(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 725**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/72 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.12.2013 E 13199619 (1)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 2750354**

(54) Título: **Procedimiento de definición de un módulo de filtrado, módulo de filtrado asociado**

(30) Prioridad:

28.12.2012 FR 1203622

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.12.2019

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

GUREGHIAN, EMMANUEL TIGRANE;
DUPUTZ, PATRICK y
GRISAL, OLIVIER

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de definición de un módulo de filtrado, módulo de filtrado asociado

[0001] La presente invención se refiere al campo de la seguridad de los sistemas de información. Se refiere, más específicamente, a la definición de un módulo de filtrado adaptado para filtrar información según una política de seguridad determinada, entre un primer módulo propio para tratar información de un primer nivel de sensibilidad, y un segundo módulo propio para tratar información de un segundo nivel de sensibilidad, estando dichos primer y segundo módulos conectados, en paralelo con el módulo de filtrado, por un módulo criptográfico adaptado para aplicar funciones criptográficas.

[0002] Tales módulos de filtrados forman en concreto parte de sistemas que presentan una arquitectura que comprende módulos de niveles de sensibilidad distintos y un módulo criptográfico. En tales sistemas, se encuentran, en concreto, los equipos criptográficos, tales como encriptadores.

[0003] Estos campos de nivel de sensibilidad distintos son, por ejemplo, denominados módulo rojo y módulo negro. El módulo rojo trata y almacena, por ejemplo, información sensible, expresada en rojo, en claro. El módulo negro trata y almacena, por ejemplo, información menos sensible que la información roja. Esta información menos sensible, expresada en negra, es o bien la información en claro, intrínsecamente menos sensible que la información roja, o bien información roja cifrada, intrínsecamente sensible pero insensibilizada por cifrado.

[0004] El módulo rojo trata e incluye, además, información negra.

[0005] Habitualmente, la información que no es identificable ni como información roja, ni como información negra, se considera como información roja por defecto, en el módulo rojo.

[0006] Habitualmente, la información que no es identificable ni como información roja, ni como información negra, se considera como información negra por defecto, en el módulo negro.

[0007] El módulo criptográfico implementa las funciones criptográficas necesarias para el cifrado de la información roja. Se ubica en la desconexión entre los módulos rojo y negro. Los sistemas criptográficos comprenden también dos interfaces externas: una primera interfaz o interfaz de usuario o interfaz de red privada, conectada al módulo rojo, y una segunda interfaz o interfaz de red pública por cable o radio, conectada al módulo negro.

[0008] El sistema criptográfico comprende, en concreto, un modo "código" propio para el tratamiento de información sensible.

[0009] En el modo "código":

- la información roja, que se introduce en la interfaz de usuario, se encriptan por el bloque criptográfico y sale ensuciada en la interfaz de red pública por cable o radio del módulo negro.

- la información que se introduce en la interfaz de red pública por cable es descifrada por el bloque criptográfico y sale, en claro, en la interfaz de usuario del módulo rojo.

[0010] El módulo de filtrado está también dispuesto entre el módulo rojo y el módulo negro.

[0011] El módulo de filtrado aplica una política de seguridad, que define el conjunto de información negra autorizada para atravesarlo, del módulo rojo al módulo negro, y del módulo negro al módulo rojo.

[0012] Por ejemplo, la información negra, tratada por el módulo rojo y con destino al módulo negro, se transmite en claro a través del módulo de filtrado. Este último asegura que solo la información negra sea trasmitida al módulo negro. La información roja es bloqueada por el módulo de filtrado que disminuye así el riesgo de compromiso de esta información en la red por cable o radio.

[0013] El comportamiento de tal módulo de filtrado es con mayor frecuencia congelado en el tiempo, ya que se implementa en forma de hardware y/o en forma de un programa de software dedicado. Por tanto, es difícil y costoso modificar y adaptar el comportamiento del módulo de filtrado. El procedimiento de fabricación de nuevos módulos de filtrado resulta igualmente difícil y costoso.

[0014] Además, las llamadas al módulo de filtrado son realizadas directamente por las aplicaciones del módulo rojo (respectivamente del módulo negro) y, por lo tanto, la política de seguridad realmente aplicada no es explícita, pero es implícitamente definida por las invocaciones del filtro efectuadas por las aplicaciones del módulo rojo (respectivamente negro).

[0015] El documento "Policy-based management: bringing the gap", Proceedings/15th annual computer security applications conference, 6-10 diciembre de 1999, describe una técnica de traducción de reglas generales para las configuraciones de firewalls por ejemplo, por medio de un compilador.

[0016] El documento US 2008/101222 A1 describe un filtrado de paquetes basado en las reglas que usan t-uplas de tamaño variable y que almacenan parámetros que definen las reglas.

[0017] El documento US 2012/036581 A1 describe un módulo de seguridad colocado entre un módulo de tratamiento de datos de nivel de seguridad A y un módulo de tratamiento de datos de nivel de seguridad B, estando este módulo de seguridad adaptado para filtrar los datos entre los dos módulos.

[0018] El documento "Handlung stateful Firewall Anomalies" de F. Cuppens, N Cuppens-Boulahia, J. Garcia-Alfaro, T. Moataz y X. Rimasson", describe un procedimiento de validación de la coherencia de las reglas de filtrado de un cortafuegos con estado.

[0019] La presente invención tiene por objeto proponer una solución a estas limitaciones.

[0020] La presente invención se define en las reivindicaciones 1 y 8, respectivamente. Los modos de realizaciones particulares se definen en las reivindicaciones dependientes.

[0021] Según un primer aspecto, la invención propone un procedimiento de definición de un módulo de filtrado del tipo mencionado anteriormente, caracterizado porque comprende las etapas según las cuales:

- un conjunto de reglas de filtrado es definido, al traducir la política de seguridad determinada, en un idioma apto para ser compilado, definiendo dichas reglas de filtrado las propiedades de información cuya transmisión es autorizada por el módulo de filtrado entre el primer y el segundo módulos;

- un tratamiento de validación del conjunto de reglas definido es llevado a cabo, validando que una autorización o un rechazo de transmisión ha sido de hecho proporcionado por aplicación de dicho conjunto de reglas a cualquier información susceptible de ser proporcionada en la entrada del módulo de filtrado;

- dicho conjunto de reglas definido es compilado;

- dicho conjunto de reglas compilado se integra en una base de reglas del módulo de filtrado.

[0022] Tal procedimiento disminuye los costos y los esfuerzos de trabajo necesarios para la definición iterativa de un módulo de filtrado y para su modificación, tanto en la fase de su concepción como en una fase de mantenimiento durante su funcionamiento operativo. Tal procedimiento también reduce el riesgo de error de concepción del módulo de filtrado, y permite, de este modo, minimizar el riesgo de vulnerabilidades de seguridad. Permite además disminuir la complejidad y la carga de cálculo necesarios para las modificaciones, tanto correctivas como evolutivas, de un módulo de filtrado.

[0023] En unos modos de realización, el procedimiento de definición de un módulo de filtrado según la invención comporta además una o varias de las características siguientes:

- el conjunto de reglas de filtrado define propiedades estáticas, temporales y dinámicas de la información autorizada a transmitirse;

- el conjunto de reglas de filtrado incluye al menos un autómata protocolario, definido por un conjunto de estados correspondientes a las etapas sucesivas de implementación de un protocolo de comunicación, y de eventos que provocan las transiciones entre dichos estados;

- el módulo de filtrado incluye un módulo de tratamiento apto para ejecutar el conjunto de reglas integrado en la base de datos de reglas tras la recepción de información a filtrar y apto para autorizar o rechazar la transmisión por el módulo de filtrado de dicha información entre los primer y segundo módulos según un rechazo o una autorización proporcionada después de la ejecución de dicho conjunto de reglas;

- variables de estado asociadas con las reglas de filtrados son definidas, y un rechazo o autorización se proporciona tras la ejecución de dicho conjunto de reglas como una función de valores actuales calculados para dichos valores de variables de estado;

- el tratamiento de validación del conjunto de reglas definido comprende además una etapa de validación de la coherencia de las reglas del conjunto de reglas;

- la etapa de validación de la coherencia de las reglas comprende la detección de al menos una anomalía entre:

- la existencia en el conjunto de reglas de una primera y segunda reglas asociadas con acciones diferentes, siendo la primera regla aplicada en todos los objetos de la segunda;

- la existencia en el conjunto de reglas de dos reglas asociadas con acciones diferentes, y cada una de entre ellas se aplica en un subconjunto de objetos en la que se aplica la otra.

- la existencia de dos reglas que ejecutan la misma acción sobre los mismos objetos,

- el conjunto de reglas se define según una estructura de árbol de reglas;

- el módulo de filtrado se define de manera que la información del primer módulo cuya transmisión es autorizada por el módulo de filtrado sea transmitida al segundo módulo en claro;

- la orden de aplicación y la composición lógica de los resultados de las reglas se define por el conjunto de reglas de filtrado.

[0024] Según un segundo aspecto, la presente invención propone un módulo de filtrado adaptado para filtrar información según una política de seguridad entre un primer módulo propio para tratar información sensible, y un segundo módulo propio para tratar información no sensible, estando dichos primer y segundo módulos conectados, en paralelo con el módulo de filtrado, por un módulo criptográfico adaptado para aplicar funciones criptográficas, estando dicho módulo de filtrado caracterizado porque comprende un módulo de tratamiento y una base de datos de reglas que incluye un conjunto de reglas que define la política de seguridad determinada, en un idioma compilado, definiendo dichas reglas de filtrado las propiedades de información cuya transmisión es autorizada por el módulo de filtrado entre el primer y el segundo módulos.

[0025] Según un tercer aspecto, la presente invención propone un equipo criptográfico que incluye:

- un primer módulo propio para tratar información de un primer nivel de sensibilidad;

- un segundo módulo propio para tratar información de un segundo nivel de sensibilidad distinto del primer nivel de sensibilidad;

- un módulo criptográfico adaptado para aplicar funciones criptográficas, que conecta dichos primer y segundo módulos;

- un módulo de filtrado, adaptado para filtrar información según una política de seguridad entre el primer módulo y el segundo módulo.

[0026] Estas características y ventajas de la invención se mostrarán con la lectura de la descripción que aparece a continuación, y realizada en referencia a los dibujos anexos, en los cuales:

- la figura 1 representa un sistema criptográfico en un modo de realización de la invención;

- la figura 2 define un diagrama funcional de etapas de un procedimiento de definición de un módulo de filtrado en un modo de realización de la invención.

[0027] En un modo de realización de la invención, se considera un sistema criptográfico, ilustrado en la figura 1. En el ejemplo considerado, el sistema criptográfico es un equipo criptográfico 1 del tipo encriptador.

[0028] Este equipo se caracteriza por una arquitectura de seguridad que incluye cuatro módulos principales: un módulo 2 que trata información sensible, denominado también módulo rojo, un módulo 3 que trata información no sensible, denominado módulo negro, un módulo criptográfico 4 y un módulo de filtrado 5.

[0029] En un modo de realización, el módulo rojo detecta un primer nivel de seguridad, y el módulo negro detecta un segundo nivel de seguridad, que por ejemplo es inferior al primer nivel.

[0030] El módulo 2 rojo y el módulo 3 negro están cada uno conectados, por una parte, al módulo criptográfico 4 y, por otra parte, al módulo de filtrado 5.

[0031] El módulo rojo 2 es propio para tratar, en concreto, usando aplicaciones 6, mensajes 7 sensibles en claro.

[0032] El módulo negro 3 es propio para tratar, en concreto, usando aplicaciones 9, solamente mensajes no sensibles 10, es decir, sin comprometer la seguridad en caso de divulgación. Esta información es o bien información

en claro, intrínsecamente no sensible, o bien información encriptada, intrínsecamente sensible pero convertida en no sensible por cifrado.

[0033] El equipo criptográfico 1 es propio además para asegurar el descifrado de los mensajes que transitan del módulo negro 3 al módulo rojo 2, al proporcionar estos mensajes al módulo criptográfico 4, que por ejemplo, implementa algoritmos y claves criptográficas para descifrar estos mensajes.

[0034] El equipo criptográfico 1 está adaptado además para permitir la transmisión de mensajes desde el módulo negro 3 al módulo rojo 2 sin realizar descifrado, al proporcionar estos mensajes al módulo de filtrado 5 y con la condición de que estos mensajes sean juzgados, por el módulo de filtrado 5, como que no afecten a la seguridad del módulo rojo y que su transmisión en claro sea indispensable para el funcionamiento nominal del equipo criptográfico 1, por ejemplo la información sobre planos de control y gestión (señalización, encaminamiento...). En particular, los mensajes no integrados (por ejemplo, no fieles y/o no auténticos, en concreto, ciertos mensajes mal formados, son detectados y luego rechazados.

[0035] El equipo criptográfico 1 está adaptado para asegurar el cifrado de los mensajes sensibles a transmitir del módulo rojo 2 al módulo negro 3, al proporcionar estos mensajes sensibles al módulo criptográfico 4, que por ejemplo, implementa algoritmos y claves criptográficas para cifrar estos mensajes.

[0036] El equipo criptográfico 1 está adaptado además para permitir la transmisión en claro de mensajes desde el módulo rojo 2 al módulo negro 3, al proporcionar estos mensajes al módulo de filtrado 5 y con la condición de que estos mensajes sean juzgados, por el módulo de filtrado 5, no sensibles que su transmisión en claro sea indispensable para el funcionamiento nominal del equipo criptográfico 1, por ejemplo la información sobre planos de control y gestión (señalización, encaminamiento...).

[0037] El módulo de filtrado 5 está adaptado para determinar si un mensaje del módulo rojo 2 que recibe como entrada, puede transmitirse en claro al módulo negro 3. En el caso en que se haya determinado que el mensaje podría transmitirse al módulo negro 3, el módulo de filtrado 5 lo transmite a continuación al módulo negro 3.

[0038] De manera similar, el módulo de filtrado 5 está adaptado para determinar si un mensaje del módulo negro 3 que recibe como entrada, puede transmitirse en claro al módulo rojo 2. En el caso en que se haya determinado que el mensaje podría transmitirse al módulo rojo 2, el módulo de filtrado 5 lo transmite a continuación al módulo rojo 2.

[0039] En el modo de realización considerado, el módulo de filtrado 5 incluye un módulo de tratamiento 14, un base de datos de reglas 15 invariante que define la política de seguridad seleccionada, y un bloque de variables de estados 16 que incluye valores actuales de variables de estados asociados a las reglas.

[0040] Las recomendaciones de seguridad vigentes en la arquitectura de los equipos criptográficos abogan claramente por recortar el módulo criptográfico 4 y el módulo de filtrado 5 del resto del equipo.

[0041] Con el fin de obtener una aprobación que autorice el despliegue del equipo criptográfico 1 en una infraestructura cliente, una evaluación de seguridad se lleva a cabo para verificar la conformidad del equipo criptográfico 1 con respecto a las normas y recomendaciones de seguridad.

Procedimiento de fabricación de un módulo de filtrado

[0042] Según un primer aspecto, la invención propone un procedimiento de fabricación 100 de un módulo de filtrado similar al módulo de filtrado 5 del equipo criptográfico 1.

[0043] Tal procedimiento permite elaborar una política de seguridad en una forma que puede ser aplicable por un módulo de filtrado.

[0044] Este procedimiento 100 incluye varias etapas a fin de generar una base de datos de reglas 15, a partir de una política de seguridad determinada.

[0045] En una primera etapa 101, la política de seguridad a aplicar por el módulo de filtrado 5 es descrita, por la definición de un conjunto de reglas de filtrado.

[0046] En el modo de realización considerado, una o más reglas de filtrados se definen usando uno o más autómatas protocolarios.

[0047] Estas reglas de filtrado, comprendiendo los autómatas protocolarios, se definen en un idioma de descripción flexible, determinista y legible.

[0048] En un modo de realización, la descripción de la política de seguridad adopta la forma de un árbol, con un elemento de tipo raíz (por ejemplo: el elemento "POLÍTICA"), que incluye uno o más elementos hijo de tipo nodo intermedio, algunos de los cuales a su vez, incluyen uno o más elemento hijo de tipo nodo intermedio (por ejemplo: el elemento de tipo nodo intermedio "CAMPO" define una propiedad del mensaje en el que se pueden aplicar reglas de filtrado), hasta alcanzar elementos de tipo terminal (por ejemplo: los elementos de tipo terminal "FRECUENCIA" y "VELOCIDAD" constituyen reglas de filtrado, que estipulan los valores de frecuencia o velocidad que permite el paso del mensaje o que impone el rechazo del mensaje), que no tienen elementos hijo.

[0049] En un modo de realización, se definen dos categorías de elementos de política de seguridad:

- los elementos evaluables de tipo "regla de filtrado", que definen una condición de paso del mensaje. Esta condición permite verificar el mensaje como una función de una propiedad estática (formato del mensaje, sentido de paso del mensaje, valor de los campos de información del mensaje), temporal (frecuencia de paso del mensaje, velocidad binaria generada por un campo información) o dinámica (autómata protocolario) dada.

- los elementos descriptivos (por ejemplo "AUTÓMATA" y "ESTADO", "TRANSICIÓN"), que definen un autómata protocolario. Un autómata protocolario se caracteriza por un conjunto de estados, un conjunto de transiciones entre estados, y un estado inicial. Cada estado del autómata protocolario indica una fase particular en una secuencia predeterminada de mensajes, intercambiados de manera sucesiva entre los módulos rojo y negro, según un protocolo de comunicación dado. Tal autómata protocolario permite, por ejemplo, controlar que el paso de un mensaje de tipo "SIP REPLY", siga el paso de un mensaje de tipo "SIP REQUEST".

[0050] En un modo de realización, los elementos de política de seguridad de tipo "regla de filtrado" son evaluables (individualmente), y devuelven un resultado de tipo booleano:

- Verdadero o "A TRANSMITIR",

- Falso o "NO TRANSMITIR".

[0051] Además, los elementos de política de seguridad de tipo "regla de filtrado" definen la orden de evaluación de sus reglas hija, y la composición lógica de sus resultados booleanos, por ejemplo:

- Evaluación de esta regla (Y) Evaluación de la regla hija n.º 1 (Y) Evaluación de la regla hija n.º 2 (Y)... Evaluación de la regla hija n.º N

- Evaluación de esta regla (O) Evaluación de la regla hija n.º 1 (O) Evaluación de la regla hija n.º 2 (O)... Evaluación de la regla hija n.º N.

[0052] Las reglas de filtrado dependen de las variables de estado 16. Por ejemplo, una variable de estado representa una velocidad, un número de un cierto tipo de mensajes recibidos por el módulo de filtrado, o el momento de recepción del último mensaje recibido de un tipo dado etc.

[0053] La evaluación de un elemento de la política de seguridad, de tipo regla de filtrado, puede causar la modificación de variables de estados 16 asociados a la política de seguridad. Esta modificación es eficaz, si el mensaje es totalmente coherente con la política de seguridad aplicada por el módulo de filtrado 5 (es decir que todas las reglas de filtrado evaluadas han devuelto VERDADERO o "A TRANSMITIR").

[0054] Un elemento, de tipo regla de filtrado, puede asociarse a un autómata protocolario, de tal manera que la recepción de un mensaje dado provoca una transición de estados dada, de un autómata protocolario. La evaluación de tal elemento provoca la modificación de al menos una variable de estado que contiene el estado actual de este autómata protocolario.

[0055] A modo de ejemplo, un autómata protocolario simple, compuesto de dos estados {"Idle", "Running"} y controlado por dos eventos "Start" y "Stop" tales que la aparición del evento "Start" cuando se encuentra en el estado "Idle" le hace pasar al estado "Running", y que la aparición del evento "Stop" cuando se encuentra en el estado "Running" le hace pasar al estado "Idle".

[0056] Una regla es definida por el conjunto de objetos a los que se aplica (generalmente mensajes que verifican la condición definida por la regla, normalmente propiedades de mensaje tales como un sentido de paso, un valor de campo, una frecuencia, etc.), y por las acciones asociadas que aplica a estos objetos.

[0057] Estas acciones son por ejemplo la provisión de un resultado "A TRANSMITIR" o "NO TRANSMITIR", y la modificación de posibles variables de estado asociadas con la regla.

[0058] La o las acciones se aplican en concreto como una función de si el mensaje recibido verifica o no la

condición, es decir, si el mensaje recibido es un objeto al que se aplica.

[0059] Las reglas son diversas.

[0060] Algunas reglas permiten discriminar los formatos de datos autorizados de formatos de datos no autorizados.

[0061] Por ejemplo, se supone que algunos mensajes autorizados a ser transmitidos por el módulo de filtrado por la política de seguridad considerada deben componerse de una secuencia de tres campos de información "Tipo", "Tamaño" y "Valor", es decir, tienen un formato de datos de tipo TLV (en inglés Type-Length-Value"), tales que:

- el campo "Tipo" debe tener un tamaño fijo, igual a 16 bits,

- el campo "Tamaño" debe tener un tamaño fijo, igual a 16 bits,

- el campo "Valor" tiene un tamaño variable, igual valor del campo "Tamaño" que debe estar en el intervalo de bits [0, 1020].

[0062] La regla de verificación de la sintaxis de un mensaje enuncia así las condiciones que definen los mensajes-objetos a los que se aplica:

```
CAMPO id='Tipo' tamaño='2'
[...]
CAMPO id='Tamaño' tamaño='2'
[...]
CAMPO id='Valor' tamaño='$Tamaño' min='0' máx='1024'
[...]
```

en el que $Tamaño es una variable temporal que contiene el valor del campo cuyo identificador (id) es 'Tamaño'; [...] indica que los elementos hijo también se pueden definir en este nivel, tales como las reglas o propiedades o la llamada de los autómatas.

[0063] Las reglas permiten reducir los canales ocultos temporales.

[0064] Cabe recordar que, se entiende por "canales ocultos", implementado por los mensajes transmitidos por el módulo de filtrado, la transmisión de información diferente a la transmitida dentro del propio mensaje, pero tales que la información se determina como una función de la frecuencia de emisión de ciertos tipos de mensajes (canales ocultos temporales), y/o toda la información necesaria para el envío correcto de dados de un emisor a un receptor. La implementación de canales ocultos necesita la existencia de un código definido entre la parte emisora y la parte receptora.

[0065] Por ejemplo, una regla puede limitar la velocidad, generada por los mensajes con formato TLV con un campo de información "Valor", a 1 Kbyte durante el mismo periodo fijo de una hora (3600 segundos) y se escribirá por ejemplo:

```
CAMPO id='Tipo' tamaño='2'
[...]
CAMPO id='Tamaño' tamaño='2'
[...]
CAMPO id='Valor' tamaño='$Tamaño' min='0' máx='1024'
      VELOCIDAD máx='1024o' periodo "3600 s'"
[...]
```

[0066] Una variable de estado que indica el valor actual de la velocidad de este tipo de mensaje y una variable de estado que define la velocidad del periodo fijo están en concreto asociadas a dicha regla.

[0067] Otras reglas permiten aún adaptar el funcionamiento del módulo de filtrado como una función del protocolo de comunicación implementado por un mensaje recibido como entrada del módulo de filtrado.

[0068] En concreto, al usar una radio estación táctica, un usuario malintencionado podría usar las conmutaciones entre el modo de escucha y el modo de emisión para transmitir información sensible en morse, mientras que su voz está sistemáticamente cifrada. La política de seguridad podrá limitar este canal oculto limitando el número de conmutaciones de modo emisión/recepción por minuto.

[0069] Se considera ahora una regla que controla el valor del campo de información "Tipo" de un mensaje de formato TLV, y el sentido de paso, autorizado por el módulo de filtrado, del mensaje para cada valor de este campo,

esta política de seguridad aplica además el límite de canales ocultos temporales indicados anteriormente. Se escribirá por ejemplo:

```
REGLAS
      CAMPO id='Tipo' tamaño='2'
            VALOR oculto='FFFFh'
                  FIJO valor='0100h'
                        ROJO-A-NEGRO
                        [...]
                  FIJO valor='0101h'
                        ROJO-A-NEGRO
                        [...]
                  INTERVALO min='0200h' máx='0202h'
                        NEGRO-A-ROJO
                        [...]
                  FIJO valor='0300h'
                        ROJO-A-NEGRO
                        [...]
                  INTERVALO min='0400h' máx='0410h'
                        NEGRO-A-ROJO
                        [...]
                  FIJO valor='0500h'
                        NEGRO-A-ROJO
                        [...]
                  [...]
            [...]
      CAMPO id='Tamaño' tamaño='2'
            [...]
      CAMPO id='Valor' tamaño='$Tamaño' min='0' máx='1020'
            VELOCIDAD máx='1024o' periodo "3600s'
            [...]
```

[0070] En un modo de realización, una o más reglas de filtrado (FRECUENCIA) controlan la frecuencia de ciertos tipos de mensajes transmitidos entre los módulos rojo y negro.

[0071] Por ejemplo, una regla impone un valor máximo de frecuencia de paso por el módulo de filtrado de mensajes del módulo rojo al módulo negro, cuyo primer campo de información, con un tamaño de 2 bytes, toma el valor 100h (valor hexadecimal).

[0072] El periodo mínimo entre dos transmisiones de dos mensajes de este tipo es por ejemplo de 10 s.

[0073] Esta regla puede escribirse:

```
REGLA
      CAMPO tamaño='2'
            VALOR oculto='FFFFh'
                  FIJO valor='100h'
                        ROJO-A-NEGRO
                        FRECUENCIA periodo='10s'
```

[0074] Esta disposición permite limitar la existencia de canales ocultos.

[0075] El módulo de filtrado se define de manera tal que cualquier mensaje no explícitamente declarado en la base de datos de reglas como "A TRANSMITIR", es por defecto declarado como "NO TRANSMITIR".

[0076] En una etapa 102, se verifican la coherencia y la completitud del conjunto de reglas de filtrado así definido.

[0077] En modos de realización, esta verificación se lleva a cabo mediante un procedimiento de relectura por una persona, o automatizado, lo que es particularmente adecuado cuando se dispone de una semántica de coherencia resoluble o semiresoluble.

[0078] El conjunto de reglas se considera como que verifica el criterio de coherencia sin ninguna regla del conjunto de reglas definido en la etapa 101 que solo genera anomalías con otra regla. En concreto, si se sigue una lógica deóntica, ninguna de las anomalías nombradas anteriormente A1 a A4 debe autorizarse.

[0079] Anomalía de generalización A1: una regla es una generalización de otra, si tienen acciones diferentes y la primera regla se aplica también en todos los objetos de la segunda, (si dos reglas R1, respectivamente R2, son candidatas a una aplicación a un conjunto de mensajes E1, respectivamente E2), cuyas acciones asociadas son

diferentes y E1 se incluye en E2, existe anomalía ya que entonces en imposible decidir qué regla debe aplicarse).

[0080] Anomalía de recubrimiento A2: una regla es recubierta cuando una regla anterior se aplica en todos los objetos, sabiendo que las dos reglas tienen acciones diferentes.

[0081] Anomalía de correlación A3: dos reglas, con acciones diferentes, se correlacionan si cada una de ellas también se aplica a un subconjunto de objetos sobre la que se aplica la otra.

[0082] Anomalía de redundancia A4: una regla es redundante si ejecuta la misma acción en los mismos objetos que otra regla.

[0083] El conjunto de reglas se considera como que verifica el criterio de integridad si se demuestra que las reglas del conjunto de reglas definido en la etapa 101 son capaces de filtrar todos los mensajes susceptibles de ser proporcionados como entrada del módulo de filtrado. En un modo de realización, el conjunto de reglas es considerado como que verifica el criterio de integridad si además, por el contrario, todas las reglas son usadas.

[0084] Si el conjunto de reglas no verifica el criterio de completitud o de coherencia, su definición es revisada de modo que estos criterios sean verificados.

[0085] En modos de realización, solo se verifican algunos criterios o algunas líneas de estos criterios.

[0086] En una etapa 103, el conjunto de reglas de filtrado así definido, que comprende los autómatas protocolarios y que representa la política de seguridad seleccionada, y cuya integridad y coherencia se han validado, se compila, de manera que la hace legible y explotable directamente por el bloque de tratamiento 14.

[0087] El conjunto de reglas así compilado se registra en una base de datos de reglas 15, elemento del módulo de filtrado 5. Las variables de estado asociadas a la política de seguridad también se almacenan en un bloque 16 de variables de estado del módulo de filtrado.

[0088] La base de datos de reglas 15 y el bloque 16 de variables de estado son adaptadas para funcionar en colaboración con un bloque de tratamiento 14.

[0089] Según los modos de realización de la invención, la totalidad o parte de las etapas del procedimiento 100 se implementan tras la ejecución, en los medios de cálculo, de instrucciones de software de un programa informático de definición de un módulo de filtrado en un modo de realización de la invención.

[0090] En una etapa 104 (no representada), la política de seguridad se aplica, por la implementación operativa del módulo de filtrado 5, en mensajes que le son proporcionados.

Módulo de filtrado

[0091] Según un segundo aspecto, la invención propone un módulo de filtrado, por ejemplo similar al módulo de filtrado 5 del equipo criptográfico 1.

[0092] En este módulo de filtrado 5, la base de datos de reglas 15, obtenida al final del procedimiento 100 por la compilación de la política de seguridad, es almacenada.

[0093] En el bloque de variables de estados 16, se inician los valores de las variables de estados definidas en una asociación con las reglas durante la implementación del procedimiento 100.

[0094] El bloque de tratamiento 14 está adaptado para, tras la recepción de un mensaje que procede del módulo rojo 2, proceder a la evaluación de las reglas de filtrado definidas en la base de reglas 15, para autorizar su transferencia al módulo negro 3.

[0095] El bloque de tratamiento 14 está adaptado para, tras la recepción de un mensaje que procede del módulo negro 3, proceder a la evaluación de las reglas de filtrado definidas en la base de reglas 15, para autorizar su transferencia al módulo rojo 2.

[0096] El bloque de tratamiento 14, más precisamente, evalúa la regla de filtrado de raíz definida en la base de datos de reglas 15, tras la recepción de un mensaje.

[0097] La evaluación de la regla de filtrado de raíz conduce a la evaluación de sus reglas hija. De forma recursiva, la evaluación de las reglas hija conduce a la evaluación de la totalidad o parte del árbol de reglas de filtrado que constituye la base de datos de reglas 15.

[0098] Los valores de las variables de estado en el bloque de variables de estado 16 se actualizan a lo largo de la aplicación de las reglas de la política de seguridad, en los mensajes controlados por el módulo de filtrado durante su funcionamiento operativo.

[0099] En concreto, la evaluación de una regla de filtrado puede causar la modificación del valor actual de una o más variables de estado. Las variables de estado no se modifican inmediatamente a fin de mantener la coherencia de las variables de estado durante la aplicación de la política de seguridad en el mensaje. Cuando finaliza la evaluación de las reglas de filtrado y si todas las reglas de filtrado evaluadas han devuelto VERDADERO o A TRANSMITIR, entonces el bloque de tratamiento 14, procede a la actualización de las variables de estado modificadas por las reglas de filtrado evaluadas.

[0100] Cabe destacar que durante el funcionamiento operativo del módulo de filtrado 5, la base de reglas 15 es invariante, mientras que los valores de las variables de estado del bloque de variables de estado 16 se actualizan a lo largo de la aplicación de las reglas en los mensajes.

[0101] La solución propuesta consiste en basar la arquitectura del módulo de filtrado en tres partes principales, que son el bloque de tratamiento, la base de datos de reglas y el bloque de las variables de estado 16. La política de seguridad está totalmente definida y configurada en la base de datos de reglas mediante las reglas de filtrado asociadas a autómatas. La aplicación de estas reglas se determina por el bloque de tratamiento 14 cuyo comportamiento se pueden congelar. Esta separación de la aplicación de la política de seguridad y su definición facilita la implementación de modificaciones de la política de seguridad.

[0102] La invención se caracteriza por:

- esta implantación de la política de seguridad de filtrado en forma de reglas, permitiendo estas reglas controlar las propiedades estáticas, temporales y dinámicas de mensajes autorizados a pasar por el módulo de filtrado.

- la separación de la concepción, del desarrollo y de la segurización de la política de seguridad de su aplicación;

- la integración retardada de las reglas en el módulo de filtrado.

[0103] Por lo tanto, la invención permite configurar las políticas de seguridad en el módulo de filtrado, en lugar de implantarlas por una codificación en duro.

[0104] La invención permite, de este modo, responder a las limitaciones de los módulos de filtrado de la técnica anterior en cuanto a su falta de capacidades de evolución: de hecho, según la invención, para modificar el comportamiento del módulo de filtrado, es suficiente modificar la política de seguridad, y después compilarla y cargarla en el módulo de filtrado en la forma de una base de datos de reglas, sin modificación del bloque de tratamiento. Es más, la invención permite además disponer de un módulo de filtrado para el comportamiento adaptativo. Del mismo modo, el bloque de tratamiento podrá ser idéntico en los módulos de filtrado de niveles de privacidad diferentes y/o al aplicar políticas de seguridad diferentes, solo difieren las bases de reglas.

[0105] Las ventajas de la solución propuesta están presentes durante toda la vida del módulo de filtrado.

[0106] De hecho, durante el desarrollo, permite responder a la necesidad de las configuraciones cambiantes durante el desarrollo y autoriza una integración casi continua del módulo de filtrado.

[0107] Durante la certificación/calificación de equipo, proporciona una garantía elevada y la prueba de la coherencia y de la completitud de las reglas. Lleva a cabo una implantación rigurosa del idioma adaptado, permite desequilibrar el procedimiento de concepción del módulo de filtrado, del procedimiento de concepción de las políticas de seguridad (100). Permite generar el compromiso de eficacia/seguridad de forma flexible adaptando la definición de la política de seguridad a la necesidad de seguridad (nivel de aprobación del equipo criptográfico).

[0108] La invención se ha descrito anteriormente con referencia a un encriptador. Sin embargo, puede implementarse en cada módulo de filtrado en un sistema con campos D1 y D2, de niveles de confidencialidad distintos N1 y N2 respectivamente, en concreto cuando se requiere para comunicar entre D1 y D2, información de nivel N2.

[0109] Tal módulo de filtrado según la invención puede por lo tanto implementarse en los sistemas de cortafuegos, pasarela de seguridad, equipos multiniveles de seguridad tales como terminales, servidores, diodos, encriptadores, routers, etc.

[0110] En el caso del equipo criptográfico 1, la información considerada como la descrita son mensajes en los planos de control y gestión (ejemplo: información de enrutamiento y calidad del servicio). No obstante, en otros modos de realización, la información son datos distintos de los mensajes en los planos de control y gestión, a transmitir entre los módulos negro y rojo.

[0111] En el modo de realización considerado, el conjunto de reglas se organiza según una estructura de árbol. En otros modos de realización, el conjunto de reglas está estructurado de manera diferente, por ejemplo en forma de lista de reglas a secuenciar. Lo que importa es que el orden según el cual el módulo de tratamiento debe tener en cuenta las reglas entre sí le sea proporcionado por la base de datos.

REIVINDICACIONES

1. Procedimiento de definición (100) de un módulo de filtrado (5) adaptado para filtrar información, según una política de seguridad determinada, entre un primer módulo (2) propio para tratar información de un primer nivel de sensibilidad, y un segundo módulo (3) propio para tratar información de un segundo nivel de sensibilidad distinto del primer nivel de sensibilidad, estando dichos primer y segundo módulos conectados, en paralelo con el módulo de filtrado, por un módulo criptográfico (4) adaptado para aplicar funciones criptográficas, comprendiendo el procedimiento las etapas según las cuales:

- un conjunto de reglas de filtrado es definido (101), al traducir la política de seguridad determinada, en un idioma apto para ser compilado, definiendo dichas reglas de filtrado las propiedades de información cuya transmisión es autorizada por el módulo de filtrado (5) entre el primer y el segundo módulos;

- dicho conjunto de reglas definido es compilado (103);

- dicho conjunto de reglas compilado se integra en una base (15) de reglas del módulo de filtrado;

siendo dicho procedimiento **caracterizado porque**:

- un tratamiento de validación del conjunto de reglas definido es llevado a cabo (102), validando que una autorización o un rechazo de transmisión ha sido proporcionado correctamente por aplicación de dicho conjunto de reglas a cualquier información susceptible de ser proporcionada en la entrada del módulo de filtrado; y **porque**

- el conjunto de reglas de filtrado incluye al menos un autómata protocolario, definido por un conjunto de estados correspondientes a las etapas sucesivas de implementación de un protocolo de comunicación, y de eventos que provocan las transiciones entre dichos estados; definiendo el conjunto de reglas de filtrado propiedades estáticas, temporales y dinámicas de información autorizada para ser transmitida,

el tratamiento de validación del conjunto de reglas definido comprende además una etapa de validación de la coherencia de las reglas del conjunto de reglas,

la etapa de validación de la coherencia de las reglas comprende la detección de al menos una anomalía entre:

- la existencia en el conjunto de reglas de una primera y segunda reglas asociadas con acciones diferentes, siendo la primera regla aplicada en todos los objetos de la segunda;

- la existencia en el conjunto de reglas de dos reglas asociadas con acciones diferentes, y cada una de entre ellas se aplica en un subconjunto de objetos en la que se aplica la otra, y

- la existencia de dos reglas que ejecutan la misma acción sobre los mismos objetos.

2. Procedimiento de definición (100) de un módulo de filtrado (5) según la reivindicación 1, según el cual el conjunto de reglas de filtrado incluye reglas de verificación de formatos de mensaje, indicando cada estado una fase particular en una secuencia predeterminada de mensajes.

3. Procedimiento de definición de un módulo de filtrado (5) según la reivindicación 1 o 2, según el cual el módulo de filtrado incluye un módulo de tratamiento (14) apto para ejecutar el conjunto de reglas integrado en la base de datos (15) de reglas tras la recepción de información a filtrar y apto para autorizar o rechazar la transmisión por el módulo de filtrado de dicha información entre los primer (2) y segundo (3) módulos según un rechazo o una autorización proporcionada después de la ejecución de dicho conjunto de reglas.

4. Procedimiento de definición de un módulo de filtrado (5) según la reivindicación 3, según el cual las variables de estado (16) asociadas con las reglas de filtrados son definidas, y un rechazo o autorización se proporciona tras la ejecución de dicho conjunto de reglas en función de valores actuales calculados para dichos valores de variables de estado.

5. Procedimiento de definición de un módulo de filtrado (5) según cualquiera de las reivindicaciones anteriores, según el cual el conjunto de reglas se define según una estructura arborescente de reglas.

6. Procedimiento de definición de un módulo de filtrado (5) según cualquiera de las reivindicaciones anteriores, según el cual el módulo de filtrado se define de manera que la información del primer módulo (2) cuya transmisión es autorizada por el módulo de filtrado sean transmitidas al segundo módulo (3) en claro.

7. Procedimiento de definición de un módulo de filtrado (5) según cualquiera de las reivindicaciones anteriores, según el cual la orden de aplicación y la composición lógica de los resultados de las reglas se define por

el conjunto de reglas de filtrado.

8. Módulo de filtrado (5) adaptado para filtrar información según una política de seguridad entre un primer módulo (2) propio para tratar información sensible, y un segundo módulo (3) propio para tratar información no sensible, estando dichos primer y segundo módulos conectados, en paralelo con el módulo de filtrado, por un módulo criptográfico (4) adaptado para aplicar funciones criptográficas,

comprendiendo dicho módulo de filtrado un módulo de tratamiento (14) y una base (15) de datos de reglas que incluye un conjunto de reglas de filtrado que definen la política de seguridad determinada, en un idioma compilado, definiendo dichas reglas de filtrado las propiedades de la información cuya transmisión es autorizada por el módulo de filtrado (5) entre el primer y el segundo módulos;

siendo dicho módulo de filtrado **caracterizado porque** el conjunto de reglas de filtrado incluye al menos un autómata protocolario, definido por un conjunto de estados correspondientes a las etapas sucesivas de implementación de un protocolo de comunicación, y de eventos que provocan las transiciones entre dichos estados; definiendo el conjunto de reglas de filtrado propiedades estáticas, temporales y dinámicas de información autorizada para ser transmitida,

llevándose a cabo un tratamiento de validación del conjunto de reglas definido, comprendiendo el tratamiento de validación del conjunto de reglas definido además una etapa de validación de la coherencia de las reglas del conjunto de reglas, comprendiendo la etapa de validación de la coherencia de las reglas la detección de al menos una anomalía entre:

- la existencia en el conjunto de reglas de una primera y segunda reglas asociadas con acciones diferentes, siendo la primera regla aplicada en todos los objetos de la segunda;

- la existencia en el conjunto de reglas de dos reglas asociadas con acciones diferentes, y cada una de entre ellas se aplica en un subconjunto de objetos en la que se aplica la otra, y

- la existencia de dos reglas que ejecutan la misma acción sobre los mismos objetos.

9. Módulo de filtrado (5) según la reivindicación 8, según el cual el conjunto de reglas de filtrado incluye reglas de verificación de formatos de mensaje, indicando cada estado una fase particular en una secuencia predeterminada de mensajes.

10. Módulo de filtrado según la reivindicación 8 o 9, en el que el conjunto de reglas integrado en la base de datos de reglas es resultado de un procedimiento según cualquiera de las reivindicaciones 1 a 7.

11. Equipo criptográfico que incluye:

- un primer módulo (2) propio para tratar información de un primer nivel de sensibilidad;

- un segundo módulo (3) propio para tratar información de un segundo nivel de sensibilidad distinto del primer nivel de sensibilidad;

- un módulo criptográfico (4) adaptado para aplicar funciones criptográficas, que conecta dichos primer y segundo módulos;

- un módulo de filtrado (5) según cualquiera de las reivindicaciones 8 a 10, adaptado para filtrar información según una política de seguridad entre el primer módulo (2) y el segundo módulo (3).

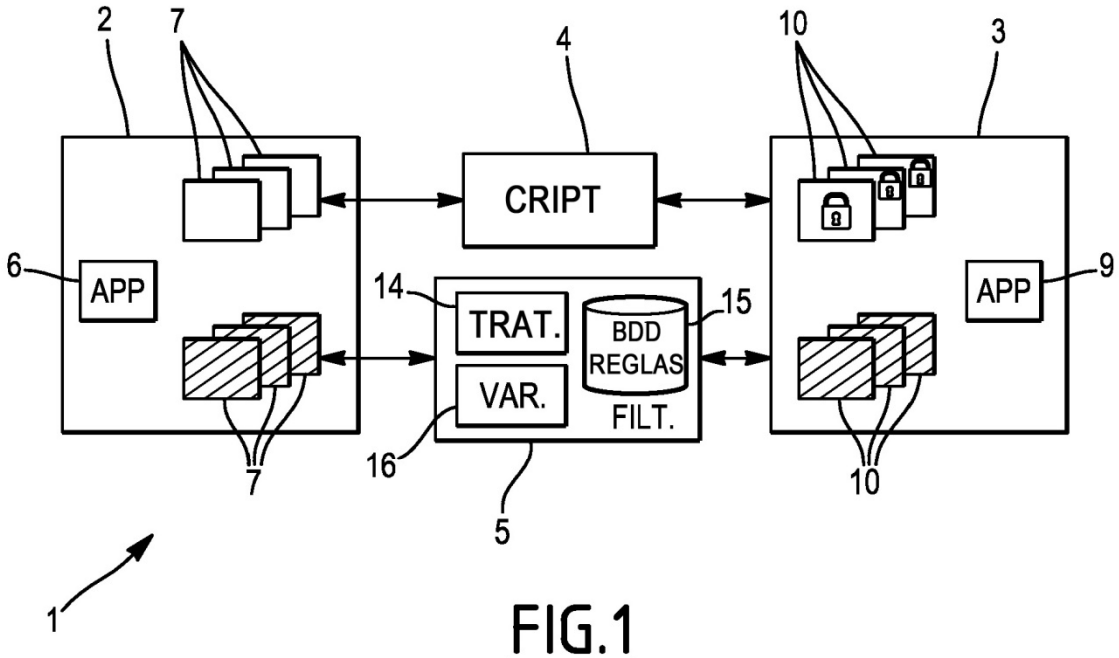
2
7
4
10
3
CRIPT
6
APP
14
TRAT.
VAR.
BDD
REGLAS
FILT.
15
APP
9
7
16
5
10
1

FIG.1

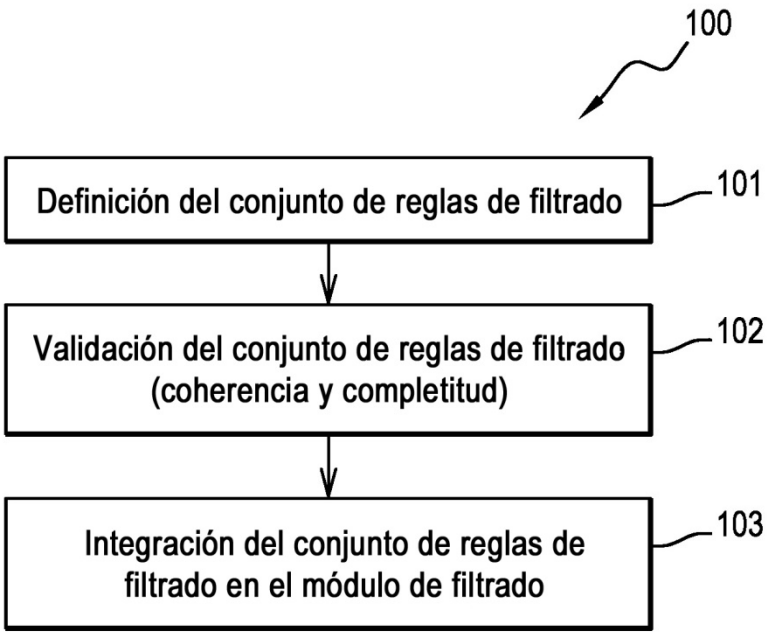
100
Definición del conjunto de reglas de filtrado
101
Validación del conjunto de reglas de filtrado (coherencia y completitud)
102
Integración del conjunto de reglas de filtrado en el módulo de filtrado
103

FIG.2