(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 727**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.07.2011 PCT/EP2011/061697**

(87) Fecha y número de publicación internacional: **19.01.2012 WO2012007402**

(96) Fecha de presentación y número de la solicitud europea: **08.07.2011 E 11731341 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2016 EP 2593896**

(54) Título: **Supervisión de la seguridad en un sistema informático**

(30) Prioridad:

13.07.2010 FR 1055715

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2017

(73) Titular/es:

AIRBUS DS SAS (100.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR

(72) Inventor/es:

PONCHEL, CHRISTOPHE y
BOEUF, JEAN-FRANÇOIS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Supervisión de la seguridad en un sistema informático

La presente invención se refiere al campo de la seguridad en los sistemas informáticos.

Un sistema informático comprende varios componentes informáticos, también denominados “entidades”, u “objetos”, o “componentes”. Los componentes informáticos son, por ejemplo, equipos informáticos, tales como varios ordenadores, terminales fijos o móviles, servidores, enrutadores, pasarelas, conmutadores, etc., aplicaciones y sistemas operativos instalados en los equipos, redes de comunicación que interconectan los equipos, como una red de servidores y una red de terminales de usuario, y servicios proporcionados por los equipos.

Más particularmente, esta invención se refiere a un método y a un dispositivo para supervisar la seguridad de un sistema informático para recopilar y analizar datos relativos a los estados de los componentes informáticos incluidos en el sistema informático, y que dependen de los eventos y de los comportamientos de los componentes.

Se sabe modificar la herramienta de software libre o “código abierto” de supervisión Nagios para supervisar la seguridad de los equipos reunidos en redes.

La herramienta Nagios modificada caracteriza la seguridad de un equipo informático a través de cuatro indicadores de “nivel bajo” que están relacionados con la criticidad, la vulnerabilidad, la detección de incidencias y el servicio. La criticidad representa la importancia del equipo. Tiene cinco valores: mínimo, bajo, medio, alto y máximo. La vulnerabilidad está representada por los recuentos de los contadores de vulnerabilidad categorizados por sus severidades que podrían ser información, baja, media y alta. El indicador de incidencias asocia todas las incidencias relacionadas con el equipo, cualquiera que sea la naturaleza de las mismas, y depende de los recuentos de los contadores de incidencias categorizados por las severidades de las mismas que podrían ser información, baja, media y alta. Un punto de supervisión en un equipo es un servicio proporcionado por el equipo, tal como la vigilancia de la apertura de un puerto. Se comprueba el punto de supervisión mediante una vigilancia de la herramienta Nagios realizado por medio de un agente Nagios instalado en el equipo. El indicador de servicio está representado por una tasa de disponibilidad, expresada en porcentaje, de los servicios de aplicación presentes en el equipo. Los niveles de servicio son “disponible”, “pendiente” (que está siendo revisado), “peligroso”, “crítico” y “desconocido” (no disponible).

Para cada equipo, se determina un indicador de seguridad en función de los tres primeros indicadores previos de “nivel bajo” y es igual a la suma de los indicadores de vulnerabilidad e incidencias que están ponderados por los niveles de severidad, que se pueden parametrizar en la configuración, y multiplicados por la criticidad del equipo.

Se determina un indicador general para cada equipo en función del indicador de seguridad y del indicador de servicio y está compuesto por el máximo de esos dos indicadores.

El significado de los indicadores de vulnerabilidad, incidencias y servicio se establece rígidamente en el código, lo que lleva a modificar la aplicación si se va a cambiar el modo de cálculo de un indicador de nivel bajo.

Los equipos se registran en los archivos de configuración de Nagios. Cualquier nuevo equipo registrado en la configuración sólo se tiene en cuenta cuando se reinicia la herramienta Nagios, iniciando entonces las comprobaciones por los servicios en el equipo.

Los equipos podrían ser reunidos por la red. Las redes se registran en los archivos de configuración de Nagios y cualquier nueva red registrada en la configuración sólo se tiene en cuanta al reiniciar la herramienta Nagios. Una red tiene una criticidad deducida de las criticidades de los componentes informáticos, tales como redes y/o equipos, contenidos en la red, y es igual al promedio de las criticidades de los componentes contenidos. Se determina un indicador general para cada red en función de los indicadores generales de los componentes contenidos en la red y es igual al promedio ponderado de los indicadores generales de los componentes contenidos, como redes y/o equipos.

Los datos de estado son recuperados por la herramienta Nagios y sus extensiones instaladas en un servidor ya sea en los modos nativos Nagios para el indicador de servicio, o por paquetes de alarma o “trampas” de acuerdo con el protocolo de supervisión SNMP (“Protocolo de Gestión de Red Simple”) para el indicador de incidencias y el indicador de vulnerabilidad. Los datos de estos indicadores no están estandarizados, lo que no facilita su lectura. Además, la parametrización sólo podría modificarse mediante la actualización manual de los archivos de configuración de la herramienta Nagios y sus extensiones, debiendo reiniciarse el servidor para tener en cuenta estas modificaciones. Las funciones de agregación de los indicadores son fijas y determinadas en el código de la aplicación. El indicador de incidencias agrega los recuentos de incidencias, cualquiera que sea la naturaleza de las incidencias relacionadas con un equipo, como una intrusión por ejemplo.

Además, la herramienta de supervisión de Nagios muestra al administrador de la seguridad del sistema informático supervisado sólo el reflejo exacto de la disposición técnica de los componentes informáticos supervisados incluidos en el sistema. Esta representación podría ser difícilmente procesable por el administrador cuando el sistema

informático supervisado es complejo y los datos técnicos que permiten describirlo no dan ninguna representación del estado de la seguridad en el sistema que sea fácil de entender.

La patente americana US6.839.850 B1 describe un método para proporcionar detección temprana de una amenaza de seguridad potencial usando un motor de advertencia e indicación de seguridad (SI&W) que mide eventos SI&W clave con un mecanismo llamado indicadores. Los indicadores pueden ser simples indicadores de contador que miden las ocurrencias de un evento o pueden ser indicadores estadísticos que contienen medidas nominales. Los indicadores asociados con un conjunto completo de eventos SI&W clave se denominan conjuntos de indicadores. El motor SI&W mantiene un conjunto de indicadores separado para cada usuario y equipo monitorizados. El motor SI&W utiliza una agregación jerárquica de la información recopilada en los indicadores para evaluar en última instancia el potencial de una amenaza para el sistema monitorizado.

El objetivo de la invención es proporcionar una supervisión de la seguridad en un sistema informático que oculta la complejidad técnica del sistema, al tiempo que muestra el estado de seguridad del sistema a través de los estados de seguridad de grupos funcionales de componentes informáticos elementales, tales como equipos y aplicaciones incluidas en el sistema, correspondiendo estos grupos funcionales al trabajo del usuario del sistema y siéndole familiares.

Para alcanzar este objetivo, un método para supervisar la seguridad en un sistema informático que comprende varios componentes informáticos elementales, siendo supervisado cada componente elemental dependiendo de medidas de base representativas de estados predeterminados del componente elemental y de varios componentes de reunión que reúnen, respectivamente, componentes elementales supervisados, está caracterizado por que comprende la determinación de varios indicadores de seguridad de diferentes tipos para cada componente elemental supervisado, siendo determinado cada indicador de seguridad según una función respectiva de medidas de base asociadas con el indicador de seguridad, y la determinación de varios indicadores de seguridad de diferentes tipos para cada componente de reunión, siendo determinado cada indicador de seguridad de un tipo dado de un componente de reunión según una función respectiva de los indicadores de seguridad del tipo dado de los componentes elementales reunidos en el componente de reunión.

Unos pocos indicadores de seguridad, que son todos determinados según un proceso común, son suficientes para indicar, en un modo rápidamente comprensible, el estado de seguridad de un componente elemental y de un componente de reunión.

El método de supervisión de la invención puede así supervisar varios tipos de componente de reunión pertenecientes a la distribución organizativa, lógica y geográfica de los componentes elementales en el sistema informático supervisado, tales como equipos informáticos y aplicaciones. En particular, un componente de reunión podría ser una red de equipos informáticos como componentes elementales reunidos en el componente de reunión, o un servicio basado en aplicaciones, como componentes elementales reunidos en el componente de reunión, por ejemplo, implementado en varios servidores, o un sitio geográfico que reúne equipos informáticos y/o redes como componentes elementales reunidos en el componente de reunión. Estos componentes de reunión corresponden a las artes del usuario del sistema informático y los indicadores de seguridad de los mismos podrían ser visualizados simultáneamente para rastrear fácilmente un componente de reunión relativamente deficiente.

Con el fin de conocer el estado de seguridad de los diferentes componentes elementales en el sistema informático supervisado y en consecuencia, comprender el impacto en los componentes de reunión de un problema de seguridad en cualquier componente elemental del sistema, uno de los indicadores de seguridad de cada componente elemental podría depender de medidas de base relacionadas con la disponibilidad del componente, o podría depender de medidas de base relacionadas con al menos un tipo de incidencia en el componente y con un factor de gravedad del tipo de incidencia, o podría depender de medidas de base relacionadas con la vulnerabilidad del componente y representativas de una estimación del impacto de al menos un fallo de seguridad de un tipo predeterminado en el componente y un factor de gravedad del fallo, o podría depender de medidas de base relacionadas con una garantía de conformidad del componente con respecto a una política de seguridad preestablecida. Estos cuatro tipos de indicadores podrían establecerse y mostrarse para cada componente elemental y para cada componente de reunión.

De acuerdo con otra característica del método destinado a determinar los indicadores de seguridad de un componente elemental tal como un equipo, una aplicación o partes de la misma, de acuerdo con funciones que se pueden parametrizar que agregan por categoría las medidas de base asociadas con el componente y que estandarizan el proceso de actualización de los indicadores, cualquiera que sea su tipo, la determinación de un indicador de seguridad de un tipo dado del componente elemental comprende, además de una modificación de una de las medidas de base asociadas con el indicador de seguridad,

estimar una medida derivada de acuerdo con una función de la medida de base modificada y de al menos otra medida de base interdependiente con la medida de base modificada, y

estimar una métrica de acuerdo con una función de la medida derivada estimada y de al menos una segunda medida derivada de acuerdo con una función de las medidas de base interdependientes asociadas con el indicador de seguridad de un tipo dado y diferente de las medidas de base anteriores,

determinándose el indicador de seguridad de un tipo dado de acuerdo con una función dependiente de la métrica estimada.

Si el componente elemental supervisado incluye uno o más de otros componentes elementales, la determinación del indicador de seguridad del tipo dado del componente elemental podría comprender una agregación de indicadores de seguridad del tipo dado de los componentes elementales origen incluidos en el componente elemental en un indicador de agregación, determinándose el indicador de seguridad del componente elemental de acuerdo con una función dependiente de la métrica estimada y del indicador de agregación.

La invención se refiere también a un dispositivo para supervisar la seguridad de un sistema informático que comprende varios componentes informáticos elementales. El dispositivo es capaz de recoger medidas de base asociadas con cada componente elemental y representativas de estados predeterminados del componente elemental. Varios componentes de reunión reúnen componentes elementales respectivamente. El dispositivo está caracteriza porque comprende un medio para determinar varios indicadores de seguridad de diferentes tipos para cada componente elemental supervisado, determinándose cada indicador de seguridad de acuerdo con una función respectiva de medidas de base asociadas con el indicador de seguridad, y un medio para determinar varios indicadores de seguridad de diferentes tipos para cada componente de reunión, determinándose cada indicador de seguridad de un tipo dado de un componente de reunión de acuerdo con una función respectiva de los indicadores de seguridad del tipo dado de los componentes elementales reunidos en el componente de reunión.

Un componente de reunión podría ser al menos uno de los siguientes componentes de reunión: una red de equipos informáticos, como componentes elementales reunidos, un servicio basado en aplicaciones como componentes elementales reunidos y un sitio geográfico que reúne equipos informáticos y/o redes como componentes elementales reunidos. El dispositivo podría así presentar el estado de seguridad del sistema informático a supervisar de acuerdo con tres orientaciones familiares.

Los medios para determinar el indicador de seguridad del componente podrían adaptarse para determinar al menos uno de los siguientes indicadores de seguridad para un componente elemental y un componente de reunión: un indicador de seguridad dependiente de las medidas de base relacionadas con la disponibilidad del componente, un indicador de seguridad dependiente de las medidas de base relacionadas con al menos un tipo de incidencia en el componente y un factor de gravedad del tipo de incidencia, un indicador de seguridad dependiente de las medidas de base relacionadas con la vulnerabilidad del componente y representativas de una estimación del impacto de al menos un fallo de seguridad de un tipo predeterminado en el componente y un factor de gravedad del fallo, y un indicador de seguridad dependiente de las medidas de base relacionadas con una garantía de conformidad del componente con respecto a una política de seguridad preestablecida. El dispositivo de acuerdo con la invención gestiona así varios tipos de indicador y las reacciones que se están aplicando o se han de aplicar como resultado de la modificación de cualquier indicador. Notificar la modificación de un indicador lleva al administrador del dispositivo a conocer el detalle de un problema de seguridad del sistema informático para intervenir en el componente notificado por el indicador modificado para resolver el correspondiente problema de seguridad.

La invención se refiere también a un programa informático que puede implementarse en un dispositivo de supervisión de la invención, comprendiendo dicho programa instrucciones que, cuando el programa se lleva a cabo en el dispositivo de supervisión, realizan los pasos del método de la invención.

La invención está definida por las reivindicaciones independientes 1, 11 y 14. Otras realizaciones de la invención están definidas por las reivindicaciones dependientes 1-9 y 12-13.

Las características y ventajas adicionales de la presente invención resultarán fácilmente de manifiesto a partir de la lectura de la descripción que sigue de varias realizaciones de la invención dadas como ejemplos no limitativos, con referencia a los correspondientes dibujos adjuntos, en los que:

- La FIG. 1 es un diagrama de bloques esquemático de un dispositivo de supervisión de acuerdo con la invención para supervisar componentes informáticos de un sistema informático;

- La FIG. 2 es un algoritmo del método de supervisión de acuerdo con la invención para determinar, más particularmente, un indicador de seguridad de un componente elemental y un indicador de seguridad de un componente de reunión.

- La FIG. 3 es un diagrama de bloques esquemático de un sistema informático con varios componentes de reunión tales como redes, servicios y sitios;

- La FIG. 4 es un diagrama del impacto de una anomalía de la garantía de conformidad en un cortafuegos del sistema informático de la FIG. 3 en los componentes de reunión; y

- La FIG. 5 muestra esquemáticamente una página de pantalla con el impacto de la anomalía de la garantía de conformidad propagada en los componentes de reunión del sistema informático.

Con referencia a la FIG. 1, un dispositivo de supervisión de seguridad DS de acuerdo con la invención se adapta para supervisar la seguridad de un sistema informático SY que comprende numerosos componentes informáticos elementales BI y que por lo tanto es generalmente complejo. Supervisa el estado de seguridad de los componentes informáticos elementales para presentar los estados de seguridad de los componentes de reunión BIg que reúnen componentes informáticos elementales con el fin de proporcionar un plan de reacción para inhibir las anomalías detectadas en los componentes informáticos elementales.

Por ejemplo, el sistema informático perteneciente a una empresa, o a una empresa y sus filiales, se organiza en redes dispuestas en sitios geográficos y en servicios empresariales prestados al personal-usuario de la empresa.

Los componentes informáticos elementales BI que se han de supervisar en el sistema informático SY tienen varios tipos técnicos. Por ejemplo, los componentes elementales BI son equipos informáticos, tales como ordenadores, periféricos, terminales fijos o móviles, servidores, enrutadores, pasarelas, interfaces, conmutadores, etc., algunos de los cuales podrían ser componentes secundarios que incluyen componentes origen tales como componentes de hardware y software incluidos. Los componentes elementales BI podrían ser además aplicaciones y sistemas operativos previstos en los equipos informáticos, algunos de los cuales podrían ser componentes secundarios que incluyen componentes origen tales como módulos software y programas informáticos. Así, de manera más general, un componente elemental BI que se ha de supervisar no podría comprender ningún otro componente origen elemental, ni comprender un conjunto de componentes elementales origen a supervisar, algunos de los cuales podrían ser componentes elementales compuestos. Por ejemplo, un conjunto de componentes elementales origen a supervisar podría ser un equipo como un componente subordinado que comprende varias aplicaciones y/o dispositivos hardware o software, tales como controladores, que se han de supervisar.

Los componentes de reunión BIg son redes de comunicación locales o extendidas que interconectan equipos, tales como una red de servidores y una red de terminales de usuario, servicios que tienen cada uno partes se han de supervisar implementados en al menos dos equipos, como aplicaciones implementadas en varios servidores, y sitios geográficos, reuniendo cada uno equipos y/o una o más redes y/o uno o más servicios a supervisar.

El dispositivo de supervisión DS podría ser un ordenador con una interfaz hombre-equipo IHM que incluye una consola de supervisión. El dispositivo de supervisión DS está en comunicación con unidades de gestión UG y comprende una unidad de estandarización de datos UU, una unidad de determinación de indicadores UDI, conectada a la unidad UU, y la interfaz hombre-equipo IHM conectada a la unidad UDI. La interfaz IHM se utiliza especialmente para activar bien automáticamente o bien manualmente el dispositivo DS, para capturar diversos datos tales como identificadores y características de los componentes BI y BIg, para parametrizar funciones para la determinación de indicadores de seguridad de los componentes y funciones en las unidades de gestión UG asociadas con ellas, para capturar la arquitectura del sistema SY, para visualizar, entre otros, los indicadores de los componentes y el estado de seguridad del sistema, y para notificar alarmas.

Las unidades de gestión UG analizan los estados de seguridad de los componentes del sistema SY. Cada componente informático elemental BI que se ha de supervisar es un componente que a menudo se asocia con numerosas unidades de gestión UG respectivas. Sin embargo, un componente de reunión BIg que comprende varios componentes elementales a supervisar, tal como una red, un servicio o un sitio, no está asociado directamente con unidades de gestión, y sólo se asocia indirectamente con las unidades de gestión de los componentes elementales que comprende, solamente a través de estos componentes elementales, de acuerdo con una jerarquía en forma de árbol de los componentes del sistema, como se ilustra en las FIGS. 2 y 4, que se describirán más adelante. La asociación de un componente elemental BI con una unidad de gestión UG respectiva podría ser un enlace bien interno y/o externo al componente elemental, cuando la unidad de gestión se localiza en el componente elemental o en su proximidad. Por ejemplo, una unidad de gestión es un sensor, una sonda, un robot o un agente de software integrado o añadido al componente BI, y capaz de detectar estados de seguridad, tales como eventos o comportamientos predeterminados que ocurren en el componente elemental BI, y de controlarlos en función de reglas pre programadas, para notificar anomalías operativas del componente. Por ejemplo, una anomalía podría ser un acceso no autorizado a una aplicación en un equipo, o relacionado con un servicio, un error en el análisis del funcionamiento de un protocolo de comunicación, un mensaje predeterminado entrante o saliente o un paquete sondeado en el tráfico en un puerto de un equipo o un componente interno de este equipo o en un enlace a o en un equipo, una red o un sitio. La asociación de un componente elemental BI a una unidad de gestión UG respectiva también podría ser una relación conceptual cuando la unidad de gestión se basa en datos estadísticos proporcionados por una base de conocimientos relativos a eventos o comportamientos predeterminados de un componente similar a dicho componente elemental BI, notificado por un tercero. El código de cada unidad de gestión podría modificarse para parametrizar la estimación de la medida de base asociada.

Como se muestra esquemáticamente en la FIG. 1, un componente informático elemental BI podría asociarse con una o más unidades de gestión de disponibilidad UGD, y/o a una o más unidades de gestión de incidencias UGI, y/o a una o más unidades de gestión de vulnerabilidad UGV y/o a una o más unidades de garantía de conformidad UGA. Cada unidad de gestión UGD, UGI, UGV, UGA transmite, bien periódicamente o dependiendo de la ocurrencia

de al menos un evento o comportamiento que sea específico para ella, datos respectivos DD, DI, DV, DA a la unidad de estandarización de datos UU. Estos datos son, entre otros, una dirección, un identificador del componente asociado y una medida de base MB adaptada para la determinación de un indicador respectivo ID, II, IV, IA del componente elemental BI al que la unidad de gestión está asociado. La unidad de estandarización de datos UU recoge a través de redes seguras todos los datos DD, DI, DV, DA notificados por las unidades de gestión UG y los formatea en estructuras uniformes de datos SDD, SDI, SDV, SDA en las que se encuentran todos los datos necesarios para la determinación en la unidad UDI de los indicadores de seguridad ID, II, IV, IA, independientemente de la naturaleza técnica del componente. Cada indicador depende de una o más estructuras uniformes de datos.

Cada una de las estructuras de datos SDD, SDI, SDV y SDA para la determinación de los indicadores respectivos ID, II, IV e IA de un componente elemental BI incluye una métrica ME. Una métrica ME es una combinación de medidas derivadas MD relacionadas con un tema común, tales como organizar una gestión remota del componente, o vigilar protocolos de red o protocolos de transporte, o pasos predeterminados de sesiones en el componente elemental. Una medida derivada MD es una combinación de medidas de base MB interdependientes transmitidas por las unidades de gestión a la unidad de estandarización UU. Una medida de base MB representa un control medido en un punto particular del componente elemental BI por una unidad de gestión UG. La interdependencia de dos medidas de base MB respecto al componente elemental significa que las medidas de base tienen características comunes. Por ejemplo, dentro del marco de conexiones de un equipo que depende de protocolos de transporte que están asegurados de modo remoto, las medidas de base interdependientes comprueban que los protocolos de transporte son aceptables por una política de seguridad, o que las direcciones de los paquetes entrantes sean compatibles con las reglas de seguridad.

Una medida de base MBD relacionada con la disponibilidad es una tasa de disponibilidad expresada en porcentaje de un componente del componente elemental asociado. Los valores de la tasa de disponibilidad son por ejemplo, 100%, 75%, 50%, 25% y 0%, cuando la disponibilidad del componente asociado es completamente disponible, pendiente, peligroso, crítico o desconocido, respectivamente. Por ejemplo, las medidas de base MBD de un terminal son medidas de tasas de disponibilidad de varias aplicaciones de oficina automáticas y de varios periféricos de los tipos de impresora y escáner directamente conectados al terminal. Dos medidas derivadas MDD relacionadas con este ejemplo de disponibilidad son el promedio de las tasas de disponibilidad de las aplicaciones y el promedio de las tasas de disponibilidad de los periféricos medidos en los puertos del terminal conectado a los periféricos. La métrica MED para este ejemplo de disponibilidad es una relación lineal de dos promedios de las tasas de disponibilidad proporcionadas con diferentes factores y representa una disponibilidad del terminal en el campo de la automatización de oficinas. De acuerdo con otro ejemplo, las medidas de base relativas a la disponibilidad de un servidor de servicio podrían basarse en los recuentos de contadores de usuarios visitantes para aplicaciones de servicio predeterminadas durante un período de tiempo dado y/o en el número de puertos abiertos y el número de puertos cerrados de protocolos predeterminados.

La medida de base MBA relacionada con la garantía de conformidad es una tasa de garantía que expresa en porcentaje, que se garantiza un paso o un proceso de operación del componente elemental asociado para cumplir con una o más reglas de una política de seguridad preestablecida. Los valores de la tasa de garantía son, por ejemplo, 100%, 75%, 50%, 25% y 0%, cuando el paso o el proceso de operación es conforme completamente, está un poco alterado, bastante alterado, fuertemente alterado y no es conforme, respectivamente. Por ejemplo, las medidas de base MBA para la garantía de conformidad de un acceso remoto a un servidor de autenticación están relacionadas con un control de la instalación para una prohibición de acceso a usuarios predeterminados en el servidor y con un control de una autenticación mutua entre el servidor y un terminal de usuario para abrir una sesión segura. La medida derivada MDA relacionada con este ejemplo de garantía de conformidad es el valor mínimo de las tasas de garantía asociadas con los dos controles previos, que expresa el acceso al servidor de autenticación para que sea seguro de manera remota. La métrica MEA para este ejemplo de garantía de conformidad es el valor mínimo de la medida derivada MDA previa, y de otra medida derivada que expresa medidas de base relacionadas con el control de solicitudes de un protocolo de transporte particular en una interfaz de conexión de servidor y representa, una garantía de conformidad de un acceso al servidor de autenticación de acuerdo con el protocolo de transporte particular.

Una estructura de datos SDI para determinar un indicador de intrusión II podría ser registrada en el formato IODEF (“Formato de Intercambio de Descripción de Objeto de Incidencia”) de la recomendación 5070 de la RFC y ser definida, entre otras, por una clase del componente elemental BI involucrado en la incidencia relacionada con la intrusión, una instancia que indica el tipo del componente infectado por la incidencia, los instantes iniciales y finales de la incidencia, el tipo de incidencia y la descripción de la historia de la incidencia, contribuyendo a la trazabilidad de la incidencia, y la descripción de una acción para remediar la incidencia. En particular, la estructura de datos SDI comprende una métrica MEI que depende de los recuentos de contadores para incidencias de intrusión, como medidas de base, asociados con factores de gravedad y un tipo de incidencia. Un contador de incidencias de intrusión se incrementa en una unidad tan pronto como la unidad de gestión, que incluye el contador de incidencias, detecta una incidencia de intrusión respectiva en el componente elemental BI correspondiente al factor de gravedad y al tipo de incidencia asociada con el contador de incidencias, y se decrementa cuando se supera tal incidencia. El factor de gravedad asociado con un contador de incidencias es tanto mayor cuanto más seria es la incidencia. Los contadores de incidencias incluidos en las unidades de gestión UGI asociadas con el componente BI podrían categorizarse por tipo de incidencia. Por ejemplo, el componente elemental BI se asocia con tres contadores de

incidencias asociados con un tipo de incidencia y con factores de gravedad representativos de una incidencia menor, una incidencia media y una incidencia mayor. Los recuentos de los tres contadores de incidencias, como medidas de base MBI, se combinan en una medida derivada MDI dependiente de los factores de gravedad, y la medida derivada MDI relativa a tipos de incidencias de una categoría común se combina en una métrica de incidencia MEI que representa la gravedad de las incidencias de esta categoría ocurridas y no superadas en el componente elemental BI. Una incidencia en un equipo o una aplicación podría ser un ataque más o menos grave, como por ejemplo, la intrusión de un comando en un programa defectuoso por un atacante para instalar una secuencia de comandos descargada, la inyección de un código malicioso en una parte de una aplicación para modificar su código y llevar a cabo comandos particulares, en respuesta a un mensaje o paquete duplicado, una saturación de un servidor de asignación de direcciones IP o de un enlace conectado al servidor a través de un desbordamiento con un elevado número de peticiones, etc.

Una estructura de datos SDV para determinar un indicador de vulnerabilidad IV de un componente elemental BI comprende una métrica MEV que es representativa de la estimación del impacto de un fallo de seguridad en el componente elemental BI al que está relacionado. Un fallo de seguridad es una amenaza potencial y podría permitir a un intruso acceder, más o menos fácilmente, al componente elemental. Podría ser un fallo resultante de errores de programación de una aplicación o que se produce tras la instalación de una nueva aplicación en un equipo que permite, por ejemplo, acceder a datos confidencias o la apertura de un puerto, una interpretación errónea de una secuencia de comandos o un comando, etc. La estructura de datos SDV incluye una métrica de vulnerabilidad MEV que estima el impacto de fallos de seguridad de una misma categoría. Cada fallo de esta categoría está definido por una tasa de confianza en el impacto del fallo en el componente elemental BI, un factor de gravedad y un tipo del fallo. La estructura de datos SDV además comprende un nombre corto y una descripción detallada del fallo de seguridad de esta categoría, soluciones para superar el fallo, y referencias a bases de conocimiento de vulnerabilidad relativas al fallo y mantenidas por terceros. Una referencia se caracteriza por un único identificador y el nombre de la base de conocimiento, como por ejemplo, las bases CVE (“Vulnerabilidades y Exposiciones Informáticas”) y Bugtraq. Por ejemplo, una unidad de gestión asociada con el componente BI incluye un contador de vulnerabilidad asociado con un factor de gravedad y un tipo de fallo que tiene su recuento, como una medida de base, siendo incrementado por la tasa de confianza de un fallo notificado a la unidad de gestión y que tiene un factor de gravedad y un tipo asociado con la unidad de gestión. Los contadores de vulnerabilidad incluidos en las unidades de gestión OGV asociadas con el componente elemental BI podrían clasificarse por factor de gravedad y tipo de fallo. Para un tipo de fallo, podrían contemplarse tres factores de gravedad, bajo, medio y alto. Una medida derivada MDV combina los recuentos de los tres contadores de vulnerabilidad, como medidas de base MBV, como una función de los factores de gravedad. Una métrica de vulnerabilidad MEV que representa la vulnerabilidad de fallos de una categoría combina las medidas derivadas MDV de una categoría de fallos en el componente BI como una función de los tipos de fallos.

La unidad de estandarización de datos UU trasmite las estructuras uniformes de datos SDD, SDI, SDV y SDA a la unidad de determinación de indicadores UDI.

Cada componente elemental BI en la unidad UDI se caracteriza más específicamente por la siguiente información que se memoriza en la unidad UI:

- una criticidad CR que indica la importancia del componente elemental en comparación con la necesidad de que el usuario del sistema SY sea definido preliminarmente por el administrador del dispositivo de supervisión DS y que sea una función de la implementación y del papel del componente elemental BI que juega en la actividad empresarial del usuario. Por ejemplo, la criticidad de un servidor o un enrutador es mayor que la de un terminal de usuario, y la criticidad de una aplicación de autenticación en un equipo es mayor que un servicio o una aplicación de automatización de oficina;

- estructuras uniformes de datos SDD, SDI, SDV y SDA del componente elemental con el objetivo de determinar respectivamente los indicadores de disponibilidad ID, de intrusión II, de vulnerabilidad IV y de garantía de conformidad IA del componente elemental; y

- los indicadores de seguridad de disponibilidad ID, de intrusión II, de vulnerabilidad IV y de garantía de conformidad IA que resultan en el nivel general de seguridad del componente elemental; y,

si el componente es un componente subordinado, tal como un componente de reunión BIg, que comprende varios componentes elementales supervisados, en los indicadores de seguridad de los componentes origen que contiene.

Un componente de reunión BIg también se supervisa gracias a la determinación de un indicador de disponibilidad, un indicador de intrusión, un indicador de vulnerabilidad y un indicador de garantía de conformidad. Cada uno de estos indicadores depende de indicadores del mismo tipo de los componentes elementales que contienen los componentes de reunión y no depende directamente de ninguna métrica específica del componente de reunión. Las métricas se asocian sólo con componentes elementales.

El método de determinación de un indicador de seguridad se ilustra en la FIG. 2 y comprende las etapas DI1 a DI6 para determinar un indicador, referido por I, de un componente elemental BI, que es uno de los indicadores ID, II, IV

e IA del componente BI tal como un equipo, o un hardware o una parte de software del mismo o una aplicación o parte de la misma. La determinación del indicador I se activa automáticamente para el componente BI cada vez que una medida de base MBm del componente del que depende el indicador I se modifica adicionalmente a un evento o comportamiento predeterminado detectado en el componente elemental por una UGm de las unidades de gestión asociadas con el componente elemental, en el paso DI1. El indicador I del componente BI también se determina automáticamente cada vez que un indicador de seguridad Igp del mismo tipo que el indicador I y asociado con un componente elemental origen BIP incluido en el componente BI, como un componente subordinado, se actualiza, como se detallará más adelante. Todos los datos actualizados resultantes de la modificación de una medida de base MBm se guardan en las unidades UU y UDI de modo que se utilicen para actualizaciones posteriores de los indicadores, como resultado de modificaciones de otras medidas de base. Preliminarmente, antes de que se implemente el dispositivo de supervisión DS, su administrador ha introducido la jerarquía en forma de árbol de los componentes supervisados en el sistema SY para memorizarla en la unidad UDI. Un ejemplo de una jerarquía en forma de árbol se muestra esquemáticamente en la FIG. 5 que se describirá más adelante. Todas las funciones referidas de aquí en adelante como “algoritmos” para determinar medidas derivadas, métricas e indicadores pueden ser parametrizadas por el administrador del dispositivo DS a través de la interfaz IHM en las fases de configuración.

La actualización de las medidas de base MBm del componente elemental BI, denominada como una interpretación, se produce si un comando, o una incidencia, es recibido por la unidad de gestión UGm asociada con el componente BI y gestiona la medida de base MBm, modificando así el valor de la medida de base MBm, en el paso DI1. La unidad de gestión UGm contiene un algoritmo de interpretación específico para variar la medida de base MBm. La unidad de estandarización de datos UU reestima en el paso DI2 la medida derivada Mdm que depende de la medida de base modificada MBm y de las otras medidas de base MB asociadas con el componente BI e interdependientes con la medida de base MBm de acuerdo con otro algoritmo de interpretación específico AMD incluido en la unidad UU. Entonces, la unidad UU reestima y memoriza en el paso DI3 la métrica MEm que depende de la medida derivada reestimada MDm y de las otras medidas derivadas MD asociadas con el componente BI de acuerdo con un algoritmo de estandarización específico AME incluido en la unidad UU. La unidad UU constituye una estructura de datos SD especialmente con la medida derivada reestimada MDm.

La unidad de determinación de indicadores UDI determina entonces automáticamente el indicador I del componente BI dependiendo de la métrica actualizada reestimada MEm, mientras que realiza respectivamente algoritmos de agregación implementados en la unidad UDI, de acuerdo con los tres siguientes pasos DI4, DI5 y DI6. Estos algoritmos agregan variables homogéneas y respetan el formalismo establecido por la unidad UDI. Para cada uno de los indicadores de seguridad ID, II, IV e IA, tres algoritmos de agregación específicos para el indicador de seguridad pueden haber sido preseleccionados en una librería de algoritmos de la unidad UDI por el administrador del dispositivo de supervisión DS, respetando el formalismo establecido por la unidad UDI. Estos algoritmos son intercambiables y se pueden parametrizar en función de las necesidades del usuario del sistema, especialmente de la arquitectura del sistema informático SY y de los tipos de los componentes supervisados que contiene. Los algoritmos incluidos por defecto en la librería son, por ejemplo, el mínimo, el máximo y el promedio ponderados por las criticidades de los componentes origen contenidos en el componente elemental BI, cuyo indicador debe determinarse. El administrador podría agregar otros algoritmos para resolver problemas específicos.

En el paso DI4, la unidad de determinación de indicadores UDI agrega la métrica reestimada MEm en el paso DI3 y, si existen, una o más métricas memorizadas ME del componente elemental BI relacionadas con el mismo tipo de indicador, mientras aplica un algoritmo de agregación de métricas AAM en estas métricas para producir una métrica de agregación MEA (BI) del componente BI. Por ejemplo, si el componente BI tiene otra métrica ME y si el algoritmo AAM se basa en el mínimo, la métrica de agregación es:

MEA(BI) = AAM(MEm, ME) = min(MEm, ME).

En el paso DI5, la unidad UDI agrega indicadores Igp de los componentes origen BIgp incluidos en el componente BI, si el componente BI incluye al menos un componente origen BIgp, o más generalmente, si es un componente compuesto. La unidad UDI aplica a este fin un algoritmo de agregación de indicador AAI del componente origen en los indicadores Igp para producir un indicador de agregación IA (BI) del componente origen. Por ejemplo, si el componente BI, como un equipo informático, incluye tres componentes origen BIgp1, BIgp2 y BIgp3 que tienen indicadores Igp1, Igp2 e Igp3, como aplicaciones implementadas en el equipo, y si el algoritmo AAI se base en el promedio ponderado por las criticidades CRgp1, CRgp2 y CRgp3, el indicador de agregación del componente origen es:

IA(BI) = AAI(Igp1, Igp2, Igp3), es decir

IA(BI) = [CRgp1 x Igp1 + CRgp2 x Igp2 + CRgp3 x Igp3]/[CRgp1 + CRgp2 + CRgp3].

En el paso DI6, la unidad UDI agrega los resultados MEA(BI) e IA(BI) de las agregaciones previas, si existen, aplicando un algoritmo de agregación general AAG sobre estos resultados para producir el indicador actualizado I del componente BI. Por ejemplo, el algoritmo AAG se basa en el máximo, y el indicador actualizado es:

I(BI) = AAG(MEA(BI), IA(BI)) = max(MEA(BI), IA(BI)).

Si el componente BI, como un componente origen, está incluido en uno o más componentes subordinados BIe de acuerdo con la jerarquía en forma de árbol de los componentes supervisados del sistema SY, como una aplicación, o un equipo, o un módulo de hardware o de software incluido como un componente elemental en un componente de reunión BIg, tal como una red, un servicio o un sitio, el indicador de seguridad de cada componente subordinado BIe hereda automáticamente la actualización del indicador I del componente elemental BI. Preliminarmente, para cualquier componente subordinado BIe y en particular, para cualquier componente de reunión BIg, el método comprende un paso de reunión inicial DI0 para configurar en la unidad UDI el componente subordinado BIe con los identificadores de los componentes elementales BI que contiene.

Con el fin de actualizar el indicador de seguridad del componente subordinado BIe, la unidad UDI realiza entonces el paso DI7, similar al paso DI5, y si el componente subordinado no es un componente de reunión BIg, el paso DI8 es similar al paso DI6. En el paso DI7, la unidad UDI agrega indicadores Ip de los componentes origen BIp incluidos en el componente BIe, incluyendo el indicador I del componente BI, si el componente BIe incluye al menos un componente origen, o más generalmente, si es un componente compuesto. La agregación se realiza aplicando un algoritmo de agregación de indicador AAIe específico del componente subordinado BIe sobre los indicadores Ip de los componentes origen BIp y sus criticidades, para producir un indicador de agregación IA(BIe) del componente origen. En el paso DI8, si el componente subordinado BIe no es un componente de reunión y es un componente elemental asociado con al menos una métrica MEA(BIe), la unidad UDI agrega la métrica de agregación MEA (BIe) del componente subordinado BIe memorizada en la unida UDI y el indicador de agregación IA(BIe) del componente origen que resulta de la agregación previa, mientras se aplica un algoritmo de agregación general AAGe específico del componente subordinado BIe sobre las variables MEA(BIe) e IA(BIe) para producir el indicador actualizado I(BIe) del componente subordinado BIe.

Pasos similares a los pasos DI7 y DI8 son realizados por la unidad UDI para actualizar los indicadores del mismo tipo que el indicador I del componente BI, asociados a todos los componentes, incluido el componente BI, para todas las “generaciones” del componente para heredar la actualización del indicador I en el árbol de jerarquía del sistema SY. Por ejemplo, el componente BI es una aplicación Ap incluida en un servidor Sr1, incluida también en una Res1 de las redes localizadas en un sitio geográfico Si1. El servidor Sr1 está involucrado en un servicio Sc1. Los indicadores del mismo tipo que el indicador actualizado de la aplicación Ap, asociados al servidor Sr1, se actualizan primero. Luego, los indicadores del mismo tipo asociados a la red Res1, al servicio Sc1 y al sitio Si1 se actualizan respectivamente.

La interfaz hombre-equipo IHM muestra rápidamente de forma comprensible la propagación del impacto de la modificación de cualquier medida de base o de cualquier indicador a través del sistema supervisado SY. Por ejemplo, la propagación del probable impacto de la indisponibilidad de un servidor, o de una incidencia detectada durante el funcionamiento de una aplicación, o de una infección de una página o de una secuencia de comandos que se descarga en un equipo, o un incumplimiento de una actualización de una aplicación, se presenta inmediatamente en la pantalla de la interfaz IHM en el sistema modelado SY.

Por lo tanto, de acuerdo con la invención, la unidad de determinación de indicadores UDI considera orientaciones diferentes de análisis relativas a los componentes de reunión BIg que son:

- una orientación a una o más de las redes informáticas a las que pertenecen los equipos informáticos, incluyendo, a su vez, aplicaciones;

- una orientación a uno o más servicios relacionados con los trabajos de los usuarios y necesarios para las actividades de la empresa propietaria del sistema supervisado SY; y

- una orientación a uno o más sitios que representan la distribución geográfica de los componentes de hardware y de software de la empresa.

Estas orientaciones son integrales con un modelo único que contiene el conjunto de componentes a supervisar en el sistema SY, las relaciones que tienen entre sí y las divisiones jerárquicas correspondientes a las orientaciones descritas anteriormente. Tan pronto como se actualiza un indicador para un componente, la unidad UDI determina automáticamente los indicadores de todos los componentes impactados de acuerdo con estas orientaciones.

Además, la unidad de determinación de indicadores UDI considera el estado conectado o desconectado de los equipos en el sistema informático SY, por ejemplo mediante el control de la apertura de puertos, para comprobar el perímetro de supervisión de cada usuario autorizado a utilizar al menos uno de los equipos y al menos uno de los servicios del sistema SY. El perímetro de supervisión representa el conjunto de componentes que el usuario está autorizado a supervisar. La unidad UDI evalúa así el estado general de seguridad en el perímetro de supervisión del usuario conectado y la interfaz IHM podría presentar el impacto de la modificación de cualquier medida de base o de cualquier indicador en el perímetro de supervisión con el fin de, más específicamente, invitar al usuario a no emprender o detener ciertas acciones y comandos que serían perjudiciales para sus trabajos.

De manera más general, en función de las modificaciones de los indicadores de seguridad ID, II, IV e IA procesados por la unidad UDI, esta última es capaz de definir un plano de reacción que debe ser iniciado por el administrador del dispositivo de supervisión DS. Por ejemplo, la unidad UDI establece una lista que asocia, para cada componente, los

cuatro indicadores de seguridad, los fallos actuales, una incidencia y el plano de reacción asociado. La unidad UDI transmite la lista a la interfaz IHM que la presenta claramente de acuerdo con una organización particular, tal como se ilustra en la FIG. 5.

Con el fin de entender mejor las ventajas de la invención, se detalla a continuación un ejemplo del impacto de una anomalía detectada en una sonda, a través de un sistema informático SY. Como se muestra en la FIG. 3, el sistema informático se implementa esencialmente en dos sitios diferentes SI1 y SI2 de una empresa en dos ciudades diferentes. El sistema informático SY requiere el posicionamiento de una red global dividida en una red RS de servidores SE y dos redes de usuarios RU1 y RU2 a la vez en los sitios SI1 y SI2. Cada red de usuarios RU1, RU2 comprende un servidor SE1, SE2 y terminales TU1, TU2 conectados por un conmutador CU1, CU2. La red de servidores RS se instala en un centro informático del primer sitio SI1, que comprende un enrutador RO1 que da servicio a las redes RS y RU1. Las redes RS, RU1 y RU2 están supervisadas, en términos de seguridad, por una red de hipervisión RH a través de una red segura dedicada RSD de un operador de telecomunicaciones que comprende, entre otros, enrutadores RO. La red de hipervisión RH se instala en el primer sitio SI1 y comprende, más específicamente, un dispositivo de supervisión de seguridad DS, de acuerdo con la invención, conectado a un servidor de hipervisión SEH, conectado a través de un corta-fuegos PH a un enrutador RO de la red segura dedicada RSD.

La empresa pone a disposición de sus usuarios-empleados un servicio de acceso a una mensajería electrónica de “Correo Web” a través de una página Web. En la red de servidores RS, el servicio de Correo Web es proporcionado por un servidor Web y un servidor de Correo electrónico y requiere la presencia de un servidor de nombres de dominio DNS (“Sistema de Nombres de Dominio”) y de un servidor de asignación dinámica de direcciones DHCP (“Protocolo de Configuración Dinámica de Anfitrión”). La red de servidores RS comprende además un servidor de acceso a directorios de información de usuario LDAP (“Protocolo Ligero de Acceso a Directorios”), un conmutador CS conectado a los servidores y un corta-fuegos PRS a cargo de la protección de los servicios prestados por los servidores en la red RS.

La información de seguridad procedente de la red de servidores RS de las redes de usuarios RU1 y RU2 y de la red de hipervisión RH se notifica por sondas, como unidades de gestión UG, dispuestas en estas redes para el dispositivo de supervisión de seguridad DS. Con el fin de no sobrecargar la FIG. 3, se representan esquemáticamente algunas sondas SS, SPRS, SU1, SS1, SU2, SS2 y SPH en estas redes.

Se asume que la anomalía detectada en una sonda SPRS se relaciona con una medida de base MBA relacionada con la garantía de conformidad del corta-fuegos PRS en la red de servidores RS. El siguiente escenario mostrado en la FIG. 4, muestra cómo se propaga el impacto de un fallo de conformidad del corta-fuegos PRS en las redes, servicios y sitios supervisados y se notifica al dispositivo DS.

Inicialmente, todos los controles realizados en el sistema supervisado SY notifican una conformidad total con la política de seguridad preestablecida. Por lo tanto, las tasas de garantía MBA, como medidas de base, relacionadas con todos los componentes informáticos supervisados mencionados anteriormente en el sistema SY son del 100%.

Más específicamente en el corta-fuegos PRS que protege el servicio de Correo Web, se vigilan dos métricas por sondas SPRS: la gestión remota MEA1 y el filtrado MEA2, como se muestra en la FIG. 4. Las métricas MEA1 y MEA2 requieren medidas de base MBA11 y MBA21 para controlar los protocolos de acceso remoto de parametrización, tales como UDP (“Protocolo de Datagrama de Usuario”), TCP (“Protocolo de Control de Transmisión”) e ICMP (“Protocolo de Mensajes de Control de Internet”) y la escucha de conexiones por estos protocolos al corta-fuegos PRS, y medidas de base MBA12 y MBA22 para controlar la integridad de los archivos de parametrización de las reglas de filtrado y su adecuación a la política de seguridad. Estas medidas de base se realizan periódicamente.

La unidad de estandarización de datos UU combina las medidas de base MBA11 y MBA12 en medidas derivadas MDA11 y MDA12 y las medidas de base MBA21 y MBA22 en medidas derivadas MDA21 y MDA22, y las medidas derivadas MDA11 y MDA12 en la métrica MEA1 y las medidas derivadas MDA21 y MDA22 en la métrica MEA2. La unidad de determinación de indicadores UDI combina las métricas MEA1 y MEA2 en un indicador de garantía de conformidad IAPRS para el componente elemental formado por el corta-fuegos PRS. Como todos los controles resultan en una conformidad total, las medidas de base, las medidas derivadas, las métricas y el indicador de garantía están en un estado “verde” correspondiente a tasas de garantía del 100%.

Tras los controles en el corta-fuegos PRS, una sonda SPRS detecta una anomalía en las reglas de filtrado, por ejemplo al detectar que un protocolo TCP no seguro se declara como autorizado mientras que la política de seguridad estipula que no debe serlo.

Automáticamente, el indicador de garantía de conformidad IAPRS del corta-fuegos PRS se determina de nuevo de la siguiente manera. La medida de base MBA21 relativa al filtrado del protocolo TCP cambia a un estado de no conformidad “rojo”. Suponiendo que la función de interpretación de la medida derivada MDA21 relativa al filtrado de protocolos estipula que su valor es una función del valor mínimo de las medidas de base MBA21 de las que depende, la medida derivada MDA21 cambia a un estado “rojo”. Suponiendo que la función de estandarización de la

métrica MEA2 relativa al filtrado estipulado es el mínimo de las medidas derivadas MDA21 y MDA22 de las que depende, la métrica MEA2 también cambia a un estado “rojo”. Suponiendo que la función de agregación para el indicador de garantía IAPRS del corta-fuegos PRS es el promedio ponderado de las métricas MEA1 y MEA2 y que el peso de la métrica de filtrado MEA2 es mayor que el de la métrica de administración remota MEA1, el indicador IAPRS del corta-fuegos PRS cambia a un estado “naranja oscuro” (rayado doble) para dar como resultado una garantía fuertemente no conforme, por ejemplo correspondiente a una tasa de garantía que varía entre el 25% y el 49%. Los miembros de rayado doble en la FIG. 4 ilustran una primera indicación del impacto de la anomalía detectada en el componente PRS directamente relevante.

La unidad UDI en el dispositivo de supervisión DS también propaga el impacto de la anomalía detectada a todos los componentes informáticos subordinados de Correo Web SI1, RS y SY que dependen del componente PRS relevante.

Al proteger el corta-fuegos PRS el servicio de Correo Web, la garantía de conformidad se altera. El impacto depende del algoritmo de agregación relativo a los indicadores de garantía de los componentes incluidos en el servicio de Correo Web. Este algoritmo de agregación es por ejemplo, un promedio de los indicadores de garantía de los componentes ponderados por el peso del corta-fuegos PRS y por los pesos de los otros componentes supervisados definidos en el servicio. Suponiendo que el indicador IAPRS del corta-fuegos tiene un peso muy bajo, el indicador de garantía IAWM del servicio de Correo Web apenas se ve afectado y cambia a un estado apenas alterado “amarillo” (línea de puntos), correspondiente por ejemplo a un tasa de garantía que varía entre el 75% y el 99%. Esto es interpretado como un bajo impacto en los terminales de usuario que utilizan el servicio de Correo Web.

En el primer sitio SI1, el corta-fuegos PRS juega un papel importante, pero entre otros componentes. El indicador de garantía IASI1 del sitio SI1 también se altera apenas y cambia a un estado “amarillo” (línea de puntos). Esto se interpreta como un bajo impacto físico.

Cualquier componente de la red de servidores RS se considera indispensable. La alteración del indicador de garantía de tal componente, como el indicador IAPRS del corta-fuegos PRS, se interpreta en la unidad UDI como la de toda la red RS, que depende de un algoritmo de agregación basado en el mínimo de los indicadores de garantía de los componentes supervisados incluidos en la red RS. La red de servidores RS tiene por lo tanto, un indicador de garantía IARS fuertemente alterado y cambia a un estado “naranja oscuro” (rayado doble) como el indicador de garantía IAPRS. Esto se interpreta como un impacto muy fuerte en la red RS.

En el sistema informático supervisado SY, la red de servidores RS se considera como más importante que las redes de usuarios RU1 y RU2 y que la red de hipervisión RH. El algoritmo de agregación para la garantía de conformidad del sistema SY es por ejemplo, un promedio de los indicadores de garantía IARS, IARU1, IARU2 e IARH de las redes RS, RU1, RU2 y RH ponderado por los pesos bajos de las redes RU1, RU2 y RH y por el mayor peso de la red RS. El sistema SY tiene por lo tanto, un indicador de garantía IASY ligeramente alterado y cambia al estado “naranja” (rayado simple), por ejemplo correspondiente a una tasa de garantía que varía entre el 50% y el 74%. Esto se interpreta como un impacto fuerte en el sistema SY.

Como se muestra en la FIG. 5, la consola de supervisión en la interfaz hombre-equipo IHM muestra, entre otros, los estados de seguridad del servicio de Correo Web, de los sitios SI1 y SI2 y del sistema SY relativos a sus indicadores de garantía de conformidad IAWM, IASI1, IASI2 e IASY con los indicadores de garantía de conformidad de los componentes origen respectivos de los que heredan. Parece que la detección de una anomalía de no-conformidad en el corta-fuegos PRS se transmite simultáneamente de acuerdo con las tres orientaciones de las redes, los servicios y los sitios geográficos. La detección de la anomalía ha llevado a un bajo impacto para los usuarios y a un problema que debe superarse con urgencia por el servicio informático de la empresa, para remediar un fallo significativo de la seguridad de la red de servidores RS.

La invención descrita aquí se refiere a un método y a un dispositivo para la supervisión de la seguridad de un sistema informático SY que comprende varios componentes informáticos elementales BI. De acuerdo con una implementación, los pasos del método de la invención se determinan por las instrucciones de un programa informático incorporado en la estación base. El programa que se puede implementar en el dispositivo de supervisión de esta invención comprende instrucciones que, cuando dicho programa se lleva a cabo en el dispositivo de supervisión que tiene su funcionamiento entonces controlado a través del programa que se está llevando a cabo, realizan los pasos del método de acuerdo con la invención.

Por consiguiente, esta invención también se aplica a un programa informático, especialmente a un programa informático grabado sobre o en un medio de grabación legible por un ordenador y cualquier dispositivo de procesamiento de datos, adaptado para implementar esta invención. Este programa podría utilizar cualquier lenguaje de programación, y estar en forma de un código fuente, un código objeto o un código intermedio entre un código fuente y un código objeto tal como una forma parcialmente compilada o cualquier otra forma deseada para implementar el método de acuerdo con la invención. El programa podría descargarse en la estación base a través de una red de comunicación, tal como internet.

El medio de grabación puede ser cualquier entidad o dispositivo que sea capaz de almacenar el programa. Por ejemplo, el medio puede comprender un medio de almacenamiento, sobre el que se graba el programa informático de acuerdo con la invención, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico, o una llave USB, o un medio de grabación magnético, por ejemplo, un disco duro.

REIVINDICACIONES

1. Un método para supervisar la seguridad de un sistema informático (SY) que comprende:

varios componentes informáticos elementales (BI), siendo cada componente elemental supervisado en dependencia de medidas de base (MB) representativas de estados predeterminados del componente elemental, y

varios componentes de reunión (BIe, BIg) que reúnen cada uno varios componentes elementales, caracterizado por que comprende:

la determinación (DI6) de varios indicadores de seguridad (I) de diferentes tipos para cada componente elemental supervisado (BI), siendo determinado cada indicador de seguridad de acuerdo con funciones respectivas (AMD, AME, AAM, AAG) de medidas de base (MB) asociadas con el indicador de seguridad, en donde la determinación (DI6) de un indicador de seguridad de un tipo dado (I) para un componente elemental (BI) comprende, como resultado de una modificación (DI1) de una (MBm) de las medidas de base asociadas con el indicador de seguridad (I):

estimar (DI2) una primera medida derivada (MD) de acuerdo con una función (AMD) de la medida de base modificada (MBm) y al menos otra medida de base (MB) interdependiente con la medida de base modificada,

estimar al menos una segunda medida derivada (MD) estimada de acuerdo con una función de medidas de base (MB) interdependientes asociadas con el indicador de seguridad del tipo dado (I),

estimar (DI3) métricas (ME) de acuerdo con una función (AME) de dichas primera y segunda medidas derivadas (MD), y

determinar el indicador de seguridad del tipo dado de acuerdo con una función dependiente de al menos dichas métricas estimadas, y

determinar (DI7) varios indicadores de seguridad (IA(BIe)) de diferentes tipos para cada componente de reunión, siendo determinado cada indicador de seguridad de un tipo dado para cada componente de reunión de acuerdo con una función respectiva (AAIe) de los indicadores de seguridad (I) del tipo dado de los componentes elementales (BIp) reunidos en el componente de reunión (BIe, BIg).

2. El método de acuerdo con la reivindicación 1, en donde la determinación (DI6) del indicador de seguridad (I) del tipo dado en el componente elemental (BI) comprende una agregación (DI5) de indicadores de seguridad (I), del tipo dado en los componentes origen elementales (BIgp) incluidos en el componente elemental, en un indicador de agregación (IA(BI)), siendo determinado el indicador de seguridad (I) del componente elemental de acuerdo con una función (AAG) que depende de dichas métricas estimadas (ME) y del indicador de agregación (IA(BI)).

3. El método de acuerdo con la reivindicación 1 ó 2, en donde uno de los componentes de reunión es una red (RS; RU1; RU2) de equipos informáticos como componentes elementales reunidos en el componente de reunión.

4. El método de acuerdo con una de las reivindicaciones 1 a 3, en donde uno de los componentes de reunión es un servicio basado en aplicaciones, como componentes elementales reunidos en el componente de reunión.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en donde uno de los componentes de reunión es un sitio geográfico (SI1; SI2) que reúne equipos informáticos y/o redes como componentes elementales reunidos en el componente de reunión.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en donde uno (ID) de los indicadores de seguridad de cada componente elemental (BI) depende de medidas de base relativas a la disponibilidad del componente (BI).

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 6, en donde uno (II) de los indicadores de seguridad de cada componente elemental (BI) depende de medidas de base relativas a al menos un tipo de incidencia en el componente (BI) y a un factor de gravedad del tipo de incidencia.

8. El método de acuerdo con cualquiera de las reivindicaciones 1 a 7, en donde uno (IV) de los indicadores de seguridad de cada componente elemental (BI) depende de medidas de base relativas a la vulnerabilidad del componente (BI) y representativas de una estimación del impacto de al menos un fallo de seguridad de un tipo predeterminado en el componente (BI) y del factor de gravedad del fallo.

9. El método de acuerdo con cualquiera de las reivindicaciones 1 a 8, en donde uno (IA) de los indicadores de seguridad determinados del componente elemental supervisado (BI) depende de medidas de base relativas a una garantía de conformidad del componente (BI) con respecto a una política de seguridad preestablecida.

10. El método de acuerdo con cualquiera de las reivindicaciones 1 a 9, en donde las funciones (AMD, AME, AAM, AAG; AAIe, AAGe) pueden ser parametrizadas.

11. Un dispositivo (DS) para supervisar la seguridad de un sistema informático (SY) que comprende:

varios componentes informáticos elementales (BI), siendo el dispositivo capaz de recoger medidas de base (MB) asociadas con cada componente elemental y representativas de estados predeterminados del componente elemental, y

varios componentes de reunión (BIe, BIg) que reúnen cada uno varios componentes elementales, caracterizado por que comprende:

medios (UU, UDI) para determinar varios indicadores de seguridad (I) de diferentes tipos para cada componente elemental supervisado (BI), siendo determinado cada indicador de seguridad de acuerdo con funciones respectivas (AMD, AME, AAM, AAG) de medidas de base (MB) asociadas con el indicador de seguridad, en el que la determinación (DI6) de un indicador de seguridad de un tipo dado (I) para un componente elemental (BI) comprende, como resultado de una modificación (DI1) de una (MBm) de las medidas de base asociadas con el indicador de seguridad (I):

estimar (DI2) una primera medida derivada (MD) de acuerdo con una función (AMD) de la medida de base modificada (MBm) y al menos otra medida de base (MB) interdependiente con la medida de base modificada,

estimar al menos una segunda medida derivada (MD) estimada de acuerdo con una función de medidas de base (MB) interdependientes asociadas con el indicador de seguridad del tipo dado (I),

estimar (DI3) métricas (ME) de acuerdo con una función (AME) de dichas primera y segunda medidas derivadas (MD), y

determinar el indicador de seguridad del tipo dado de acuerdo con una función dependiente de al menos dichas métricas estimadas, y

medios (UDI) para determinar varios indicadores de seguridad (IA(BIe)) de diferentes tipos para cada componente de reunión, siendo determinado cada indicador de seguridad de un tipo dado para cada componente de reunión de acuerdo con una función respectiva (AAIe) de los indicadores de seguridad (I) del tipo dado de los componentes elementales (BIp) reunidos en el componente de reunión (BIe, BIg).

12. El dispositivo de acuerdo con la reivindicación 11, en donde un componente de reunión (BIg) es uno por lo menos de los siguientes componentes de reunión: una red (RS; RU1; RU2) de equipos informáticos como componentes reunidos elementales, un servicio (Correo Web) basado en aplicaciones como componentes elementales reunidos y un sitio geográfico (SI1; SI2) que reúne equipos informáticos y/o redes como componentes elementales reunidos.

13. El dispositivo de acuerdo con la reivindicación 11 ó 12, en donde los medios para determinar el indicador de seguridad del componente (UU, UDI; UDI) se adaptan para determinar al menos uno de los siguientes indicadores de seguridad para un componente elemental (BI) y un componente de reunión (BIg): un indicador de seguridad que depende de medidas de base relativas a la disponibilidad del componente (BI; BIg), un indicador de seguridad (II) que depende de medidas de base relativas al menos a un tipo de incidencia en el componente (BI; BIg) y a un factor de gravedad del tipo de incidencia, un indicador de seguridad (IV) que depende de medidas de base relativas a la vulnerabilidad del componente (BI; BIg) y representativas de una estimación del impacto de al menos un fallo de seguridad de un tipo predeterminado en el componente (BI; BIg) y de un factor de gravedad del fallo y un indicador de seguridad (IA) que depende de medidas de base relativas a una garantía de conformidad del componente (BI) con respecto a una política de seguridad preestablecida.

14. Un programa informático que puede ser implementado en un dispositivo de supervisión (DS) de la seguridad de un sistema informático (SY) que comprende varios componentes informáticos elementales (BI), estando supervisado cada componente elemental en dependencia de medidas de base (MB) representativas de estados predeterminados del componente elemental, y varios componentes de reunión (BIe, BIg) que reúnen, respectivamente, componentes elementales, caracterizado por que comprende instrucciones que, cuando el programa se lleva a cabo en el dispositivo de supervisión, realizan los pasos del método de acuerdo con cualquiera de las reivindicaciones 1 a 10.

FIG. 1

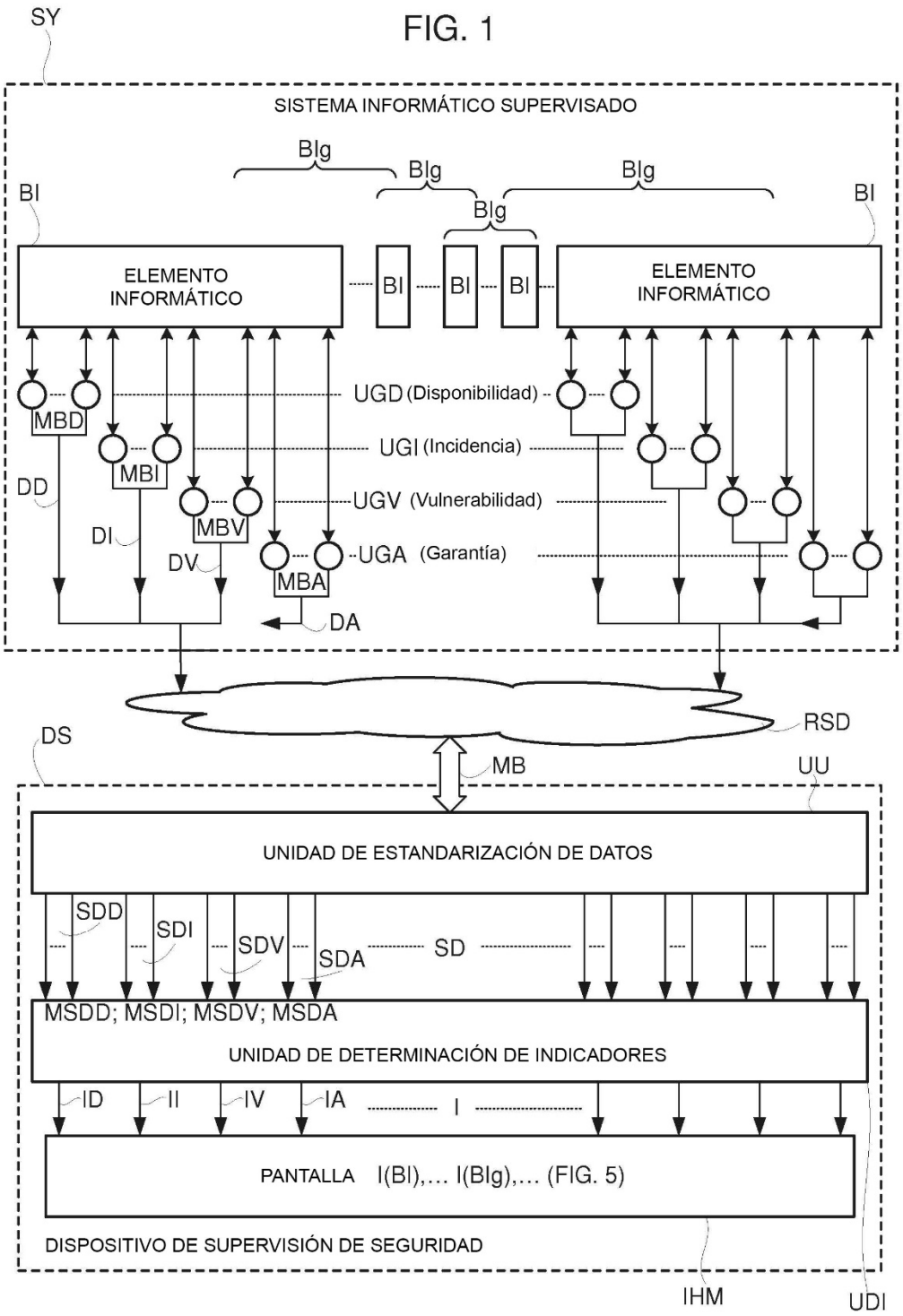

SY
SISTEMA INFORMÁTICO SUPERVISADO
BIg
BIg
BIg
BIg
BI
BI
ELEMENTO INFORMÁTICO
BI
BI
BI
ELEMENTO INFORMÁTICO
UGD (Disponibilidad)
UGI (Incidencia)
UGV (Vulnerabilidad)
UGA (Garantía)
MBD
MBI
MBV
MBA
DD
DI
DV
DA
RSD
DS
MB
UU
UNIDAD DE ESTANDARIZACIÓN DE DATOS
SDD
SDI
SDV
SDA
SD
MSDD; MSDI; MSDV; MSDA
UNIDAD DE DETERMINACIÓN DE INDICADORES
ID
II
IV
IA
I
PANTALLA I(BI),... I(BIg),... (FIG. 5)
DISPOSITIVO DE SUPERVISIÓN DE SEGURIDAD
IHM
UDI

FIG. 2

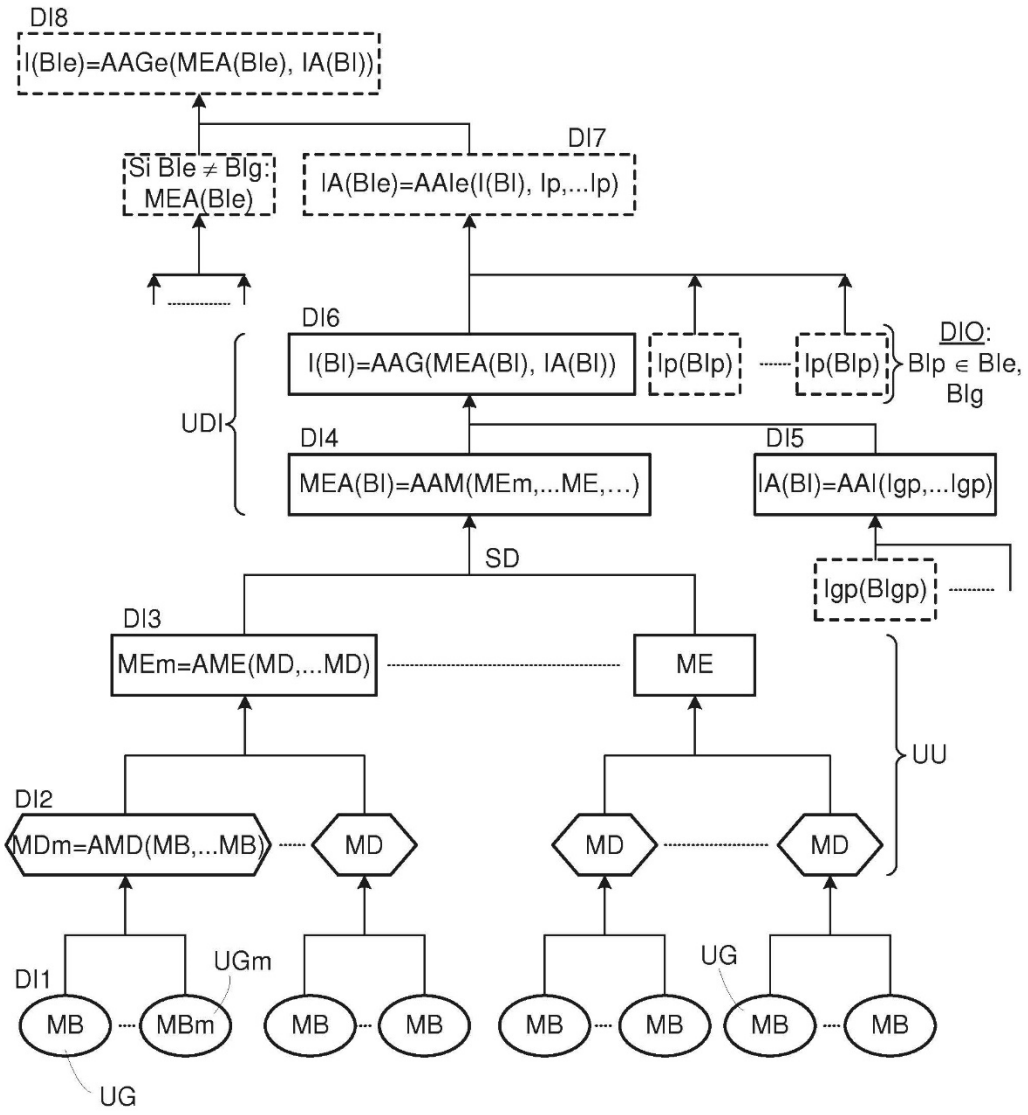

DI8
I(BIe)=AAGe(MEA(BIe), IA(BI))
DI7
Si BIe ≠ BIg:
MEA(BIe)
IA(BIe)=AAIe(I(BI), Ip,...Ip)
DI6
I(BI)=AAG(MEA(BI), IA(BI))
Ip(BIp)
Ip(BIp)
DIO:
BIp ∈ BIe, BIg
UDI
DI4
MEA(BI)=AAM(MEm,...ME,...)
DI5
IA(BI)=AAI(Igp,...Igp)
SD
Igp(BIgp)
DI3
MEm=AME(MD,...MD)
ME
UU
DI2
MDm=AMD(MB,...MB)
MD
MD
MD
DI1
UGm
UG
MB
MBm
MB
MB
MB
MB
MB
MB
UG

FIG. 3

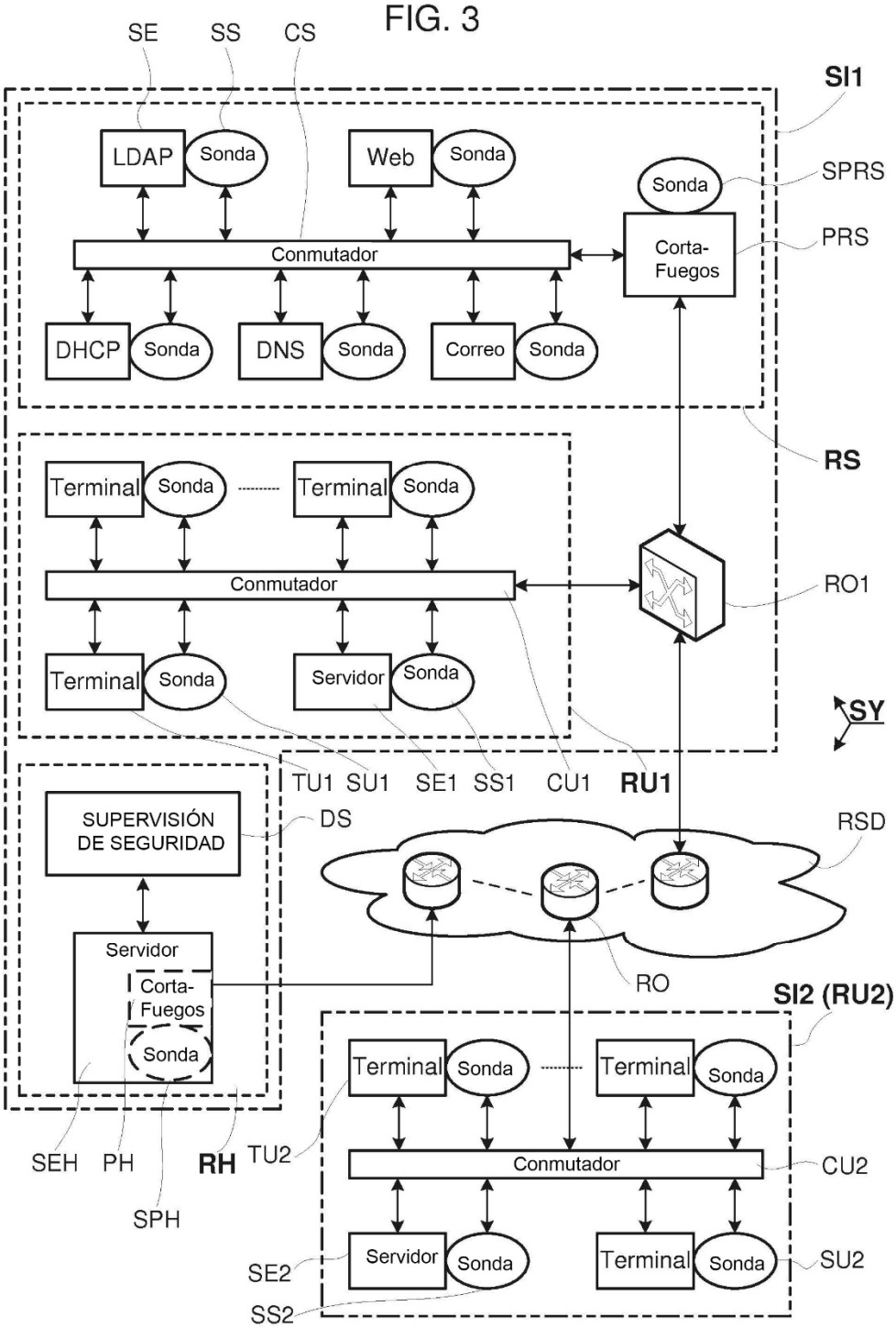

SE
SS
CS
SI1
LDAP
Sonda
Web
Sonda
Sonda
SPRS
Conmutador
Corta-
Fuegos
PRS
DHCP
Sonda
DNS
Sonda
Correo
Sonda
RS
Terminal
Sonda
Terminal
Sonda
Conmutador
RO1
Terminal
Sonda
Servidor
Sonda
SY
TU1
SU1
SE1
SS1
CU1
RU1
SUPERVISIÓN
DE SEGURIDAD
DS
RSD
Servidor
Corta-
Fuegos
Sonda
RO
SI2 (RU2)
Terminal
Sonda
Terminal
Sonda
SEH
PH
RH
TU2
Conmutador
CU2
SPH
Servidor
Sonda
Terminal
Sonda
SU2
SE2
SS2

FIG. 4

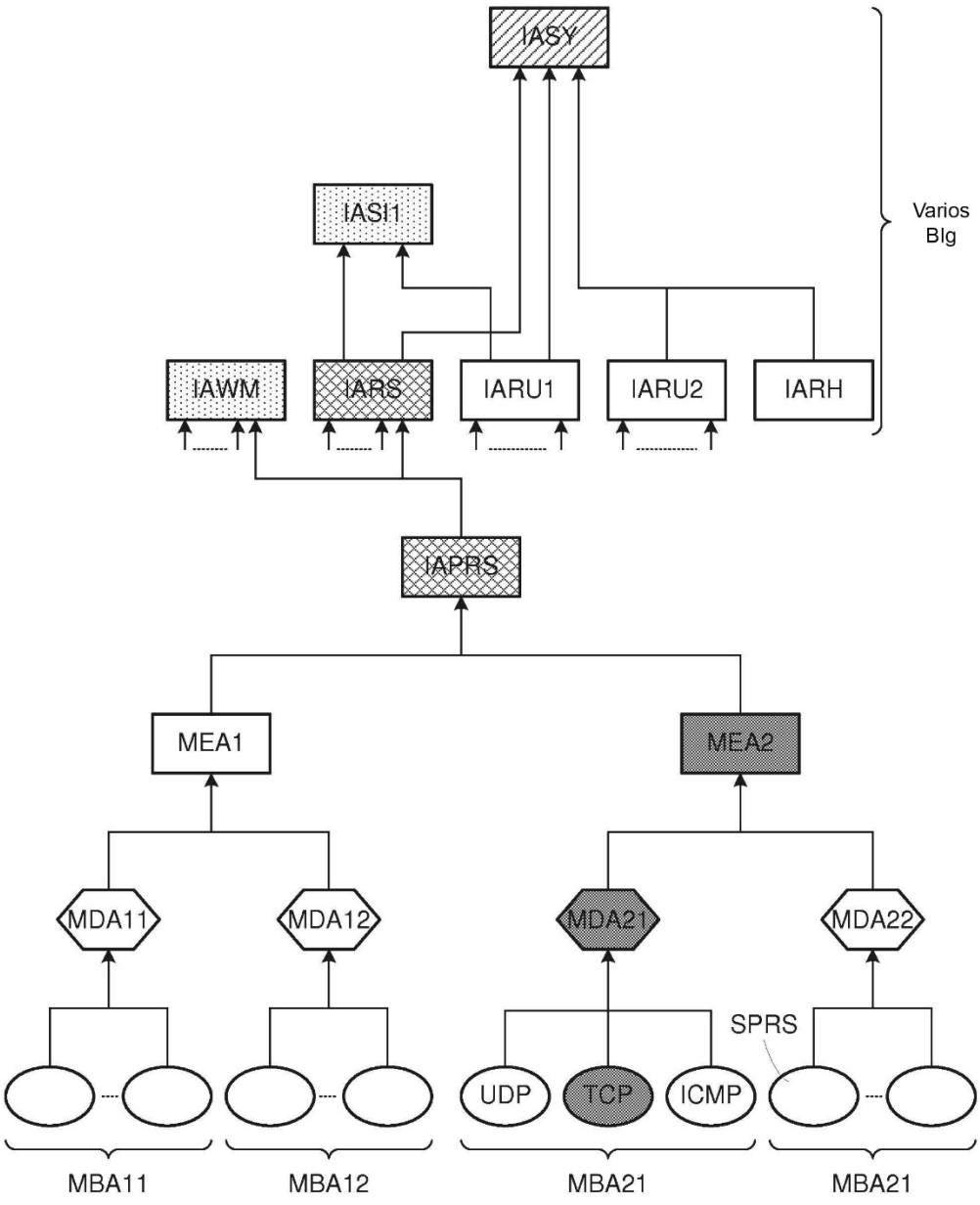
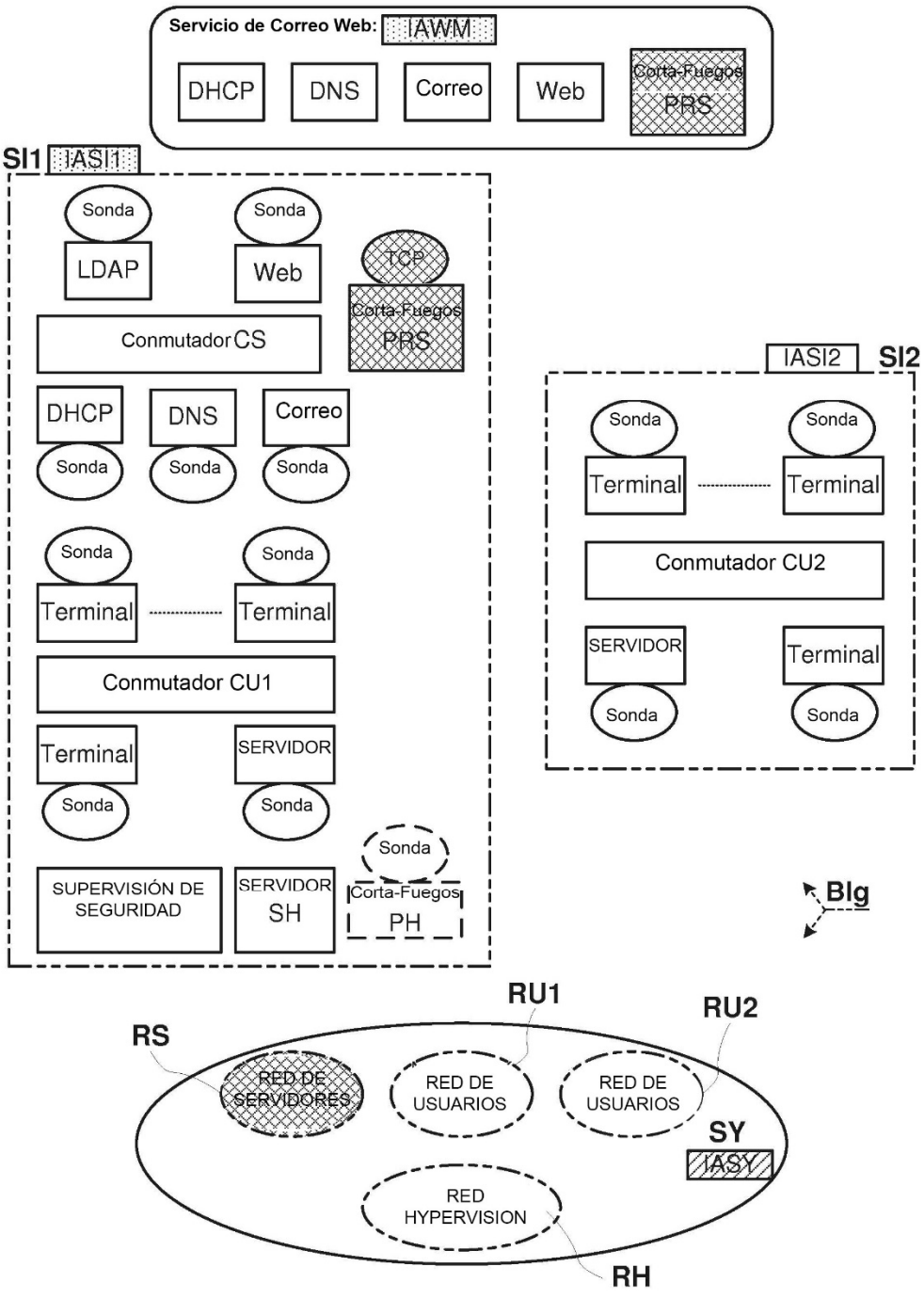

IASY
IASI1
Varios
Blg
IAWM
IARS
IARU1
IARU2
IARH
IAPRS
MEA1
MEA2
MDA11
MDA12
MDA21
MDA22
SPRS
UDP
TCP
ICMP
MBA11
MBA12
MBA21
MBA21

FIG. 5


Servicio de Correo Web:
IAWM
DHCP
DNS
Correo
Web
Corta-Fuegos PRS
SI1
IASI1
Sonda
LDAP
Web
TCP
Corta-Fuegos PRS
Conmutador CS
DHCP
DNS
Correo
Terminal
Conmutador CU1
SERVIDOR
SUPERVISIÓN DE SEGURIDAD
SERVIDOR SH
Corta-Fuegos PH
IASI2
SI2
Conmutador CU2
BIg
RU1
RU2
RS
RED DE SERVIDORES
RED DE USUARIOS
SY
IASY
RED HYPERVISION
RH