(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 532 806**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.09.2008 E 08165132 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.11.2014 EP 2169899**

(54) Título: **Sistema y un procedimiento para la detección de ataques distribuidos de denegación de servicio**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2015

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

ROSHANDEL, MEHRAN;
ZSEBY, TANJA y
HIRSCH, THOMAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y un procedimiento para la detección de ataques distribuidos de denegación de servicio

La presente invención se refiere a un sistema y un procedimiento para la detección de ataques distribuidos de denegación de servicio a través de una red basada en paquetes, en particular para la ampliación en tiempo real del dispositivo de medición del sistema mediante una definición métrica para la adaptación a ataques distribuidos de denegación de servicio.

Antecedente técnico

Los ataques a sistemas de computación por medio de la Internet se pueden dividir, esencialmente, en dos tipos de ataques, concretamente la intrusión en servicios de servidores y manipulación de los servicios; y la denegación de servicios (Denial of Service: DoS) mediante la generación de consultas sin sentido y/o automáticos, es decir ataques de saturación.

Los ataques de saturación pueden ser usados sobre diferentes recursos de destino. Además de la saturación de la infraestructura de red y ruteadores, ancho de banda también se observan ataques a aplicaciones. Es así que muchas consultas generadas automáticamente producen, la mayoría de las veces, una saturación de los servicio, por lo cual ya no están disponibles para usuarios normales, es decir se produce una denegación de servicio. La generación automática de estas consultas se hacen, por regla general, a partir de muchos ordenadores capturados, en particular memorias infectadas de un virus sin el conocimiento del usuario, de manera que este tipo de ataques es denominado ataque distribuido de denegación de servicio (Distributed Denial of Service, abreviatura: DDoS).

Los sistemas para la detección de ataques por medio de la red se conocen como Intrusion Detection System (IDS) o Anomaly Detection System (ADS). Detectan ataques mediante patrones característicos (en el caso de IDS) o mediante desviaciones respecto de un estado normal (en el caso de ADS).

Debido a que el atacante humano advierte si el ataque ha sido exitoso, variará constantemente las técnicas aplicadas mientras se lo rechace exitosamente. Por esta razón, también la estrategia de defensa debe ser adaptada permanentemente a las condiciones básicas. También la utilización regular de los servicios a proteger está en un cambio constante.

O sea, la defensa contra estos ataques presupone un sistema de medición que mediante una unidad de control puede ser adaptada permanentemente a las nuevas necesidades. De esta manera, los nuevos fenómenos pueden ser descritos y detectados mediante métricas características.

Los sistemas de medición puros convencionales o dispositivo de medición y componentes de medición de ADS e IDS no tienen dicha funcionalidad. Algunos dispositivos de medición según el estado actual de la técnica son, por ejemplo: IBM Aurora™, Lucent VitalSuite™, CA Spectrum™. IDS ejemplares son: Cisco Anomaly Detector™ con Cisco Guard™ y Radware DefensePro™. Las métricas más usuales son programadas como componentes del sistema de medición y pueden ser aplicadas en caso de necesidad. Nuevas métricas no pueden ser definidas y transmitidas al dispositivo de medición en tiempo real. Cuando el fabricante pone a disposición una nueva métrica es necesario un tiempo de paro de todo el sistema para integrar la nueva métrica al sistema.

Los documentos US-B-6785818 y US-A-20070094730 describen una detección de ataques de Registry Mapping o gusanos de ordenador. Este tipo de ataques se produce en otro plano, concretamente mediante el aprovechamiento de vulnerabilidades en un sistema o una red del atacado. Se produce, habitualmente, una búsqueda de “signaturas” dañinas, o sea patrones característicos, en el contenido de paquetes, tal como se conoce de los antivirus. Primariamente, el ataque tampoco se dirige al bloqueo de servicios, sino a controlar sistemas.

Contrariamente, un ataque DDoS que se basa solamente en la saturación de recursos también puede ser iniciado contra sistemas completamente seguros. Se basa exclusivamente en el volumen de consultas. Los ataques DDoS se diferencian, principalmente, en el objetivo – ataques sencillos obstruyen la línea de red con paquetes, recursos: ancho de banda. Los ataques más complejos, con el fin de sobrecargar la CPU o las memorias producen, por ejemplo en bancos de datos de páginas Web, muchas consultas que requieren la compresión de datos.

Lo que estos ataques tienen en común es que mediante patrones y fenómenos característicos ya es posible que puedan ser detectados en la red. Ello se produce mediante la detección de patrones conocidos (IDS) o bien por la desviación de patrones normales (ADS).

El documento US-A-20060242705 describe un ADS para la detección de gusanos. Se buscan elementos dañinos en la propia red, o sea que no se rechaza en el Inbound Link ningún ataque desde el exterior. El procedimiento describe un sistema completo para la detección de y la defensa contra gusanos, mediante procedimientos de medición concretos. Sin embargo, no se propone una adaptación de métricas a nuevos tipos de gusanos.

En el sistema Cisco nombrado anteriormente, el proceso de verificación múltiple nombrado describe un procedimiento de varias etapas con medidas concretas, por ejemplo la verificación del origen: los remitentes de

paquetes son verificados mediante contraconsultas sencillas. Tampoco en este caso está prevista una adaptación del esquema. En la publicación de Thomas Gamer et al: „Distack - A Framework for Anomaly- Based Large Scale Attack Detection, “EMERGENCY SECURTIY INFORMATION, SYSTEMS AND TECHNOLOGIES, 2008, SECUWARE ‘08. SECOND INTERNATIONAL CONFERENCE ON, IEEE se describe una estructura para la detección de ataques que permiten la integración de diferentes procedimientos de detección en forma de módulos.

El documento US 6.477.651 B1 se refiere a un sistema y un procedimiento para la detección del uso no autorizado o malintencionado de los recursos de red.

Resumen de la invención

La presente invención tiene el objetivo de brindar un sistema y un procedimiento para la detección de ataques distribuidos de denegación de servicio por medio de una red basada en paquetes, el cual permite una definición de métrica para la ampliación flexible en tiempo real del dispositivo de medición del sistema, mediante lo cual se posibilita una adaptación dinámica a los ataques distribuidos de denegación de servicio.

Este objetivo se consigue mediante el objeto de las reivindicaciones.

La presente invención se refiere a un procedimiento para la detección de ataques distribuidos de denegación de servicio por medio de una red basada en paquetes según la reivindicación 1 y un sistema para la detección de ataques distribuidos de denegación de servicio por medio de una red basada en paquetes según la reivindicación 6. Las reivindicaciones secundarias se refieren a formas de realización preferentes de la invención.

El procedimiento según la presente invención, mediante el uso de lenguaje de encriptación para la definición métrica permite la ampliación del sistema de medición, teniendo pocos conocimientos de programación, y la definición de una métrica nueva. De esta manera, es posible transmitir la nueva métrica durante el tiempo de ejecución, sin necesidad de reiniciar, e incluirla en la operación. La nueva métrica, es decir la métrica ampliada puede suplantar o ampliar la métrica básica existente. En otras palabras, la métrica en el sistema según la presente invención puede ser ampliada o modificada de manera dinámica. Por lo tanto, el dispositivo de medición del sistema puede ser adaptado a nuevas tareas, es decir que el sistema puede ser adaptado en tiempo real a las estructuras de ataque permanentemente cambiantes. Consecuentemente, se puede evitar un tiempo de paro del sistema para la reconfiguración de la métrica.

Descripción de las figuras

A continuación, la invención se describe en detalle mediante los dibujos anexos. Muestran:

La figura 1, una representación esquemática del modo del funcionamiento del sistema según una forma de realización preferente de la presente invención; y

la figura 2, un desarrollo a modo de ejemplo para la adaptación de la métrica en el dispositivo de medición.

A continuación, el procedimiento para la detección de ataques distribuidos de denegación de servicio a través de una red basada en paquetes se explica, según una forma de realización preferente, mediante la figura 1 y la figura 2.

La invención describe un procedimiento para la reconfiguración de un sistema de medición o dispositivo de medición 11 que, de esta manera, es capaz de recibir nuevas métricas 13 características durante el tiempo de ejecución y hacer cálculos durante la operación en curso. Una definición métrica 15 se produce en un lenguaje de encriptación interpretado mediante módulos cortos de programa.

La figura 1 muestra una representación esquemática del modo del funcionamiento del sistema 10 según una forma de realización preferente de la presente invención. Para ello, el sistema de medición o el dispositivo de medición 11 son controlados por el sistema de control o el dispositivo de control 12 de un IDS 10 que opera la detección real del ataque y asigna tareas 14 al sistema de medición 11. Una tarea de medición 14 es, por ejemplo, la indicación "mide durante 10 minutos los tamaños de paquete y ejecuta la métrica existente 'valor medio de todos los tamaños de paquete'..".

En cuanto el EDS 10, automáticamente o mediante la intervención de un administrador, ha detectado y caracterizado una modificación en la estructura de ataque, emite una definición métrica 15 en lenguaje de encriptación. La definición métrica 15 es descargada por el sistema de control 12 en el sistema de medición 11. Gracias a que el lenguaje de encriptación es procesado en tiempo de ejecución por un interpretador existente en el programa, no es necesario convertir el módulo o, a continuación, reiniciar el sistema 10.

Gracias a un interpretador para el lenguaje de encriptación, el sistema de medición 11 es capaz ahora de utilizar inmediatamente la definición 15 durante la operación en curso. Para ello, el sistema de control 12 define una nueva tarea 14 que atribuye la nueva métrica 13. El sistema de medición recoge los datos descritos en la definición de tareas 14 y ejecuta, a continuación, el módulo métrico para calcular las métricas 13.

Una redefinición de métricas de este tipo se puede producir, por ejemplo, en el caso de un ataque. La figura 2

muestra un desarrollo, a modo de ejemplo, para la adaptación de métricas 13 al dispositivo de medición 11. En estado normal, por motivos de recursos un IDS monitorea el tránsito de red 16 solamente con una resolución aproximada – la métrica básica 13a. Si se detecta que se está produciendo un ataque, los datos recopilados hasta el momento pueden no ser suficientes. El IDS 10 puede identificar a través de que interfaces se produce el ataque a la red, y que partes de la red 16 están afectadas. Además, las informaciones más precisas sobre el tipo de ataque pueden dar indicios respecto de la eliminación y del autor.

O sea, si el DS 10 detecta un ataque puede distribuirse una serie de nuevas tareas de medición 14a, 14b. En este caso, si el modo de ataque es novedoso es posible proceder sin un esquema fijo. Las nuevas definiciones métricas pueden extraer de los paquetes de datos determinados datos de encabezamiento o datos de usuario, delimitar la medición a determinados segmentos de red, fuentes o tipos de paquete, y realizar cualesquiera funciones matemáticas basadas en dichos datos.

Si el IDS 10 detecta, por ejemplo, que se produce un tránsito perjudicial de manera particularmente frecuente en un puerto determinado, es posible monitorear selectivamente sólo el tránsito en ese número de puerto, y generar datos estadísticos especiales, por ejemplo tránsito total, distribuciones o desviaciones. Si el IDS registra una acumulación de determinados patrones es posible intercalar especialmente una rutina que reconoce dicho patrón en los datos existentes, e informa de la acumulación de la presencia de dicho patrón.

Como se ha descrito anteriormente, en caso de necesidad en el IDS 10 puede ser ampliada la métrica básica 13a y/o la definición métrica 15, ampliando la métrica básica 13a mediante la métrica 13 ampliada. Opcionalmente, la métrica básica 13a y/o la definición métrica 15 en el IDS 10 puede, en cada caso, también ser sustituida por la nueva métrica, es decir la métrica 13 ampliada o la definición métrica 15, sirviendo en el futuro la métrica ampliada como métrica total en el EDS 10. En ambos casos, visto globalmente, la métrica y/o la definición métrica en el IDS 10 pueden ser modificadas dinámicamente, con lo cual se posibilita en tiempo real la adaptación dinámica del IDS 10 a estructuras de ataque permanentemente cambiantes. De esta manera se puede evitar el tiempo de paro del IDS 10.

La invención comprende también características individuales en las figuras, aun cuando allí se muestren en relación con otras características y/o no se hubiesen nombrado anteriormente o seguidamente.

Asimismo, la invención incluye formas de realización con cualquier combinación de características que anteriormente o seguidamente se nombran o muestran respecto de diferentes formas de realización.

REIVINDICACIONES

1. Procedimiento para la detección de ataques distribuidos de denegación de servicio por medio de una red (16) basada en paquetes, con las etapas monitoreo de la red (16) con un dispositivo de medición (11) que está configurado con al menos una métrica dinámicamente definible; y control del dispositivo de medición (11) y detección de los ataques con un dispositivo de control (12),
en donde el procedimiento presenta, además, las etapas
monitoreo de la red (16) con una métrica básica (13a);
cuando se detecta una modificación en los ataques distribuidos de denegación de servicio;
determinación de al menos una nueva tarea de monitoreo (14b) con el dispositivo de control (12) para el ajuste del dispositivo de medición (11) a la modificación detectada; caracterizado por
puesta a disposición de una definición de métrica (15) en un lenguaje de encriptación para una métrica ampliada (13) con el dispositivo de control (12) para el cumplimiento de la nueva tarea de monitoreo (14b);
descarga de la definición de métrica (15) del dispositivo de control (12) al dispositivo de medición (11); e
interpretación de la métrica ampliada (13) sobre la base de la definición de métrica (15) con el dispositivo de medición (11).

2. Procedimiento según la reivindicación 1, por el cual la métrica ampliada (13) suplanta la métrica básica (13a).

3. Procedimiento según las reivindicaciones 1 o 2, por el cual la definición de métrica (15) presenta en la red (16) determinados datos de encabezamiento y/o datos de usuario provenientes de paquetes de datos.

4. Procedimiento según la reivindicación 3, por el cual el monitoreo mediante el dispositivo de medición (11) está definido sobre parámetros y segmento de red, fuentes y/o tipos de paquetes.

5. Procedimiento según las reivindicaciones 3 o 4, por el cual sobre los paquetes de datos se realiza una función matemática.

6. Sistema para la detección de ataques distribuidos de denegación de servicio por medio de una red (16) basada en paquetes, con:
un dispositivo de medición (11) para el monitoreo de la red (16);
un dispositivo con una métrica para la configuración del dispositivo de medición (11), siendo la métrica adaptable dinámicamente a los ataques distribuidos de denegación de servicios; y
un dispositivo de control (12) conectado con el dispositivo de medición (11) para el control del dispositivo de medición (11) y la ejecución de la detección de ataques distribuidos de denegación de servicios;
estando el sistema configurado
para el monitoreo de la red (16) mediante una métrica básica (13a);
cuando se detecta un cambio en los ataques distribuidos de denegación de servicios,
determinación de al menos una nueva tarea de monitoreo (14b) con el dispositivo de control (12) para el ajuste del dispositivo de medición (11) a la modificación detectada; caracterizado por la
puesta a disposición de una definición de métrica (15) en un lenguaje de encriptación para una métrica ampliada (13) con el dispositivo de control (12) para el cumplimiento de la nueva tarea de monitoreo (14b);
la descarga de la definición de métrica (15) del dispositivo de control (12) al dispositivo de medición (11); e
interpretación de la métrica ampliada (13) sobre la base de la definición de métrica (15) con el dispositivo de medición (11).

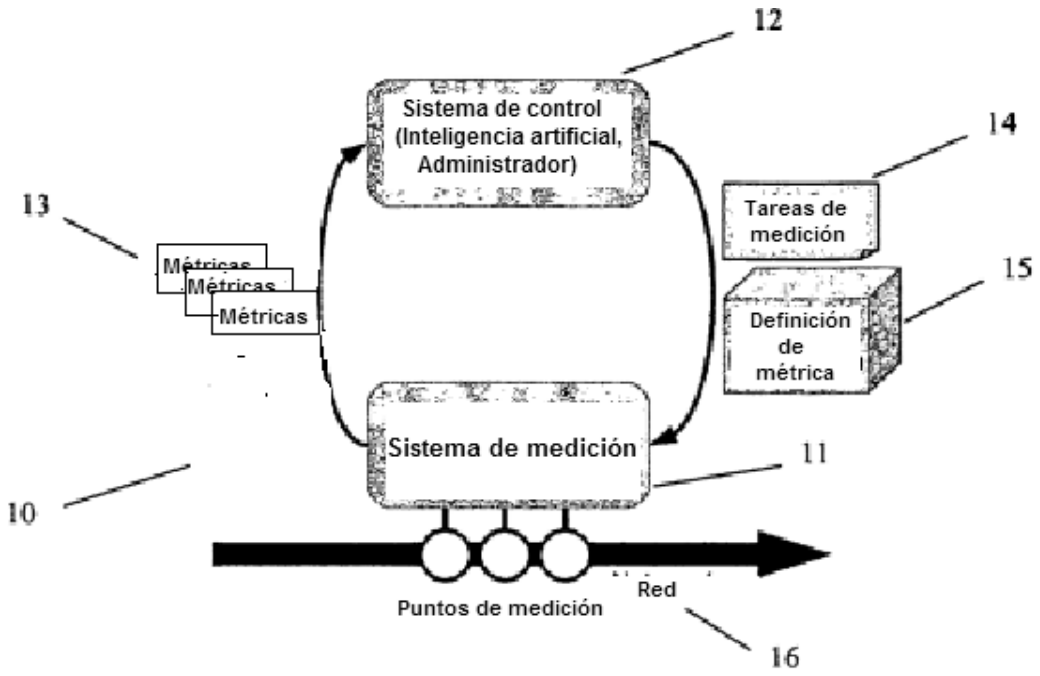
12
Sistema de control
(Inteligencia artificial,
Administrador)
14
Tareas de
medición
13
Métricas
Métricas
Métricas
15
Definición
de
métrica
Sistema de medición
11
10
Red
Puntos de medición
16

Fig. 1

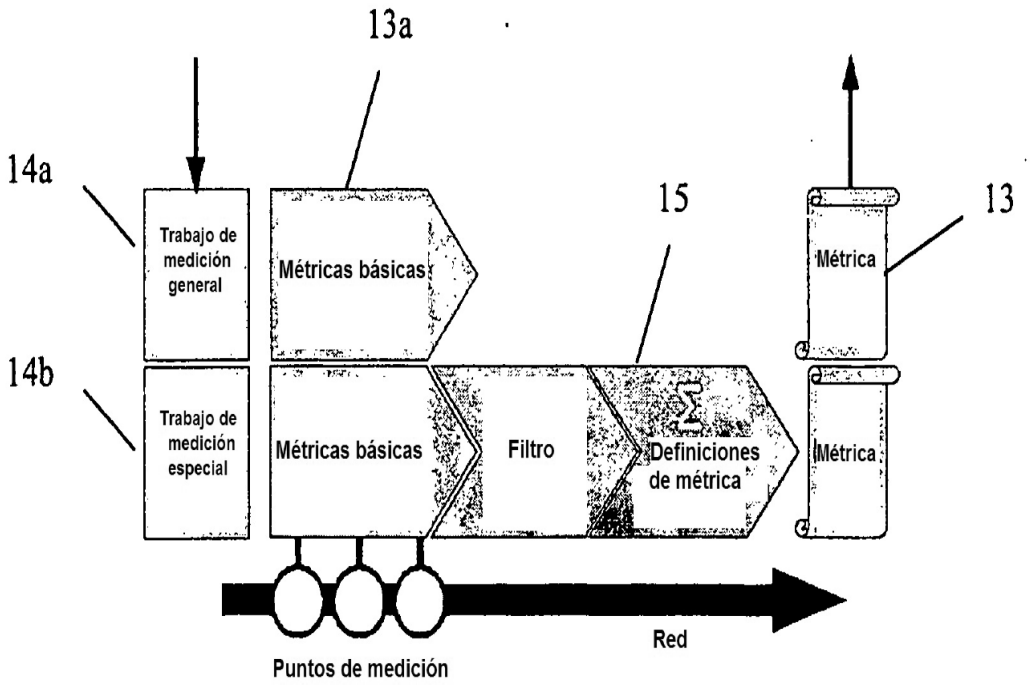
13a
14a
Trabajo de
medición
general
Métricas básicas
15
Métrica
13
14b
Trabajo de
medición
especial
Métricas básicas
Filtro
Definiciones
de métrica
Métrica
Red
Puntos de medición

Fig. 2