(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 509 040**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.07.2008 E 08773227 (7)**

(97) Fecha y número de publicación de la concesión europea: **03.09.2014 EP 2180632**

(54) Título: **Método para una conexión de red fiable basada en autenticación entre tres elementos del mismo nivel**

(30) Prioridad:

01.08.2007 CN 200710018395

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.10.2014

(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 Industrial Development Zone
Xi'an, Shaanxi 710075, CN

(72) Inventor/es:

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

(74) Agente/Representante:

TEMIÑO CENICEROS, Ignacio

DESCRIPCIÓN

Método para una conexión de red fiable basada en autenticación entre tres elementos del mismo nivel

Campo de la invención

La presente invención se refiere al campo de la seguridad en las redes y, en particular, a un método de conexión de red fiable basado en autenticación entre tres elementos del mismo nivel.

Antecedentes de la invención

Software maliciosos tales como virus y gusanos se han convertido en un gran problema a medida que se ha ido desarrollando la informatización. Ha habido más de treinta y cinco mil software maliciosos, y más de cuarenta millones de ordenadores se infectan cada año. Para proteger los ordenadores de este tipo de ataques, debe considerarse una transmisión segura y una comprobación de datos mientras se introducen, y debe realizarse una protección desde el origen, es decir, puntos de extremo conectados a la red. Sin embargo, las tecnologías de seguridad tradicionales no protegen contra numerosos ataques maliciosos.

El Grupo para la Informática Fiable (TCG, Trusted Computing Group) definió una especificación de conexión de red basada en la informática fiable, la conexión de red fiable (TNC, Trusted Network Connect), denominada de manera abreviada TCG-TNC, que incluye una arquitectura abierta para una integridad de punto de extremo y un conjunto de normas que garantizan interoperaciones seguras. Este conjunto de normas pueden proteger una red cuando lo necesite el usuario, y el usuario puede decidir en qué medida se protege la red. Básicamente, la TCG-TNC pretende establecer conexiones partiendo de la integridad de punto de extremo. En primer lugar, debe crearse un conjunto de políticas para el estado operativo de un sistema interno de la red fiable. Sólo los puntos de extremo que cumplan con la política establecida para la red pueden acceder a la red, y la red aísla y localiza dispositivos que no cumplan con las políticas. Los ataques de tipo *rootkit* también pueden bloquearse mediante el uso de un módulo de plataforma fiable (TPM, Trusted Platform Module). Un *rootkit* es una instrucción de programa de ataque, un programa de sistema modificado, o un conjunto de instrucciones de programa de ataque y herramientas que se usan para obtener ilegalmente un privilegio de control máximo de un sistema objetivo.

En la arquitectura TCG-TNC, se ilustra una transmisión de información completa de una conexión de red fiable en la figura 1. Antes del establecimiento de la conexión de red, el cliente TNC prepara información de integridad de plataforma requerida, y la envía al recopilador de medición de integridad, IMC (Integrity Measurement Collector). En un punto de extremo con un TPM, esto también significa que la información de plataforma requerida para una política de red se trocea (*hashed*) y se almacena en registros de configuración de plataforma (PCR, Platform Configuration Register). El servidor TNC establece previamente un requisito de verificación de integridad de plataforma y lo envía al verificador de medición de integridad, IMV (Integrity Measurement Verifier). El proceso se detalla tal como sigue:

(1) Un solicitante de acceso a la red inicia una petición de acceso a un aplicador de políticas.

(2) El aplicador de políticas envía una descripción de petición de acceso a un autorizador de acceso a la red.

(3) Tras la recepción de la descripción de petición de acceso desde el solicitante de acceso a la red, el autorizador de acceso a la red realiza un protocolo de autenticación de usuario con el solicitante de acceso a la red. Tras una autenticación de usuario satisfactoria, el autorizador de acceso a la red envía la petición de acceso e información de éxito de autenticación de usuario al servidor TNC.

(4) Tras la recepción de la petición de acceso y la información de éxito de autenticación de usuario enviada por el autorizador de acceso a la red, el servidor TNC realiza una autenticación de credenciales de plataforma bidireccional con el cliente TNC, por ejemplo, para verificar una clave de identidad de certificación (AIK, Attestation Identity Key) de la plataforma.

(5) Tras una autenticación de credenciales de plataforma satisfactoria, el cliente TNC notifica al IMC que se ha iniciado una conexión de red nueva y debe realizarse un protocolo de conformidad (*handshake*) de integridad. El IMC devuelve la información de integridad de plataforma requerida a través de una interfaz de recopilador de medición de integridad, IF-IMC. El servidor de TMC envía la información de integridad de plataforma al IMV a través de una interfaz de verificador de medición de integridad, IF-IMV.

(6) El cliente TNC y el servidor TNC realizan uno o más cambios de datos durante la ejecución del protocolo de conformidad de integridad hasta que se satisfaga al servidor TNC.

(7) Tras finalizar la ejecución del protocolo de conformidad de integridad sobre el cliente TNC, el servidor TNC envía una recomendación al autorizador de acceso a la red para solicitar que se permita el acceso. Si hay otras consideraciones de seguridad, el punto de decisión de políticas puede no permitir el acceso del solicitante de

acceso.

(8) El autorizador de acceso a la red envía una decisión de acceso al aplicador de políticas, y el aplicador de políticas aplica finalmente la decisión de acceso para controlar el acceso del solicitante de acceso.

Actualmente, no han salido al mercado productos desarrollados con la arquitectura TCG-TNC. Algunos aspectos importantes de la arquitectura TCG-TNC están todavía en una fase de investigación y normalización y tienen principalmente los siguientes inconvenientes:

1. Mala capacidad de ampliación. Se predefine un canal seguro entre el punto de aplicación de políticas y el punto de decisión de políticas, y el punto de decisión de políticas gestiona posiblemente un gran número de puntos de aplicación de políticas, por consiguiente, el punto de aplicación de políticas tiene que configurar un gran número de canales seguros, lo que da como resultado una gestión complicada y mala capacidad de ampliación.

2. Proceso de acuerdo de claves complicado. Con el fin de proteger datos en la capa de acceso a la red, debe establecerse un canal seguro entre el solicitante de acceso y el punto de decisión de políticas, es decir, debe realizarse un acuerdo de claves de sesión entre el solicitante de acceso y el punto de decisión de políticas. Sin embargo, también se requiere una protección de datos entre el solicitante de acceso y el punto de aplicación de políticas, por tanto debe realizarse de nuevo un acuerdo de claves de sesión entre el solicitante de acceso y el punto de aplicación de políticas, lo que complica el proceso de acuerdo de claves.

3. Nivel de seguridad bajo. Se envía la clave primaria, que resulta del acuerdo entre el solicitante de acceso y el punto de decisión de políticas, desde el punto de decisión de políticas hasta el punto de aplicación de políticas. Dado que la clave se transmite a través de la red, pueden introducirse puntos de ataque de seguridad nuevos, y disminuye el nivel de seguridad. Además, las dos veces que tiene lugar un acuerdo de claves de sesión se usa la misma clave primaria, lo que también puede reducir el nivel de seguridad de toda la arquitectura TNC.

4. El solicitante de acceso puede no poder verificar la validez del certificado de AIK del punto de decisión de políticas. Durante la autenticación de credenciales de plataforma, el solicitante de acceso y el punto de decisión de políticas usan una clave privada de AIK y un certificado para la autenticación de credenciales de plataforma bidireccional, y ambos deben verificar la validez del certificado de AIK. Si el punto de decisión de políticas es un proveedor de servicios de red para el solicitante de acceso, entonces el solicitante de acceso no puede acceder a la red antes de que se establezca una conexión de red fiable, es decir, no puede verificarse la validez del certificado de AIK del punto de decisión de políticas, lo que disminuye el nivel de seguridad.

5. La evaluación de integridad de plataforma no es paralela. En la arquitectura TCG-TNC, el punto de decisión de políticas realiza una evaluación de integridad de plataforma sobre el solicitante de acceso, pero el solicitante de acceso no realiza una evaluación de integridad de plataforma sobre el punto de decisión de políticas. Si la plataforma del punto de decisión de políticas no es fiable, no es seguro que el solicitante de acceso se conecte con un dispositivo no fiable. Sin embargo, se requiere una fiabilidad paralela en redes ad hoc. El documento “TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.1, Revision 2” da a conocer flujos de mensajes básicos a través de interfaces en la arquitectura TNC. El documento EP1182557A2 da a conocer un método para realizar un servicio para un solicitante sobre una plataforma informática en la que el solicitante proporciona una especificación del servicio a la plataforma informática y la especificación del servicio establece niveles especificados de fiabilidad para al menos algunos de los procesos en el servicio.

Sumario de la invención

La invención proporciona un método de TNC basado en autenticación entre tres elementos del mismo nivel, que puede resolver los problemas técnicos en la técnica anterior de mala capacidad de ampliación, proceso de acuerdo de claves complicado, baja seguridad, posible incapacidad del solicitante de acceso de verificar la validez del certificado de AIK y evaluación de integridad de plataforma no paralela.

La solución técnica de la invención se describe tal como sigue:

Un método de conexión de red fiable basado en autenticación entre tres elementos del mismo nivel incluye:

(1.) etapa de inicialización:

(1.1) preparar previamente, por parte de un cliente TNC de un solicitante de acceso y un servidor TNC de un controlador de acceso, información de integridad de plataforma, y enviar la información de integridad de plataforma a recopiladores de medición de integridad, IMC, respectivos en una capa de medición de integridad;

(1.2) establecer previamente, por parte del cliente TNC y el servidor TNC, un requisito de verificación de integridad que incluye una lista de registros de configuración de plataforma, PCR, que el solicitante de acceso

y el controlador de acceso se solicitan mutuamente para verificación; y

(1.3) trocear, por parte de módulos de plataforma fiables, TPM, del solicitante de acceso y el controlador de acceso, información requerida para una política de red, y almacenarla en los PCR;

(2.) etapa de autenticación de usuario:

(2.1) iniciar, por parte de un solicitante de acceso a la red, una petición de acceso a un controlador de acceso a la red;

(2.2) iniciar, por parte del controlador de acceso a la red, tras la recepción de la petición de acceso, un proceso de autenticación de usuario bidireccional, e iniciar un protocolo de autenticación entre tres elementos del mismo nivel entre el solicitante de acceso a la red, el controlador de acceso a la red y una unidad de servicio de autenticación de usuario en una capa de acceso a la red, de modo que se realice una autenticación de usuario bidireccional y un acuerdo de claves del solicitante de acceso y el controlador de acceso; y

(2.3) enviar, por parte del solicitante de acceso a la red y el controlador de acceso a la red, tras una autenticación de usuario bidireccional satisfactoria, información de éxito de autenticación de usuario al cliente TNC y al servidor TNC respectivamente, y controlar puntos del solicitante de acceso a la red y el controlador de acceso a la red según un resultado de autenticación de usuario;

(3.) etapa de evaluación de integridad:

usar, por parte del cliente TNC, el servidor TNC y una unidad de servicio de evaluación de plataforma en una capa de evaluación de integridad, un método de autenticación entre tres elementos del mismo nivel para realizar una evaluación de integridad de plataforma del solicitante de acceso y el controlador de acceso cuando el servidor TNC del controlador de acceso recibe la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red; y

(4.) etapa de control de acceso:

reunir, por parte del servidor TNC y el cliente TNC, resultados de la evaluación de integridad de plataforma del controlador de acceso y el solicitante de acceso respectivamente, y enviar recomendaciones al solicitante de acceso a la red y al controlador de acceso a la red respectivamente, y controlar, por parte del solicitante de acceso a la red y el controlador de acceso a la red, los puertos según las recomendaciones recibidas respectivamente, de modo que se realice un control de acceso mutuo del solicitante de acceso y el controlador de acceso.

Preferiblemente, la evaluación de integridad de plataforma puede realizarse tal como sigue:

realizar una autenticación de credenciales de plataforma: verificar, por parte de un gestor de políticas, la validez de certificados de clave de identidad de certificación, AIK, del solicitante de acceso y el controlador de acceso; y

realizar una verificación de integridad de plataforma: verificar, por parte del gestor de políticas, la integridad de plataforma del solicitante de acceso y el controlador de acceso.

Preferiblemente, la etapa de usar, por parte del cliente TNC, el servidor TNC y la unidad de servicio de evaluación de plataforma en la capa de evaluación de integridad, el método de autenticación entre tres elementos del mismo nivel para realizar la evaluación de integridad de plataforma del solicitante de acceso y el controlador de acceso, incluye:

(3.1) enviar, por parte del servidor TNC del controlador de acceso, al solicitante de acceso un número aleatorio N_S generado por un TPM del controlador de acceso, el certificado de AIK $Cert_{AC\text{-}AIK}$ del controlador de acceso y la lista de PCR $PCRList_{AR}$ que el controlador de acceso solicita al solicitante de acceso, tras la recepción de la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red o tras recibir confirmación de que la autenticación de usuario es satisfactoria;

(3.2) extraer, por parte del solicitante de acceso, tras la recepción de la información enviada en la etapa (3.1) por el controlador de acceso, valores de PCR correspondientes del TPM según la lista de PCR solicitada por el controlador de acceso; después, firmar los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con una clave privada de AIK en el TPM; y enviar, por parte del solicitante de acceso, al controlador de acceso, el número aleatorio N_S generado por el TPM del controlador de acceso, un número aleatorio N_{AR} generado por un TPM del solicitante de acceso, el certificado de AIK $Cert_{AR\text{-}AIK}$ del solicitante de acceso, la lista de PCR $PCRList_{AC}$ que el solicitante de acceso

solicita al controlador de acceso, valores de PCR PCR_{AR} solicitados por el controlador de acceso, un logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, y la firma generada por el solicitante de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con la clave privada de AIK en el TPM;

(3.3) verificar, por parte del TPM, tras recibir el controlador de acceso la información enviada en la etapa (3.2) por el solicitante de acceso, la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso, y verificar la validez de una firma de AIK del solicitante de acceso usando una clave pública en el certificado de AIK del solicitante de acceso; extraer valores de PCR correspondientes del TPM según la lista de PCR solicitada por el solicitante de acceso; firmar, por parte del controlador de acceso, los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso con una clave privada de AIK en el TPM; y enviar, por parte del controlador de acceso, a un gestor de políticas, el número aleatorio N_S generado por el TPM del controlador de acceso, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, los valores de PCR PCR_{AR} solicitados por el controlador de acceso, el logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, la firma generada por el solicitante de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con la clave privada de AIK en el TPM, un número aleatorio N_{AC} generado para un usuario del controlador de acceso, el certificado de AIK $Cert_{AC-AIK}$ del controlador de acceso, valores de PCR PCR_{AC} solicitados por el solicitante de acceso, un logaritmo de medición Log_{AC} que corresponde a los valores de PCR solicitados por el solicitante de acceso, y la firma generada por el controlador de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso con la clave privada de AIK en el TPM;

(3.4) verificar, por parte del gestor de políticas, tras la recepción de la información enviada en la etapa (3.3) por el controlador de acceso, la validez de las firmas de AIK y certificados de AIK del solicitante de acceso y el controlador de acceso usando claves públicas que corresponden a los certificados de AIK respectivos del solicitante de acceso y el controlador de acceso; recalcular valores de PCR correspondientes según los logaritmos de medición de los valores de PCR correspondientes extraídos de los TPM respectivos del solicitante de acceso y el controlador de acceso y valores de medición de integridad convencionales de componentes de plataforma respectivos en una base de datos, y compararlos con los valores de PCR correspondientes en la información enviada en la etapa (3.3) por el controlador de acceso; generar un resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso, $Result_{AIK-PCR}$, y firmar el resultado generado de autenticación de certificado de AIK y verificación de integridad de plataforma con una clave privada que corresponde a un certificado de identidad del gestor de políticas $[Result_{AIK-PCR}]_{Sig}$; y enviar, al controlador de acceso, el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso $Result_{AIK-PCR}$, y la firma $[Result_{AIK-PCRs}]_{Sig}$ firmada por el gestor de políticas del resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso;

(3.5) verificar, por parte del controlador de acceso, tras la recepción de la información enviada en la etapa (3.4) por el gestor de políticas, si un número aleatorio N_{AC} generado para el usuario del controlador de acceso concuerda con el número aleatorio N_{AC} enviado en la información en la etapa (3.4) por el gestor de políticas y generado para el usuario del controlador de acceso, y verificar la validez de una firma de usuario del gestor de políticas; verificar, por parte del TPM, la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso; y verificar la concordancia del certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso y los valores de PCR PCR_{AR} solicitados por el controlador de acceso; verificar el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK} y el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR}, y generar un resultado de evaluación de integridad de plataforma del solicitante de acceso; y enviar, por parte del controlador de acceso, al solicitante de acceso, la información enviada en la etapa (3.4) y la firma generada por el controlador de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso con la clave privada de AIK en el TPM; y

(3.6) verificar, por parte del solicitante de acceso, tras la recepción de la información enviada en la etapa (3.5) por el controlador de acceso, la validez de la firma de AIK del controlador de acceso y la firma de usuario del gestor de políticas; verificar, el TPM, la concordancia del número aleatorio N_{AR} generado por el TPM del solicitante de acceso; verificar la concordancia del certificado de AIK del controlador de acceso y los valores de PCR solicitados por el solicitante de acceso; y verificar el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK} y el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC}, y generar un resultado de evaluación de integridad de plataforma del solicitante de acceso.

Preferiblemente, el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso generado en la etapa (3.4) $Result_{AIK-PCR}$, incluye: el número aleatorio

N_{AC} generado para el usuario del controlador de acceso, el número aleatorio N_S generado por el TPM del controlador de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, los valores de PCR PCR_{AR} solicitados por el controlador de acceso, el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR}, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AC-AIK}$ del controlador de acceso, la lista de PCR, los valores de PCR PCR_{AC} solicitados por el solicitante de acceso, el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC}, el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK}, y el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK}.

Preferiblemente, las recomendaciones enviadas en la etapa (4.) por el servidor TNC y el cliente TNC al solicitante de acceso a la red y al controlador de acceso a la red pueden incluir información de permiso de acceso, información de prohibición de acceso o información de aislamiento y reparación.

Preferiblemente, en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.5), el controlador de acceso puede repetir las etapas (3.1) - (3.6) con el fin de intercambiar y verificar la información de integridad de nuevo con el solicitante de acceso.

Preferiblemente, en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.6), el solicitante de acceso puede repetir las etapas (3.2) a (3.6) para intercambiar y verificar información de integridad de nuevo con el controlador de acceso

Tal como puede observarse a partir de la solución técnica anterior, se realiza un acuerdo de claves entre el solicitante de acceso y el controlador de acceso, y se realiza directamente una protección de seguridad para los datos en el proceso de evaluación de integridad de plataforma y, para datos de servicio posteriores a la conexión de red fiable, no se requieren acuerdos de claves de sesión adicionales. Por tanto, puede simplificarse el proceso de acuerdo de claves y puede mejorarse la seguridad de la conexión de red fiable. La clave primaria generada para la autenticación no tiene que enviarse a través de la red, lo que garantiza la seguridad de la clave.

Además, la invención usa el método de autenticación entre tres elementos del mismo nivel, es decir, un método de autenticación bidireccional basado en una tercera parte, en la capa de evaluación de integridad para una autenticación centralizada y verificación de certificados de AIK e integridad de plataforma del solicitante de acceso y el controlador de acceso, mejorando de ese modo la seguridad del proceso de evaluación de integridad de plataforma y simplificar el mecanismo de verificación de integridad y gestión de claves de la arquitectura de conexión de red fiable.

Además, la invención usa el método de autenticación entre tres elementos del mismo nivel no sólo para la autenticación de usuario bidireccional en la capa de acceso a la red sino también para la evaluación de integridad de plataforma bidireccional en la capa de evaluación de integridad, lo que mejora la seguridad de toda la arquitectura de conexión de red fiable.

En la práctica, es posible que el gestor de políticas tenga que gestionar un gran número de controladores de acceso. La invención puede eliminar la necesidad de una fuerte asociación de seguridad entre el controlador de acceso y el gestor de políticas, mejorando de ese modo la capacidad de ampliación de la conexión de red fiable.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático de una transmisión de información completa para una conexión de red fiable en una arquitectura TCG-TNC existente;

la figura 2 es un diagrama esquemático de una transmisión de información completa para una conexión de red fiable en una arquitectura TNC según la invención; y

la figura 3 es un diagrama esquemático de un proceso de evaluación de integridad de plataforma en la arquitectura TNC según la invención.

A continuación se describen los símbolos de referencia:

N_S: número aleatorio generado por un TPM de un controlador de acceso; $Cert_{AC-AIK}$: certificado de AIK del controlador de acceso; $PCRList_{AR}$: lista de PCR que un controlador de acceso solicita al solicitante de acceso; N_{AR}: número aleatorio generado por un TPM del solicitante de acceso; $Cert_{AR-AIK}$: certificado de AIK del solicitante de acceso; PCR_{ListAC}: lista de PCR que el solicitante de acceso solicita al controlador de acceso; Log_{AR}: logaritmo de medición que corresponde a valores de PCR solicitados por el controlador de acceso; PCR_{AR}: los valores de PCR solicitados por el controlador de acceso; $[N_S, PCR_{AR}]_{Sig}$: firma por parte del solicitante de acceso que firma el número aleatorio N_S generado por el TPM del controlador de acceso y los valores de PCR correspondientes solicitados por el controlador de acceso; N_{AC}: número aleatorio generado para un usuario del controlador de acceso; Log_{AC}: logaritmo de medición que corresponde a valores de PCR solicitados por el solicitante de acceso; PCR_{AC}: los valores

de PCR solicitados por el solicitante de acceso; $[N_{AR}, PCR_{AC}]_{Sig:}$ firma por parte del controlador de acceso que firma el número aleatorio N_{AR} generado por el TPM del solicitante de acceso y los valores de PCR correspondientes solicitados por el solicitante de acceso; $Result_{AIK-PCR}$: resultado de autenticación de certificado de AIK y verificación de integridad del solicitante de acceso y el controlador de acceso; $[Result_{AIK-PCR}]_{Sig}$: firma por parte de un gestor de políticas que firma el resultado de autenticación de certificado de AIK y verificación de integridad del solicitante de acceso y el controlador de acceso; Re_{AC}: el resultado de verificación de integridad de plataforma del solicitante de acceso; Re_{AR}: el resultado de verificación de integridad de plataforma del controlador de acceso; Re_{AR-AIK}: el resultado de verificación de certificado de AIK del solicitante de acceso; y Re_{AC-AIK}: el resultado de verificación de certificación de AIK del controlador de acceso.

Descripción detallada de la invención

La invención consiste generalmente en una capa de acceso a la red, una capa de evaluación de integridad y una capa de medición de integridad. Un solicitante de acceso, un controlador de acceso y un gestor de políticas, que son las tres entidades lógicas de la invención, pueden estar distribuidos en cualquier lugar a través de una red. El solicitante de acceso también se denomina solicitante, estación de usuario, etc.; el controlador de acceso también se denomina controlador de acceso de autenticación, estación base, unidad de servicio de acceso, etc.; y el gestor de políticas también se denomina servidor de autenticación, servidor fiable, servidor de fondo, etc.

La capa de acceso a la red es responsable de realizar una autenticación de usuario bidireccional y un acuerdo de claves entre el solicitante de acceso y el controlador de acceso, y realizar un control de acceso mutuo del solicitante de acceso y el controlador de acceso según un resultado de autenticaciones de usuario de red y un resultado de evaluación de integridad de plataforma. La capa de acceso a la red puede usar un método de control de acceso basado en autenticación entre tres elementos del mismo nivel, que es la tecnología de control de acceso a la red ya definida en la norma WLAN china.

La capa de evaluación de integridad es responsable de realizar una evaluación de integridad de plataforma entre el solicitante de acceso y el controlador de acceso, incluyendo una autenticación de credenciales de plataforma y una verificación de integridad de plataforma. La autenticación entre tres elementos del mismo nivel, es decir, una autenticación bidireccional basada en una tercera parte, se realiza en la capa de evaluación de integridad entre el solicitante de acceso, el controlador de acceso y el gestor de políticas. El gestor de políticas verifica la validez de certificados de AIK del solicitante de acceso y el controlador de acceso y es responsable de verificar la integridad de plataforma del solicitante de acceso y el controlador de acceso.

La capa de medición de integridad es responsable de recopilar y verificar información relacionada con la integridad de plataforma del solicitante de acceso y el controlador de acceso.

La figura 2 ilustra un proceso de transmisión de información completa para una conexión de red fiable según la invención. Las etapas detalladas de implementación de la invención son tal como siguen:

(1.) Se realiza una inicialización. Se realizan las siguientes etapas antes del establecimiento de una conexión de red:

(1.1) Tanto un cliente TNC del solicitante de acceso como un servidor TNC del controlador de acceso preparan previamente información de integridad de plataforma, y la envían a recopiladores de medición de integridad, IMC, respectivos en la capa de medición de integridad.

(1.2) Tanto el cliente TNC como el servidor TNC establecen previamente un requisito de verificación de integridad, incluyendo una lista de PCR que el solicitante de acceso y el controlador de acceso se solicitan mutuamente para verificación.

(1.3) Los módulos de plataforma fiables, TPM, del solicitante de acceso y el controlador de acceso trocean información requerida para una política de red, y después la almacenan en registros de configuración de plataforma, PCR.

(2.) Se realiza una autenticación de usuario.

(2.1) Un solicitante de acceso a la red inicia una petición de acceso a un controlador de acceso a la red.

(2.2) Tras la recepción de la petición de acceso, el controlador de acceso a la red inicia un proceso de autenticación de usuario bidireccional e inicia un protocolo de autenticación entre tres elementos del mismo nivel, es decir, un protocolo de autenticación bidireccional basado en una tercera parte, entre el solicitante de acceso a la red, el controlador de acceso a la red y una unidad de servicio de autenticación de usuario en la capa de acceso a la red, de modo que se realice una autenticación de usuario bidireccional y un acuerdo de claves del solicitante de acceso y el controlador de acceso.

(2.3) Tras una autenticación de usuario bidireccional satisfactoria, el solicitante de acceso a la red y el

controlador de acceso a la red envían información de éxito de autenticación de usuario al cliente TNC y al servidor TNC respectivamente, y controlan puntos del solicitante de acceso a la red y el controlador de acceso a la red según el resultado de la autenticación de usuario, por lo que de ese modo pueden pasarse datos de un proceso de evaluación de integridad.

(3.) Se realiza una evaluación de integridad.

Cuando el servidor TNC del controlador de acceso recibe la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red, el cliente TNC, el servidor TNC y una unidad de servicio de evaluación de plataforma en la capa de evaluación de integridad usan un método de autenticación entre tres elementos del mismo nivel para realizar la evaluación de integridad de plataforma del solicitante de acceso y el controlador de acceso. En el proceso de evaluación de integridad de plataforma, el servidor TNC, el cliente TNC y la unidad de servicio de evaluación de plataforma realizan una interacción de información con recopiladores de medición de integridad y verificadores de medición de integridad en la capa superior. La evaluación de integridad de plataforma se realiza tal como sigue:

Se realiza una autenticación de credenciales de plataforma: el gestor de políticas verifica la validez de certificados de AIK del solicitante de acceso y el controlador de acceso; y

② Se realiza una verificación de integridad de plataforma: el gestor de políticas verifica la integridad de plataforma del solicitante de acceso y el controlador de acceso.

Haciendo referencia a la figura 3, una implementación detallada de una verificación de integridad de plataforma según la invención es tal como sigue:

(3.1) cuando el servidor TNC del controlador de acceso recibe la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red o recibe confirmación de que la autenticación de usuario es satisfactoria, se envían al solicitante de acceso un número aleatorio N_S generado por el TPM del controlador de acceso, el certificado de AIK $Cert_{AC\text{-}AIK}$ del controlador de acceso y la lista de PCR $PCRList_{AR}$ que el controlador de acceso solicita al solicitante de acceso.

(3.2) Tras la recepción de la información enviada en la etapa (3.1) por el controlador de acceso, el solicitante de acceso extrae en primer lugar valores de PCR correspondientes del TPM según la lista de PCR solicitados por el controlador de acceso, después firma con una clave privada de AIK en el TPM los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso. Finalmente, el solicitante de acceso envía al controlador de acceso el número aleatorio N_S generado por el TPM del controlador de acceso, un número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AR\text{-}AIK}$ del solicitante de acceso, la lista de PCR $PCRList_{AC}$ que el solicitante de acceso solicita al controlador de acceso, valores de PCR PCR_{AR} solicitados por el controlador de acceso, un logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, y la firma generada por el solicitante de acceso que firma con la clave privada de AIK en el TPM de los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso.

(3.3) Tras la recepción de la información enviada en la etapa (3.2) por el solicitante de acceso, el controlador de acceso hace en primer lugar que el TPM verifique la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso, y verifique la validez de una firma de AIK del solicitante de acceso con una clave pública en el certificado de AIK del solicitante de acceso; después, extrae valores de PCR correspondientes del TPM según la lista de PCR solicitada por el solicitante de acceso. Después, el controlador de acceso firma con una clave privada de AIK en el TPM los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso. Finalmente, el controlador de acceso envía al gestor de políticas el número aleatorio N_S generado por el TPM del controlador de acceso, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AR\text{-}AIK}$ del solicitante de acceso, los valores de PCR, PCR_{AR}, solicitados por el controlador de acceso, el logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, la firma generada por el solicitante de acceso con la clave privada de AIK en el TPM sobre los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso, un número aleatorio N_{AC} generado para un usuario del controlador de acceso, el certificado de AIK $Cert_{AC\text{-}AIK}$ del controlador de acceso, valores de PCR PCR_{AC} solicitados por el solicitante de acceso, un logaritmo de medición Log_{AC} que corresponde a los valores de PCR solicitados por el solicitante de acceso, y la firma generada a partir de la clave privada de AIK en el TPM por el controlador de acceso sobre los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso.

(3.4) Tras la recepción de la información enviada en la etapa (3.3) por el controlador de acceso, el gestor de políticas verifica en primer lugar la validez de las firmas de AIK y certificados de AIK del solicitante de acceso y el controlador de acceso con claves públicas que corresponden a los certificados de AIK respectivos del solicitante de acceso y el controlador de acceso. Después recalcula valores de PCR correspondientes según

logaritmos de medición de los valores de PCR correspondientes extraídos de los TPM respectivos del solicitante de acceso y el controlador de acceso y valores de medición de integridad convencionales de componentes de plataforma respectivos en una base de datos, y los compara con los valores de PCR correspondientes en la información enviada en la etapa (3.3) por el controlador de acceso. A continuación genera un resultado de autenticación de certificado de AIK y verificación de integridad de plataforma, $Result_{AIK-PCR}$, del solicitante de acceso y el controlador de acceso y firma $[Result_{AIK-PCR}]_{Sig}$ el resultado generado de autenticación de certificado de AIK y verificación de integridad de plataforma con una clave privada que corresponde a un certificado de identidad del gestor de políticas. Finalmente, envía al controlador de acceso el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma, $Result_{AIK-PCR}$, del solicitante de acceso y el controlador de acceso y la firma $[Result_{AIK-PCR}]_{Sig}$ realizada por el gestor de políticas sobre el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso.

Particularmente, el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma, $Result_{AIK-PCR}$, del solicitante de acceso y el controlador de acceso generado en la etapa (3.4) incluye: el número aleatorio N_{AC} generado para el usuario del controlador de acceso, el número aleatorio N_S generado por el TPM del controlador de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, los valores de PCR, PCR_{AR}, solicitados por el controlador de acceso, el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR}, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AC-AIK}$ del controlador de acceso, la lista de PCR, los valores de PCR, PCR_{AC}, solicitados por el solicitante de acceso, el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC}, el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK}, y el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK}.

(3.5) Tras la recepción de la información enviada en la etapa (3.4) por el gestor de políticas, el controlador de acceso verifica en primer lugar si un número aleatorio N_{AC} generado para el usuario del controlador de acceso concuerda con el número aleatorio N_{AC} generado para el usuario del controlador de acceso y enviado en la información en la etapa (3.4) por el gestor de políticas, y verifica la validez de una firma de usuario del gestor de políticas. A continuación hace que el TPM verifique la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso, y verifique la concordancia del certificado de AIK del solicitante de acceso $Cert_{AR-AIK}$ y los valores de PCR PCR_{AR}, solicitados por el controlador de acceso. Después verifica el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK} y el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR} y genera un resultado de evaluación de integridad de plataforma del solicitante de acceso. Finalmente, el controlador de acceso envía al solicitante de acceso la información enviada en la etapa (3.4) y la firma generada a partir de la clave privada de AIK en el TPM por el controlador de acceso sobre los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso.

Particularmente, en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.5), si el controlador de acceso no está satisfecho con el resultado, o, a petición de otra política de red, el controlador de acceso puede repetir las etapas (3.1) - (3.6) para intercambiar y verificar la información de integridad de nuevo con el solicitante de acceso, pudiendo usarse en caso de ser necesario el proceso de verificar la validez del certificado de AIK y procesos adicionales de verificación de integridad de plataforma realizados por el solicitante de acceso sobre el controlador de acceso.

(3.6) Tras la recepción de la información enviada en la etapa (3.5) por el controlador de acceso, el solicitante de acceso verifica en primer lugar la validez de una firma de AIK del controlador de acceso y la firma de usuario del gestor de políticas. Después, hace que el TPM verifique la concordancia del número aleatorio N_{AR} generado por el TPM del solicitante de acceso. A continuación verifica la concordancia del certificado de AIK del controlador de acceso y los valores de PCR solicitados por el solicitante de acceso. Finalmente, verifica el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK} y el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC} y genera un resultado de evaluación de integridad de plataforma del solicitante de acceso.

Particularmente, en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.6), si el solicitante de acceso no está satisfecho con el resultado, o, a petición de otra política de red, el solicitante de acceso puede repetir las etapas (3.2) - (3.6) para intercambiar y verificar información de integridad de nuevo con el controlador de acceso, pudiendo usarse en caso de ser necesario el proceso de verificar la validez el certificado de AIK y procesos adicionales de verificación de integridad de plataforma realizados por el controlador de acceso sobre el solicitante de acceso.

(4.) Se realiza un control de acceso.

El servidor TNC y el cliente TNC reúnen los resultados de la evaluación de integridad de plataforma del controlador de acceso y el solicitante de acceso respectivamente, y después envían recomendaciones al solicitante de acceso a la red y al controlador de acceso a la red respectivamente. Las recomendaciones enviadas por el servidor TNC y el

cliente TNC al solicitante de acceso a la red y al controlador de acceso a la red pueden incluir: información de permiso de acceso, información de prohibición de acceso, información de aislamiento y reparación, etc. El solicitante de acceso a la red y el controlador de acceso a la red controlan los puertos según las recomendaciones recibidas respectivamente, de modo que se realice control de acceso mutuo del solicitante de acceso y el controlador de acceso.

En las realizaciones anteriores de la invención, se realiza un acuerdo de claves entre el solicitante de acceso y el controlador de acceso, y se realiza directamente una protección de seguridad para los datos en el proceso de evaluación de integridad de plataforma y, para datos de servicio posteriores a la conexión de red fiable, no se requieren acuerdos de claves de sesión adicionales. Por tanto, puede simplificarse el proceso de acuerdo de claves y puede mejorarse la seguridad de la conexión de red fiable. La clave primaria generada para la autenticación no tiene que enviarse a través de la red, garantizándose de ese modo la seguridad de la clave.

Además, el método de autenticación entre tres elementos del mismo nivel, es decir, el método de autenticación bidireccional basado en una tercera parte, se usa en la capa de evaluación de integridad para una autenticación centralizada y verificación de los certificados de AIK respectivos e integridad de plataforma del solicitante de acceso y el controlador de acceso para mejorar de ese modo la seguridad del proceso de evaluación de integridad de plataforma y simplificar el mecanismo de verificación de integridad y gestión de claves de la arquitectura de conexión de red fiable.

Además, las realizaciones de la invención usan el método de autenticación entre tres elementos del mismo nivel no sólo para autenticación de usuario bidireccional en la capa de acceso a la red sino también para una evaluación de integridad de plataforma bidireccional en la capa de evaluación de integridad para mejorar de ese modo la seguridad de toda la arquitectura de conexión de red fiable.

Además, en la práctica, es posible que el gestor de políticas tenga que gestionar un gran número de controladores de acceso. Las realizaciones de la invención pueden eliminar la necesidad de una fuerte asociación de seguridad entre el controlador de acceso y el gestor de políticas para mejorar de ese modo la capacidad de ampliación de la conexión de red fiable.

Anteriormente se ha detallado el método de conexión de red fiable basado en autenticación entre tres elementos del mismo nivel según la invención. El principio y las realizaciones de la invención se han expuesto en el contexto a modo de ejemplos, y las descripciones anteriores de las realizaciones están previstas meramente para ayudar a entender la solución de la invención; y los expertos en la técnica puedan realizar variaciones en las realizaciones y ámbitos de aplicación sin apartarse del alcance de la invención, y la descripción en el presente documento no se tomará en ningún sentido como que limita el alcance de la invención.

REIVINDICACIONES

1. Método de conexión de red fiable, TNC, basado en autenticación entre tres elementos del mismo nivel, que comprende:

(1.) etapa de inicialización:

(1.1) preparar previamente, por parte de un cliente TNC de un solicitante de acceso y un servidor TNC de un controlador de acceso, información de integridad de plataforma, y enviar la información de integridad de plataforma a recopiladores de medición de integridad, IMC, respectivos en una capa de medición de integridad;

(1.2) establecer previamente, por parte del cliente TNC y el servidor TNC, un requisito de verificación de integridad que comprende una lista de registros de configuración de plataforma, PCR, que el solicitante de acceso y el controlador de acceso se solicitan mutuamente para verificación; y

(1.3) trocear, por parte de módulos de plataforma fiables, TPM, del solicitante de acceso y el controlador de acceso, información requerida para una política de red, y almacenarla en los PCR;

(2.) etapa de autenticación de usuario:

(2.1) iniciar, por parte de un solicitante de acceso a la red, una petición de acceso a un controlador de acceso a la red;

(2.2) iniciar, por parte del controlador de acceso a la red, tras la recepción de la petición de acceso, un proceso de autenticación de usuario bidireccional, e iniciar un protocolo de autenticación entre tres elementos del mismo nivel entre el solicitante de acceso a la red, el controlador de acceso a la red y una unidad de servicio de autenticación de usuario en una capa de acceso a la red, de modo que se realice una autenticación de usuario bidireccional y un acuerdo de claves del solicitante de acceso y el controlador de acceso; y

(2.3) enviar, por parte del solicitante de acceso a la red y el controlador de acceso a la red, tras una autenticación de usuario bidireccional satisfactoria, información de éxito de autenticación de usuario al cliente TNC y al servidor TNC respectivamente, y controlar puntos del solicitante de acceso a la red y el controlador de acceso a la red según un resultado de autenticación de usuario;

(3.) etapa de evaluación de integridad:

usar, por parte del cliente TNC, el servidor TNC y una unidad de servicio de evaluación de plataforma en una capa de evaluación de integridad, un método de autenticación entre tres elementos del mismo nivel para realizar una evaluación de integridad de plataforma del solicitante de acceso y el controlador de acceso cuando el servidor TNC del controlador de acceso recibe la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red; y

(4.) etapa de control de acceso:

reunir, por parte del servidor TNC y el cliente TNC, los resultados de la evaluación de integridad de plataforma del controlador de acceso y el solicitante de acceso respectivamente, y enviar recomendaciones al solicitante de acceso a la red y al controlador de acceso a la red respectivamente, y controlar, por parte del solicitante de acceso a la red y el controlador de acceso a la red, los puertos según las recomendaciones recibidas respectivamente, de modo que se realice un control de acceso mutuo del solicitante de acceso y el controlador de acceso.

2. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 1, en el que la evaluación de integridad de plataforma comprende: verificar, por parte de un gestor de políticas, la validez de un certificado de AIK y la integridad de plataforma del solicitante de acceso y el controlador de acceso.

3. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 1, en el que la etapa de usar, por parte del cliente TNC, el servidor TNC y la unidad de servicio de evaluación de plataforma en la capa de evaluación de integridad, el método de autenticación entre tres elementos del mismo nivel para realizar la evaluación de integridad de plataforma del solicitante de acceso y el controlador de acceso comprende:

(3.1) enviar, por parte del servidor TNC del controlador de acceso, al solicitante de acceso un número aleatorio N_S generado por un TPM del controlador de acceso, el certificado de AIK $Cert_{AC\text{-}AIK}$ del

controlador de acceso y la lista de PCR $PCRList_{AR}$ que el controlador de acceso solicita al solicitante de acceso, tras la recepción de la información de éxito de autenticación de usuario enviada por el controlador de acceso a la red o tras recibir confirmación de que la autenticación de usuario es satisfactoria;

(3.2) extraer, por parte del solicitante de acceso, tras la recepción de la información enviada en la etapa (3.1) por el controlador de acceso, valores de PCR correspondientes del TPM según la lista de PCR solicitada por el controlador de acceso; después, firmar los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con una clave privada de AIK en el TPM; y enviar, por parte del solicitante de acceso, al controlador de acceso, el número aleatorio N_S generado por el TPM del controlador de acceso, un número aleatorio N_{AR} generado por un TPM del solicitante de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, la lista de PCR $PCRList_{AC}$ que el solicitante de acceso solicita al controlador de acceso, valores de PCR PCR_{AR} solicitados por el controlador de acceso, un logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, y la firma generada por el solicitante de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con la clave privada de AIK en el TPM;

(3.3) verificar, por parte del TPM, tras recibir el controlador de acceso la información enviada en la etapa (3.2) por el solicitante de acceso, la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso, y verificar la validez de una firma de AIK del solicitante de acceso usando una clave pública en el certificado de AIK del solicitante de acceso; extraer valores de PCR correspondientes del TPM según la lista de PCR solicitada por el solicitante de acceso; firmar, por parte del controlador de acceso, los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso con una clave privada de AIK en el TPM; y enviar, por parte del controlador de acceso, a un gestor de políticas, el número aleatorio N_S generado por el TPM del controlador de acceso, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, los valores de PCR PCR_{AR} solicitados por el controlador de acceso, el logaritmo de medición Log_{AR} que corresponde a los valores de PCR solicitados por el controlador de acceso, la firma generada por el solicitante de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_S generado por el TPM del controlador de acceso con la clave privada de AIK en el TPM, un número aleatorio N_{AC} generado para un usuario del controlador de acceso, el certificado de AIK $Cert_{AC-AIK}$ del controlador de acceso, valores de PCR PCR_{AC} solicitados por el solicitante de acceso, un logaritmo de medición Log_{AC} que corresponde a los valores de PCR solicitados por el solicitante de acceso, y la firma generada por el controlador de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número aleatorio N_{AR} generado por el TPM del solicitante de acceso con la clave privada de AIK en el TPM;

(3.4) verificar, por parte del gestor de políticas, tras la recepción de la información enviada en la etapa (3.3) por el controlador de acceso, la validez de las firmas de AIK y certificados de AIK del solicitante de acceso y el controlador de acceso usando claves públicas que corresponden a los certificados de AIK respectivos del solicitante de acceso y el controlador de acceso; recalcular valores de PCR correspondientes según los logaritmos de medición de los valores de PCR correspondientes extraídos de los TPM respectivos del solicitante de acceso y el controlador de acceso y valores de medición de integridad convencionales de componentes de plataforma respectivos en una base de datos, y compararlos con los valores de PCR correspondientes en la información enviada en la etapa (3.3) por el controlador de acceso; generar un resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso, $Result_{AIK-PCR}$, y firmar el resultado generado de autenticación de certificado de AIK y verificación de integridad de plataforma con una clave privada que corresponde a un certificado de identidad del gestor de políticas $[Result_{AIK-PCR}]_{Sig}$; y enviar, al controlador de acceso, el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso $Result_{AIK-PCR}$, y la firma $[Result_{AIK-PCR}]_{Sig}$ firmada por el gestor de políticas del resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso;

(3.5) verificar, por parte del controlador de acceso, tras la recepción de la información enviada en la etapa (3.4) por el gestor de políticas, si un número aleatorio N_{AC} generado para el usuario del controlador de acceso concuerda con el número aleatorio N_{AC} enviado en la información en la etapa (3.4) por el gestor de políticas y generado para el usuario del controlador de acceso, y verificar la validez de una firma de usuario del gestor de políticas; verificar, por parte del TPM, la concordancia del número aleatorio N_S generado por el TPM del controlador de acceso; y verificar la concordancia del certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso y los valores de PCR PCR_{AR} solicitados por el controlador de acceso; verificar el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK} y el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR} ,y generar un resultado de evaluación de integridad de plataforma del solicitante de acceso; y enviar, por parte del controlador de acceso, al solicitante de acceso, la información enviada en la etapa (3.4) y la firma generada por el controlador de acceso que firma los valores de PCR correspondientes extraídos del TPM y el número

aleatorio N_{AR} generado por el TPM del solicitante de acceso con la clave privada de AIK en el TPM; y

(3.6) verificar, por parte del solicitante de acceso, tras la recepción de la información enviada en la etapa (3.5) por el controlador de acceso, la validez de la firma de AIK del controlador de acceso y la firma de usuario del gestor de políticas; verificar, el TPM, la concordancia del número aleatorio N_{AR} generado por el TPM del solicitante de acceso; verificar la concordancia del certificado de AIK del controlador de acceso y los valores de PCR solicitados por el solicitante de acceso; y verificar el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK} y el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC}, y generar un resultado de evaluación de integridad de plataforma del solicitante de acceso.

4. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 3, en el que el resultado de autenticación de certificado de AIK y verificación de integridad de plataforma del solicitante de acceso y el controlador de acceso generado en la etapa (3.4) $Result_{AIK-PCR}$ comprende: el número aleatorio N_{AC} generado para el usuario del controlador de acceso, el número aleatorio N_S generado por el TPM del controlador de acceso, el certificado de AIK $Cert_{AR-AIK}$ del solicitante de acceso, los valores de PCR PCR_{AR} solicitados por el controlador de acceso, el resultado de verificación de integridad de plataforma del solicitante de acceso Re_{AR}, el número aleatorio N_{AR} generado por el TPM del solicitante de acceso, el certificado de AIK $Cert_{AC-AIK}$ del controlador de acceso, la lista de PCR, los valores de PCR PCR_{AC} solicitados por el solicitante de acceso, el resultado de verificación de integridad de plataforma del controlador de acceso Re_{AC}, el resultado de verificación de certificado de AIK del solicitante de acceso Re_{AR-AIK}, y el resultado de verificación de certificado de AIK del controlador de acceso Re_{AC-AIK}.

5. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 1, 2, 3 ó 4, en el que las recomendaciones enviadas en la etapa (4.) por el servidor TNC y el cliente TNC al solicitante de acceso a la red y al controlador de acceso a la red comprenden información de permiso de acceso, información de prohibición de acceso o información de aislamiento y reparación.

6. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 5, en el que en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.5), las etapas (3.1) a (3.6) se repiten si el controlador de acceso debe intercambiar información de integridad de nuevo con el solicitante de acceso y verificar la información de integridad.

7. Método TNC basado en autenticación entre tres elementos del mismo nivel según la reivindicación 6, en el que en el proceso de generar el resultado de evaluación de integridad de plataforma del solicitante de acceso en la etapa (3.6), las etapas (3.2) a (3.6) se repiten si el solicitante de acceso debe intercambiar información de integridad de nuevo con el controlador de acceso y verificar la información de integridad.

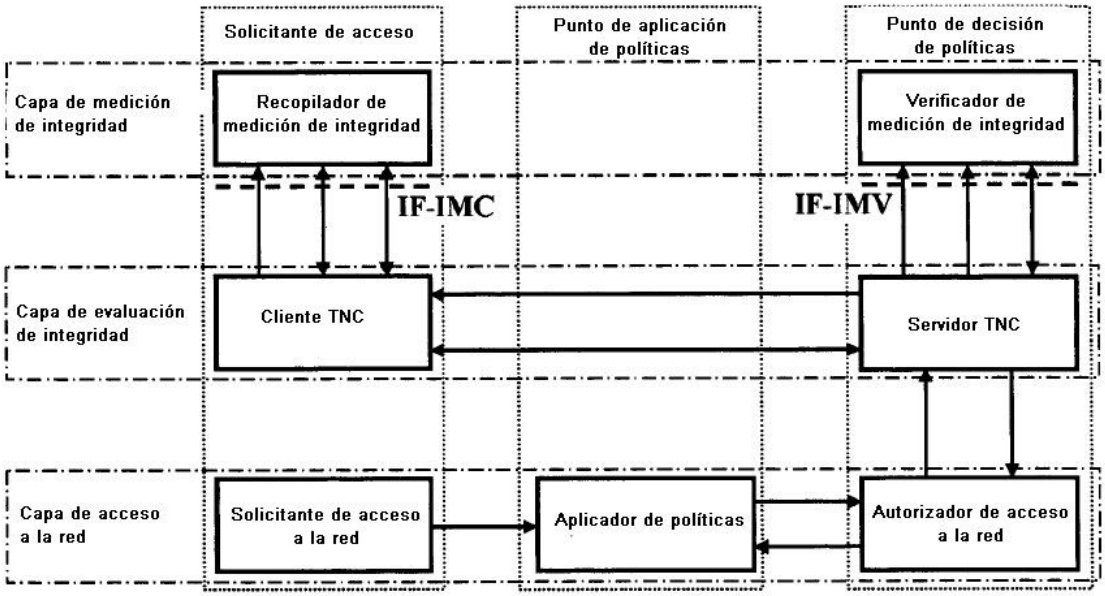
Solicitante de acceso
Punto de aplicación de políticas
Punto de decisión de políticas
Capa de medición de integridad
Recopilador de medición de integridad
Verificador de medición de integridad
IF-IMC
IF-IMV
Capa de evaluación de integridad
Cliente TNC
Servidor TNC
Capa de acceso a la red
Solicitante de acceso a la red
Aplicador de políticas
Autorizador de acceso a la red

FIG. 1

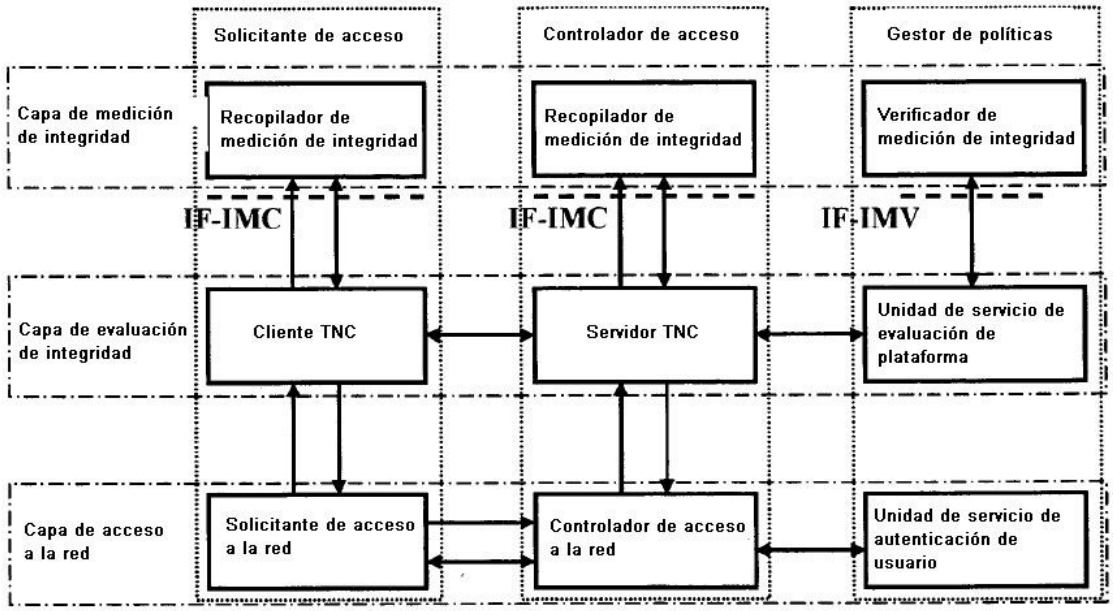
Solicitante de acceso
Controlador de acceso
Gestor de políticas
Capa de medición de integridad
Recopilador de medición de integridad
Recopilador de medición de integridad
Verificador de medición de integridad
IF-IMC
IF-IMC
IF-IMV
Capa de evaluación de integridad
Cliente TNC
Servidor TNC
Unidad de servicio de evaluación de plataforma
Capa de acceso a la red
Solicitante de acceso a la red
Controlador de acceso a la red
Unidad de servicio de autenticación de usuario

FIG. 2

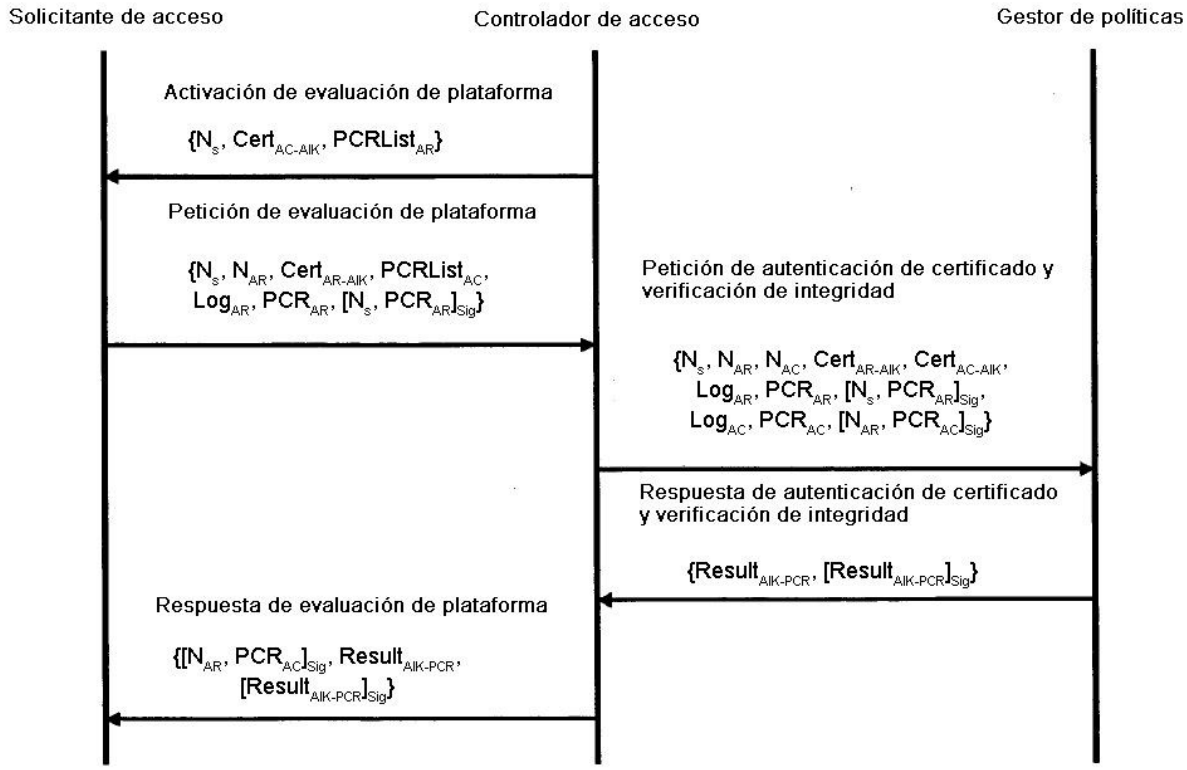
Solicitante de acceso
Controlador de acceso
Gestor de políticas
Activación de evaluación de plataforma
{Ns, Cert AC-AIK, PCRList AR}
Petición de evaluación de plataforma
{Ns, NAR, Cert AR-AIK, PCRList AC,
Log AR, PCR AR, [Ns, PCR AR]Sig}
Petición de autenticación de certificado y verificación de integridad
{Ns, NAR, NAC, Cert AR-AIK, Cert AC-AIK,
Log AR, PCR AR, [Ns, PCR AR]Sig,
Log AC, PCR AC, [NAR, PCR AC]Sig}
Respuesta de autenticación de certificado y verificación de integridad
{Result AIK-PCR, [Result AIK-PCR]Sig}
Respuesta de evaluación de plataforma
{[NAR, PCR AC]Sig, Result AIK-PCR,
[Result AIK-PCR]Sig}

FIG. 3