para indicar la autenticación de usuario satisfactoria desde el solicitante de acceso a la red NAR y el controlador de acceso a la red NAC al TNAC cliente TNACC y el TNAC servidor TNACS respectivamente, y controlar, respectivamente, los puertos del solicitante de acceso a la red NAR y el controlador de acceso a la red NAC en base a los resultados de autenticación de usuario del controlador de acceso AC y el solicitante de acceso AR, de manera que pueden pasarse los datos en el proceso de evaluación de la plataforma confiable.
3) si el resultado de la autenticación de usuario bidireccional es satisfactorio o la política local requiere ejecutar el proceso de evaluación de la plataforma confiable, ejecutar el protocolo de autenticación entre pares de tres elementos en base a un tercero que es el gestor de políticas por el solicitante de acceso, el controlador de acceso y el gestor de políticas en la capa de evaluación de la plataforma confiable para implementar la evaluación bidireccional de la plataforma confiable entre el solicitante de acceso y el controlador de acceso.
Cuando el TNAC servidor TNACS del controlador de acceso AC recibe la información para indicar el éxito de autenticación de usuario enviado por el controlador de acceso a la red NAC, el TNAC cliente TNACC, el TNAC servidor TNACS y el servidor de políticas de evaluación EPS de la capa de evaluación de la plataforma confiable utilizan el protocolo de autenticación entre pares de tres elementos para implementar la evaluación bidireccional de la plataforma confiable entre el solicitante de acceso AR y el controlador de acceso AC. En el proceso de evaluación de la confiabilidad, la información interactuada entre el TNAC cliente y el TNAC servidor se transfiere bajo la protección de la clave de sesión negociada en la etapa 2.3). En el proceso de evaluación de la confiabilidad, la información para identificar la configuración de la plataforma del solicitante de acceso, por ejemplo, el registro de la medición correspondiente al valor del registro de la configuración de la plataforma PCRs, y la información de reparación de la configuración de la plataforma, etc., es necesario que sea transferida entre el solicitante de acceso y el gestor de políticas, lo cual requiere que sea transferida en secreto para evitar que el controlador de acceso o un atacante conozca la información. Del mismo modo, la información de configuración de la plataforma de identificación del controlador de acceso también requiere ser trasferida en secreto entre el controlador de acceso y el gestor de políticas para evitar que el solicitante de acceso o un atacante conozca la información. La técnica de transmisión secreta utilizable puede ser encriptado por clave simétrica y encriptado por clave asimétrica. En el proceso de evaluación de plataforma confiable, el servidor de políticas de evaluación EPS actúa como tercero, y el TNAC servidor TNACS, el TNAC cliente TNACC y el servidor de políticas de evaluación EPS requieren, además, realizar una interacción de información con el colector de medición de la confiabilidad y el verificador de medición de confiabilidad en la capa superior. La evaluación de plataforma confiable puede ser implementada de las siguientes maneras:

□ realizar una autenticación de credenciales de la plataforma: verificar la validez de los certificados AIK del solicitante de acceso AR y el controlador de acceso AC por el gestor de políticas PM.

□ comprobar una plataforma de verificación de confiabilidad: verificar la confiabilidad de la plataforma del solicitante de acceso AR y el controlador de acceso AC por el gestor de políticas PM.

4) generar, por parte del TNAC cliente del solicitante de acceso y el TNAC servidor del controlador de acceso, una recomendación correspondiente en base a los resultados de la evaluación de la confiabilidad de la plataforma que se producen en el proceso de evaluación de la confiabilidad de la plataforma para enviarlos al solicitante de acceso a la red y el controlador de acceso a la red respectivamente, de manera que el solicitante de acceso a la red y el controlador de acceso a la red realizan el control de puertos para el acceso de manera interactiva de acuerdo con la recomendación respectivamente.

En la práctica, la etapa puede comprender específicamente lo siguiente: el servidor de políticas de la plataforma genera los resultados de la evaluación de la plataforma confiable del solicitante de acceso y el controlador de acceso en el proceso de evaluación de la plataforma confiable para enviar los resultados al TNAC cliente y el TNAC servidor. El TNAC cliente y el TNAC servidor generan una recomendación correspondiente en base a los resultados de la evaluación de la plataforma confiable generados por el servidor de políticas de plataforma para enviar la recomendación al solicitante de acceso a la red y el controlador de acceso a la red, respectivamente. La recomendación incluye permiso, prohibición, reparación en aislamiento, etc. El solicitante de acceso a la red y el controlador de acceso a la red controlan los puertos en base a la recomendación recibida por ellos, respectivamente, controlando, de este modo, el acceso entre el solicitante de acceso y el controlador de acceso. Si la recomendación recibida por el solicitante de acceso a la red y el controlador de acceso a la red es aislamiento, el solicitante de acceso a la red y el controlador de acceso a la red realizan una reparación en base a información de reparación de la configuración de la plataforma obtenida por ellos en el proceso de evaluación de la confiabilidad de la plataforma, y luego vuelven a realizar la evaluación de la plataforma confiable.

Para el control de puertos anterior pueden utilizarse siguientes maneras de implementación:

Tanto el solicitante de acceso como el control de acceso definen dos tipos de puertos lógicos: puertos no controlados y puertos controlados. Los puertos no controlados del solicitante de acceso pueden pasar a través de la autenticación de usuario y datos de protocolo de negociación de claves, los datos de protocolo de evaluación de plataforma confiable y los datos del servidor de reparación de la plataforma, y los puertos controlados del solicitante de acceso sólo pueden pasar a través de los datos del servidor de aplicación. Los puertos no controlados del controlador de acceso sólo pueden pasar a través de la autenticación de usuario y datos de protocolo de negociación de claves y los puertos controlados del controlador de acceso implementan el control del paso de los datos del protocolo de evaluación de plataforma confiable, datos de servicio de reparación de la composición de la plataforma y datos de servicio de aplicación en un modo de control de múltiples niveles. El solicitante de acceso y el controlador de acceso controlan los puertos controlados en base al resultado de la autenticación de usuario y el resultado de la evaluación de la plataforma confiable.

REIVINDICACIONES

1. Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, en el que el sistema comprende un solicitante de acceso AR, un controlador de acceso AC y un gestor de políticas PM, en el que

el PM está adaptado para verificar la validez de certificados AIK de claves de identidad de certificación del AR y el AC comprueba la confiabilidad de la plataforma del AR y el AC;
el AR está conectado al AC a través de una interfaz de protocolo a través de la red, el AC está conectado al PM a través de una interfaz de protocolo a través de la red y el AR está conectado al PM a través del CA a través de la red;
la interfaz de protocolo que conecta el AR con el AC comprende: una interfaz de transporte de red confiable IF-TNT y una interfaz IF-TNACCS entre un TNAC cliente y un TNAC servidor; la IF-TNT es una interfaz de intercambio de información entre un solicitante de acceso a la red NAR y un controlador de acceso a la red NAC en una capa de control de acceso a la red, y la IF-TNACCS es una de interfaz de intercambio de información entre el TNAC cliente y el TNAC servidor en una capa de evaluación de plataforma confiable;
la interfaz de protocolo entre el AC y el PM comprende: una interfaz de servicio de políticas de autenticación IF-APS, una interfaz de servicio la políticas de evaluación IF-EPS y una interfaz de medición de confiabilidad IF-TM; la IF-APS es una interfaz de intercambio de información entre un controlador de acceso a la red NAC y un servidor de políticas de autenticación APS en la capa de control de la red, y la IF-EPS es una interfaz de intercambio de información entre un TNC servidor y un servidor de políticas de evaluación EPS en la capa de evaluación de la plataforma confiable; y la IF-TM es una interfaz entre un colector de medición de confiabilidad y un verificador de medición de confiabilidad en la capa de medición de la confiabilidad;
la interfaz de protocolo que conecta el AR y el PM comprende una interfaz de medición de confiabilidad IF-TM, y la IF-TM es una interfaz entre el colector de medición de confiabilidad y el verificador de medición de confiabilidad en la capa de medición de confiabilidad;
en el que puertos no controlados del solicitante de acceso pasan a través de datos de autenticación de usuario y de protocolo de negociación de claves, datos de protocolo de evaluación de plataforma confiable y datos de servidor de reparación de la plataforma, puertos controlados del solicitante el acceso pasan a través de datos del servidor de aplicación; puertos no controlados del controlador de acceso pasan a través de los datos de autenticación de usuario y de protocolo de claves de negociación, y puertos controlados del controlador de acceso implementan un control de paso de los datos de protocolo de evaluación de la plataforma confiable, datos de servicio de reparación de la composición de la plataforma y datos de servicio de aplicación en un modo de control de múltiples niveles.

2. Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, de acuerdo con la reivindicación 1, caracterizado por el hecho de que el AR comprende un solicitante de acceso a la red NAR, un TNAC cliente TNACC y un colector de medición de confiabilidad TMC_1 del solicitante de acceso, el NAR está conectado al TNACC de manera que transporta datos, y el TNAC cliente TNACC está conectado al TMC_1 del AR a través de una interfaz de colector de medición de confiabilidad IF-TMC;

el AC comprende un NAC, un TNAC servidor TNACS y un colector de medición de confiabilidad TMC_2 del AC, el NAC está conectado al TNACS de manera que transporta datos, y el TNAC servidor TNACS está conectado al TMC_2 del AC a través de la IF-TMC;
el PM comprende un APS, un EPS y un verificador de medición de la confiabilidad TMV, el APS está conectado al EPS de manera que transporta datos, y el EPS está conectado al TMV a través de la interfaz del verificador de medición de confiabilidad IF-TMV;
el NAR está conectado al NAC a través de una interfaz de transporte de red confiable IF-TNT, y el NAC está conectado al APS a través de la IF-APS;
el TNACC está conectado al TNACS través de una interfaz IF-TNACCS entre el TNAC cliente y el TNAC servidor, y el TNACS está conectado al EPS a través de la IF-EPS;
el TMC_1 del AR está conectado al TMV a través de la IF-TM, y el TMC_2 del AC está conectado al TMV a través de la IF-TM.

3. Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, de acuerdo con la reivindicación 1 o 2, caracterizado por el hecho de que el AR y el AC son entidades lógicas con un módulo de plataforma confiable TPM.

4. Sistema de control de acceso a una red confiable basado en autenticación entre pares de tres elementos, de acuerdo con la reivindicación 3, caracterizado por el hecho de que el TMC_1 del AR es un paquete para recoger

información de la confiabilidad de la plataforma del AR, el TMC_2 del AC es un paquete para recoger información de la confiabilidad de la plataforma del AC, y el TMV es un paquete para comprobar la medición de la confiabilidad de la plataforma para el AR y el AC.

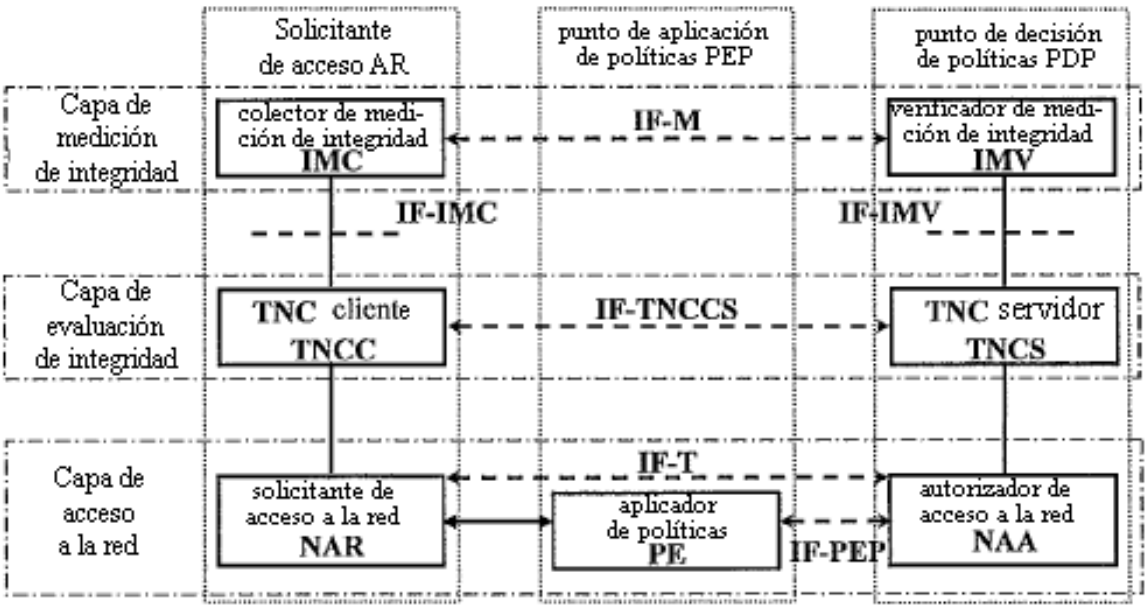

Figura 1

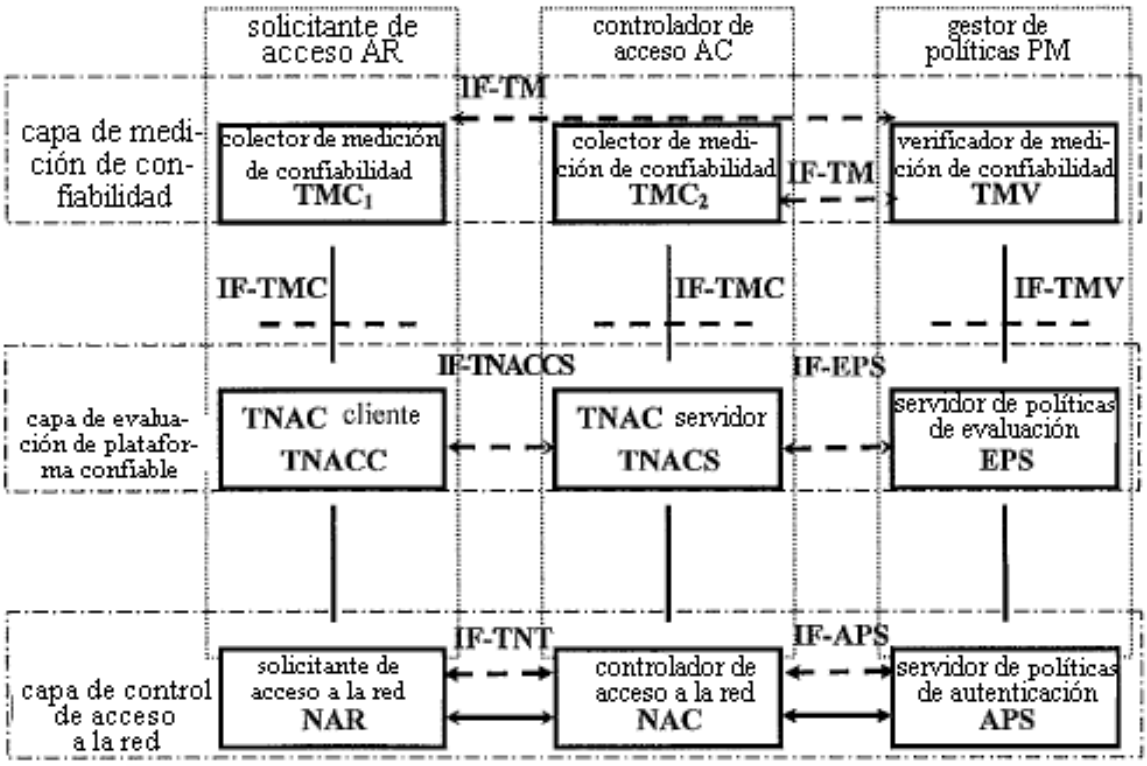

Figura 2

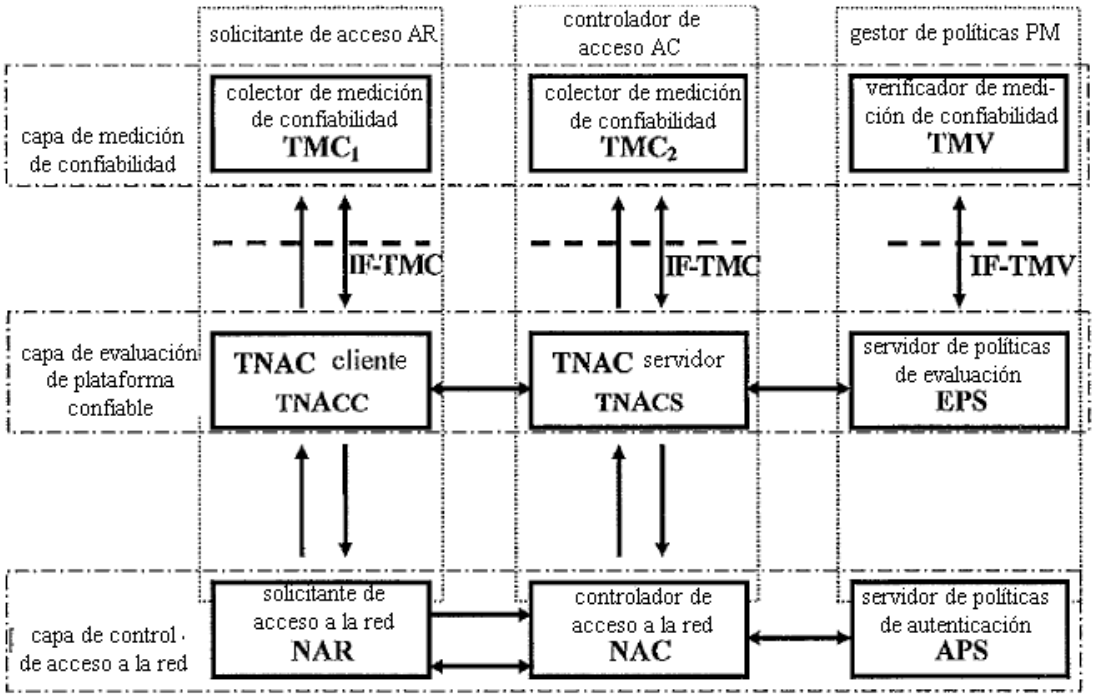
solicitante de acceso AR
controlador de acceso AC
gestor de políticas PM
capa de medición de confiabilidad
colector de medición de confiabilidad TMC1
colector de medición de confiabilidad TMC2
verificador de medición de confiabilidad TMV
IF-TMC
IF-TMC
IF-TMV
capa de evaluación de plataforma confiable
TNAC cliente TNACC
TNAC servidor TNACS
servidor de políticas de evaluación EPS
capa de control de acceso a la red
solicitante de acceso a la red NAR
controlador de acceso a la red NAC
servidor de políticas de autenticación APS

Figura 3

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

- CN 200710019094 **[0001]**
- US 20050138417 A **[0008]**