(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 366 730**

(21) Número de solicitud: 200901708

(51) Int. Cl.:
G06F 21/00 (2006.01)
H04L 12/28 (2006.01)
H04W 12/00 (2009.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **03.08.2009**

(43) Fecha de publicación de la solicitud: **25.10.2011**

Fecha de la concesión: **06.06.2012**

(45) Fecha de anuncio de la concesión: **18.06.2012**

(45) Fecha de publicación del folleto de la patente: **18.06.2012**

(73) Titular/es:
UNIVERSIDAD DE SEVILLA
OTRI-PABELLÓN DE BRASIL PASEO DE LAS DELICIAS S/N
41013 SEVILLA, ES

(72) Inventor/es:
Romero Ternero, Maria Carmen y
Diaz Ruiz, Sergio

(74) Agente/Representante:
No consta

(54) Título: **SISTEMA Y MÉTODO DE RESOLUCIÓN CENTRALIZADA Y CONFIABLE DE DIRECCIONES DE RED EN DIRECCIONES FÍSICAS NO VULNERABLE A ATAQUES DE ENVENENAMIENTO DE CACHÉ.**

(57) Resumen:
Se propone un sistema confiable de resolución de direcciones de red en direcciones físicas, aplicable a redes telemáticas de área local, para evitar la vulnerabilidad por envenenamiento de caché que actualmente sufre el protocolo ARP (RFC826). A diferencia de las soluciones técnicas existentes a este problema, la resolución es centralizada y se fundamenta en un servicio que actúa como tercera parte de confianza, gracias al empleo de una infraestructura de clave pública que permite firmar digitalmente los mensajes de resolución para asegurar su autenticidad e integridad.

ES 2 366 730 B1

DESCRIPCIÓN

Sistema y método de resolución centralizada y confiable de direcciones de red en direcciones físicas no vulnerable a ataques de envenenamiento de caché.

La invención se ubica en el área de las comunicaciones telemáticas y más concretamente, en el de la seguridad en redes de área local. La presente invención tiene por objeto un sistema y método centralizado para la resolución de las direcciones de red en direcciones físicas no vulnerables a los ataques por envenenamiento de la caché.

Estado de la técnica anterior

El protocolo de resolución de direcciones más ampliamente extendido en el ámbito de las redes locales es ARP (*Address Resolution Protocol*, RFC826, literalmente protocolo de resolución de direcciones). Se han descrito varios sistemas para neutralizar los ataques de envenenamiento de la caché asociada a dicho protocolo ARP. Siguiendo el enfoque original de ARP, dichos sistemas asumen un mecanismo de resolución distribuido, según el cual el equipo de red cuya dirección física se desea resolver a partir de la dirección de red es el encargado de enviar esta información al equipo que origina el proceso de resolución. Lo que distingue a estos sistemas del resto es el método usado para verificar que la correspondencia entre la dirección física obtenida y la dirección de red es la auténtica. Entre estos métodos es posible destacar los siguientes:

(a) *Método basado en inspección de paquetes ARP y DHCP* (*Dynamic Host Configuration Protocol*, RFC2131 literalmente protocolo de configuración dinámica del Host). Las redes de área local se basan en equipos electrónicos que distribuyen por la red las transmisiones de nivel físico. Dado que el tráfico de la red atraviesa forzosamente dichos equipos, éstos pueden ser dotados de los procesos necesarios para inspeccionar los mensajes ARP y DHCP generados desde equipos considerados de confianza para establecer las correspondencias válidas entre direcciones físicas y de red. Sin embargo, los equipos de red que incorporan esta funcionalidad son sustancialmente más costosos ya que necesitan de mayores recursos de memoria y capacidad de cómputo. Por otra parte, las asignaciones de direcciones de red estáticas, no gestionadas por el servicio DHCP, deben configurarse manualmente y ser distribuidas debidamente en los equipos de red. Es el caso del *Dynamic ARP Inspection* [1],

(b) *Método criptográfico*. Se basan en el uso de la criptografía para generar testigos que permitan autentificar las correspondencias entre direcciones físicas y de red. Se han propuesto las siguientes variantes:

(b.1) *S-ARP* [2]. A los mensajes ARP clásicos se les añade una cola que incluye la firma digital que permite verificar la autenticidad del paquete y una marca de tiempo. En la red existe un nodo de confianza que sirve de repositorio de claves públicas, denominado AKD (*Authoritative Key Distributor* literalmente distribuidor de llaves autorizado). Cada equipo de la red dispone de su propio certificado digital (par de claves pública y privada), que usa para firmar los mensajes ARP que envía. El certificado incluye las direcciones IP y MAC del equipo, así como las del AKD. Los equipos mantienen una caché local de claves públicas para acelerar el proceso de autentificación, conectando solamente con el AKD cuando reciben un mensaje firmado cuyo remitente no conocen. Existen algunas propuestas, como las descritas en [3] para mejorar la eficiencia de este sistema, aunque no se modifica el enfoque seguido.

(b.2) *AuthARP* [4], Los equipos usan el protocolo ARP normalmente, sin embargo, cada vez que reciben un mensaje ARP-reply, inician un proceso de autenticación contra el equipo que lo ha enviado, lo que implica un nuevo intercambio de mensajes solicitud-respuesta. El proceso de autenticación (tipo *challenge*) se resuelve gracias a que cada equipo en la red dispone de su propio certificado digital (par de claves pública y privada).

(b.3) *Arquitectura de seguridad para proteger las interacciones en LAN* [5]. La resolución es distribuida, pero involucra una comunicación con un servicio (KDC) que provee de claves de sesión a los equipos finales, las cuales permiten realizar la transacción de resolución de forma segura.

(b.4) *TARP* [6]. La resolución es distribuida, pero los equipos finales disponen de un ticket generado de forma segura por un tercero de confianza (servidor LTA) usando mecanismos de clave pública. Dicho ticket incluye la correspondencia entre IP y MAC, además de un periodo de validez. Las respuestas de resolución incluyen el ticket correspondiente, cuya validez es verificable a partir del certificado digital (clave pública) del servidor LTA.

(c) *Método de mejora del comportamiento del protocolo ARP*. Se basa en modificar el procesamiento de mensajes ARP especificado en RFC826, para disminuir o eliminar el riesgo de envenenamiento de la caché. Se han propuesto las siguientes variantes:

(c.1) *Autenticación de capa 2* [7]. Resolución distribuida, remodela el procesado de mensajes ARP, de forma que ignora ARP-reply gratuitos e incluye un mecanismo para comprobar qué ARP-reply es válido en caso de recibir más de uno, consultando a una tercera parte de confianza (que responde con mensajes firmados).

(c.2) *Detección y prevención de envenenamiento de caché ARP* [8]. Básicamente consiste en una revisión del algoritmo que rige el flujo de mensajes ARP de un equipo, tratando de incluir en la caché ARP únicamente aquellas correspondencias IP-MAC que han sido explícitamente solicitadas por el equipo, y de detectar cualquier uso sospechoso de los mensajes ARP. Sin embargo, no incluye ningún mecanismo de autenticación, por lo que sigue siendo vulnerable.

(c.3) *Prevención de envenenamiento de caché ARP* [9]. Cuando un equipo recibe un ARP-reply, solicita a un tercero la validación de la información contenida en el mismo. Este tercer equipo está ubicado en otra red y mantiene una caché ARP de confianza.

Referencias

[1] Y. **Bhaiji**: Network Security Technologies and Solutions. Capítulo 8: Dynamic ARP Inspection (DAI). Ed. Cisco Press. 2008. ISBN-13: 978-1-58705-246-0.

[2] D. **Bruschi**, A. **Ornaghi**, E. **Rosti**. S-ARP: a secure address resolution protocol. Proc. 19th Annual Computer Security Applications Conference, ACSAC 2003, pp 66-74, Las Vegas, NV (USA), Diciembre 2003.

[3] V. **Goyal**, R. **Tripathy**. An Efficient Solution to the ARP Cache Poisoning Problem, 1 Oth Australasian Conference on Information Security and Privacy (ACISP 2005), LNCS 3574, *Springer-Verlag*. Julio, 2005.

[4] H. **Urtubia**. Local area network security: Authenticating the ARP protocol, Master's Thesis, HKU Libraries, *Electronic Resources*, 2003.

[5] A. **Zúquete**, H. **Marques**: A Security Architecture for Protecting LAN Interactions. Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006. Proceedings. Lecture Notes in Computer Science 4176, pp 311-326, *Springer*, 2006, ISBN 3-540-38341-7.

[6] W. **Lootah**, W. **Enck**, P. **McDaniel**: TARP: Ticket-based address resolution protocol. Computer Networks: The International Journal of Computer and Telecommunications Networking, v.51 n.15, p.4322-4337. Association for Computing Machinery (ACM), Octubre, 2007.

[7] S. **Whalen**, M. **Bishop**: Layer 2 Authentication. Febrero 2005.

[8] M.V. **Tripunitara**, P. **Dutta**: A Middleware Approach to Asynchronous and Backward Compatible Detection and Prevention of ARP Cache Poisoning. Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC). *IEEE Computer Society*, December, 1999.

[9] P.B. **Finley**, T.L. **McLane**, E.L. **Reyes**: Preventing asynchronous ARP cache poisoning of múltiple hosts. United States Patent Application US7471684. 12/30/2008.

Explicación de la invención

El problema técnico objetivo que la presente invención resuelve frente a las soluciones aportadas en el estado de la técnica radica en que el protocolo ARP presenta una vulnerabilidad de diseño que permite a un equipo atacante manipular la caché de resolución de direcciones de red en direcciones físicas de los equipos de una red de área local. A consecuencia del ataque, los equipos víctima dispondrán de una o más correspondencias falsificadas entre direcciones de red y direcciones físicas, lo cual puede implicar una denegación de servicio, al no poder acceder a otros equipos de la red, como el enrutador, o la intercepción por parte del equipo atacante de las comunicaciones entre equipos víctima.

Tradicionalmente, el estado de la técnica se ha considerado que la resolución de direcciones de red debe ser distribuida con objeto de evitar los puntos únicos de fallo. Sin embargo, en la actualidad, es común encontrar en la red recursos lógicos, tales como los servicios DHCP, DNS, LDAP, entre otros, y físicos, tales como enrutadores y conmutadores, todos ellos centralizados y necesarios para el correcto funcionamiento de la infraestructura informática de red. La centralización de estos recursos facilita su instalación, administración y mantenimiento. La existencia de puntos únicos de fallo en una red con recursos centralizados se resuelve mediante redundancia y mecanismos de alta disponibilidad.

No obstante, a diferencia de los sistemas propuestos en el estado de la técnica, la presente invención propone la incorporación de un servicio centralizado de resolución de direcciones (en adelante SRD) que actúa como tercera parte de confianza en el proceso de resolución, así como el empleo de un protocolo de resolución cuyos mensajes de respuesta disponen de una firma digital que acredita su autenticidad. De este modo, los equipos de la red se comunican directamente con el SRD cuando necesiten obtener la dirección física asociada a una dirección de red dada, en lugar de difundir mensajes de solicitud de resolución por toda la red. El SRD responde con un mensaje firmado digitalmente, por tanto, el equipo solicitante puede verificar la autenticidad del mismo antes de incluir la correspondencia entre direcciones físicas y de red en su caché de resoluciones. El proceso de resolución únicamente involucra el intercambio de este par de mensajes, a diferencia de las soluciones existentes, que pueden requerir intercambios adicionales por verificación o distribución de claves o *tickets*.

Más concretamente, en un aspecto de la invención, el método de resolución centralizada y confiable de direcciones de red en direcciones físicas, no vulnerable a ataques de envenenamiento de caché, sincronizado mediante una medida de tiempo común comprende, al menos,

(i) un primer proceso lógico configurado para la resolución centralizada de direcciones físicas a partir de direcciones de red en un servidor de resolución de direcciones (SRD), para el que se ha generado una infraestructura de clave pública, un par de claves asimétrica, pública y privada, y un certificado digital con una validez preestablecida; en donde dicho primer proceso tiene acceso a:

(a) la clave privada correspondiente al par de claves asimétricas asociadas al SRD;

(b) el repositorio que almacena las correspondencias reales entre direcciones de red y direcciones físicas, habilitando al SRD como tercera parte de confianza en el proceso de resolución;

(c) la medida del tiempo común;

en donde dicho primer proceso lógico, al recibir el mensaje de solicitud de resolución enviado por un equipo informático conectado a la red de área local (cliente) que incluya una dirección de red con objeto de obtener del SRD la dirección física correspondiente, el SRD envía un mensaje de respuesta de resolución firmado digitalmente empleando su clave privada, en el que incluye la correspondencia entre dirección de red y dirección física solicitada por el cliente junto con una marca temporal indicativa del instante en que se realiza la operación de firma digital; y donde en el caso de que el SRD no conozca la dirección física solicitada, enviará en su lugar un valor especial que tendrá la consideración de nulo por ambas partes;

(ii) un segundo proceso lógico de solicitud de resolución de direcciones asociado al cliente que tiene acceso a:

(a) las direcciones físicas y de red del SRD;

(b) el certificado digital del SRD, conteniendo la clave pública del mismo; y

(c) la memoria caché de resolución de direcciones, que almacena temporalmente las correspondencias entre direcciones de red y direcciones físicas que se han obtenido mediante consultas al SRD siguiendo el procedimiento de resolución de direcciones del primer proceso lógico;

en donde, cuando, por la propia operación del cliente, resulte necesario determinar la dirección física asociada a una determinada dirección de red, y la correspondencia entre ambas no se encuentra almacenada en la caché, el cliente envía un mensaje de solicitud de resolución hacia el SRD conteniendo dicha dirección de red; y donde al recibir un mensaje de respuesta de resolución, aplica la clave pública del SRD sobre la firma digital incluida en dicho mensaje para comprobar si éste ha sido emitido por el SRD, y comprueba si la marca temporal se corresponde con la hora local del cliente con una diferencia menor que la desviación máxima admisible, aceptando el cliente la correspondencia entre dirección de red y dirección físicas aportadas en el mensaje, incluyéndolas en la caché, sólo si ambas comprobaciones resultan positivas.

En un segundo aspecto de la invención, el sistema de resolución centralizada y confiable de direcciones de red en direcciones físicas, no vulnerable a ataques de envenenamiento de caché, configurado para implementar el método anteriormente descrito y que comprende medios de sincronización horaria, que proporciona a los equipos integrantes de la red de área local, al menos un servidor y al menos un dispositivo cliente, de una medida de tiempo común a todos ellos, comprende, al menos:

(i) un primer servidor de resolución de direcciones (SRD) configurado para la resolución centralizada de direcciones físicas a partir de direcciones de red, que a su vez comprende una infraestructura de clave pública, un par de claves asimétrica, pública y privada, y un certificado digital con una validez preestablecida; en donde dicho primer servidor SRD tiene acceso a:

(a) la clave privada correspondiente al par de claves asimétricas asociadas al SRD;

(b) el repositorio que almacena las correspondencias reales entre direcciones de red y direcciones físicas, habilitando al SRD como tercera parte de confianza en el proceso de resolución;

(c) la medida del tiempo común;

y en donde dicho servidor comprende medios configurados para recibir el mensaje de solicitud de resolución enviado por el cliente y medios configurados para enviar un mensaje de respuesta de resolución firmado digitalmente empleando su clave privada, en el que incluye la correspondencia entre dirección de red y dirección física solicitada por el cliente junto con una marca temporal indicativa del instante en que se realiza la operación de firma digital; y donde en el caso de que el SRD no conozca la dirección física solicitada, enviará en su lugar un valor especial que tendrá la consideración de nulo por ambas partes;

(ii) un elemento cliente con acceso a las direcciones físicas y de red del SRD; el certificado digital del SRD, conteniendo la clave pública del mismo; y la memoria caché de resolución de direcciones, que almacena temporalmente las correspondencias entre direcciones de red y direcciones físicas que se han obtenido mediante consultas al SRD siguiendo el procedimiento de resolución de direcciones del primer proceso lógico de la reivindicación 1;

en donde, dicho cliente comprende medios configurados para enviar un mensaje de solicitud de resolución hacia el SRD conteniendo la dirección de red; y medios configurados para recibir un mensaje de respuesta de resolución y aplicar la clave pública del SRD sobre la firma digital incluida en dicho mensaje para comprobar si éste ha sido emitido por el SRD, y comprobar si la marca temporal se corresponde con la hora local del cliente con una diferencia menor que la desviación máxima admisible, aceptando el cliente la correspondencia entre dirección de red y dirección físicas aportadas en el mensaje, incluyéndolas en la caché, sólo si ambas comprobaciones resultan positivas.

A lo largo de la descripción y las reivindicaciones la palabra "comprende" y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención. Los siguientes ejemplos y dibujos se proporcionan a modo de ilustración, y no se pretende que sean limitativos de la presente invención. Además, la presente invención cubre todas las posibles combinaciones de realizaciones particulares y preferidas aquí indicadas.

Exposición detallada de modos de realización y Ejemplos

El sistema de resolución centralizada de direcciones de red en direcciones físicas propuesto en la presente invención requiere de la existencia de los siguientes componentes en la red de área local:

(i) Un primer proceso lógico encargado de la resolución de direcciones físicas a partir de direcciones de red, en adelante Servidor de Resolución de Direcciones (SRD).

(ii) Un segundo proceso lógico de solicitud de resolución de direcciones asociado a los equipos integrantes de la red, en adelante, equipos cliente.

(iii) Un sistema de sincronización horaria, que proporciona a los equipos cliente y al SRD una medida común de tiempo.

En particular, las direcciones de red pueden ser direcciones IP definidas según la norma RFC791, y las direcciones físicas pueden ser direcciones MAC definidas según la norma IEEE STD. 802.

El SRD debe tener acceso a un repositorio que almacene las correspondencias reales entre direcciones de red y direcciones físicas, siendo ésta la información que habilita al SRD como tercera parte de confianza en el proceso de resolución. Dicho repositorio puede corresponderse con:

(a) el conjunto de asignaciones dinámicas realizadas por el servidor DHCP de la red de área local, en caso de existir, y de

(b) un conjunto de asignaciones estáticas, para aquellas asignaciones que no sean gestionadas por el servidor DHCP.

Mediante una infraestructura de clave pública (PKI, *Public Key Infraestructure*), se genera un par de claves pública y privada, para el SRD. Asimismo, se emite un certificado digital asociado al SRD, que incluirá sus direcciones física y de red, además de su clave pública, y que podrá ser autofirmado (lo que resulta especialmente adecuado para redes de pequeña o mediana envergadura), o bien firmado por una Autoridad de Certificación previamente existente o creada al efecto (siendo éste un enfoque apropiado para grandes redes corporativas).

El certificado digital del SRD se distribuirá a los equipos cliente por algún mecanismo fuera de banda, mientras que su clave privada será la que le permita firmar los mensajes de respuesta de resolución, asegurando así su autenticidad.

El proceso de resolución implica el intercambio de un mensaje de solicitud y un mensaje de respuesta (encapsulados como 2-SDU según el modelo OSI, ISO/IEC Standard 7498-1:1994), así como la existencia de los correspondientes procedimientos de resolución en los equipos cliente y SRD. Así pues, sea "S" el equipo que emite la solicitud de resolución, y "T" el equipo cuya dirección física desea obtener "S" en el proceso de resolución, tendremos que:

(a) El mensaje de solicitud de resolución, emitido por S hacia el SRD a nivel de enlace de datos, debe incluir la siguiente información: dirección de red de T.

(b) El mensaje de respuesta de resolución, emitido por el SRD hacia S a nivel de enlace de datos, debe incluir la siguiente información: dirección de red de T, dirección física de T, marca temporal, firma digital.

Al igual que en ARP, el proceso de resolución se apoya en parte en el uso de una memoria caché de resoluciones, en adelante caché, que almacena durante un determinado intervalo de tiempo la correspondencia entre direcciones físicas y de red obtenidas previamente mediante el proceso de resolución. La caché permite mejorar las prestaciones del mecanismo de resolución, evitando el intercambio de mensajes de resolución si las direcciones correspondientes ya se encuentran almacenadas en la caché. El proceso de resolución opera del siguiente modo:

(i) cuando S necesita determinar la dirección física asociada a la dirección de red de T, por no tener en su caché de resolución la correspondencia entre ambas, el cliente envía un mensaje de solicitud hacia el SRD;

(ii) al recibir el mensaje de solicitud, el SRD:

a. consulta su repositorio, obteniendo la dirección física de T; si ésta no se encuentra en el repositorio, se usará un valor especial de dirección física que tendrá la consideración de nulo por ambas partes;

b. calcula la firma digital aplicando su clave privada sobre el bloque de información integrado por la dirección de red de T, la dirección física de T y marca temporal correspondiente al instante de tiempo en que se inicia el cálculo de dicha firma, y

c. finalmente envía un mensaje de respuesta hacia S;

(iii) al recibir un mensaje de respuesta de resolución, S aplica la clave pública del SRD sobre la firma digital incluida en dicho mensaje para comprobar si éste ha sido emitido por el SRD, y comprueba si la marca temporal se corresponde con la hora local del cliente con una diferencia menor que la desviación máxima admisible (el valor mínimo para esta desviación debe contemplar el tiempo de firma, el procesado del paquete en el SRD, el tiempo de vuelo y el tiempo de procesado del paquete en el cliente). El cliente acepta la correspondencia entre dirección de red y dirección físicas aportadas en el mensaje, incluyéndolas en la caché, sólo si ambas comprobaciones resultan positivas.

Adicionalmente, los equipos cliente deben ignorar todo mensaje ARP recibido, para evitar el envenenamiento de caché de resolución en caso de ataque. Si se desea mantener interoperabilidad con el protocolo ARP, los equipos cliente deben procesar los mensajes ARP-request según lo previsto en la norma RFC826, exceptuando que no se incluirá la correspondencia entre dirección de red y dirección física del emisor del mensaje en la caché de resolución, e ignorar todos los mensajes ARP-reply recibidos.

El sistema descrito, al incluir mecanismos basados en PKI que aseguran la autenticidad e integridad de las resoluciones de direcciones, evita los posibles ataques de envenenamiento de caché, empleando para ello un protocolo basado en un intercambio de dos mensajes (solicitud y respuesta), a diferencia de algunas soluciones existentes, que pueden requerir el intercambio de varios mensajes adicionales, para verificación o distribución de claves o tickets. Por otra parte, al tratarse de una resolución centralizada, los mensajes de solicitud están dirigidos únicamente al SRD, en contraste con lo que ocurre con los mecanismos de resolución distribuida, que requieren la difusión de estos mensajes a toda la red de área local.

En cuanto a la administración del direccionamiento de la red, el sistema descrito permite integrar la gestión del direccionamiento dinámico con el servicio DHCP, en caso de existir, y unificarla con la gestión del direccionamiento estático en un único servicio centralizado, a diferencia de las soluciones existentes basadas en inspección de paquetes ARP y DHCP.

Ejemplo de aplicación

Sea una red de área local de tipo Ethernet (IEEE Standard 802.3) en la que se ha desplegado un servicio DHCP (RFC2131) y un servicio de sincronización horaria NTP (RFC1305), y en la que todos los equipos emplean el protocolo ARP (RFC826) para la resolución de direcciones IP (RFC791) en direcciones MAC (IEEE Standard 802) en donde:

- Sea D el equipo que presta el servicio DHCP
- Sean C1...Cn los equipos que obtienen la configuración automáticamente de D
- Sean S1...Sm los equipos configurados con direccionamiento estático
- Sea T el equipo que presta el servicio de sincronización horaria NTP a todos los anteriores.

Esta red es vulnerable a ataques de envenenamiento de caché. Para resolver este problema de seguridad, sobre la red se realizan las siguientes actuaciones, según el sistema preconizado por la presente invención:

(i) Se agrega el SRD a D, de tal forma que el SRD pueda leer el fichero histórico de reservas generado por el servicio DHCP, y por tanto, conocer la correspondencia actual entre direcciones IP y MAC de los equipos C1...Cn. Adicionalmente, el SRD tendrá acceso a un fichero en el que se hayan incluido las correspondencias estáticas entre las direcciones IP y MAC de los equipos S1...Sm. Ambos ficheros implementan, en definitiva, el repositorio de correspondencias entre direcciones IP y MAC que permite al SRD llevar a cabo las resoluciones de direcciones.

(ii) Se genera un par de claves pública y privada mediante un software criptográfico, p. ej., openssl, y con ellas se genera un certificado autofirmado con las direcciones IP y MAC de D, que además incluye la clave pública. Dicho certificado se empaqueta en formato PKCS#7 (RFC2315) para su distribución a otros equipos. La clave privada no se comunica en ningún momento y solamente está accesible al SRD.

(iii) Se despliega en los sistemas operativos de los equipos C1...Cn, S1...Sm y T el módulo ejecutable que implementa el procedimiento de resolución de direcciones a través del SRD, así como el certificado indicado anteriormente.

De este modo, todos los equipos de la red dejan de usar ARP. Las solicitudes generadas por C1...Cn, S1...Sm y T se envían encapsuladas en tramas ethernet unicast hacia D, indicando la dirección IP del equipo cuya dirección MAC desean obtener. En el campo ethertype de la trama ethernet se usa el valor reservado para ARP.

Una vez que las solicitudes llegan a D, son atendidas por el SRD. Éste consulta las reservas DHCP actuales y el fichero de correspondencias estáticas para obtener la dirección MAC solicitada a partir de la dirección IP contenida en el mensaje de solicitud. El SRD genera una firma digital aplicando su clave privada sobre el bloque de información compuesto por estas direcciones IP y MAC, y una marca temporal, derivada de su reloj interno, indicativa del inicio del proceso de firma. Esta información, así como la propia firma digital, componen el mensaje de respuesta, que se encapsula en una trama ethernet unicast y se envía al solicitante. Si el SRD no conoce la dirección MAC, usa el valor reservado 00-00-00-00-00-00 para indicar al solicitante tal situación.

Cuando el mensaje de respuesta llega al solicitante, éste comprueba la autenticidad de la firma digital, para lo cual hace uso de la clave pública del SRD incluida en el certificado, y compara la marca temporal incluida en el mensaje con la derivada de su reloj. Si la diferencia entre ambas es inferior a 5 segundos, y la firma es auténtica, se considera que la correspondencia entre dirección IP y MAC obtenida es válida y se almacena en la caché de resolución.

REIVINDICACIONES

1. Método de resolución centralizada y confiable de direcciones de red en direcciones físicas, no vulnerable a ataques de envenenamiento de caché, sincronizado mediante una medida de tiempo común, **caracterizado** porque comprende, al menos,

(i) un primer proceso lógico configurado para la resolución centralizada de direcciones físicas a partir de direcciones de red en un servidor de resolución de direcciones (SRD), para el que se ha generado una infraestructura de clave pública, un par de claves asimétrica, pública y privada, y un certificado digital con una validez preestablecida; en donde dicho primer proceso tiene acceso a:

(a) la clave privada correspondiente al par de claves asimétricas asociadas al SRD;

(b) el repositorio que almacena las correspondencias reales entre direcciones de red y direcciones físicas, habilitando al SRD como tercera parte de confianza en el proceso de resolución;

(c) la medida del tiempo común;

en donde dicho primer proceso lógico, al recibir el mensaje de solicitud de resolución enviado por un equipo informático conectado a la red de área local (cliente) que incluya una dirección de red con objeto de obtener del SRD la dirección física correspondiente, el SRD envía un mensaje de respuesta de resolución firmado digitalmente empleando su clave privada, en el que incluye la correspondencia entre dirección de red y dirección física solicitada por el cliente junto con una marca temporal indicativa del instante en que se realiza la operación de firma digital; y donde en el caso de que el SRD no conozca la dirección física solicitada, enviará en su lugar un valor especial que tendrá la consideración de nulo por ambas partes;

(ii) un segundo proceso lógico de solicitud de resolución de direcciones asociado al cliente que tiene acceso a:

(a) las direcciones físicas y de red del SRD;

(b) el certificado digital del SRD, conteniendo la clave pública del mismo; y

(c) la memoria caché de resolución de direcciones, que almacena temporalmente las correspondencias entre direcciones de red y direcciones físicas que se han obtenido mediante consultas al SRD siguiendo el procedimiento de resolución de direcciones del primer proceso lógico;

en donde, cuando, por la propia operación del cliente, resulte necesario determinar la dirección física asociada a una determinada dirección de red, y la correspondencia entre ambas no se encuentra almacenada en la caché, el cliente envía un mensaje de solicitud de resolución hacia el SRD conteniendo dicha dirección de red; y donde al recibir un mensaje de respuesta de resolución, aplica la clave pública del SRD sobre la firma digital incluida en dicho mensaje para comprobar si éste ha sido emitido por el SRD, y comprueba si la marca temporal se corresponde con la hora local del cliente con una diferencia menor que la desviación máxima admisible, aceptando el cliente la correspondencia entre dirección de red y dirección físicas aportadas en el mensaje, incluyéndolas en la caché, sólo si ambas comprobaciones resultan positivas.

2. Método según la reivindicación 1 **caracterizado** porque las direcciones de red son direcciones IP definidas según la norma RFC791, y las direcciones físicas son direcciones MAC definidas según la norma IEEE Standard 802, siendo 00-00-00-00-00-00 la dirección MAC que se considera de valor nulo.

3. Método según la reivindicación 1 y 2 **caracterizado** porque el certificado digital del SRD es un certificado emitido por una Autoridad de Certificación.

4. Método según la reivindicación 1 y 2 **caracterizado** porque el certificado digital del SRD es un certificado autofirmado.

5. Método según la reivindicación 1, 2, y 3 o 4 **caracterizado** porque el repositorio que almacena las correspondencias entre direcciones de red y direcciones físicas a las que tiene acceso el SRD se obtiene de el conjunto de asignaciones dinámicas realizadas por el servidor DHCP de la red de área local, en caso de existir, y de un conjunto de asignaciones estáticas, para aquellas asignaciones que no sean gestionadas por el servidor DHCP.

6. Método según las reivindicaciones anteriores **caracterizado** por incorporar el siguiente comportamiento en el procedimiento de resolución de direcciones asociado a los clientes, con objeto de evitar ataques por envenenamiento de caché ARP (Address Resolution Protocol, RFC826): ignora todo mensaje ARP recibido.

7. Método según las reivindicaciones anteriores **caracterizado** por incorporar el siguiente comportamiento en el procedimiento de resolución de direcciones asociado a los clientes, con objeto de mantener la interoperabilidad con

el protocolo de resolución ARP y evitar ataques por envenenamiento de caché ARP: ignora todo mensaje ARP-reply recibido; y al recibir un mensaje ARP-request, lo procesa según lo previsto en la norma RFC826, excepto que no se incluye la correspondencia entre dirección de red y dirección física del emisor del mensaje en la caché.

8. Sistema de resolución centralizada y confiable de direcciones de red en direcciones físicas, no vulnerable a ataques de envenenamiento de caché, configurado para implementar el método de las reivindicaciones 1 a 7, que comprende medios de sincronización horaria, que proporciona a los equipos integrantes de la red de área local, al menos un servidor y al menos un dispositivo cliente de una medida de tiempo común a todos ellos **caracterizado** porque comprende, al menos

(i) un primer servidor de resolución de direcciones (SRD) configurado para la resolución centralizada de direcciones físicas a partir de direcciones de red, que a su vez comprende una infraestructura de clave pública, un par de claves asimétrica, pública y privada, y un certificado digital con una validez preestablecida; en donde dicho primer servidor SRD tiene acceso a:

(a) la clave privada correspondiente al par de claves asimétricas asociadas al SRD;

(b) el repositorio que almacena las correspondencias reales entre direcciones de red y direcciones físicas, habilitando al SRD como tercera parte de confianza en el proceso de resolución;

(c) la medida del tiempo común;

y en donde dicho servidor comprende medios configurados para recibir el mensaje de solicitud de resolución enviado por el cliente y medios configurados para enviar un mensaje de respuesta de resolución firmado digitalmente empleando su clave privada, en el que incluye la correspondencia entre dirección de red y dirección física solicitada por el cliente junto con una marca temporal indicativa del instante en que se realiza la operación de firma digital; y donde en el caso de que el SRD no conozca la dirección física solicitada, enviará en su lugar un valor especial que tendrá la consideración de nulo por ambas partes;

(ii) un elemento cliente con acceso a las direcciones físicas y de red del SRD; el certificado digital del SRD, conteniendo la clave pública del mismo; y la memoria caché de resolución de direcciones, que almacena temporalmente las correspondencias entre direcciones de red y direcciones físicas que se han obtenido mediante consultas al SRD siguiendo el procedimiento de resolución de direcciones del primer proceso lógico de la reivindicación 1;

en donde, dicho cliente comprende medios configurados para enviar un mensaje de solicitud de resolución hacia el SRD conteniendo la dirección de red; y medios configurados para recibir un mensaje de respuesta de resolución y aplicar la clave pública del SRD sobre la firma digital incluida en dicho mensaje para comprobar si éste ha sido emitido por el SRD, y comprobar si la marca temporal se corresponde con la hora local del cliente con una diferencia menor que la desviación máxima admisible, aceptando el cliente la correspondencia entre dirección de red y dirección físicas aportadas en el mensaje, incluyéndolas en la caché, sólo si ambas comprobaciones resultan positivas.

9. Sistema según la reivindicación 8 **caracterizado** porque las direcciones de red son direcciones IP definidas según la norma RFC791, y las direcciones físicas son direcciones MAC definidas según la norma IEEE Standard 802, siendo 00-00-00-00-00-00 la dirección MAC que se considera de valor nulo.

10. Sistema según la reivindicación 8 y 9 **caracterizado** porque el certificado digital del SRD es un certificado emitido por una Autoridad de Certificación.

11. Sistema según la reivindicación 8 y 9 **caracterizado** porque el certificado digital del SRD es un certificado autofirmado.

12. Sistema según la reivindicación 8, 9, y 10 o 11 **caracterizado** porque el repositorio está configurado para almacenar las correspondencias entre direcciones de red y direcciones físicas a las que tiene acceso el SRD se obtiene de el conjunto de asignaciones dinámicas realizadas por el servidor DHCP de la red de área local, en caso de existir, y de un conjunto de asignaciones estáticas, para aquellas asignaciones que no sean gestionadas por el servidor DHCP.

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 200901708

(22) Fecha de presentación de la solicitud: 03.08.2009

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
Y	BRUSCHI D; ORNAGHI A; ROSTI E. "S-ARP: a secure address resolution protocol". Proceedings. 19th Annual Computer Security Applications Conference, 2003. Págs: 66-74. 8-12 Dic. 2003. ISBN 978-0-7695-2041-4; ISBN 0-7695-2041-3 doi:10.1109/CSAC.2003.1254311.	1-12
Y	GOUDA M G; HUANG C-T. "A secure address resolution protocol". COMPUTER NETWORKS. VOL.: 41, Núm.: 1, Págs.: 57-71. 15-01-2003. ISSN 1389-1286 doi:10.1016/S1389-1286(02)00326-2.	1-12

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
07.10.2011	M. Muñoz Sanchez	1/5

CLASIFICACIÓN OBJETO DE LA SOLICITUD

G06F21/00 (2006.01)
H04L12/28 (2006.01)
H04W12/00 (2009.01)

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, H04L, H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

EPODOC, INVENES, WPI,XPMISC, XPI3E, XPIETF, XPIEE, XPESP, NPL, COMPDX

Fecha de Realización de la Opinión Escrita: 07.10.2011

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-12	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-12	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	BRUSCHI D; ORNAGHI A; ROSTI E. "S-ARP: a secure address resolution protocol". Proceedings. 19th Annual Computer Security Applications Conference, 2003. Págs: 66-74. 8-12 Dic. 2003. ISBN 978-0-7695-2041-4; ISBN 0-7695-2041-3 doi:10.1109/CSAC.2003.1254311	
D02	GOUDA M G; HUANG C-T. "A secure address resolution protocol". COMPUTER NETWORKS. VOL.: 41, Núm.: 1, Págs.: 57-71. 15-01-2003. ISSN 1389-1286 doi:10.1016/S1389-1286(02)00326-2	

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento del estado de la técnica más próximo al objeto de la solicitud.
Reivindicaciones independientes:
Reivindicación 1:
Siguiendo la redacción de la reivindicación 1, el documento D01 divulga un método de resolución de direcciones de red en direcciones físicas evitando envenenamiento de caché. En este método existe un servidor (AKD) encargado de distribuir a cada cliente una clave pública y otra privada. Este servidor tiene acceso a la medida de tiempo común y dispone también de una clave pública y otra privada.
Para resolver una dirección de red en una dirección física el procedimiento es análogo al protocolo ARP. La diferencia es la inclusión de información adicional de autenticación. Cuando un cliente recibe un mensaje de respuesta a un mensaje de solicitud de resolución, se verifica la autenticidad del emisor a través de la clave pública (certificado digital) asociada a su dirección ip, caso de encontrarse ya almacenada, o bien previa consulta al servidor obteniendo de este el certificado digital del emisor firmado con la clave privada del servidor que se autenticará en el cliente con la clave pública de dicho servidor.
Además cada cliente conoce la dirección MAC del servidor para poder comunicarse con él.
La diferencia del documento de la solicitud y D01 se refiere a utilizar una solución localizada en lugar de una distribuida en los clientes y con soporte del servidor (AKD). En esta alternativa las solicitudes se realizan directamente al SRD, del que cada cliente conoce además su dirección de red. El SRD almacena las correspondencias de direcciones de red y físicas y responde al cliente con un mensaje firmado que este tendrá que autenticar antes de modificar su tabla local de correspondencias entre direcciones de red y direcciones físicas. Se reserva además un valor especial con el significado de □dirección desconocida□.
El efecto técnico que se deriva de esta diferencia es una simplificación del procedimiento de resolución y una reducción del tráfico de red.
A la vista de D01 el problema técnico objetivo consistiría entonces en cómo simplificar el diseño del método y seguir previniendo el envenenamiento de caché.
En el documento D02 por su parte se divulga un protocolo de resolución de direcciones de red en direcciones físicas en el que cada cliente envía a un único servidor (del que conoce su dirección física/ip) una solicitud de resolución de dirección de red y este le responde con la dirección física correspondiente. Además se usa un secreto compartido por el cliente y el servidor para generar un hash para cada uno de los dos mensajes que se intercambian y que sirve como prueba de integridad. Por otra parte se devuelve una dirección física "vacía" en el caso de que la dirección de red solicitada sea desconocida por el servidor.
Teniendo en cuenta D01 y D02 el experto en la materia reconocería el problema técnico objetivo y combinaría los documentos D01 y D02 para resolverlo.
Por tanto la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el artículo 8.1 de la Ley de Patentes.
Reivindicación 8:
El sistema reivindicado se corresponde directamente con el método de la reivindicación 1 y por tanto la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 8 según el artículo 8.1 de la Ley de Patentes.
Reivindicaciones dependientes:
Reivindicación 2: elegir la dirección “0” es una opción de diseño alternativa a la dirección "vacía" que se divulga en D02.
Reivindicaciones 3 y 4: el contenido de estas reivindicaciones son meras opciones de diseño relativas a quién emite el certificado y que derivan en ventajas e inconvenientes conocidos por el experto en la materia.

Reivindicación 5: la interacción con un servidor DHCP para la gestión de direcciones de red dinámicas se contempla en D01 y asimismo en el caso de direcciones estáticas.
Reivindicaciones 6 y 7: la compatibilidad con ARP se contempla también en D01.
Por tanto la combinación de los documentos D01 y D02 afecta a la actividad inventiva de las reivindicaciones 2-7 según el artículo 8.1 de la Ley de Patentes.
Reivindicaciones 9-12: el contenido de estas reivindicaciones se corresponde directamente con las reivindicaciones dependientes del método reivindicado y por tanto la combinación de los documentos D01 y D02 afecta a la actividad inventiva de las reivindicaciones 9-12 según el artículo 8.1 de la Ley de Patentes.