



Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

I.E.

06010919

SOLICITUD

PATENTE DE INVENCION

06010919

21 EXPEDIENTE No

54 TÍTULO Sistema y Metodo para ESTABLECER
QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN
E-MAIL SEGURO Y COMPATIBLE

51 CLASIFICACIÓN INTERNACIONAL 206 F 17/60

71 SOLICITANTE MICROSOFT CORPORATION

DOMICILIO REDMOND, WASHINGTON, ESTADOS
UNIDOS DE AMERICA

74 APODERADO DARIO CALDENAS NAVAS

22 BOGOTÁ, D C.,

PETITORIO

Industria y Comercio
SUPERINTENDENCIA

REGISTRO Y COMERCIO
Radicación: 60/659-279-000000
Fecha (Hr): 2005-02-06 12:45:19
Trámite: 002 PATENTES D 1 REGISTRO/ 411 PRESENTAC
Procedencia: 2000 DIVISION DE NUEVAS OPERACIONES

Folios: 159

FORMULARIO UNICO DE SOLICITUD DE PATENTE 2000-3

SOLICITUD DE:

1

X

Patente de Invención

Patente de Modelo de Utilidad

SOLICITANTE
(71)

Nombre: MICROSOFT CORPORATION
Dirección: One Microsoft Way Redmond, Washington 98052, Estados Unidos de America.
Teléfono: 3123600 Fax: 3122410
E-Mail: general@cardenasycardenas.com
Lugar de Constitución: Estado de Washington, Estados Unidos de América.
Domicilio: REDMOND, WASHINGTON, ESTADOS UNIDOS DE AMERICA.

IDENTIFICACION

C.C. ☐ NIT ☐

C.E. ☐ Otro ☒

Número _____

REPRESENTANTE
O APODERADO
(74)

Nombre: DARIO CARDENAS NAVAS
Dirección: Carrera 7 No 71-52 Torre B Piso 9
Teléfono: 3123600 Fax: 3122410
E-Mail: general@cardenasycardenas.com

IDENTIFICACION

C.C. ☒ NIT ☐

C.E. ☐ Otro ☐

Número 17.068.629 BTA
TP 1.250 C.S.J.

INVENTOR(ES)
(72)

Nombre:
1. Eric D. Tribble
2. Trevor W. Freeman
1. One Microsoft Way Redmond, Washington 98052, Estados Unidos de América
Dirección: 2. One Microsoft Way Redmond, Washington 98052, Estados Unidos de América
Teléfono: 3123600 Fax: 3123600
E-Mail: general@cardenasycardenas.com
Domicilio:
1. REDMOND, WASHINGTON, ESTADOS UNIDOS DE AMERICA.
2. REDMOND, WASHINGTON, ESTADOS UNIDOS DE AMERICA.

IDENTIFICACION

C.C. ☐ NIT ☐

C.E. ☐ Otro ☒

Título(54):

SISTEMA Y METODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE

6

Prioridad

SI ☒ NO ☐

(33) País de Origen

U.S.A.

U.S.A.

(32) Fecha

Marzo 7, 2005

Abril 15, 2005

(31) N° de Solicitud

60/659,279

11/107,011

Para publicar a partir de la fecha de la presente solicitud a los:

☐ 6 meses ☐ 12 meses ☐ 18 meses ☐ Otro

ANEXOS

- ☒ Comprobante de pago de la tasa de presentación de la solicitud. (06-8,875)
- ☐ Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación.
- ☒ Comprobante de pago de la tasa por concepto de reivindicación de prioridad. (06-8,876 / 06-8,877)
- ☒ Poderes, si fuere el caso. (Protocolo No 16.068)
- ☒ Certificado de existencia y representación legal cuando el solicitante sea persona jurídica. Protocolo No 16.068)
- ☐ Copia certificada de la primera solicitud, si se reivindica prioridad.
- ☒ Traducción simple de la primera solicitud, si se reivindica prioridad.
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☒ Descripción de la invención.
- ☒ Una o más reivindicaciones.
- ☒ Dibujos y/o planos necesarios.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de la comunidad de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☒ Arte final 12x12 y 6x6 cm.
- ☒ Resumen y extracto para publicación.

10

NOMBRE:

DARIO CARDENAS NAVAS

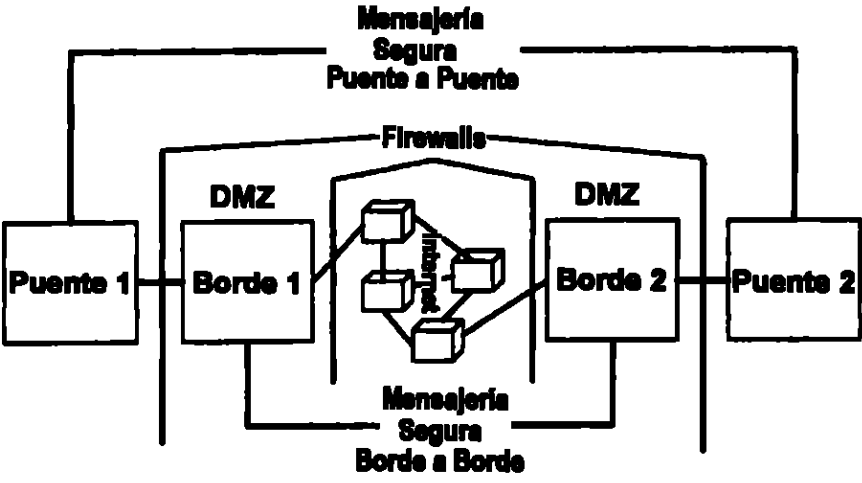
FIRMA:



C.C. 17.066.629 BTA

TP. 1.250 C.SJ.

FIG. 1



4

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 06 - 8,875
FECHA : FEBRERO 2 DE 2006

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Radicacion : 06010919 00000000 Folios: 159
Fecha (GPD) : 2006-02-06 12:45:19
Tramite : 002 PATENTES D 1 REGISTRAR 411 PRESENTAR
Dependencia : 2020 DIVISION DE NUEVAS CREACIONES

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PBO	Vr. PAGO
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519686	02/02/2006	4,149,000.00
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519687	02/02/2006	1,573,800.00

***** C O N C E P T O *****

NT. RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1 50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	463,000.00
	TOTAL :	\$ 463,000.00

SON: CUATROCIENTOS SESENTA Y TRES MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

Microsoft Corporation.

Sistema y método para establecer
que un servidor y un correspondiente
tienen e-mail seguro y compatible.

CARDENAS & CARDENAS
ABOGADOS

6

5

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 04 - 8.876
FECHA : FEBRERO 2 DE 2006

SUPERINDUSTRIA Y COMERCIO
Radicación : 46418919 000000000
Fecha (AMD) : 2006-02-06 12:45:19
Trámite : 002 PATENTES 0 1 REGISTRADO/ 411 PRESENYAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

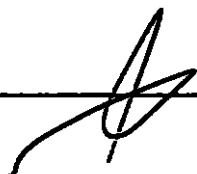
***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519686	02/02/2006	4,149,000.00
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519687	02/02/2006	1,573,800.00

***** C O N C E P T O *****

NT. RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1 50005-01-01 SOLICITUDES	82 INVOCACION DE UNA PRIORIDAD EN MU	130,000.00
	TOTAL :	\$ 130,000.00

SON: CIENTO TREINTA MIL PESOS

RESPONSABLE : 

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

Microsoft Corporation
Sistema y metodo para establecer
que un servidor y un correspondiente
tienen e-mail seguro y compatible

CARDENAS & CARDENAS
109/06

7

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Radicacion : 46410919
Fecha (MM): 2006-02-06 12:45:19
Folios: 159
Fuente : 002 PUNTOES D 1 REGISTRO/ 411 PRESENTAC
NIT : 800176089-2 Dependencia: 2620 DIVISION DE NUEVAS CREACIONES

RECIBO OFICIAL DE CAJA : 06 - 8,877
FECHA : FEBRERO 2 DE 2006

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519686	02/02/2006	4,149,000.00
CARDENAS Y CARDENAS P.I. CONSIGNACION		BANCO POPULAR	050-00110-6	47519687	02/02/2006	1,573,800.

***** CONCEPTO *****

NT. RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1 50005-01-01 SOLICITUDES	82 INVOCACION DE UNA PRIORIDAD EN NU	130,000.00
	TOTAL :	130,000.00

SOM: CIENTO TREINTA MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

Microsoft Corporation.
Sistema y método para establecer
que un servidor y un correspondiente
tienen e-mail seguro y compatible

CARDENAS & CARDENAS
ABOGADOS

APR 04 2005



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 148
Alexandria, Virginia 22313-1480
www.uspto.gov

APPL NO.	FILING OR 371 (s) DATE	ART UNIT	PL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLMS	IND CLMS
60/659,279	03/07/2005		200	MS#311810.01 (5189)	8		

000038779
SENNIGER, POWERS, LEAVIT & ROEDEL
ONE METROPOLITAN SQUARE, 18TH FLOOR
ST. LOUIS, MO 63102

CONFIRMATION NO. 3956

FILING RECEIPT



OC000000015813389

Date Mailed: 03/31/2005

Receipt is acknowledged of this provisional Patent Application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections, facsimile number 703-748-9195. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

Applicant(s)

Eric D. Tribble, Redmond, WA;
Trevor W. Freeman, Redmond, WA;

Power of Attorney: The patent practitioners associated with Customer Number 000038779.

If Required, Foreign Filing License Granted: 03/30/2005

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US60/659,279

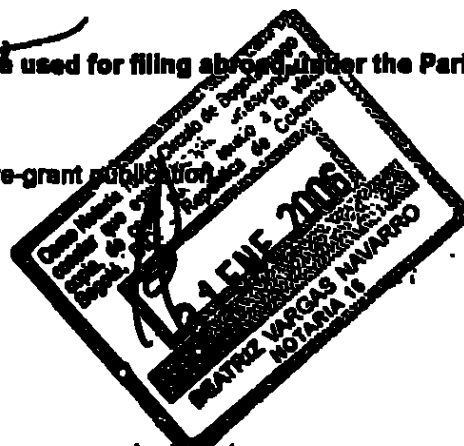
Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

System and method for establishing a link between a server and a target



LICENSE FOR FOREIGN FILIN UNDER

a
mmrr.

4

**Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15**

GRANTED

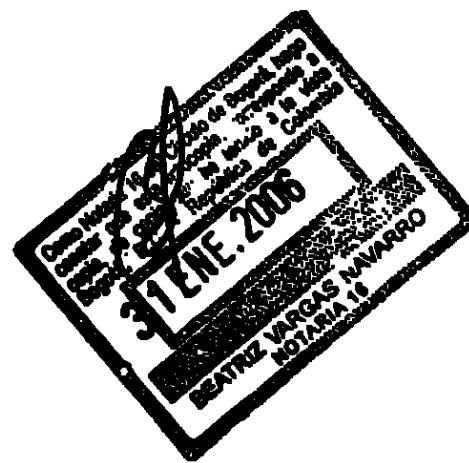
The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



10



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

9

MAY 13, 2005

PTAS

5000913824

ROBERT M. BAIN /FRA
ONE METROPOLITAN SQUARE, 16TH FLOOR
SENNIGER POWERS
ST. LOUIS, MO 63102

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT SERVICES DIVISION, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 05/13/2005

REEL/FRAME: 016013/0231
NUMBER OF PAGES: 2

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

✓ TRIBBLE, ERIC D.

✓ DOC DATE: 04/14/2005

ASSIGNOR:

✓ FREEMAN, TREVOR W.

✓ DOC DATE: 04/14/2005

ASSIGNEE:

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WASHINGTON 98052

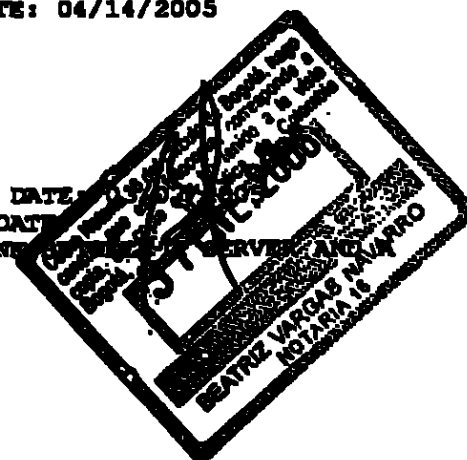
✓ SERIAL NUMBER: 60659279

PATENT NUMBER:

TITLE: SYSTEM AND METHOD FOR ESTABLISHING A LINE
TARGET ✓

FILING DATE: 05/13/2005

ISSUE DATE:

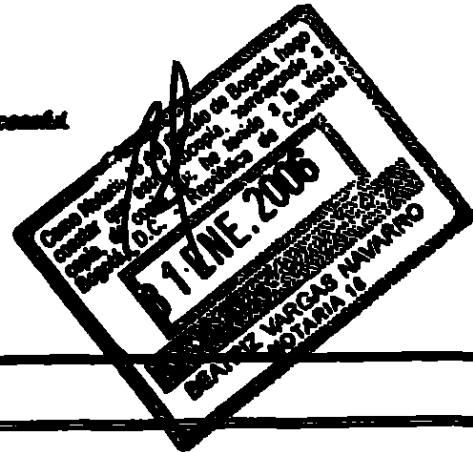
11
mm

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

05/13/2005
500031382

SUBMISSION TYPE:	NEW ASSIGNMENT										
NATURE OF CONVEYANCE:	ASSIGNMENT										
CONVEYING PARTY DATA											
<table border="1"><thead><tr><th>Name</th><th>Execution Date</th></tr></thead><tbody><tr><td>Eric D. Tribble</td><td>04/14/2005</td></tr><tr><td>Trevor W. Freeman</td><td>04/14/2005</td></tr></tbody></table>		Name	Execution Date	Eric D. Tribble	04/14/2005	Trevor W. Freeman	04/14/2005				
Name	Execution Date										
Eric D. Tribble	04/14/2005										
Trevor W. Freeman	04/14/2005										
RECEIVING PARTY DATA											
<table border="1"><tr><td>Name:</td><td>Microsoft Corporation</td></tr><tr><td>Street Address:</td><td>One Microsoft Way</td></tr><tr><td>City:</td><td>Redmond</td></tr><tr><td>State/Country:</td><td>WASHINGTON</td></tr><tr><td>Postal Code:</td><td>98062</td></tr></table>		Name:	Microsoft Corporation	Street Address:	One Microsoft Way	City:	Redmond	State/Country:	WASHINGTON	Postal Code:	98062
Name:	Microsoft Corporation										
Street Address:	One Microsoft Way										
City:	Redmond										
State/Country:	WASHINGTON										
Postal Code:	98062										
PROPERTY NUMBERS Total: 1											
<table border="1"><thead><tr><th>Property Type</th><th>Number</th></tr></thead><tbody><tr><td>Application Number:</td><td>80898279</td></tr></tbody></table>		Property Type	Number	Application Number:	80898279						
Property Type	Number										
Application Number:	80898279										
CORRESPONDENCE DATA											
Fax Number: (314)231-4342 <i>Correspondence will be sent via US Mail when the fax attempt is unsuccessful.</i>											
Phone: 3142316400											
Email: uspatents@senniger.com											
Correspondent Name: Robert M. Bain											
Address Line 1: One Metropolitan Square, 16th Floor											
Address Line 2: Senniger Powers											
Address Line 4: St. Louis, MISSOURI 63102											
NAME OF SUBMITTER:	Robert M. Bain										
Total Attachments: 1 source=000781478page1.tif											



PATENT ASSIGNMENT

I/WE, Eric D. Tribble and Trevor W. Freeman ("ASSIGNOR"), have invented subject matter ("INVENTION") disclosed and/or claimed in a patent application entitled "SYSTEM AND METHOD FOR ESTABLISHING A LINK BETWEEN A SERVER AND A TARGET" ("APPLICATION"), which:

☐ will be filed without this executed PATENT ASSIGNMENT. ASSIGNOR hereby authorizes, and requests, ASSIGNEE'S legal representatives, of SENNIGER POWERS, who are associated with customer number 000038779, to insert here in parenthesis (U.S. Serial No. 60/659,279, filed 03/07/2005) this APPLICATION's U.S. Serial Number and filing date, when known;

☒ was filed on March 7, 2005 and was given U.S. Serial No. 60/659,279;

☐ Is filed concurrently herewith;

Microsoft Corporation, a Washington Corporation, on behalf of itself and its successors and assigns ("ASSIGNEE"), is entitled to, and is desirous of acquiring, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and all other applications and patents derived therefrom, such as continuing applications, in and for the United States, its territories, and all foreign countries ("APPLICATION DERIVATIVES")):

For good and valuable consideration, the receipt of which is hereby acknowledged by the ASSIGNOR, the ASSIGNOR hereby sells, assigns and transfers to the ASSIGNEE, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and APPLICATION DERIVATIVES);

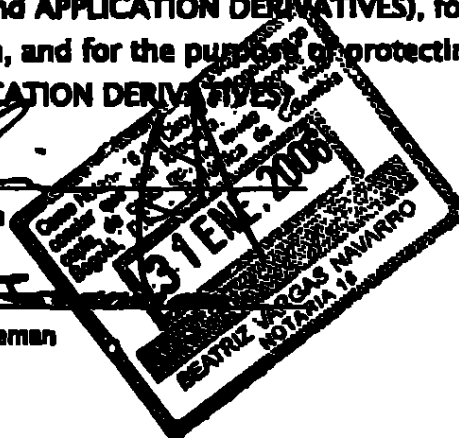
ASSIGNOR agrees to execute all instruments and documents required for the making and prosecution of the APPLICATION (and APPLICATION DERIVATIVES), for litigation regarding letters patent derived therefrom, and for the purpose of protecting and perfecting title to the APPLICATION (and APPLICATION DERIVATIVES).

4/14/05
DATE

4/14/05
DATE

[Signature]
Eric D. Tribble

[Signature]
Trevor W. Freeman

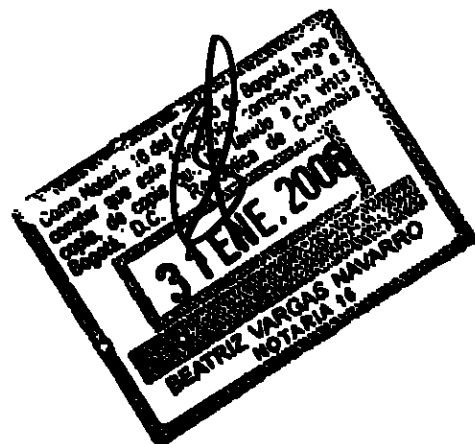


FRAcva

12

016013/0231 PAGE 2

DOROTHY RILEY, PARALEGAL
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS



14

13

SYSTEM AND METHOD FOR ESTABLISHING A LINK BETWEEN A SERVER AND A TARGET

TECHNICAL FIELD

[0001] Embodiments of the present invention relate to the field of establishing a compatible interconnection between two domains. In particular, embodiments of this invention relate to a system and method to reveal and discover mail servers with advanced capabilities.

BACKGROUND OF THE INVENTION

[0002] Some prior systems attempt to identify potential partners by communicating directly. However, these systems become vulnerable when communicating and, in particular, create a vulnerability to SPAM.

[0003] Accordingly, a system for discretely identifying a potential partner and progressive establishing a secure link between a server and a potential partner is desired to address one or more of these and other disadvantages.

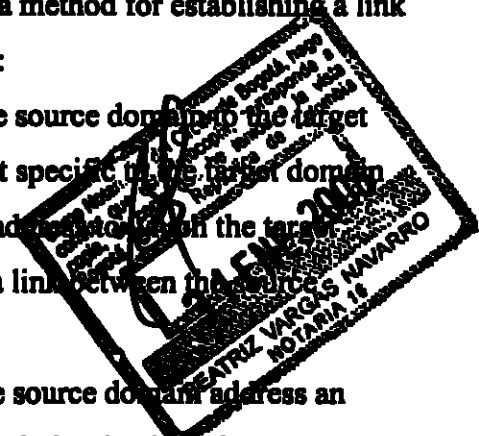
SUMMARY OF THE INVENTION

[0004] Embodiments of the invention include a method for establishing a link between a source domain and a target domain comprising:

[0005] Transmitting an advertisement from the source domain to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

[0006] Receiving by the source domain via the source domain address an invitation from the target domain wherein the invitation includes the data element or a data element corresponding to the data element wherein the source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

[0007] An advertisement is transmitted from the source domain to the target domain. The advertisement includes a data element specific to the target domain and.



CS

The advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain. The advertisement is received by the target domain including receiving the data element and the source domain address. An invitation is transmitted from the target domain to the source domain address. The invitation includes the data element or a data element corresponding to the data element. The source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

[0008] The invention also includes a system and a data structure.

[0009] Alternatively, the invention may comprise various other methods and apparatuses.

[0010] Other features will be in part apparent and in part pointed out hereinafter.

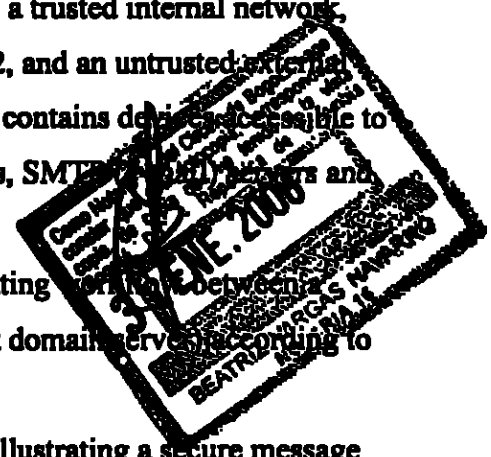
BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 is an exemplary block diagram of edge servers 1 and 2 within a DMZ and having secure messaging therebetween. The servers are connected via a firewall to bridges 1 and 2 which are part of a separate secure messaging system. Edge servers 1 and 2 form a subnetwork that is located between a trusted internal network, such as a secure messaging system linking bridges 1 and 2, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP servers and DNS servers via firewalls.

[0012] FIG. 2 is an exemplary diagram illustrating communication between a source domain server and a potential partner (e.g., a target domain server) according to the invention.

[0013] FIG. 3 is an exemplary block diagram illustrating a secure message manager according to the invention.

[0014] FIG. 4 is a flow diagram illustrating operation of SMM administrative routing according to the invention.



15

[0015] FIG. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention.

[0016] FIG. 6 is an exemplary block diagram illustrating an inter-organization workflow summary between a server (admin organization A) and a partner (admin organization B) according to the invention.

[0017] FIG. 7 is a flow diagram illustrating a state diagram after a new security association implemented between a server and a partner according to the invention.

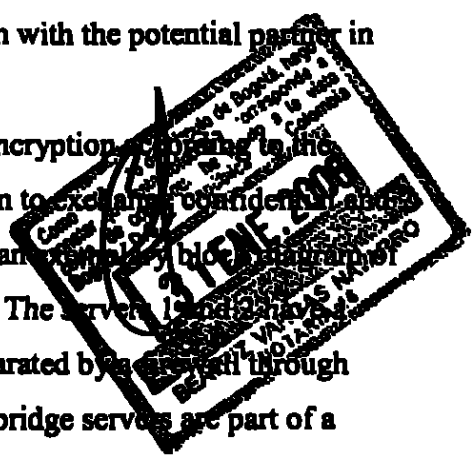
[0018] FIG. 8 is a block diagram illustrating one example of a suitable computing system environment in which the invention may be implemented.

[0019] Corresponding reference characters indicate corresponding parts throughout the drawings.

DETAILED DESCRIPTION OF THE INVENTION

[0020] The invention relates to a system and method for establishing a link between a server and a target. In particular, the invention relates to a system and method for establishing a secure link for the deployment of secure email. The invention allows a server to determine that a potential partner can be established as a target because of compatible secure email technology. As a result, once a potential partner is identified, the server can securely exchange key material information with the potential partner in order to establish the secure link.

[0021] The objective of domain signing and encryption according to the invention is to provide a transport independent mechanism to exchange confidential and server authenticated messages between servers. Fig. 1 is an exemplary block diagram of edge servers 1 and 2 within a demilitarized zone (DMZ). The servers 1 and 2 have a secure messaging link therebetween. The servers are separated by a firewall through which they are connected to bridge servers 1 and 2. The bridge servers are part of a secure messaging system. Edge servers 1 and 2 form a sub-network that is located between a trusted internal network, such as the secure messaging system linking bridge servers 1 and 2 and the untrusted external network, such as the public internet. Firewalls are also positioned between the edge servers and the internet. In this illustration of Fig.



17

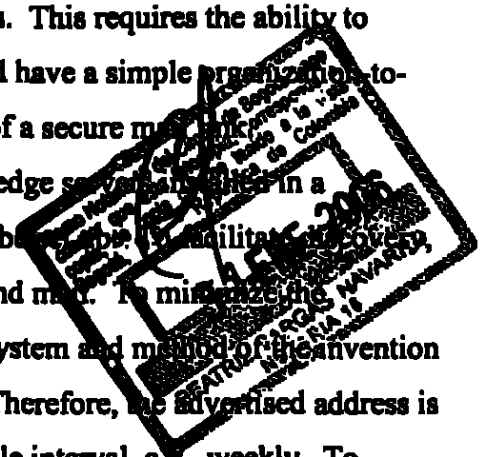
1/b

1, edge server 1 can exchange signed and encrypted mail with edge server 2 and bridge server 1 can exchange signed and encrypted mail with bridge server 2. In addition, bridge server 1 can forward to its DMZ edge server 1 either signed or signed and encrypted mail where the decryption recipient is bridge server 2. The edge servers treat all mail as clear text and encrypt all mail edge to edge. If the edge and bridge servers do not share the same encryption keys, the edge servers cannot decrypt bridge encrypted mail.

[0022] There is a need for a single point of administration for the authoritative data for all internal and external relationships. Optionally, a single master model rather than a multiple-master model is implemented because it is simpler and because it does not have to resolve replication conflicts. Secure message management (SMM) operations are usually infrequent and the database size is usually small so that there is sufficient time to repair or replace hardware or do a system restore before any loss of service. In one embodiment, critical data for operation is replicated to other edge servers. Since there is no single point of management, not all data is replicated and the replicated data is read only.

[0023] A server may engage with a number of its partners to set up secure mail links for a specific project. However, the management coordination of such projects does not usually scale. For secure messaging to make an impact, secure mail is enabled with the majority of the organizations business partners. This requires the ability to discover which partners have edge servers installed and have a simple organization-to-organization workflow to negotiate the establishment of a secure mail link.

[0024] The invention permits discovery of edge servers installed in a organization's partners so that a secure connection can be established. To facilitate discovery the server advertises the presence of itself with outbound mail. To minimize the advertisement process being vulnerable to attack, the system and method of the invention do not use a hard coded address in its advertisement. Therefore, the advertised address is a random mailbox name which can rotate at a reasonable interval, e.g., weekly. To ensure that the vulnerabilities are minimized, the advertisement is also bound to the domain to which it is sent, e.g., the target domain. In the event that the advertising

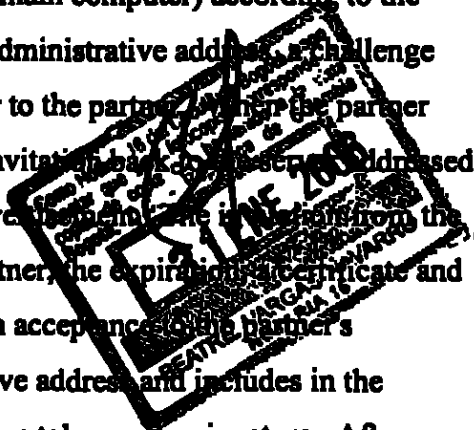


18

address is discovered by a third party the only domain that would be affected is the domain whose invitation address was compromised.

[0025] In one form, the advertisement is an 822 header containing the ephemeral 822 address for invitations and the expiration time in hours of the 822 address relative to when the message was sent. Inbound mail is filtered by the receiving server (e.g., target or partner server) for advertisements from edge servers and compared against a list of known edge servers. Any additions to that list are communicated to the local administrative SMM. On discovery of a new edge server, the SMM can send a probe message (e.g., an invitation) to the other SMM to offer a turn on domain signing and encryption. On receipt of an invitation or advertisement from another SMM administrator, if the message is verifiable under the existing trust policy then the local SMM could invoke a policy to automatically accept the invitation. Alternatively, the SMM administrator may require manual approval before accepting the invitation. On receipt of the invitation acceptance by the server, if the message is intrinsically verifiable, then the receiving SMM would invoke a policy to automatically start using domain signing and encryption. The configuration of a new secure domain is an asynchronous process and is not used for real data until the link is confirmed operationally by receipt of the ping acknowledgements.

[0026] Fig. 2 is a exemplary diagram illustrating workflow between a source domain server and a potential partner (e.g., target domain computer) according to the invention. Initially, an advertisement including an administrative address, a challenge token and an expiration date are sent from the server to the partner. When the partner recognizes the advertisement, the partner sends an invitation back to the server addressed to the administrative address that was part of the advertisement. The invitation from the partner includes an administrative address of the partner, the expiration, a certificate and the challenge token. In response, the server sends an acceptance to the partner's administrative address from the server's administrative address and includes in the acceptance the expiration, the certificate, the challenge token and a signature. After receipt of the acceptance, the partner pings the server and the ping is acknowledged by the server to establish the connection. If the invitation message is not verifiable using the

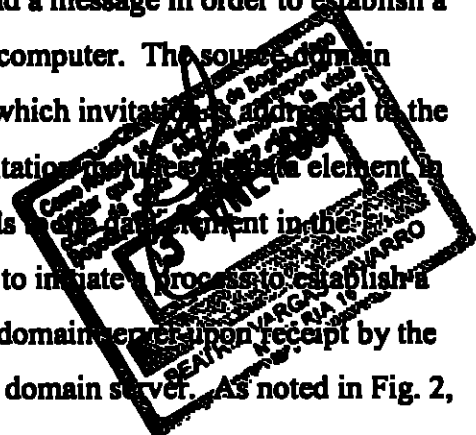


14

trust policy as illustrated in Fig. 2, then the request may be cued awaiting manual approval.

[0027] Referring to Fig. 3, an exemplary block diagram illustrating a secure message manager according to the invention is illustrated. The acceptance of the invitation by the partner creates a cross certificate on the administrative SMM agent which is then pushed to the worker SMM agents along with the encryption certificate. The cross certificate constrains the set of names accepted by the new trust and the restriction to domain edge server communication. In order to facilitate improved performance, the sending SMMs assign a session key and reuse the session key across multiple messages to a recipient SMM. The session key may also be distributed in this case from administration SMM to all worker SMM so all workers use the same key to reduce cache size. To allow for scaling out, the corresponding decryption private key for the encryption certificate should be available on all internet facing edge servers to allow any to decrypt inbound mail. This may be generated in a single place, i.e., the administration agent and distributed to all worker servers. Once a trust relationship is established, it should be maintained. For example, the original certificate may be retained and a renewal request sent to the other SMMs before the certificate expires.

[0028] From the server's perspective, the method according to the invention establishes a link between a source domain and a target domain. Initially a source domain server transmits an advertisement to potential target domains. The advertisement includes a data element such as a mention or a token or other secret which is specifically assigned to the target domain. In addition, the advertisement includes a source domain address to which the target domain is permitted to send a message in order to establish a link between the source domain server and the target computer. The source domain server receives an invitation from the target domain which invitation is addressed to the source domain address previously provided. The invitation includes a data element in the advertisement or a data element which corresponds to the data element in the advertisement. This allows the source domain server to initiate a process to establish a link between the target domain server and the source domain server upon receipt by the source domain server of the invitation from the target domain server. As noted in Fig. 2,



201

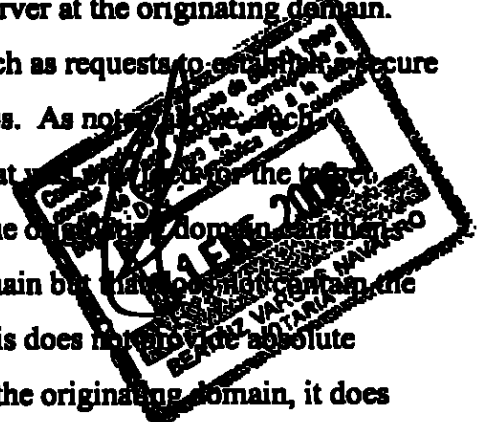
19

the source domain server transmits an acceptance to the target domain server to establish the link therebetween.

[0029] In one embodiment, the source domain selectively transmits the advertisement to target domains from which the source domain has received a message. Alternatively or in addition, the source domain may send advertisements to target domains which have been specifically identified in advance. Alternatively or in addition, the source domain may send the advertisement to randomly selected target domains.

[0030] In one embodiment, the advertisement may be a message which is generated in response to user action. Alternatively or in addition, the advertisement may be a message with a single target domain and/or a message to a target domain which is an operator. The single message to the target domain may be for each key and it may be sent on a time-based determination (e.g., one message per hour). For example, the user action may be NDRs or return receipts.

[0031] In one embodiment of the invention, an email server occasionally adds an additional header (an "x-header") to a message that will be delivered to another email domain. The data in the header includes a secret that is specific to the target domain and the email address to which the administrative messages from the target domain can be directed back to the email server. If mail at the target domain is also directed through a server that implements this embodiment of the invention, then it will detect the additional header and determine that there may be a compatible server at the originating domain. The target domain then directs administrative traffic such as requests to establish a secure connection to the contained administrative email address. As noted above, each administrative messages must also contain the secret that was specified for the target domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the target domain but that does not contain the secret corresponding to the target domain. Although this does not provide absolute assurance that the received administrative mail is from the originating domain, it does minimize the vulnerability to SPAM at the administrative address and ensures that even an attacker that can see email to the target domain can only attempt to spoof administrative addresses from the target domain rather than from any domain.



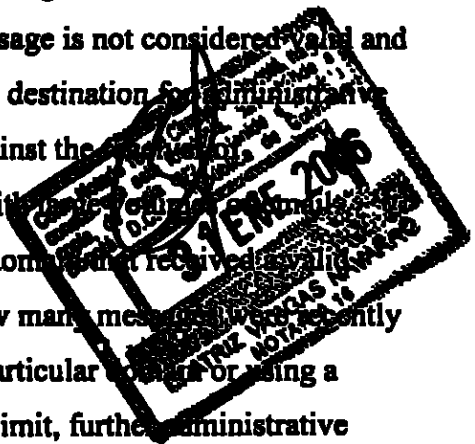
21

20

[0032] In one embodiment, the invention is implemented by using a header, called a mention, that is attached to an already outbound email from the source domain. This mention reveals the availability of specific functions on the mail server originating the outbound email while avoiding the need for generating additional, possibly undesirable, messages. As noted above, the administrative email address would be included in the mention and there would be a per-domain secret, called a token to mitigate risks of SPAM to the administrative email address. This would support workflow messages at the administrative email address.

[0033] The token (or secret) may be generated from a hash of the target domain and a secret seed that is kept on the originating server. This allows a single seed to be shared across multiple servers, so that each server will generate the same token unique to any target domain. When an administrative message is received at the originating server (because it is directed to the administrative address included in the mention), the token provided in the administrative messages is checked by the originating server. To check the token, the email server generates a token for the domain that sent the administrative message using the current internal seed. If the generated token is the same as the one in the administrative messages, then that message has the correct token and is passed through to the appropriate destination for administrative messages. If the token does not match, then the same process is applied to prior tokens (up to a bounded number). If none of the currently valid seeds can be used to generate a token that matches the token in the incoming message, then the message is not considered valid and is discarded or rejected, and not passed on to the eventual destination for administrative messages. This prevents unauthorized SPAM attacks against the destination of administrative messages, which may be unable to cope with large volumes of emails. Additionally, to prevent denial of service attacks from a domain that received a valid token, the verification process is able to keep track of how many messages were recently passed through to the administrative destination from a particular domain or using a particular token. When that number exceeds an allowed limit, further administrative messages using that token are discarded or rejected.

[0034] Fig. 4 is a flow diagram illustrating operation of the SMM administrative routing according to the invention. The signature verification and



22

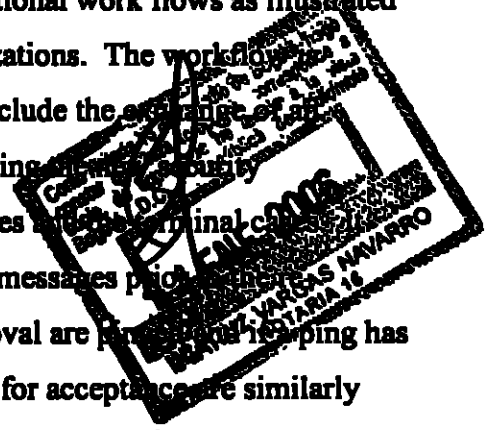
21

decryption must happen before any anti-SPAM processing because the output from the verification is necessary to set the message property flags used by the anti-SPAM agent. Signature verification should happen after the RBL and other IP address level functions. Thus, the process begins with receiving messages at the source domain address to which the target domain is permitted to send a message at 402. If it is determined at 404 that the token is not valid for the sender address, the message is dropped at 406 and the routing process ends. If the token is valid, the process proceeds to 408 to determine if the domain has a maximum account which has been exceeded. If the maximum has been exceeded, the message is dropped at 406; otherwise, if the signature is valid at 410 the message is routed to the local administrative agent.

[0035] Fig. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention. SMM signing and encryption is the last function generally. Each message going to a domain with a secure message relationship is signed and encrypted. This component also inserts the header containing the current SMM ephemeral address to all mail going to domains without a security relationship. As shown in Fig. 5, the domain looks for a valid signature at 502 and an external address at 504 after finding a valid token. If the signature is valid and there is no external address, the message is routed to the local worker agent at 506. If there is an external address, it is routed to such. Without a valid signature the message is dropped.

[0036] In one embodiment, the inter-organizational work flows as illustrated in Fig. 6 are implemented between administrative organizations. The work flows are performed by the SMM administrative agents and may include the exchange of an encryption key rollover. Fig. 7 is a state diagram illustrating the security association. This diagram only considers the positive cases and does not include other aspects such as re-transmission of messages prior to a transmission limit. In general, domains looking for approval are processed and if a ping has been received the domain is approved. Domains looking for acceptance are similarly handled.

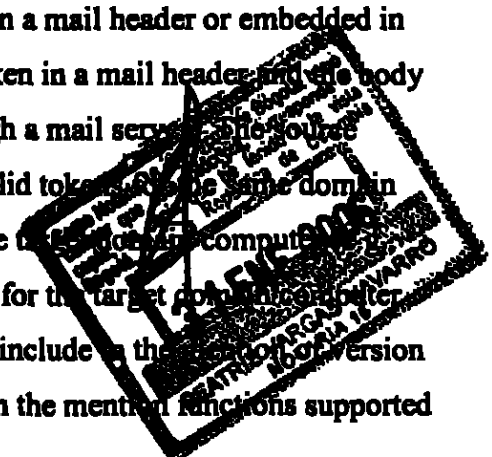
[0037] Other optional features of the invention include the following which may be implemented separately or in combination. The advertisement may comprise an expiration date in which case the source domain server would not initiate the process to



23

22

establish a link with the target domain computer (e.g., server) computer when receipt by the source domain server of the invitation is after the expiration date. The data element may be at least one of the following: a per domain secret including a pseudorandom number for each target domain computer (e.g., server), a secret generated via hashing the target domain computer (e.g., server) and a secret seed that is used to generate per-domain secrets for more than one domain; and a per-domain secret generated encrypting the target domain computer (e.g., server) and an expiration date of the secret. The data element may comprise a secret in which case the source domain server would verify the secret received from the target domain computer (e.g., server) by re-computing and then comparing the current secret for the target domain computer (e.g., server) with the secret included in the advertisement. The data element may be selected from a plurality of multiple overlapping secrets for each target domain computer (e.g., server) so that there are a plurality of valid secrets that can be used for communicating from a target domain computer (e.g., server) to the administrative address of the originating domain. A limit may be imposed on the number of messages that are passed to the source domain server address with a particular data element so that denial of service attacks using a correct data element are mitigated. The source domain server may include the ability to override the requirement for a data element for a given target domain computer (e.g., server) to enable out-of-band authorization to send invitation messages from a particular domain. The data element may be a token in the advertisement message in a mail header or embedded in the body of a message or the data element may be a token in a mail header and the body of the message remains encrypted when passing through a mail server. The source domain server may support multiple simultaneously valid tokens for the domain and verify invitation messages from sub-domains of the target domain computer (e.g., server) by verifying the incoming token against tokens for the target domain computer (e.g., server). The data element may be a mention and include in the mention or version information for the source domain server and include in the mention functions supported by the source domain server.



[0038] In one embodiment the invention comprises a data structure for the advertisement to be transmitted from the source domain server to the target domain computer (e.g., server). As noted above, this data structure is used to establish a link

24

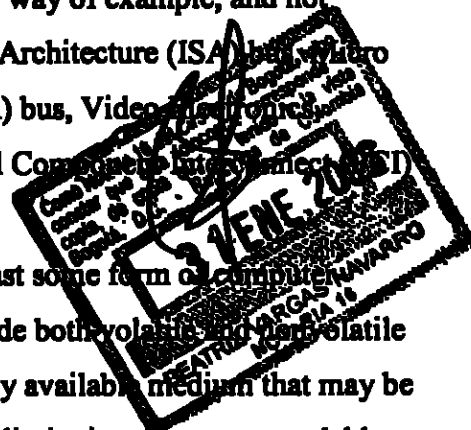
23

between the source domain server and the target domain computer (e.g., server). The data structure includes a message and its usual header relating to the message. Additionally, the data structure includes an additional header attached to the message and message header and including a data element specific to the target domain computer (e.g., server). The header also includes a source domain server address to which the target domain computer (e.g., server) is permitted to send a message to the source domain server in order to establish a link between the source domain server and the target domain computer (e.g., server). As noted above, the additional header should include an expiration date, although this is optional.

[0039] Exemplary Operating Embodiment:

[0040] FIG. 8 shows one example of a general purpose computing device in the form of a computer 130. In one embodiment of the invention, a computer such as the computer 130 is suitable for use in the other figures illustrated and described herein. Computer 130 has one or more processors or processing units 132 and a system memory 134. In the illustrated embodiment, a system bus 136 couples various system components including the system memory 134 to the processors 132. The bus 136 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0041] The computer 130 typically has at least some form of computer readable media. Computer readable media, which include both volatile and non-volatile media, removable and non-removable media, may be any available medium that may be accessed by computer 130. By way of example and not limitation, computer readable media comprise computer storage media and communication media. Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. For example,



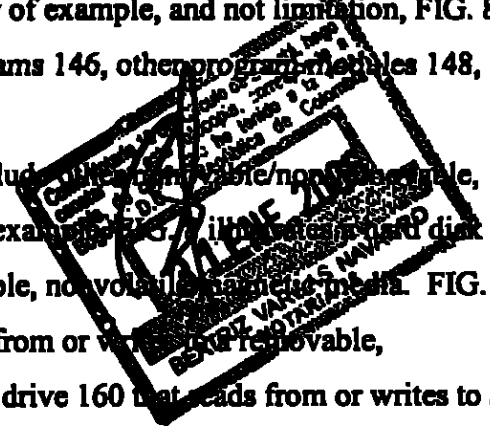
27

24

computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that may be used to store the desired information and that may be accessed by computer 130. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Those skilled in the art are familiar with the modulated data signal, which has one or more of its characteristics set or changed in such a manner as to encode information in the signal. Wired media, such as a wired network or direct-wired connection, and wireless media, such as acoustic, RF, infrared, and other wireless media, are examples of communication media. Combinations of any of the above are also included within the scope of computer readable media.

[0042] The system memory 134 includes computer storage media in the form of removable and/or non-removable, volatile and/or nonvolatile memory. In the illustrated embodiment, system memory 134 includes read only memory (ROM) 138 and random access memory (RAM) 140. A basic input/output system 142 (BIOS), containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is typically stored in ROM 138. RAM 140 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 132. By way of example, and not limitation, FIG. 8 illustrates operating system 144, application programs 146, other program modules 148, and program data 150.

[0043] The computer 130 may also include other removable/non-removable, volatile/nonvolatile computer storage media. For example, FIG. 8 illustrates a hard disk drive 154 that reads from or writes to non-removable, nonvolatile magnetic media. FIG. 8 also shows a magnetic disk drive 156 that reads from or writes to a removable, nonvolatile magnetic disk 158, and an optical disk drive 160 that reads from or writes to a removable, nonvolatile optical disk 162 such as a CD-ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that may be used in the exemplary operating environment include, but are not limited to, magnetic



26

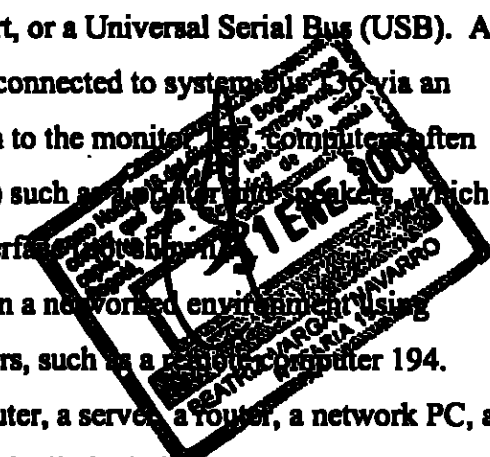
25

tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 154, and magnetic disk drive 156 and optical disk drive 160 are typically connected to the system bus 136 by a non-volatile memory interface, such as interface 166.

[0044] The drives or other mass storage devices and their associated computer storage media discussed above and illustrated in FIG. 8, provide storage of computer readable instructions, data structures, program modules and other data for the computer 130. In FIG. 8, for example, hard disk drive 154 is illustrated as storing operating system 170, application programs 172, other program modules 174, and program data 176. Note that these components may either be the same as or different from operating system 144, application programs 146, other program modules 148, and program data 150. Operating system 170, application programs 172, other program modules 174, and program data 176 are given different numbers here to illustrate that, at a minimum, they are different copies.

[0045] A user may enter commands and information into computer 130 through input devices or user interface selection devices such as a keyboard 180 and a pointing device 182 (e.g., a mouse, trackball, pen, or touch pad). Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to processing unit 132 through a user input interface 184 that is coupled to system bus 136, but may be connected by other interface and bus structures, such as a parallel port, game port, or a Universal Serial Bus (USB). A monitor 188 or other type of display device is also connected to system bus 136 via an interface, such as a video interface 190. In addition to the monitor 188, computers often include other peripheral output devices (not shown) such as a printer and speakers, which may be connected through an output peripheral interface 192.

[0046] The computer 130 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 194. The remote computer 194 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to computer 130. The logical connections depicted in FIG. 8 include a local area network (LAN) 196 and a wide area network (WAN) 198, but



27

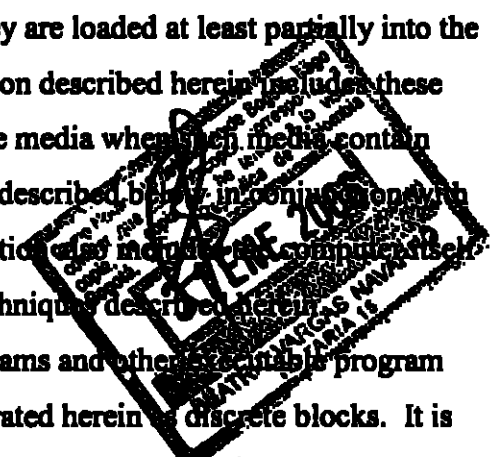
26

may also include other networks. LAN 136 and/or WAN 138 may be a wired network, a wireless network, a combination thereof, and so on. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and global computer networks (e.g., the Internet).

[0047] When used in a local area networking environment, computer 130 is connected to the LAN 196 through a network interface or adapter 186. When used in a wide area networking environment, computer 130 typically includes a modem 178 or other means for establishing communications over the WAN 198, such as the Internet. The modem 178, which may be internal or external, is connected to system bus 136 via the user input interface 184, or other appropriate mechanism. In a networked environment, program modules depicted relative to computer 130, or portions thereof, may be stored in a remote memory storage device (not shown). By way of example, and not limitation, FIG. 8 illustrates remote application programs 192 as residing on the memory device. The network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0048] Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described below in connection with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described herein.

[0049] For purposes of illustration, programs and other executable program components, such as the operating system, are illustrated herein as discrete blocks. It is recognized, however, that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.



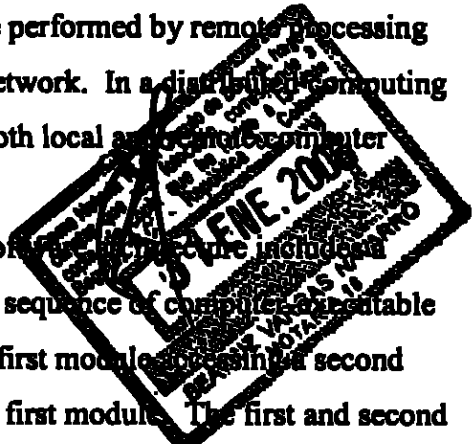
29

2

[0050] Although described in connection with an exemplary computing system environment, including computer 130, the invention is operational with numerous other general purpose or special purpose computing system environments or configurations. The computing system environment is not intended to suggest any limitation as to the scope of use or functionality of the invention. Moreover, the computing system environment should not be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the exemplary operating environment. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0051] The invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0052] An interface in the context of a software architecture includes a software module, component, code portion, or other sequence of computer-executable instructions. The interface includes, for example, a first module providing a second module to perform computing tasks on behalf of the first module. The first and second modules include, in one example, application programming interfaces (APIs) such as provided by operating systems, component object model (COM) interfaces (e.g., for peer-to-peer application communication), and extensible markup language metadata interchange format (XMI) interfaces (e.g., for communication between web services).



29

28

[0053] The interface may be a tightly coupled, synchronous implementation such as in Java 2 Platform Enterprise Edition (J2EE), COM, or distributed COM (DCOM) examples. Alternatively or in addition, the interface may be a loosely coupled, asynchronous implementation such as in a web service (e.g., using the simple object access protocol). In general, the interface includes any combination of the following characteristics: tightly coupled, loosely coupled, synchronous, and asynchronous. Further, the interface may conform to a standard protocol, a proprietary protocol, or any combination of standard and proprietary protocols.

[0054] The interfaces described herein may all be part of a single interface or may be implemented as separate interfaces or any combination therein. The interfaces may execute locally or remotely to provide functionality. Further, the interfaces may include additional or less functionality than illustrated or described herein.

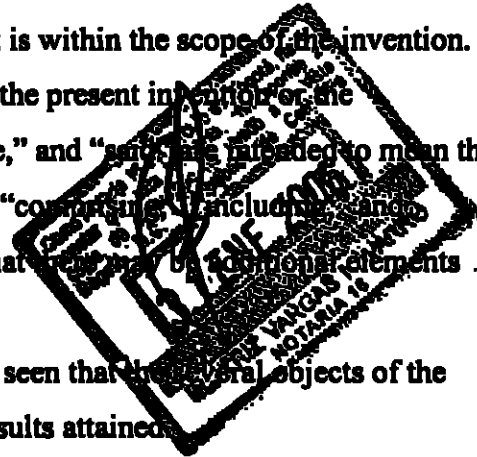
[0055] In operation, computer 130 operates as either the source domain server or the target domain computer (which may be a server) to execute computer-executable instructions as noted above, such as those illustrated in Figs. 2-7.

[0056] The order of execution or performance of the methods illustrated and described herein is not essential, unless otherwise specified. That is, elements of the methods may be performed in any order, unless otherwise specified, and that the methods may include more or less elements than those disclosed herein. For example, it is contemplated that executing or performing a particular element before, contemporaneously with, or after another element is within the scope of the invention.

[0057] When introducing elements of the present invention or the embodiment(s) thereof, the articles "a," "an," "the," and "one" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0058] In view of the above, it will be seen that the several objects of the invention are achieved and other advantageous results attained.

[0059] As various changes could be made in the above constructions, products, and methods without departing from the scope of the invention, it is intended



30

that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.



What is claimed is:

- 1. A method for establishing a link between a source domain and a target domain comprising:**

Transmitting an advertisement from the source domain to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

Receiving by the source domain via the source domain address an invitation from the target domain wherein the invitation includes the data element or a data element corresponding to the data element wherein the source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.

- 2. The method of claim 1 further comprising transmitting an acceptance from the source domain to the target domain to establish the link therebetween.**

3. The method of claim 1 wherein the advertisement is selectively transmitted to at least one of the following:

Target domains from which the source domain has received

Target domains specifically identified in advance; and

Randomly selected target domains.

4. The method of claim 1 wherein the advertisement is a message which is generated in response to user action; wherein the advertisement is a message with a single target domain; wherein the advertisement is a message to a target domain which is an operator; wherein the advertisement is a single message to the target domain for each key; or wherein the advertisement is a message send on a time-based determination.

- 5. The method of claim 1 wherein the advertisement comprises an additional header which includes the data element and the source domain address.**

31

6. The method of claim 1 wherein the advertisement comprises an expiration date and wherein the source domain does not initiate the process to establish a link with the target domain when receipt by the source domain of the invitation is after the expiration date.

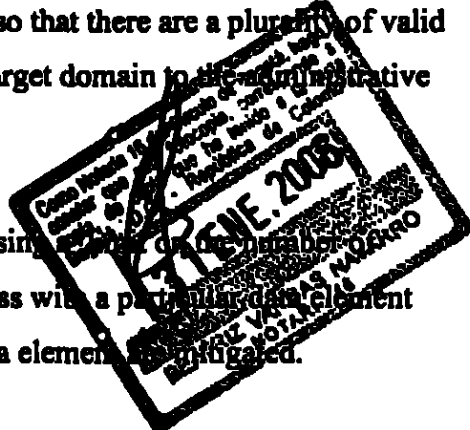
7. The method of claim 1 wherein the data element is at least one of the following:
a per domain secret including a pseudorandom number for each target domain;
a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain; and
a per-domain secret generated encrypting the target domain and an expiration date of the secret.

8. The method of claim 1 wherein the data element comprises a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement.

9. The method of claim 1 wherein the data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain.

10. The method of claim 1 further comprising imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of service attacks using a correct data element is mitigated.

11. The method of claim 1 further comprising including the ability to override the requirement for a data element for a given target domain to enable out-of-band authorization to send invitation messages from a particular domain.



11

33

12. The method of claim 1 wherein the data element is a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server.

13. The method of claim 1 further comprising supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the target domain by verifying the incoming token against tokens for the target domain.

14. The method of claim 1 wherein the data element is a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

15. A data structure for an advertisement to be transmitted from a source domain to a target domain for establishing a link between the source domain and the target domain comprising:

A message;

A header relating to the message; and

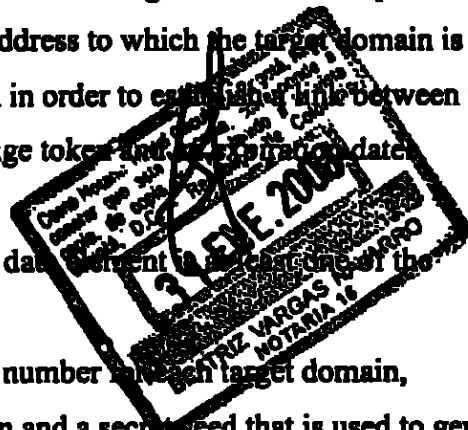
An additional header attached to the message and including a data element specific to the target domain and including a source domain address to which the target domain is permitted send a message to the source domain in order to establish a link between the source domain and the target domain, a challenge token and an expiration date.

16. The data structure of claim 15 wherein the data element is a secret one of the following:

a per domain secret including a pseudorandom number for each target domain,

a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain;

a per-domain secret generated encrypting the target domain and an expiration date of the secret;



33

a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement;

a data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain;

a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server; and

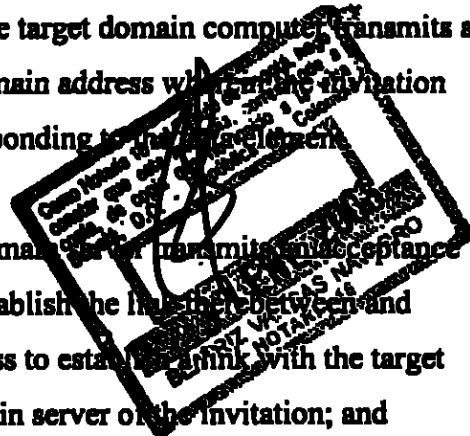
a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

17. A system for establishing a link between a source domain and a target domain comprising:

A source domain server transmitting an advertisement to the target domain wherein the advertisement includes a data element specific to the target domain and wherein the advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain; and

A target domain computer receiving the advertisement including receiving the data element and the source domain address wherein the target domain computer transmits an invitation from the target domain to the source domain address wherein the invitation includes the data element or a data element corresponding to the data element.

18. The system of claim 17 wherein the source domain server transmits an acceptance from the source domain to the target domain to establish the link between and wherein the source domain server initiates a process to establish a link with the target domain computer upon receipt by the source domain server of the invitation; and further comprising at least one of the following:



35

34

imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of Service attacks using a correct data element are mitigated;

overriding the requirement for a data element for a given target domain to enable out-of-band authorization to send invitation messages from a particular domain; and

supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the target domain by verifying the incoming token against tokens for the target domain.

19. The system of claim 17 wherein the advertisement transmitted by the source domain service comprises at least one of the following:

An advertisement selectively transmitted to target domains from which the source domain has received a message;

an advertisement selectively transmitted to target domains specifically identified in advance or randomly selected target domains;

a message which is generated in response to user action (e.g., NDRs, return receipts);

a message with a single target domain;

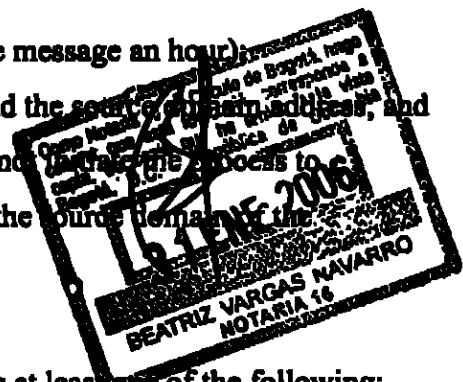
a message to a target domain which is an operator;

a single message to the target domain for each key;

a message send on a time-based determination (e.g., one message an hour);

an additional header which includes the data element and the source domain address, and

an expiration date and wherein the source domain does not establish a link with the target domain when receipt by the source domain invitation is after the expiration date.



20. The system of claim 17 wherein the data element is at least one of the following:

a per domain secret including a pseudorandom number for each target domain,

a secret generated via hashing the target domain and a secret seed that is used to generate per-domain secrets for more than one domain;

a per-domain secret generated encrypting the target domain and an expiration date of the secret;

36

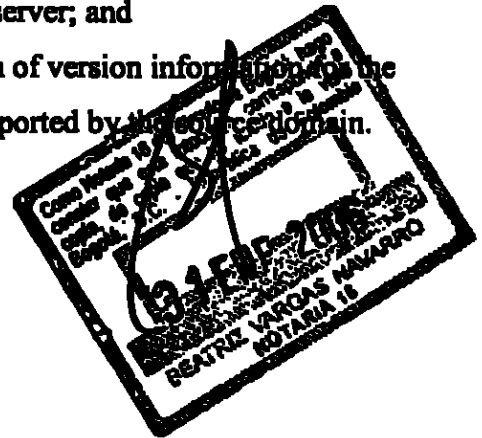
35

a secret and wherein the source domain verifies the secret received from the target domain by re-computing and then comparing the current secret for the target domain with the secret included in the advertisement;

a data element is selected from a plurality of multiple overlapping secrets for each target domain so that there are a plurality of valid secrets that can be used for communicating from a target domain to the administrative address of the originating domain;

a token in the advertisement message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server; and

a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.



37

ABSTRACT

An advertisement is transmitted from the source domain to the target domain. The advertisement includes a data element specific to the target domain and. The advertisement includes a source domain address to which the target domain is permitted send a message in order to establish a link between the source domain and the target domain. The advertisement is received by the target domain including receiving the data element and the source domain address. An invitation is transmitted from the target domain to the source domain address. The invitation includes the data element or a data element corresponding to the data element. The source domain initiates a process to establish a link with the target domain upon receipt by the source domain of the invitation.



FIG. 1

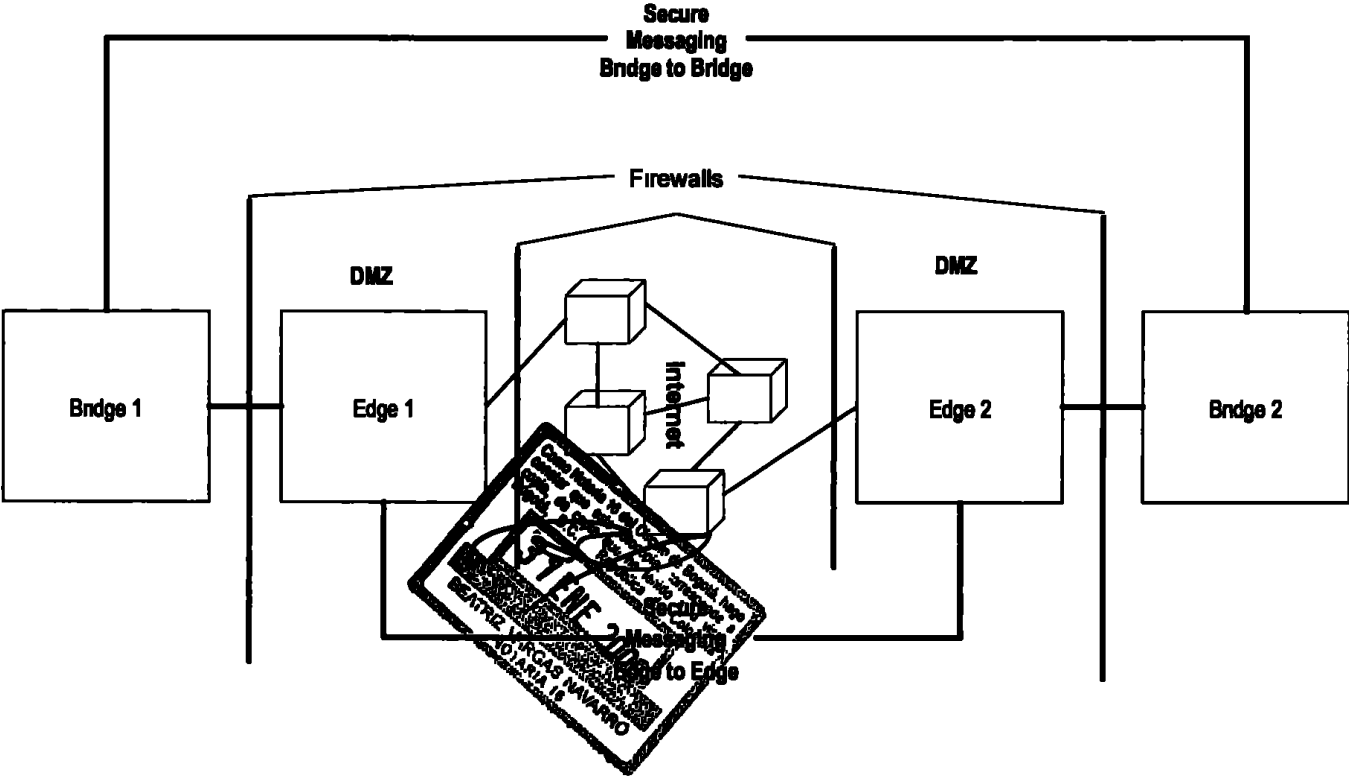


FIG. 2

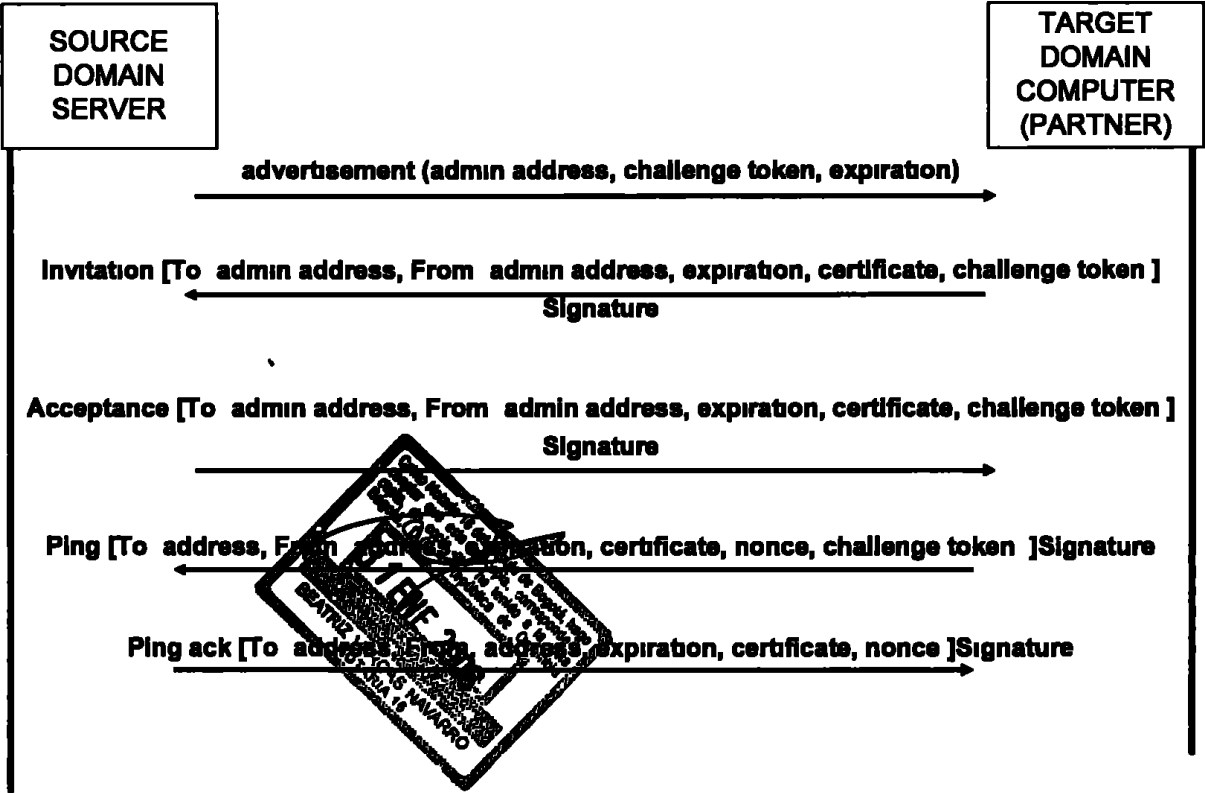


FIG. 3

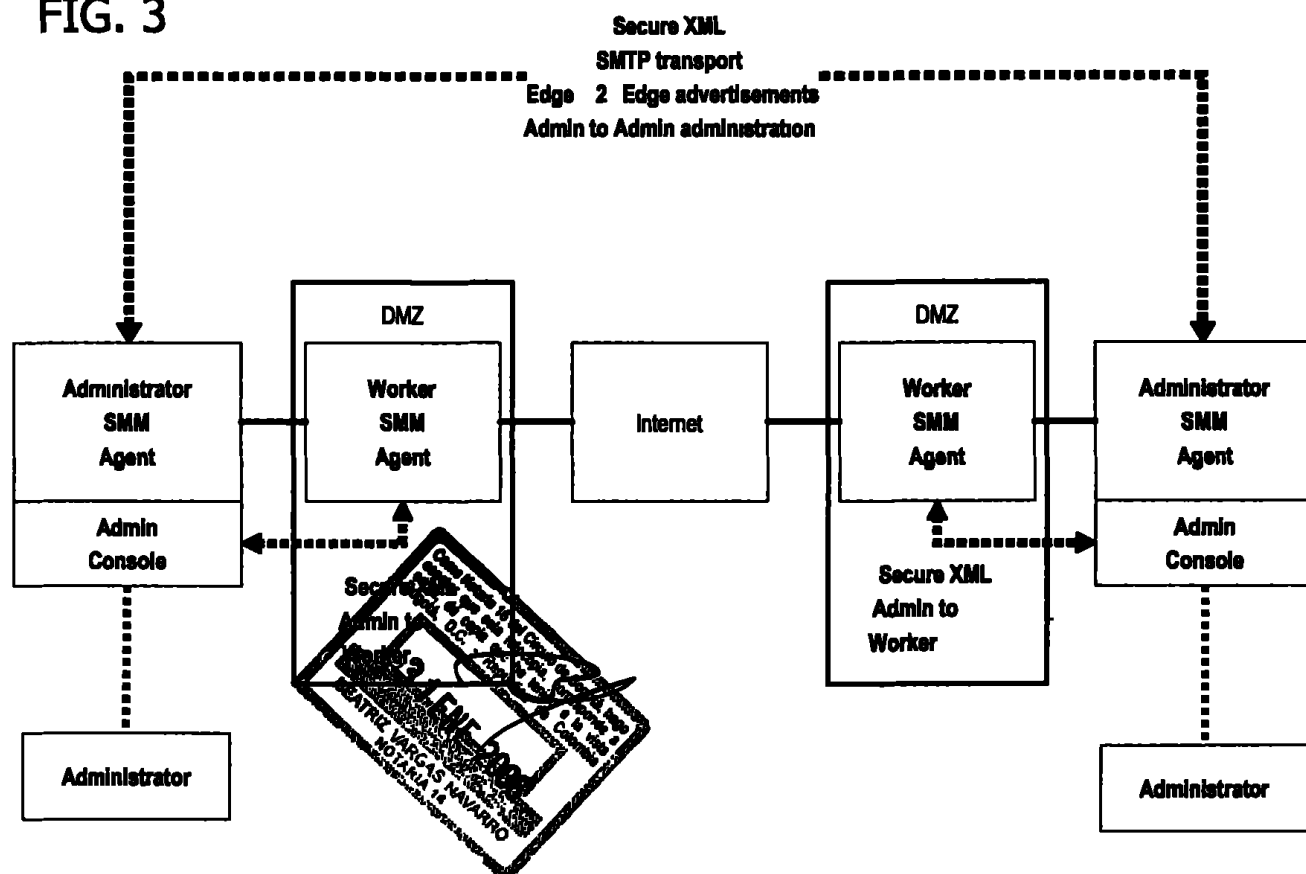


FIG. 4

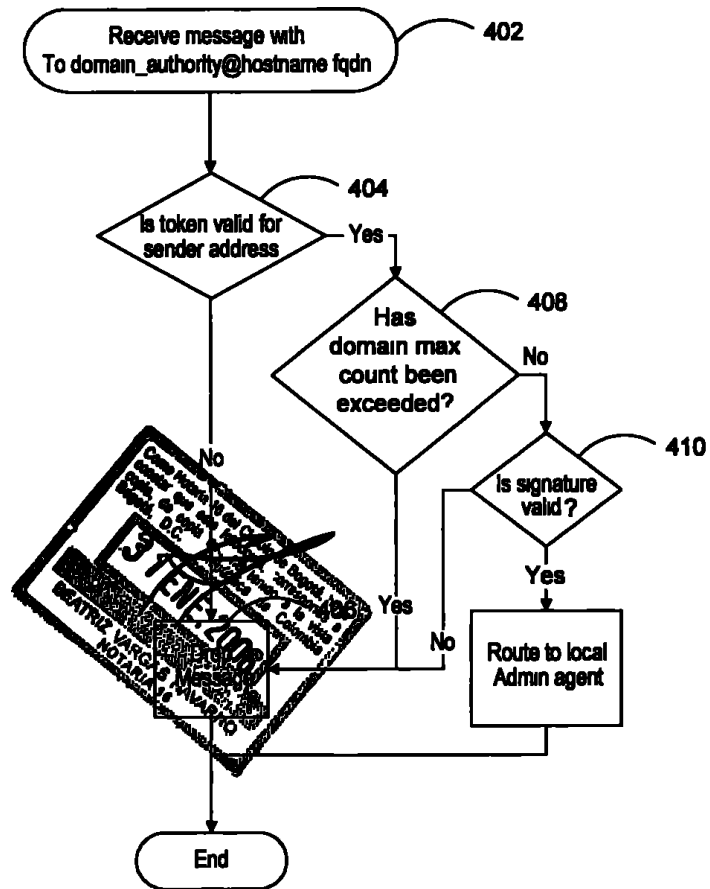
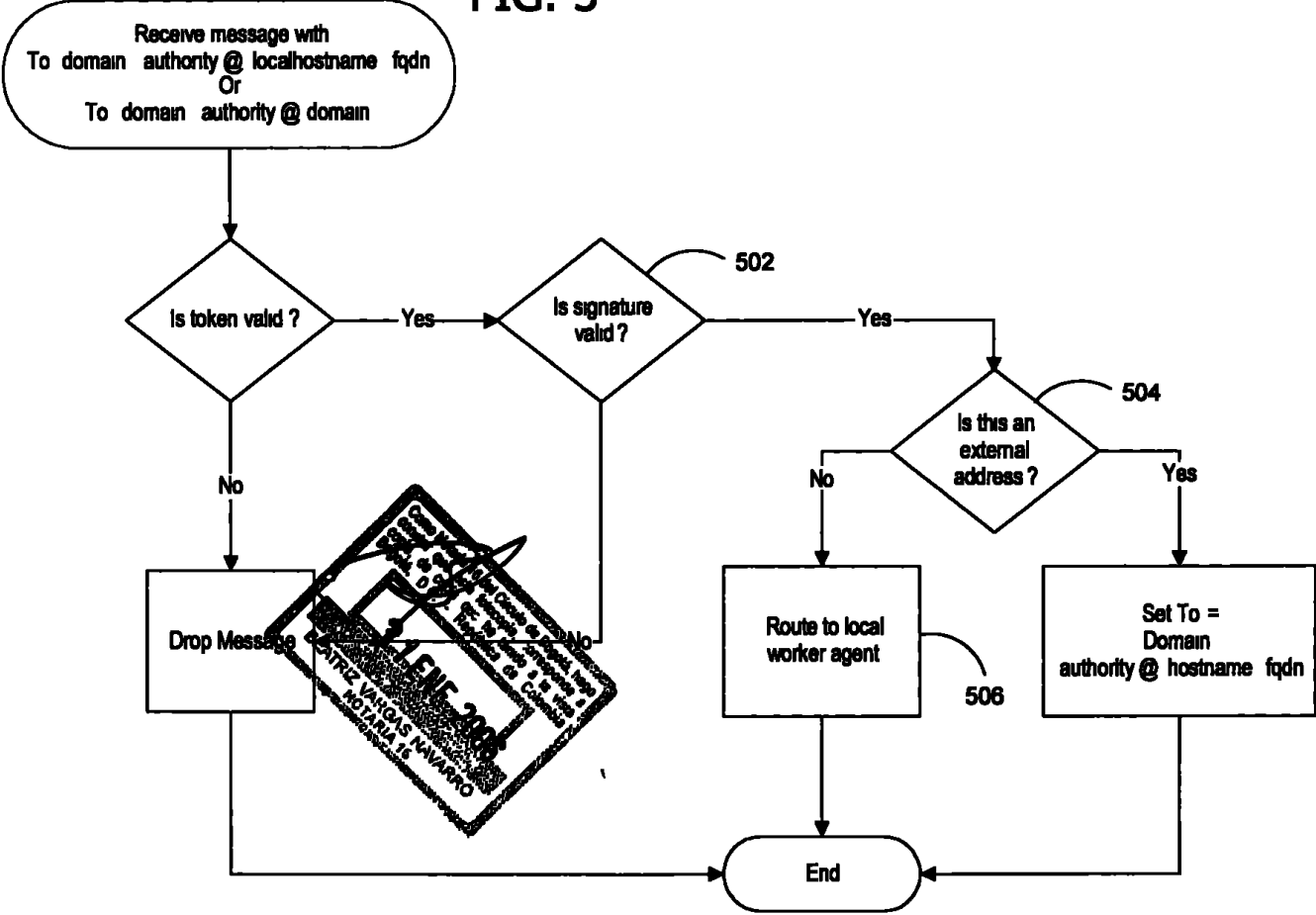


FIG. 5



5

FIG. 6

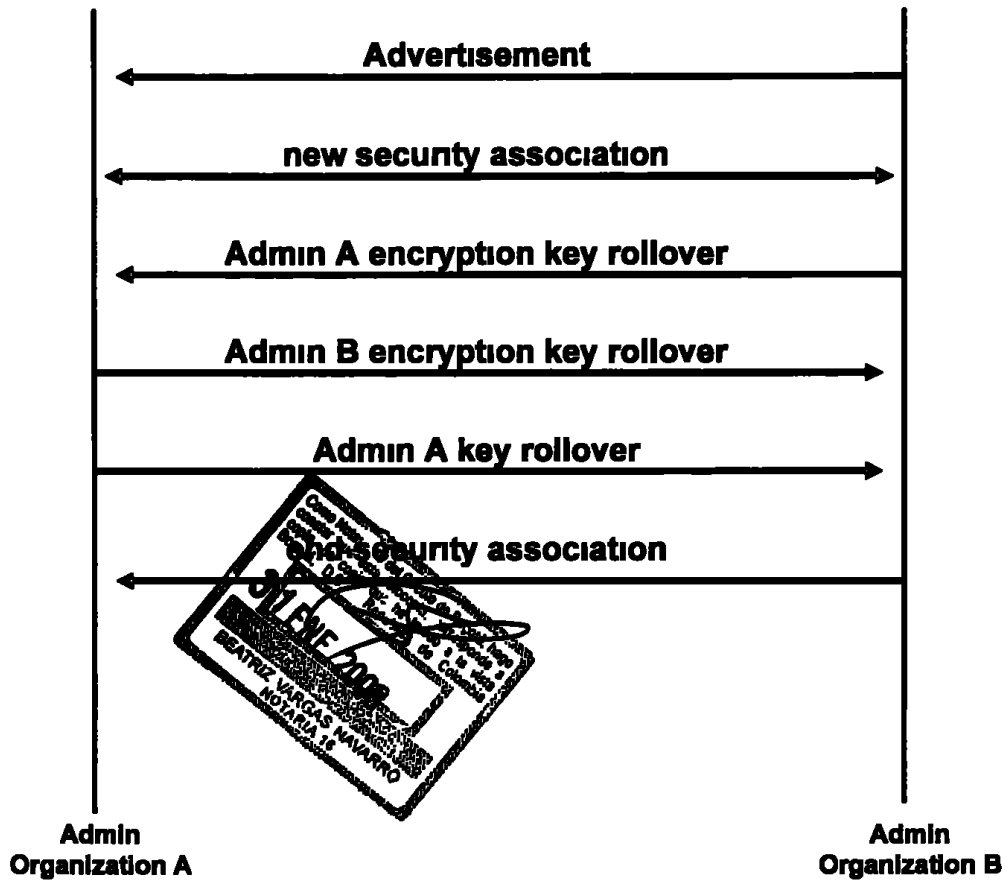
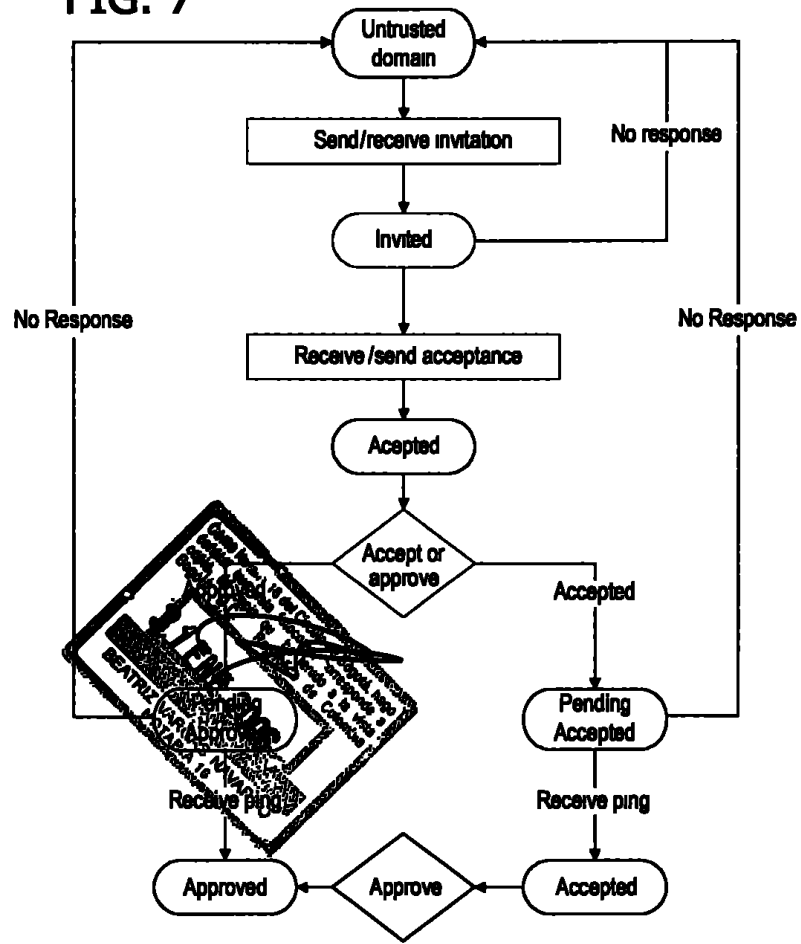
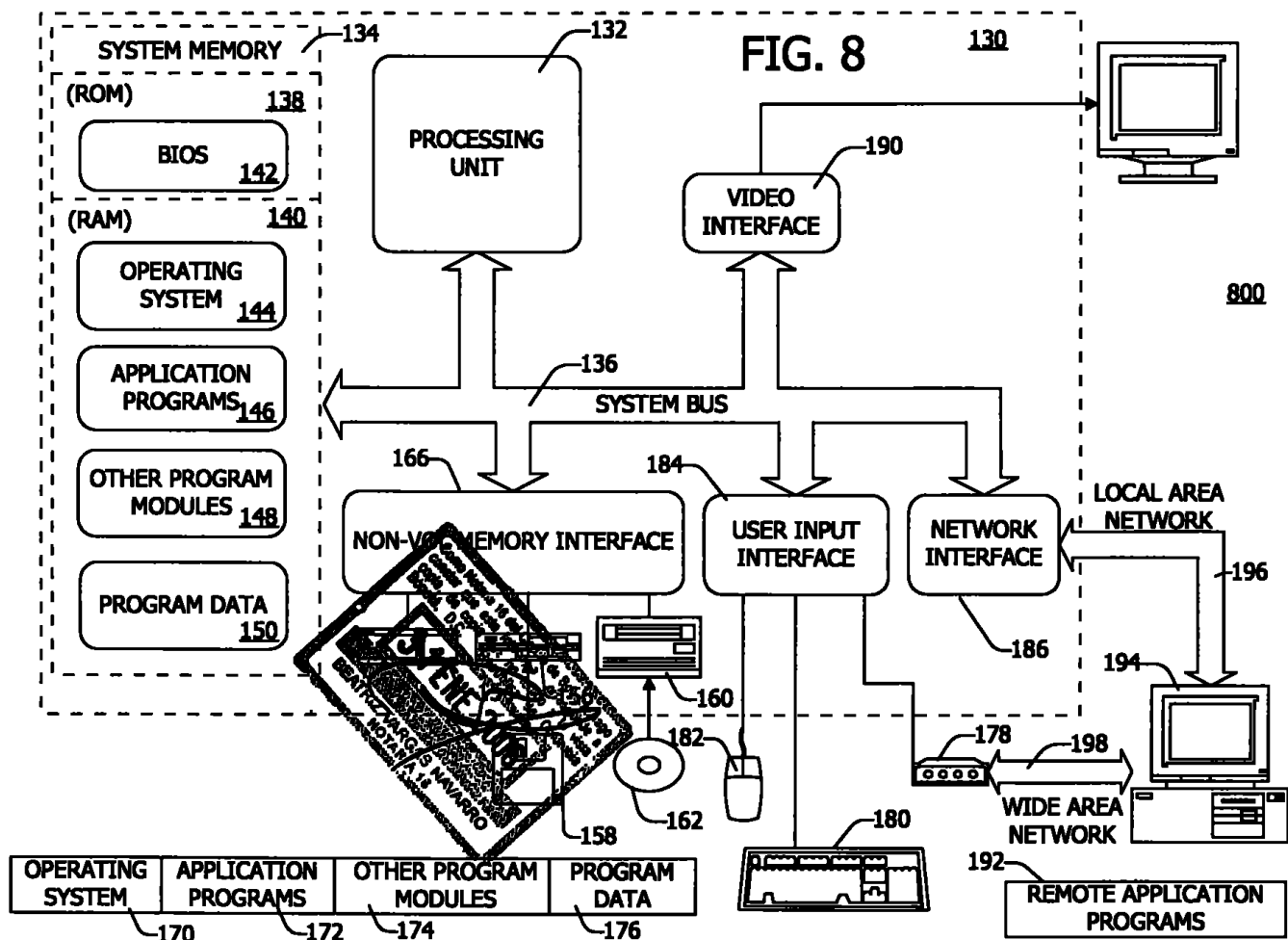


FIG. 7







UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Assistant Secretary and Commissioner
of Patents and Trademarks
Washington, D.C. 20231



*500084342A

JUNE 06, 2005

PTAS

ROBERT M. BAIN /FRA
ONE METROPOLITAN SQUARE, 16TH FLOOR
SENNIGER POWERS
ST. LOUIS, MO 63102

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT SERVICES DIVISION, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 06/06/2005

REEL/FRAME: 016095/0930
NUMBER OF PAGES: 2

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

✓ TRIBBLE, ERIC D.

✓ DOC DATE: 04/14/2005

ASSIGNOR:

✓ FREEMAN, TREVOR W.

✓ DOC DATE: 04/14/2005

ASSIGNEE:

✓ MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WASHINGTON 98052

✓ SERIAL NUMBER: 11107011

✓ PATENT NUMBER:

✓ TITLE: SYSTEM AND METHOD FOR ESTABLISHING
CORRESPONDENT HAVE COMPATIBLE SECURE

✓ FILED

INDEXED

CLASSIFIED

SERIALIZED

FILED

JUN 10 2005

FBI - NEW YORK

NOTARY PUBLIC

BEATRIZ VARGAS NAVARRO

NOTARIA 16

mmr:

46

46

016095/0930 PAGE 2

ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS



42

48

PATENT ASSIGNMENT

I/WE, Eric D. Tribble and Trevor W. Freeman ("ASSIGNOR"), have Invented subject matter ("INVENTION") disclosed and/or claimed in a patent application entitled "SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL" ("APPLICATION"), which:

☒ will be filed without this executed PATENT ASSIGNMENT. ASSIGNOR hereby authorizes, and requests, ASSIGNEE'S legal representatives, of SENNIGER POWERS, who are associated with customer number 000038779, to insert here in parenthesis (U.S. Serial No. 11/107,011, filed 04/15/2005) this APPLICATION's U.S. Serial Number and filing date, when known;

☐ was filed on and was given U.S. Serial No.;

☐ is filed concurrently herewith;

Microsoft Corporation, a Washington Corporation, on behalf of itself and its successors and assigns ("ASSIGNEE"), is entitled to, and is desirous of acquiring, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and all other applications and patents derived therefrom, such as continuing applications, in and for the United States, its territories, and all foreign countries ("APPLICATION DERIVATIVES"));

For good and valuable consideration, the receipt of which is hereby acknowledged by the ASSIGNOR, the ASSIGNOR hereby sells, assigns and transfers to the ASSIGNEE, the entire and exclusive rights, title and interest in the INVENTION and the APPLICATION (and APPLICATION DERIVATIVES);

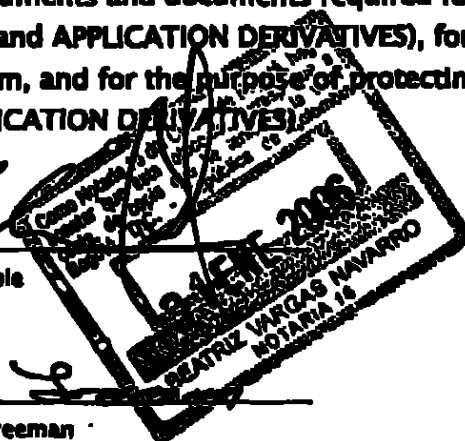
ASSIGNOR agrees to execute all instruments and documents required for the making and prosecution of the APPLICATION (and APPLICATION DERIVATIVES), for litigation regarding letters patent derived therefrom, and for the purpose of protecting and perfecting title to the APPLICATION (and APPLICATION DERIVATIVES);

4/14/05
DATE

4/14/05
DATE

Eric D. Tribble

Trevor W. Freeman



FRAcwa

49



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MAY 16 2005

APPL NO.	FILING OR 371 (a) DATE	ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLMS	IND CLMS
11/107,011	04/15/2005	2131	1000	MS#311610.02 (5169.1)	8	20	3

CONFIRMATION NO. 5704

000038779

SENNIGER, POWERS, LEAVIT & ROEDEL
ONE METROPOLITAN SQUARE, 16TH FLOOR
ST. LOUIS, MO 63102

FILING RECEIPT



0C000000016022012

Date Mailed: 05/13/2005

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

Applicant(s)

Eric D. Tribble, Redmond, WA;
Trevor W. Freeman, Sammamish, WA;

Assignment For Published Patent Application

Microsoft Corporation, Redmond, WA

Power of Attorney: The patent practitioners associated with Customer Number 000038779

Domestic Priority data as claimed by applicant

This appln claims benefit of 60/659,279 03/07/2005

Foreign Applications

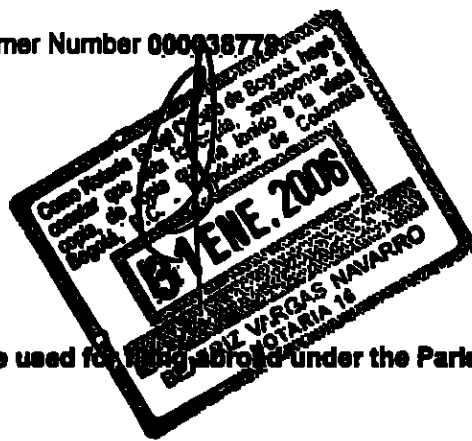
If Required, Foreign Filing License Granted: 05/13/2005

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US11/107,011**

Projected Publication Date: 09/07/2006

Non-Publication Request: No

Early Publication Request: No



Title

System and method for establishing that a server and a correspondent have compatible secure email

Preliminary Class

713

**LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15**

GRANTED

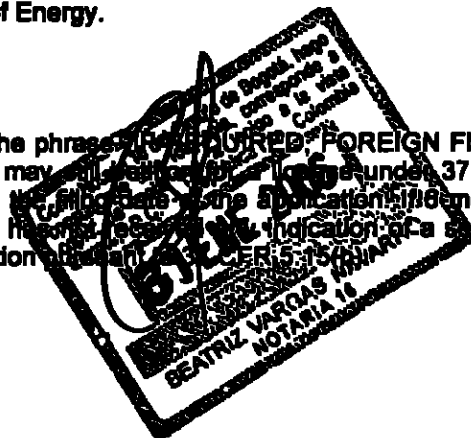
The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still obtain a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received an indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



51

SYSTEM AND METHOD FOR ESTABLISHING THAT A SERVER AND A CORRESPONDENT HAVE COMPATIBLE SECURE EMAIL

TECHNICAL FIELD

[0001] Embodiments of the present invention relate to the field of establishing a compatible interconnection between two domains. In particular, embodiments of this invention relate to a system and method to reveal and discover mail servers with advanced capabilities.

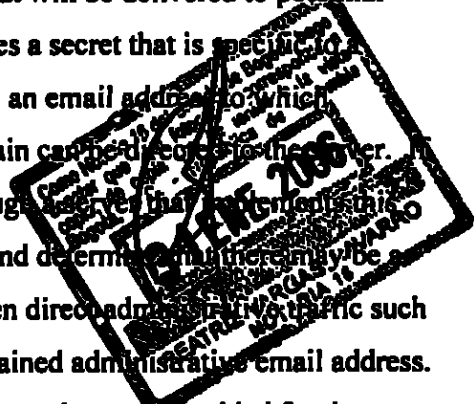
BACKGROUND OF THE INVENTION

[0002] Some prior systems attempt to identify potential correspondents by communicating directly. However, these systems become vulnerable to attackers when communicating and, in particular, can cause or be vulnerable to SPAM and denial of service attacks.

[0003] Accordingly, a system is desired to address one or more of these and other disadvantages by discretely identifying a potential correspondent so that a secure link between a server and a potential correspondent may be established.

SUMMARY OF THE INVENTION

[0004] Embodiments of the invention include an email server which occasionally adds an additional header to a message that will be delivered to potential correspondent domains. The data in the header includes a secret that is specific to a message sent to a particular correspondent domain and an email address to which administrative messages from that correspondent domain can be directed to the server. If mail at the correspondent domain is also directed through a server that implements this embodiment, then it will detect the additional header and determine that there may be a compatible server at the originating domain. It can then direct administrative traffic such as requests to establish a secure connection to the contained administrative email address. Such administrative messages must also contain the secret that was provided for that correspondent domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the correspondent domain but that does not contain the secret corresponding to the correspondent domain.



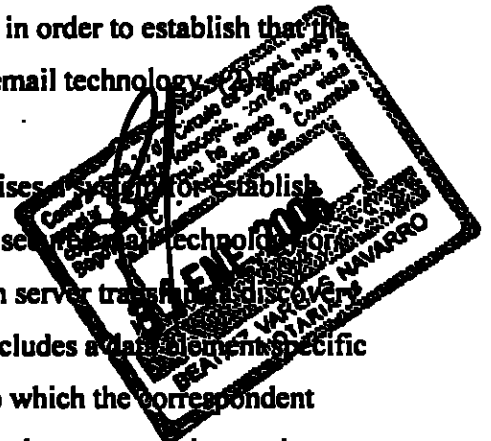
52

52

[0005] In an embodiment, the invention includes a method for determining that a potential correspondent domain has compatible secure email technology in order to establish a link between a source domain and a correspondent domain. A discovery secret is transmitted from the source domain to the correspondent domain. The discovery secret includes a data element specific to the correspondent domain and a source domain address to which the correspondent domain is permitted send a message in order to establish compatibility between the source domain and the correspondent domain. The source domain receives via the source domain address an invitation from the correspondent domain. The invitation includes the data element or an element corresponding to the data element which may be used by the correspondent domain to initiate a process to establish compatibility with the correspondent domain.

[0006] In accordance with one aspect of the invention, a data structure is provided for a discovery secret to be transmitted from a source domain to a correspondent domain for establishing that the correspondent and source domains have compatible secure email technology or other email or communication technology. The discovery secret includes a message; a header relating to the message; and an additional header attached to the message. The additional header includes (1) a data element specific to the correspondent domain and including a source domain address to which the correspondent domain is permitted to send a message to the source domain in order to establish that the correspondent and source domains have compatible secure email technology, (2) a discovery secret and (3) an expiration date.

[0007] In another form, the invention comprises a method for establishing that the correspondent and source domains have compatible secure email technology or other email or communication technology. A source domain server transmits a discovery secret to the correspondent domain. The discovery secret includes a data element specific to the correspondent domain and a source domain address to which the correspondent domain is permitted send a message in order to establish that the correspondent and source domains have compatible secure email technology. A correspondent domain computer receives the discovery secret including the data element and the source domain address. The correspondent domain computer transmits an invitation from the



53

53

correspondent domain to the source domain address. The invitation includes the data element or an element corresponding to the data element.

[0008] Alternatively, the invention may comprise various other methods and apparatuses.

[0009] Other features will be in part apparent and in part pointed out hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is an exemplary block diagram of gateway servers 1 and 2 having secure messaging therebetween.

[0011] FIG. 2 is an exemplary diagram illustrating workflow between a source domain server and a potential correspondent (e.g., a correspondent domain server) according to the invention.

[0012] FIG. 3 is an exemplary block diagram illustrating a secure message manager according to the invention.

[0013] FIG. 4 is a flow diagram illustrating operation of secure message management (SMM) administrative routing according to the invention.

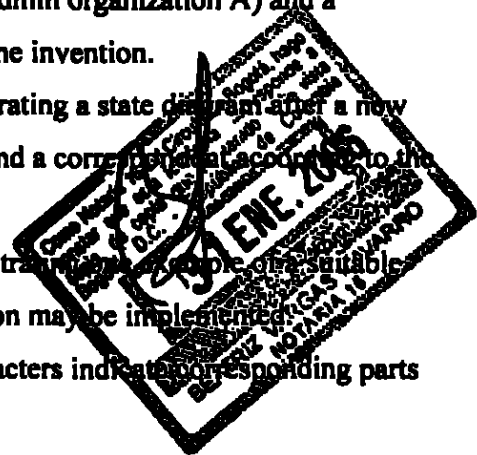
[0014] FIG. 5 is a flow diagram illustrating operation of SMM worker routing according to the invention.

[0015] FIG. 6 is an exemplary block diagram illustrating an inter-organization workflow summary between a server (admin organization A) and a correspondent (admin organization B) according to the invention.

[0016] FIG. 7 is a flow diagram illustrating a state diagram after a new security association implemented between a server and a correspondent according to the invention.

[0017] FIG. 8 is a block diagram illustrating an example of a suitable computing system environment in which the invention may be implemented.

[0018] Corresponding reference characters indicate corresponding parts throughout the drawings.



54

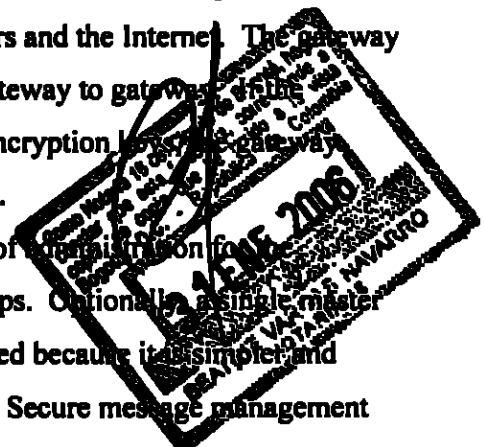
54

DETAILED DESCRIPTION OF THE INVENTION

[0019] The invention relates to a system and method for determining that a potential correspondent has compatible secure email technology in order to begin the process of establishing a link between a server and a correspondent. In particular, the invention relates to a system and method for initiating the process of establishing a secure link for the deployment of secure email. The invention allows a server to determine that a potential correspondent can be established as a target because of compatible secure email technology. As a result, once a potential correspondent is identified, the server can exchange key material information with the potential correspondent in order to establish the secure link.

[0020] The objective of domain signing and encryption according to the invention is to provide a transport independent mechanism to exchange confidential and server authenticated messages between servers. Fig. 1 is an exemplary block diagram of gateway servers 1 and 2. The gateway servers 1 and 2 have a secure messaging link therebetween. The servers may be separated by an optional firewall through which they may be connected to bridgehead servers (not shown), which may be part of a separate, secure messaging system. Gateway servers 1 and 2 form a sub-network that may be located between a trusted internal network, such as the secure messaging system linking bridgehead servers and an untrusted external network, such as the public internet. Firewalls are also positioned between the gateway servers and the Internet. The gateway servers treat all mail as clear text and encrypt all mail gateway to gateway. In the gateway and bridgehead servers do not share the same encryption key, gateway servers cannot decrypt bridgehead server encrypted mail.

[0021] There is a need for a single point of administration for authoritative data for all internal and external relationships. Optionally, a single master model rather than a multiple-master model is implemented because it is simpler and because it does not have to resolve replication conflicts. Secure message management (SMM) operations are usually infrequent and delays in SMM operations should not delay mail delivery, but only delay the setup of new secure associations. The database size is usually small (e.g., hundreds of thousands of records of a few K each; it could get up to several megabytes, but likely not 100s of megabytes) so that there is sufficient time to



55

repair or replace hardware or do a system restore before any loss of service. In one embodiment, critical data for operation is replicated to other gateway servers. Since there is no single point of management, not all data is replicated and the replicated data is read only.

[0022] A server may engage with a number of other correspondent domains to set up mail links for a specific project. However, the management coordination of such projects does not usually scale. For secure messaging to make an impact, secure mail is enabled with the majority of the organization's business correspondents. This requires the ability to discover which correspondents have gateway servers installed and have a simple organization-to-organization workflow in order to determine whether there should be negotiation to establish a secure mail link.

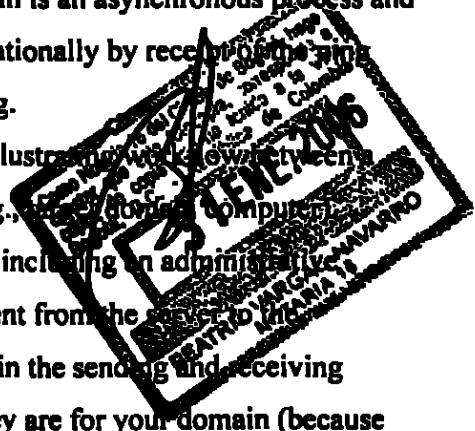
[0023] The invention enables discovery of gateway servers installed in an organization's correspondents so that a secure connection can be set up. To facilitate discovery, the server indicates (e.g., advertises) the presence of itself with outbound mail by some indication (or advertisement), herein referred to as a discovery secret. To minimize the discovery secret process being vulnerable to attack, the system and method of the invention do not use a hard coded address in its discovery secret. However, it is contemplated that in one embodiment a single address may be used with a discovery secret to be included in any email to that address. As a result, only messages from parties that have seen the discovery secret (which includes the discovery secret) can send to the administrative address. Therefore, in a preferred embodiment, a single address is used, and the discovery secrets must be provided in every message. Alternatively, the indicated address is a random mailbox name which can rotate at a reasonable interval, e.g., weekly. While this random approach is an option, it is usually a less preferred embodiment. To ensure that the vulnerabilities are minimized, the discovery secret is bound to the sending domain, e.g., the source domain, and to the domain to which it is sent, e.g., the correspondent domain. In the event that the discovery secret is available to a third party the only domain that would be affected is the domain whose invitation address was compromised.

[0024] In one form, the discovery secret may be an 822 header containing the ephemeral 822 address for negotiation and the expiration time of the 822 address

56

relative to when the message was sent. Inbound mail is scanned by the receiving server (e.g., correspondent or correspondent server) for discovery secrets from gateway servers and compared against a list of known gateway servers. Any additions to that list are communicated to the local administrative SMM. On discovery of a new correspondent, the SMM can send a probe message (e.g., an invitation) to the administrative address at the other SMM to offer a turn on domain signing and encryption or other services. On receipt of an invitation from another SMM administrator, if the message is verifiable under the existing trust policy then the local SMM could invoke a policy to automatically accept the invitation. Alternatively, the SMM administrator may require manual approval before accepting the invitation. On receipt of the invitation acceptance by the server, if the message is intrinsically verifiable, then the receiving SMM would invoke a policy to automatically start using domain signing and encryption. First, it sends an encrypted ping message with a nonce, and waits for an acknowledgement (that includes the nonce) to ensure that secure mail can be decrypted by the other side. Note that the invitation and acceptance messages are signed with the SMM's authoritative key, whereas the ping and acknowledgement are signed with the signing key (which is a child of the authority key). The process that does routine mail signing and encryption only has the authority to sign with the signing key (for security). Thus, the ping and acknowledgement also verify that secure mail will work with the signing key, not just the authority key. The configuration of a new secure domain is an asynchronous process and is not used for real data until the link is confirmed operationally by receipt of the ping acknowledgements before any administrative prompting.

[0025] Fig. 2 is an exemplary diagram illustrating a link between a source domain server and a potential correspondent (e.g., a computer) according to the invention. Initially, a discovery secret including an administrative address, a discovery secret and an expiration date are sent from the server to the correspondent. The discovery secret should also contain the sending and receiving domains, so that one can quickly determine whether they are for your domain (because they might have been relayed as the result of a mailing list). When the correspondent recognizes the discovery secret, the correspondent sends an invitation back to the server addressed to the administrative address that was part of the discovery secret. In one

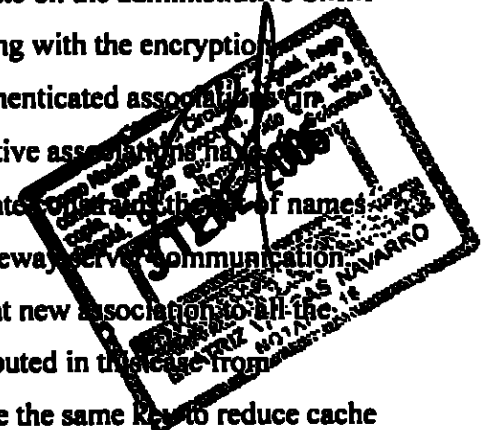


57

57

embodiment, it only responds to the discovery if it has also sent mail "to" the domain. Thus, a spammer cannot induce the source domain to invite them (because you never sent mail to them in the first place). The invitation from the correspondent includes an administrative address of the correspondent, the expiration, a certificate and the discovery secret and other information (e.g., workflow ID, contact information, sending and receiving domains, etc.). In response, the server sends an acceptance to the correspondent's administrative address from the server's administrative address and includes in the acceptance the expiration, the certificate, the discovery secret and a signature. This is administratively optional, though the default policy may include an automatic response. In one embodiment, it can also be restricted to manual, or to only respond if the inviter's certification meets some trust policy. After receipt of the acceptance, the correspondent pings the server and the ping is acknowledged by the server to establish the connection that puts the association into the ready state. It may involve an optionally automated administrative action to advance from the ready state to the active state. It may involve a further step to go from the active state (use the secure relationship but does not believe it) to the authenticated state (believe the identity claimed by the other end). If the invitation message is not verifiable using the trust policy as illustrated in Fig. 2, then the request may be cued awaiting manual approval.

[0026] Referring to Fig. 3, an exemplary block diagram illustrating a secure message manager according to the invention is illustrated. The acceptance of the invitation by the correspondent may create a cross certificate on the administrative SMM agent which is then pushed to the worker SMM agents along with the encryption certificate. (The cross certificate is usually created for authenticated associations in order to define what they are allowed to authenticate). Active associations have everything except the cross certificate.) The cross certificate contains the set of names accepted by the new trust and the restriction to domain gateway server communication. At this point, the certificates and information regarding that new association to all the workers is distributed. The session key may also be distributed in this case from administration SMM to all worker SMM so all workers use the same key to reduce cache size. To allow for scaling out, the corresponding decryption private key for the encryption certificate should be available on all internet facing gateway servers to allow



58

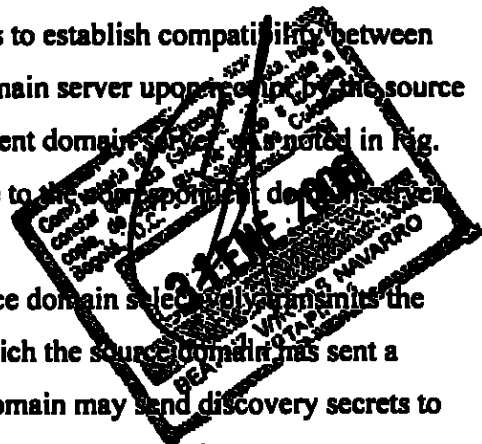
58

any to decrypt inbound mail. This is generated in a single place, i.e., the administration agent, and distributed to all worker servers. Once a trust relationship is established, it should be maintained. For example, the original certificate may be retained and a renewal request sent to the other SMMs before the certificate expires. The child encryption and signing certificate may also be updated frequently.

[0027] From the server's perspective, the method according to the invention begins the process to establish a link between a source domain and a correspondent domain. Initially, a source domain server transmits a discovery secret to potential correspondent domains via random or pseudorandom messages. The discovery secret includes a data element such as a mention or a token or other secret which is specifically assigned to the correspondent domain. The discovery secret includes a shared secret which is specific to the correspondent domain (and possibly the source domain). In the preferred embodiment, it is a hash of the seed, the correspondent domain, and the source domain (in some specified order). In addition, the discovery secret includes an address at the source domain to which the correspondent domain is permitted to send a message in order to establish a compatibility between the source domain server and the target computer. The source domain server receives an invitation from the correspondent domain which invitation is addressed to the source domain address previously provided. The invitation includes the data element in the discovery secret or an element which corresponds to the data element in the discovery secret. This allows the source domain server to initiate a process to establish compatibility between the correspondent domain server and the source domain server upon receipt by the source domain server of the invitation from the correspondent domain. As noted in Fig. 2, the source domain server transmits an acceptance to the correspondent domain server to establish compatibility therebetween.

[0028] In one embodiment, the source domain selectively transmits the discovery secret to correspondent domains from which the source domain has sent a message. Alternatively or in addition, the source domain may send discovery secrets to correspondent domains which have been specifically identified in advance.

[0029] In one embodiment, the discovery secret may be attached to a message that was sent specifically to carry the discovery secret. In one embodiment of



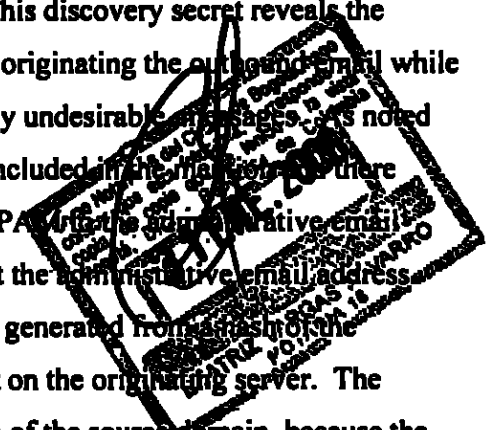
59

54

the invention, an email server occasionally adds an additional header (an "x-header") to a message that will be delivered to another email domain. The data in the header includes a secret that is specific to the correspondent domain and the email address to which the administrative messages from the correspondent domain can be directed back to the email server, as well as including the expiration, correspondent domain, sender domain, optional version, and optional features. If mail at the correspondent domain is also directed through a server that implements this embodiment of the invention, then it will detect the additional header and determine that there may be a compatible server at the originating domain. The correspondent domain then directs administrative traffic such as requests to establish a secure connection to the contained administrative email address. Such administrative messages must also contain the secret (referred to above as "discovery secret") that was provided for the correspondent domain. The mail acceptor for administrative mail at the originating domain can then discard any mail that purports to be from the correspondent domain but that does not contain the secret corresponding to the correspondent domain. Although this does not provide absolute assurance that the received administrative mail is from the originating domain, it does minimize the vulnerability to SPAM at the administrative address and ensures that even an attacker that can see email to the correspondent domain can only attempt to spoof administrative addresses from the correspondent domain rather than from any domain.

[0030] In one embodiment, the invention is implemented by using a header, called a discovery secret (sometimes called a mention), that is attached to an already outbound email from the source domain. This discovery secret reveals the availability of specific functions on the mail server originating the outbound email while avoiding the need for generating additional, possibly undesirable messages. As noted above, the administrative email address would be included in the header and there would be a per-domain secret to mitigate risks of SPAM to the administrative email address. This would support workflow messages at the administrative email address.

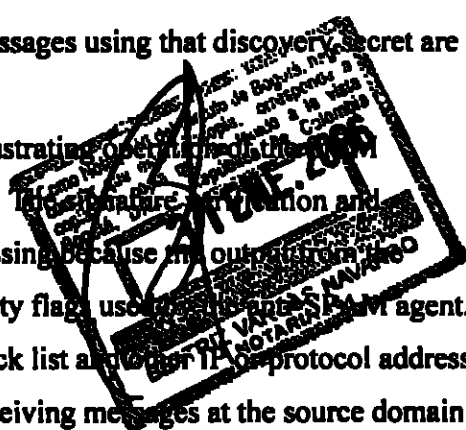
[0031] The discovery secret may be generated from a hash of the correspondent domain and a secret seed that is kept on the originating server. The discovery secret may also be generated from a hash of the source domain, because the same server may represent multiple source domains. One embodiment could potentially



60

60

have a special "source" for all domains at the source server. This allows a single seed to be shared across multiple servers, so that each server will generate the same discovery secret unique to any correspondent domain. When an administrative message is received at the originating server (because it is directed to the administrative address included in the mention), the discovery secret provided in the administrative messages is checked by the originating server. To check the discovery secret, the email server can generate (or store) a discovery secret for the domain that sent the administrative message using the current internal seed. If the generated discovery secret is the same as the one in the administrative messages, then that message has the correct discovery secret and is passed through to the appropriate destination for negotiation messages. Negotiation messages are passed between domains. If the discovery secret does not match, then the same process is applied to prior discovery secrets (up to a bounded number). If none of the currently valid seeds can be used to generate a discovery secret that matches the discovery secret in the incoming message, then the message is not considered valid and is discarded or rejected, and not passed on to the eventual destination for administrative messages. This prevents unauthorized SPAM attacks against the receiver of administrative messages, which may be unable to cope with large volumes of email. Additionally, to prevent denial of service attacks from a domain that received a valid discovery secret, the verification process permits the server to keep track of how many messages were recently passed through to the administrative destination from a particular domain or using a particular discovery secret. When that number exceeds an allowed limit or an allowed rate, further administrative messages using that discovery secret are discarded or rejected.

[0032] Fig. 4 is a flow diagram illustrating administrative routing according to the invention.  In the flow diagram, signature verification and decryption must happen before anti-SPAM processing because the output from the verification is necessary to set the message property flag, used by the anti-SPAM agent. Signature verification should happen after the block list and other IP or protocol address level functions. Thus, the process begins with receiving messages at the source domain address to which the correspondent domain is permitted to send a message at 402. If it is determined at 404 that the discovery secret is not valid for the sending domain, the

61

message is dropped at 406 and the routing process ends. If the discovery secret is valid the process proceeds to 408 to determine if the domain has a maximum amount or rate which has been exceeded. If the maximum has been exceeded, the message is dropped at 406, otherwise if the signature is valid at 410 the message is routed to the local administrative agent. However signature verification need not happen in the worker it usually happens in the SMM.

[0033] Fig 5 is a flow diagram illustrating operation of SMM worker routing according to the invention. SMM is the Secure Messaging Manager workers are the servers that the SMM administers/controls and that do the processing of mail traffic. SMM signing and encryption is the last function generally. Each message going to a domain with a secure message association is signed and encrypted. This component also inserts the header containing the current SMM ephemeral address to all mail going to domains without a security relationship. The worker will add discovery secrets as appropriate but it does not only do so to secure mail. As shown in Fig 5 the domain looks for a valid signature at 502 and an external address at 504 after finding a valid discovery secret. The discovery secret is only checked in messages that claim to be for the administrator not in normal mail. If the signature is valid and there is no external address the message is routed to the local worker agent at 506. If there is an external address, it is routed to such. If the message appears to be domain secured an invalid signature is treated identically as if the signature was not present. The message source is not authenticated.

[0034] In one embodiment, the inter-organizational workflow illustrated in Fig 6 are implemented between administrative organizations that represent the lifecycle of a relationship. Other rollovers are possible. Keys have certifications associated with them. The certifications may rollover more often than the keys. There are signing, encryption and authority certifications and keys, all of which rollover independently. Also there can be later ping/acknowledgement sequences. The workflow is performed by the SMM administrative agents and may go through an exchange in order to accomplish a rollover (rollover is the term for updating to a new key or certificate). Fig 7 is a state diagram illustrating the new security association. This

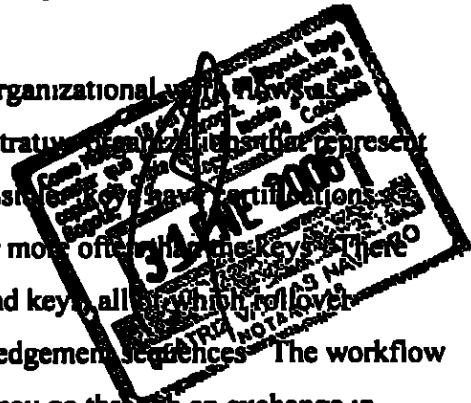
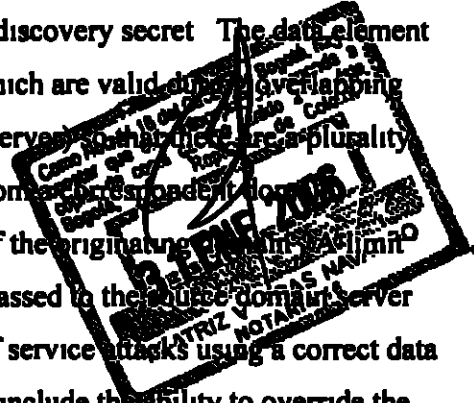


diagram only considers the positive cases and the terminal cases. It does not include other aspects such as re transmission of messages prior to the re transmission limit.

[0035] Other optional features of the invention include the following which may be implemented separately or in combination. The distinction between active and authenticated associations is 'optional' as are all the various policies that might be applied to automatically take an administrative transition. The discovery secret may comprise an expiration date in which case the source domain server would not initiate the process to establish compatibility with the correspondent domain computer (e.g., server) computer when receipt by the source domain server of the invitation is after the expiration date so that the shared secret does not become more and more exposed over time. The data element may be at least one of the following: a per domain secret including a random or pseudorandom number for each correspondent domain computer (e.g., server); a secret generated via hashing the correspondent domain computer (e.g., server) and a secret seed that is used to generate per-domain secrets for more than one domain; and a per-domain secret generated by encrypting the correspondent domain computer (e.g., server) and an expiration date of the secret. The data element may comprise a secret in which case the source domain server could remember the secret or could verify the secret received from the correspondent domain computer (e.g., server) by re-computing and then comparing the current secret for the correspondent domain computer (e.g., server) with the secret included in the discovery secret. The data element may be selected from a plurality of multiple secrets which are valid during overlapping times for each correspondent domain computer (e.g., server) so that there is a plurality of valid secrets that can be used for communicating from a correspondent domain computer (e.g., server) to the administrative address of the originating domain. A limit may be imposed on the number of messages that are passed to the source domain server address with a particular data element so that denial of service attacks using a correct data element are mitigated. The source domain server may include the ability to override the requirement for a data element for a given correspondent domain computer (e.g., server) to enable out-of band authorization to send invitation messages from a particular domain. The data element may be a token in the discovery secret message in a mail header or embedded in the body of a message or the data element may be a token in a mail header.

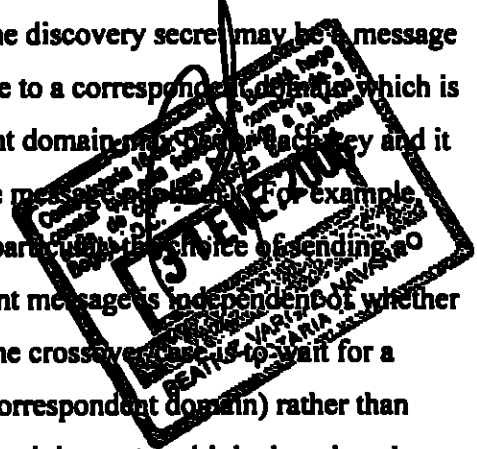


63

and the body of the message remains encrypted when passing through a mail server. The source domain server may support multiple simultaneously valid discovery secrets for the same domain and verify invitation messages from sub-domains of the correspondent domain computer (e.g., server) by verifying the incoming discovery secret against discovery secrets for the correspondent domain computer (e.g., server). The data element may be a discovery secret and include version information for the source domain server and include in the functions supported by the source domain server.

[0036] In one embodiment the invention comprises a data structure for the discovery secret to be transmitted from the source domain server to the correspondent domain computer (e.g., server). As noted above, this discovery secret is used to establish compatibility between the source domain server and the correspondent domain computer (e.g., server). Alternatively, it could be used for other purposes between the two domains. For example, it could be used for them to agree that they will send proprietary TNEF formats rather than text or HTML which would have nothing to do with encryption or security. The data structure includes a message and its usual header relating to the message. Additionally, the data structure includes an additional header attached to the message and message header and including a data element specific to the correspondent domain computer (e.g., server). The header also includes a source domain server address to which the correspondent domain computer (e.g., server) is permitted to send a message to the source domain server in order to establish compatibility between the source domain server and the correspondent domain computer (e.g., server). As noted above, the additional header should include an expiration date, although this is optional.

[0037] Alternatively or in addition, the discovery secret may be a message with a single correspondent domain and/or a message to a correspondent domain which is an operator. The single message to the correspondent domain may be a discovery secret and it may be sent on a time-based determination (e.g., one message per day). For example, the user action may be NDRs or return receipts. In particular, the choice of sending a separate message or attaching to an already being sent message is independent of whether you do it on every message or only occasionally. One cross-over point is to wait for a message that has recipients at a single domain (the correspondent domain) rather than attaching the discovery secret to a message that has recipients at multiple domains. In



G 4

64

[0038] FIG. 8 shows one example of a general purpose computing device

[0039] The computer 130 typically has at least some form of computer

of information such as computer files or other data. For example, CD-ROMs, flash memory, or other memory on hard, optical disk storage, tape or other magnetic storage store the desired information and that media typically embody computer

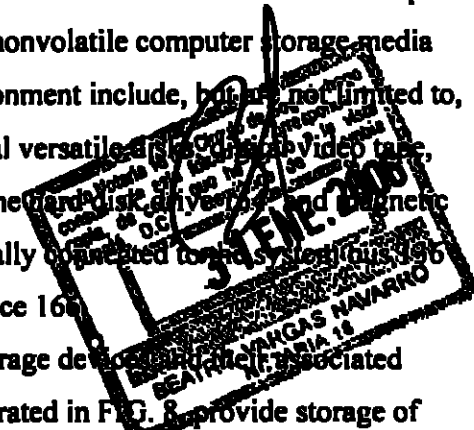
65

which has one or more of its characteristics set or changed in such a manner as to encode information in the signal. Wired media, such as a wired network or direct-wired connection, and wireless media, such as acoustic, RF, infrared, and other wireless media, are examples of communication media. Combinations of any of the above are also included within the scope of computer readable media.

[0040] The system memory 134 includes computer storage media in the form of removable and/or non-removable, volatile and/or nonvolatile memory. In the illustrated embodiment, system memory 134 includes read only memory (ROM) 138 and random access memory (RAM) 140. A basic input/output system 142 (BIOS), containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is typically stored in ROM 138. RAM 140 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 132. By way of example, and not limitation, FIG. 8 illustrates operating system 144, application programs 146, other program modules 148, and program data 150.

[0041] The computer 130 may also include other removable/non-removable, volatile/nonvolatile computer storage media. For example, FIG. 8 illustrates a hard disk drive 154 that reads from or writes to non-removable, nonvolatile magnetic media. FIG. 8 also shows a magnetic disk drive 156 that reads from or writes to a removable, nonvolatile magnetic disk 158, and an optical disk drive 160 that reads from or writes to a removable, nonvolatile optical disk 162 such as a CD-ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that may be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 154, magnetic disk drive 156 and optical disk drive 160 are typically connected to the system bus 136 by a non-volatile memory interface, such as interface 164.

[0042] The drives or other mass storage devices and their associated computer storage media discussed above and illustrated in FIG. 8, provide storage of computer readable instructions, data structures, program modules and other data for the computer 130. In FIG. 8, for example, hard disk drive 154 is illustrated as storing

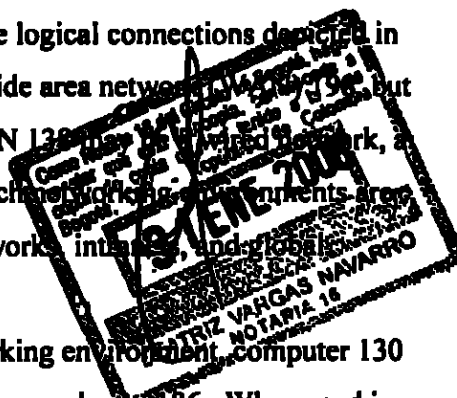


operating system 170, application programs 172, other program modules 174, and program data 176. Note that these components may either be the same as or different from operating system 144, application programs 146, other program modules 148, and program data 150. Operating system 170, application programs 172, other program modules 174, and program data 176 are given different numbers here to illustrate that, at a minimum, they are different copies.

[0043] A user may enter commands and information into computer 130 through input devices or user interface selection devices such as a keyboard 180 and a pointing device 182 (e.g., a mouse, trackball, pen, or touch pad). Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to processing unit 132 through a user input interface 184 that is coupled to system bus 136, but may be connected by other interface and bus structures, such as a parallel port, game port, or a Universal Serial Bus (USB). A monitor 188 or other type of display device is also connected to system bus 136 via an interface, such as a video interface 190. In addition to the monitor 188, computers often include other peripheral output devices (not shown) such as a printer and speakers, which may be connected through an output peripheral interface (not shown).

[0044] The computer 130 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 194. The remote computer 194 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to computer 130. The logical connections depicted in FIG. 8 include a local area network (LAN) 196 and a wide area network (WAN) 198, but may also include other networks. LAN 136 and/or WAN 138 may be a wired network, a wireless network, a combination thereof, and so on. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and global computer networks (e.g., the Internet).

[0045] When used in a local area networking environment, computer 130 is connected to the LAN 196 through a network interface or adapter 186. When used in a wide area networking environment, computer 130 typically includes a modem 178 or other means for establishing communications over the WAN 198, such as the Internet.

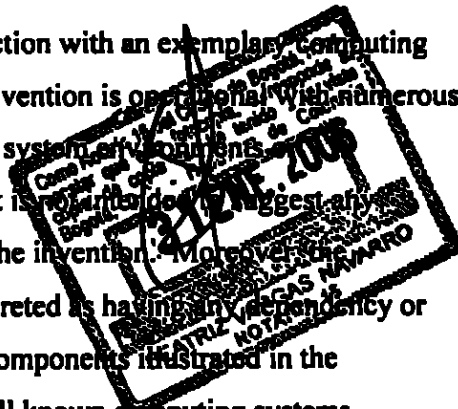


The modem 178, which may be internal or external, is connected to system bus 136 via the user input interface 184, or other appropriate mechanism. In a networked environment, program modules depicted relative to computer 130, or portions thereof, may be stored in a remote memory storage device (not shown). By way of example, and not limitation, FIG. 8 illustrates remote application programs 192 as residing on the memory device. The network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0046] Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described below in conjunction with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described herein.

[0047] For purposes of illustration, programs and other executable program components, such as the operating system, are illustrated herein as discrete blocks. It is recognized, however, that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.

[0048] Although described in connection with an exemplary computing system environment, including computer 130, the invention is operational with numerous other general purpose or special purpose computing system environments or configurations. The computing system environment is not intended to suggest any limitation as to the scope of use or functionality of the invention. Moreover, the computing system environment should not be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the exemplary operating environment. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention

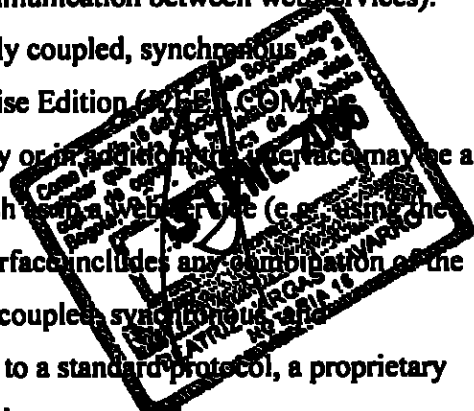


include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0049] The invention may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include, but are not limited to, routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0050] An interface in the context of a software architecture includes a software module, component, code portion, or other sequence of computer-executable instructions. The interface includes, for example, a first module accessing a second module to perform computing tasks on behalf of the first module. The first and second modules include, in one example, application programming interfaces (APIs) such as provided by operating systems, component object model (COM) interfaces (e.g., for peer-to-peer application communication), and extensible markup language metadata interchange format (XMI) interfaces (e.g., for communication between web services).

[0051] The interface may be a tightly coupled, synchronous implementation such as in Java 2 Platform Enterprise Edition (J2EE), COM, or distributed COM (DCOM) examples. Alternatively or in addition, the interface may be a loosely coupled, asynchronous implementation such as a web service (e.g., using the simple object access protocol). In general, the interface includes any combination of the following characteristics: tightly coupled, loosely coupled, synchronous, and asynchronous. Further, the interface may conform to a standard protocol, a proprietary protocol, or any combination of standard and proprietary protocols.



[0052] The interfaces described herein may all be part of a single interface or may be implemented as separate interfaces or any combination therein. The interfaces may execute locally or remotely to provide functionality. Further, the interfaces may include additional or less functionality than illustrated or described herein.

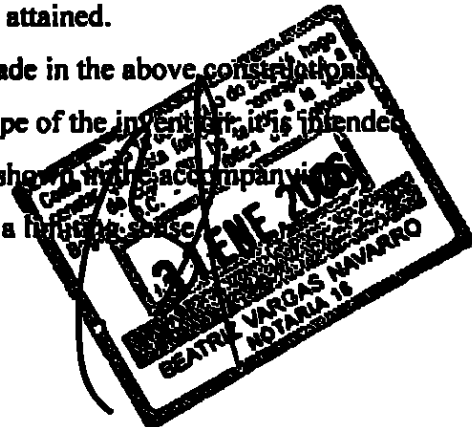
[0053] In operation, computer 130 operates as either the source domain server or the correspondent domain computer (which may be a server) to execute computer-executable instructions as noted above, such as those illustrated in Figs. 2-7.

[0054] The order of execution or performance of the methods illustrated and described herein is not essential, unless otherwise specified. That is, elements of the methods may be performed in any order, unless otherwise specified, and that the methods may include more or less elements than those disclosed herein. For example, it is contemplated that executing or performing a particular element before, contemporaneously with, or after another element is within the scope of the invention.

[0055] When introducing elements of the present invention or the embodiment(s) thereof, the articles "a," "an," "the," and "said" are intended to mean that there are one or more of the elements. The terms "comprising," "including," and "having" are intended to be inclusive and mean that there may be additional elements other than the listed elements.

[0056] In view of the above, it will be seen that the several objects of the invention are achieved and other advantageous results attained.

[0057] As various changes could be made in the above construction, products, and methods without departing from the scope of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.



70

- Receiving by the source domain via the source domain address an invitation from the correspondent domain wherein the invitation includes the data element or an element corresponding to the data element which may be used by the correspondent domain to initiate a process to establish compatibility with the correspondent domain.

3. The method of claim 1 wherein the discovery secret is selectively transmitted to at least one of the following:

Correspondent domains via randomly selected messages.

4. The method of claim 1 wherein the discovery secret is a message which is generated in response to user action; wherein the discovery secret is a message with a single correspondent domain; wherein the discovery secret is a message to a correspondent domain which is an operator; wherein the discovery secret is a single message to the correspondent domain for each key; or wherein the discovery secret is a message send on a time-based determination.

21

15

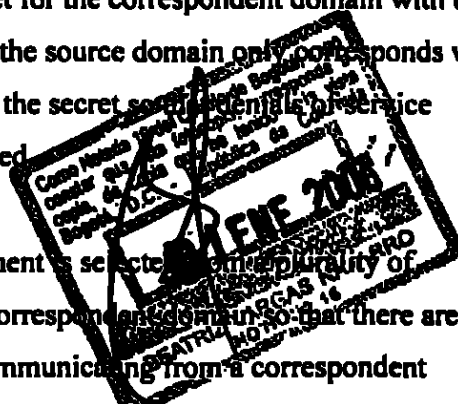
6. The method of claim 1 wherein the discovery secret comprises an expiration date and wherein the source domain does not establish that the correspondent and source domains have compatible secure email technology when receipt by the source domain of the invitation is after the expiration date.

7. The method of claim 1 wherein the data element is at least one of the following:

- a per domain secret including a random or pseudorandom number for each correspondent domain;
- a secret generated via hashing the correspondent domain and a secret seed that is used to generate per-domain secrets for more than one domain; and
- a per-domain secret generated encrypting the correspondent domain and an expiration date of the secret.

8. The method of claim 1 wherein the data element comprises a secret and wherein the source domain verifies the secret received from the correspondent domain by re-computing and then comparing the current secret for the correspondent domain with the secret included in the discovery secret whereby the source domain only corresponds with potential correspondent domains which provide the secret so that denial-of-service attacks from correspondence domains is mitigated.

9. The method of claim 1 wherein the data element is selected from a plurality of multiple simultaneously valid secrets for each correspondent domain so that there are a plurality of valid secrets that can be used for communicating from a correspondent domain to the administrative address of the originating domain.



72

72

10. The method of claim 1 further comprising imposing a limit on the number of messages that are passed to the source domain address with a particular data element whereby denial of service attacks using a correct data element are mitigated.

11. The method of claim 1 further comprising including the ability to override the requirement for a data element for a given correspondent domain to enable out-of-band authorization to send invitation messages from a particular domain.

12. The method of claim 1 wherein the data element is a token in the discovery secret message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server.

13. The method of claim 1 further comprising supporting multiple simultaneously valid tokens for the same domain and verifying invitation messages from sub-domains of the correspondent domain by verifying the incoming token against tokens for the correspondent domain.

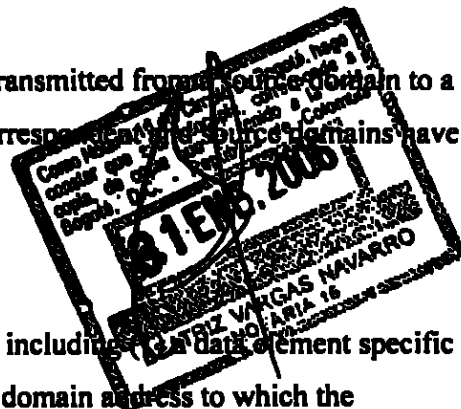
14. The method of claim 1 wherein the data element is a mention and further comprising including in the mention of version information for the source domain and including in the mention functions supported by the source domain.

15. A data structure for a discovery secret to be transmitted from a source domain to a correspondent domain for establishing that the correspondent domain's source domains have compatible secure email technology comprising:

A message;

A header relating to the message; and

An additional header attached to the message and including a domain element specific to the correspondent domain and including a source domain address to which the correspondent domain is permitted send a message to the source domain in order to



73

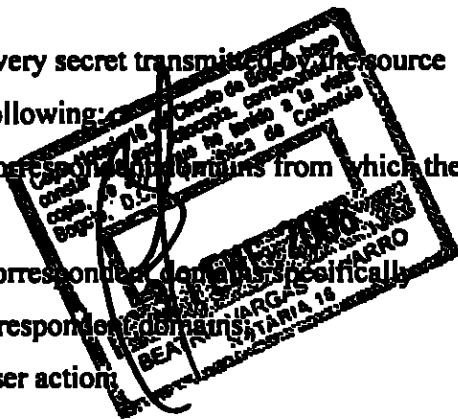
כך

SECRET

2

7A

- A discovery secret selectively transmitted to correspondents from which the source domain has received a message;**
- a discovery secret selectively transmitted to correspondents specifically identified in advance or randomly selected correspondent domains;**
- a message which is generated in response to user action;**
- a message with a single correspondent domain;**
- a message to a correspondent domain which is a server's operator address;**
- a single message to the correspondent domain for each key;**



28

75

a message send on a time-based determination;
 an additional header which includes the data element and the source domain address; and
 an expiration date and wherein the source domain does not initiate the process to establish a link with the correspondent domain when receipt by the source domain of the invitation is after the expiration date.

20. The system of claim 17 wherein the data element is at least one of the following:

a per domain secret including a random or pseudorandom number for each correspondent domain,

a secret generated via hashing the correspondent domain and a secret seed that is used to generate per-domain secrets for more than one domain;

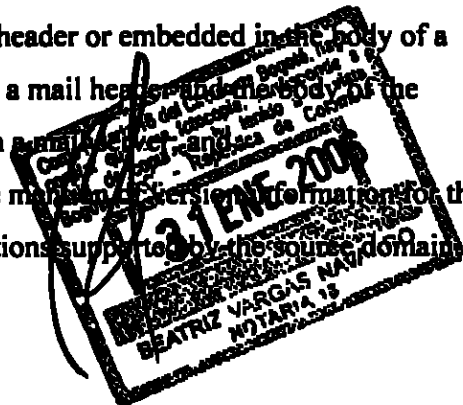
a per-domain secret generated encrypting the correspondent domain and an expiration date of the secret;

a secret and wherein the source domain verifies the secret received from the correspondent domain by re-computing and then comparing the current secret for the correspondent domain with the secret included in the discovery secret;

a data element is selected from a plurality of multiple overlapping secrets for each correspondent domain so that there are a plurality of valid secrets that can be used for communicating from a correspondent domain to the administrative address of the originating domain;

a token in the discovery secret message in a mail header or embedded in the body of a message or wherein the data element is a token in a mail header and the body of the message remains encrypted when passing through a mail server and the body of the message remains encrypted when passing through a mail server and the body of the message remains encrypted when passing through a mail server;

a mention and further comprising including in the mention information for the source domain and including in the mention functions supported by the source domain.



76

76

ABSTRACT

A discovery secret is transmitted from the source domain to the correspondent domain. The discovery secret includes a data element specific to the correspondent domain and. The discovery secret includes a source domain address to which the correspondent domain is permitted send a message in order to determine that a potential correspondent has compatible secure email technology so that a link between the source domain and the correspondent domain may be established. The discovery secret is received by the correspondent domain including receiving the data element and the source domain address. An invitation is transmitted from the correspondent domain to the source domain address. The invitation includes the data element or an element corresponding to the data element. The source domain initiates a process to establish a link with the correspondent domain upon receipt by the source domain of the invitation.



77

77

OFICINA DE PATENTES Y MARCAS REGISTRADAS DE E.U.

DEPARTAMENTO DE COMERCIO DE EU
Oficina de Patentes y Marcas Registradas de E.U.
Directorio COMISIONADO PARA PATENTES
Albuquerque, Virginia 21313-1489

Solicitud no	Fecha de presentación(c) o 371	UNIDAD API	TASA DE ANCHADO	ATY DOCKET NO	DIBUJOS	TOT CLAS	INT CLAS
60/659,279	03/07/2005		200	MS#311610.01(5169)	8		

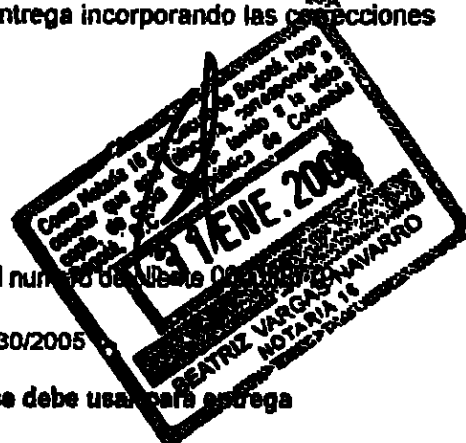
000036779
SENNIGER, POWERS, LEAVIT & ROEDEL
ONE METROPOLITAN SQUARE, 16 FLOOR
ST. LOUIS, MO 63102

CONFIRMACIÓN NO. 3956
RECIBO DE ENTREGA
0000000015813389

Fecha de envío: 03/31/2005

Se acusa recibo de esta Solicitud de Patente corriente. Se le considerará en su orden y se le notificará sobre los resultados del examen. Asegúrese de suministrar el NÚMERO DE SOLICITUD DE E.U., FECHA DE ENTREGA, NOMBRE DEL SOLICITANTE, Y TÍTULO DEL INVENTO cuando consulte acerca de esta solicitud. Las tasas que se transmiten con cheque o giro estarán sujetas a recolección. Por favor verifique que los datos presentados en este recibo estén correctos. Si encuentra un error en este recibo de entrega, por favor escriba a la Oficina de Examen Inicial de Patentes para Recibo de Correcciones, facsímil número 703-746-9195, por favor suministre una copia de este Recibo de Entrega con los cambios que desea. Si usted recibe una "Notificación de Partes Faltantes al Archivo" para esta solicitud, por favor envíe las correcciones a este recibo de entrega con su respuesta a la notificación. Cuando el USPTO procesa la respuesta a la notificación, la USPTO generara otro recibo de entrega incorporando las correcciones solicitadas (si es apropiado).

Solicitante(s)
Eric D Tribble, Redmond, WA;
Trevor W Freeman, Sammamish, WA;



Poder del abogado: Los practicantes de la patente asociados con el número de Noticia 0000000015813389

Si se requiere, Licencia de Entrega Extranjera Concedida: 03/30/2005

El código del país y el número de su solicitud de prioridad que se debe usar para entrega extranjera bajo la convención de Paris, es US60/659,279

Fecha proyectada de publicación: Ninguna, la solicitud no es elegible para publicación antes de concederse
Solicitud de no-publicación: No
Solicitud de publicación temprana: No

78

78

Título: Sistema y Método para establecer un vínculo entre un Servidor y un Objetivo

**LICENCIA PARA ENTREGA EXTRANJERA BAJO
Título 35, Código de los Estados Unidos, Sección 184
Título 37, Código de Reglamento Federal, 5.11 & 5.15**

CONCEDIDA

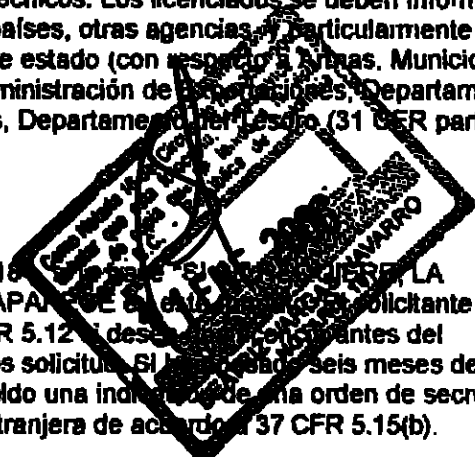
Al solicitante se le ha concedido la licencia bajo 35 U.S.C. 184, si la frase "SI SE REQUIERE, LA LICENCIA DE ENTREGA EXTRANJERA SE CONCEDE" seguida de una fecha que aparece en este formato. Estas licencias se conceden para todas las solicitudes donde las condiciones que se requieren para una licencia se han cumplido, sin importar si la licencia se requiere o no tal como se expone en 37 CFR 5.15. El alcance y las limitaciones de estas licencias se exponen en 37 CFR 5.15(a) al menos de que una licencia anterior se haya remitido bajo 37 CFR 5.15(b). La licencia está sujeta a revocación con una notificación por escrito. La fecha que se indica en la fecha efectiva de la licencia, al menos de que una licencia anterior de alcance similar se haya concedido bajo 37 CFR 5.13 o 5.14.

El licenciado debe guardar esta licencia y la puede utilizar en cualquier momento en la fecha que se hace efectiva o luego al menos de que se revoque. Esta licencia se transfiere automáticamente a cualquier aplicación relacionada que se haya entregado bajo 37 CFR 1.53(d). Esta licencia no es retroactiva.

La concesión de una licencia no aminora la responsabilidad del licenciado para la seguridad del tema a tratar como lo impone cualquier contrato con el Gobierno o las prescripciones de leyes existentes relacionadas con el espionaje y la seguridad nacional o la exportación de datos técnicos. Los licenciados se deben informar sobre el reglamento vigente especialmente respecto a ciertos países, otras agencias, y particularmente la Oficina de Defensa de Controles de Comercio, departamento de estado (con respecto a Armas, Municiones e Implementos de Guerra (22 cfr 121-128)); la Oficina de Administración de Exportaciones, Departamento de Comercio (15 cfr 370.10(J)); la Oficina de Control de Activos, Departamento del Tesoro (31 CFR partes 500+) y el Departamento de Energía.

NO CONCEDIDA

Por el momento no se ha concedido la licencia bajo 35 U.S.C. 184. Si la frase "SI SE REQUIERE, LA LICENCIA DE ENTREGA EXTRANJERA SE CONCEDE" NO APARECE EN ESTA LICENCIA, el solicitante puede todavía hacer una petición para una licencia bajo 37 CFR 5.12 si desea hacerlo antes del vencimiento de seis meses a partir de de la fecha entrega de los solicitud. Si han pasado seis meses desde la fecha de entrega de esta solicitud y la licencia no ha recibido una indicación de una orden de secreto bajo 35 U.S.C. 181, el licenciado puede entregar la solicitud extranjera de acuerdo a 37 CFR 5.15(b).



79

PTAS

500031302A

OFICINA DE PATENTES Y MARCAS REGISTRADAS DE LOS ESTADOS UNIDOS
NOTIFICACION DEL REGISTRO DEL DOCUMENTO DE CESION

POR FAVOR REVISE TODA LA INFORMACIÓN CONTENIDA EN ESTA NOTIFICACIÓN. LA INFORMACIÓN CONTENIDA EN ESTA NOTIFICACIÓN DE ARCHIVO REFLEJA LOS DATOS PRESENTES EN EL SISTEMA DE CESIÓN DE PATENTES Y MARCAS REGISTRADAS. SI USTED ENCUENTRA ALGÚN ERROR O TIENE ALGUNA PREGUNTA CONCERNIENTE A ESTA NOTIFICACIÓN, PUEDE LLAMAR AL EMPLEADO CUYO NOMBRE APARECE EN ESTA NOTIFICACIÓN AL NÚMERO 763-308-9723. POR FAVOR ENVÍE LAS SOLICITUDES PARA CORRECCIÓN A: OFICINA DE PATENTES Y MARCAS REGISTRADAS DE E.U., CORREO: ASSIGNMENT SERVICES DIVISION, P.O. BOX 1450, ALEXANDRIA, VA 22313.

FECHA DE GRABACION: 05/13/2009

CINTA/CUADRO C16013/0231
NUMERO DE PAGINAS: 2

PESUMEN: ASIGNACIÓN DE INTEPES AL CESIONARIO (VER DOCUMENTO PARA
DETALLES)

CEDENTE:
 TRIBBLE, ERIC D.
 CEDENTE:
 FREEMAN, TREVOR
 CESIONARIO:
 MICROSOFT CORPORATION
 ONE MICROSOFT WAY
 REDMONT, WASHINGTON 98052

FECHA DOC: 04/14/2005

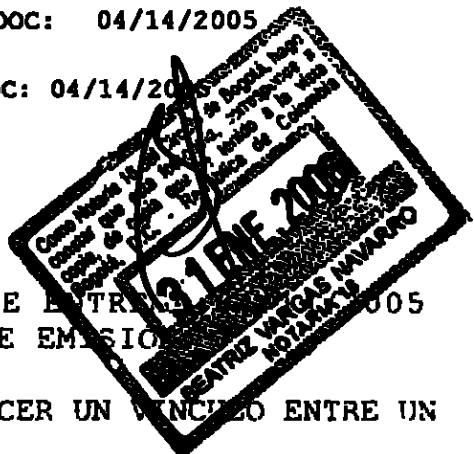
FECHA DOC: 04/14/20

NUMERO DE SERIAL: 60659273
NUMERO DE PATENTE:

FECHA DE ENTREGA: 005
FECHA DE EMISIÓN: 005

TITULO: SISTEMA Y METODO PARA ESTABLECER UN VINCULO ENTRE UN SERVIDOR Y UN OBJETIVO

DOROTHY RILEY, PARALEGAL
DIVISION DE ASIGNACIONES
OFICINA DE ARCHIVOS PUBLICOS



80

CESION DE PATENTE	
Versión electrónica v1.1	05/13/2005
Estilo de hoja versión v1.1	500031382

TIPOS DE SUMISIÓN: NUEVA CESION

NATURALEZA DE LA ENTREGA: CESION

DATOS DE LA PARTE QUE ENTREGA

Nombre	Fecha ejecución
Eric D Tribble	04/14/2005
Trevor W Freeman	04/14/2005

DATOS DE LA PARTE QUE RECIBE

Nombre:	Corporación Microsoft
Dirección:	One Microsoft Way
Ciudad	Redmont
Estado/país:	WASHINGTON
C.P.:	98052

NÚMEROS DE PROPIEDAD total: 1

Tipo De Propiedad	Número
Solicitud Numero:	60659279

DATOS DE CORRESPONDENCIA

Fax: (314) 231-4342

la correspondencia se enviará a través del correo de EU cuando el fax de enviar teléfono: 3142315400

e-mail: uspatents@senniger.com

nombre de correspondencia: Robert M. Bain

Línea de Dirección 1 One Metropolitan Square,

Línea de Dirección 2 Senniger Powers

Línea de Dirección 4 St, MISSOURI 63102

Nombre del presentador Robert M. Bain

Total anexos: 4

Fuente = 00078147##pagina1.tif



81

81

MS Docket No. MS311610.01
(OC Docket No. MSFT5169)

Cesión de patente

Yo/nosotros, Eric D Tribble, Trevor W Freeman ("Cesionistas"), hemos inventado ("INVENTO") divulgado y/o reivindicado en la solicitud de patente llamada "SISTEMA Y METODO PARA ESTABLECER UN VINCULO ENTRE UN SERVIDOR Y UN OBJETIVO" (solicitud), que:

- ☐ Se archivará sin la patente de asignación ejecutada. Por medio de la presente, el cedente autoriza, y solicita, al representante legal del cesionario, de SENNIGER POWERS, que están asociados con el número de cliente 000038779, para insertar aquí en paréntesis (U.S. No Serial. 60/659279, archivado 03/01/2005) No. serial de esta solicitud y fecha de entrega, si son conocidos;
- ☒ presentada el 7 de Marzo, 2005 y se le dio el No. Serial: 60/659,279;
- ☐ Se archiva en forma simultánea;

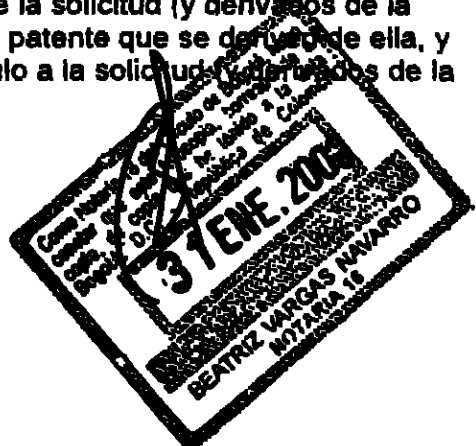
La corporación Microsoft, una corporación de Washington, en su propio nombre y el de sus sucesores y cesionarios, tiene derecho a, y está deseoso de adquirir la totalidad y exclusividad de los derechos, títulos e interés en el invento y la aplicación (y todas las demás aplicaciones de patentes que se deriven de esta, tales como aplicaciones de continuación, en y para los Estados Unidos y sus territorios, y todos los países extranjeros ("derivados de la solicitud");

En consideración buena y valiosa, en el recibo que el CEDENTE reconoce por la presente, los CEDENTE(S) venden, asignan y transfieren hacia el CESIONARIO, el derecho completo, título e interés en y dicho invento y la solicitud (y derivados de la solicitud);

El Cedente se compromete a ejecutar todos los instrumentos y documentos requeridos para el procesamiento de la solicitud (y derivados de la solicitud), para el litigio en cuanto a las cartas de patente que se deriven de ella, y con el propósito de proteger y perfeccionar el título a la solicitud (y derivados de la solicitud).

04/14/05
04/14/05

Eric D Tribble (Firma)
Trevor W Freeman (Firma)



82

SISTEMA Y METODO PARA ESTABLECER UN VÍNCULO ENTRE UN SERVIDOR Y UN OBJETIVO

CAMPO TÉCNICO

[0001] Implementaciones del presente invento se relacionan con el campo de establecer una interconexión compatible entre dos dominios. En particular, implementaciones de este invento se relacionan con un sistema y método para revelar y descubrir servidores de correo con capacidades avanzadas.

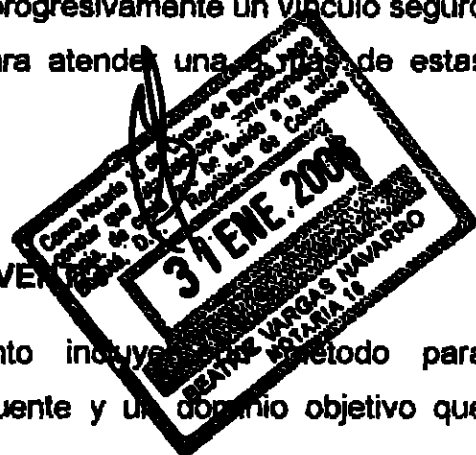
ANTECEDENTES DEL INVENTO

[0002] Algunos sistemas anteriores intentan identificar colegas potenciales comunicándose directamente. Sin embargo, estos sistemas se vuelven vulnerables cuando se comunican y, en particular, crean una vulnerabilidad al SPAM.

[0003] De esta manera, se desea un sistema para identificar en forma discreta a un colega potencial y establecer progresivamente un vínculo seguro entre el servidor y el colega potencial para atender una o más de estas desventajas.

RESUMEN DEL INVENTO

[0004] Implementaciones del invento incluyen un método para establecer un vínculo entre un dominio fuente y un dominio objetivo que comprende:



83

[0005] Transmitir un anuncio desde el dominio fuente al dominio objetivo donde el anuncio incluye un elemento de datos específicos al dominio objetivo y donde el anuncio incluye la dirección de la que el dominio fuente con cuál es dominio objetivo enviar un mensaje para establecer un vínculo entre el dominio fuente es dominio objetivo; y

[0006] Recibir del dominio fuente a través de la dirección del dominio fuente una invitación de dominio objetivo donde la invitación incluye el elemento de datos o un elemento de datos correspondientes al elemento de datos donde el dominio fuente inicia el proceso para establecer el vínculo con el dominio objetivo una res se recibe la indicación del dominio fuente.

[0007] Un anuncio se transmite del dominio fuente al dominio objetivo. El anuncio incluye un elemento de datos específico al dominio objetivo y. El anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer el vínculo entre dominio fuente y dominio objetivo. El anuncio lo recibe el dominio objetivo en incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio objetivo a la dirección del dominio fuente. La invitación incluye el elemento de datos o un elemento de datos correspondiente al elemento de datos. El Dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo, tal como el dominio fuente recibe la invitación del dominio fuente.

[0008] El invento también incluye un sistema para el almacenamiento de datos.

[0009] Alternativamente el invento también puede comprender otros métodos y aparatos.

[0010] Otros rasgos del invento serán en parte aparentes y otros se señalarán.

34

DESCIPCION BREVE DE LOS DIBUJOS

[0011] La figura 1 es un diagrama de bloque ejemplar de los servidor limítrofes 1 y 2 dentro del DMZ y que tienen una mensajería segura entre los dos. Los servidores están conectados a través de un firewall y que hace puente entre 1 y 2 que son parte de un sistema de mensajería seguro separado. Los servidores 1 y 2 forman una subred que esta localizada entre una red interna confiable, tal como un sistema de mensajería seguro que vincula los puentes 1 y 2, y una red externa no confiable, tal como la Internet pública. En forma crítica, el DMZ contiene dispositivos accesibles al tráfico de Internet, tales como servidores web (http), servidores FTP, servidores SMPT(e-mail) y servidores DNS a través de firewalls.

[0012] La figura 2 es, de acuerdo con el invento, un diagrama ejemplar que muestra el flujo de trabajo entre el servidor dominio fuente y un colega potencial (por ejemplo, un servidor de dominio objetivo).

[0013] La figura 3 es un diagrama de bloque ejemplar que muestra una administradora de mensajes segura de acuerdo con el invento.

[0014] La figura 4 es un diagrama de flujo que muestra las operaciones de ruteo. administrativo SMM de acuerdo con el invento.

[0015] La figura 5 es un diagrama de flujo que muestra las operaciones de ruteo SMM de acuerdo con el invento.

[0016] La figura 6 es un diagrama de bloque ejemplar que muestra un flujo de trabajo inter-organización entre un servidor (administración de la



45

organización A) y un colega (administración de la organización B) de acuerdo con el invento.

[0017] La figura 7 es un diagrama de flujo que muestra un diagrama de estado luego de que una asociación de seguridad nueva se implementa entre el servidor y un colega de acuerdo con el invento.

[0018] La figura 8 es un diagrama de bloque que muestra un ejemplo de un ambiente de sistema de computación adecuado en el cual el invento se puede implementar.

[0019] Caracteres de referencia correspondientes indican partes correspondientes a través de los dibujos.

DESCRIPCIÓN DETALLADA DEL INVENTO

[0020] El invento se relaciona con un sistema y método para establecer un vínculo entre un servidor y un objetivo. En particular, el invento se relaciona con un sistema y métodos para establecer un vínculo seguro para desplegar un e-mail seguro. El invento le permite a un servidor a determinar que un colega potencial se puede establecer como objetivo por qué tienen tecnologías de y e-mail seguras y compatibles. Como resultado, el colega potencial se identifica, el servidor puede proporcionar una forma segura material clave de información con el colega potencial. El invento establece un vínculo seguro.

[0021] El objetivo de firmar y codificar el dominio de acuerdo con el invento es suministrar un mecanismo de transporte para intercambiar mensajes confidenciales y autenticados por el servidor entre los servidores.

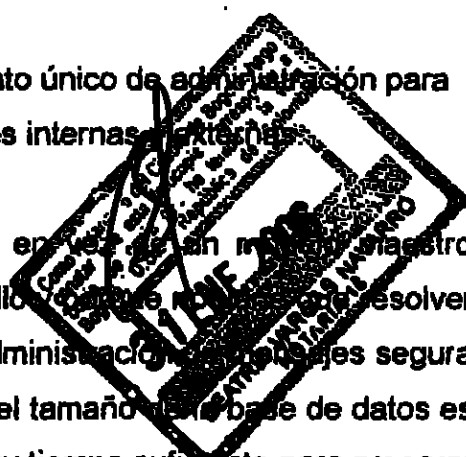


26

La figura 1 es un diagrama de bloque ejemplar del servidor limitrofe 1 y 2 dentro de la zona desmilitarizada (DMZ). Los servidores 1 y 2 tienen un vínculo de mensajería segura entre ellos. Los servidores están separados por un firewall a través del cual están conectados para hacer puente entre los servidores 1 y 2. Los servidores fuente son parte de un sistema de mensajería segura. Los servidores limitrofes 1 y 2 forman una sub-red que está localizada entre una red confiable interna, tal como un sistema de mensajería seguro que vincula los servidores puente 1 y 2 y la red externa no confiable, tal como la Internet pública. Los firewalls también están posicionados entre los servidores limitrofes y la Internet. En esta ilustración de la figura 1, el servidor limitrofe 1 puede intercambiar correo firmado y codificado con el servidor limitrofe 2 y el servidor puente 1 puede intercambiar correo firmado y codificado con el servidor puente 2. Adicionalmente, el servidor puente 1 puede reenviar a su servidor limitrofe 1 DMZ ya sea correo firmado o firmado y codificado donde el recipiente de decodificación es el servidor puente 2. Los servidores limitrofes tratan todo el correo como texto claro y codifican todo el correo punta a punta. Si los servidores limitrofes y de puente no comparten la misma clave de codificación, los servidores limitrofes no pueden decodificar el correo puente codificado.

[0022] Existe la necesidad para un punto único de administración para los datos autoritarios para todas las relaciones internas y externas.

Opcionalmente, un modelo maestro único en vez de un maestro múltiple se implementa porque es más sencillo y requiere menos tiempo para resolver conflictos de réplicas. Las operaciones de administración de mensajes segura (SMM) son generalmente poco frecuentes y el tamaño de la base de datos es generalmente pequeña de tal manera que hay tiempo suficiente para preparar o cambiar hardware o hacer una restauración del sistema ante una pérdida del servicio. En una implementación, datos críticos para la operación se

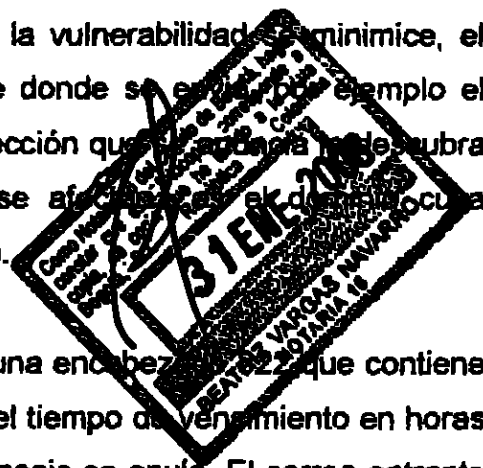


replican en otro servidor limitrofe. Como no hay un punto único de administración, no todos los datos se replican y los datos replicados son únicamente de lectura.

[0023] Un servidor puede involucrarse con un número de colegas para iniciar unos vínculos de correo seguros para un proyecto específico. Sin embargo, la administración de la coordinación de tal proyecto generalmente no escala. Para que la mensajería segura haga un impacto, el correo seguro se habilita con la mayoría de los colegas de negocios en la organización. Esto requiere la habilidad para descubrir que colegas tienen servidores limitrofes instalados y tienen un flujo de trabajo organización-organización simple para negociar el establecimiento de un vínculo de correo seguro.

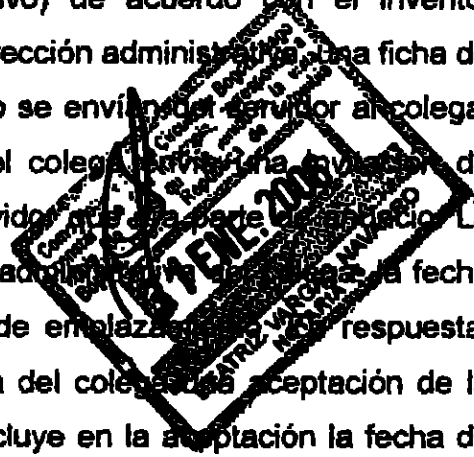
[0024] El invento permite descubrir los servidores limitrofes instalados en la organización colega de tal manera que una conexión segura se pueda iniciar. Para facilitar el descubrimiento, el servidor anuncia su presencia con un correo saliente. Para minimizar la vulnerabilidad a ser atacado el proceso de anuncio, el sistema y método del invento no utiliza una dirección codificada en duro en su anuncio. Por lo tanto, la dirección anunciada es un nombre de casilla de correo aleatoria que puede rotar con intervalos razonables, por ejemplo cada semana. Para asegurar que la vulnerabilidad se minimice, el anuncio también está ligado al dominio de donde se envía, por ejemplo el dominio objetivo. En el caso de que la dirección que se anuncia no cubra una tercera parte el único dominio que se afilia con el dominio o cuya dirección de invitación estaba comprometida.

[0025] En una forma, el anuncio es una encabezadura 822 que contiene la dirección efímera 822 con invitaciones y el tiempo de vencimiento en horas de la dirección 822 relativa a cuando el mensaje se envió. El correo entrante lo filtra el servidor receptor (por ejemplo el servidor objetivo o colega) para un



anuncio del servidor limítrofe y lo compara contra una lista de servidores limítrofes conocidos. Cualquier admisión a estas listas se comunica al administrador local SMM. Cuando se descubre un nuevo servidor limítrofe, el SMM puede enviar un mensaje de prueba (por ejemplo, una invitación) al otro servidor SMM para ofrecer un turno de firma y codificación de dominio. Tan pronto se recibe la invitación o el anuncio de otro administrador SMM, si el mensaje se puede verificar bajo la política actual de confiabilidad el SMM local entonces puede invocar una política para aceptar automáticamente la invitación. En forma alterna, el administrador SMM puede requerir una aprobación manual antes de aceptar la invitación. Tan pronto se recibe la aceptación de la invitación por el servidor, si el mensaje es verificable intrínsecamente, entonces el SMM receptor puede invocar una política para iniciar automáticamente las firmas y codificación del dominio. La configuración de dominio nuevo y seguro es un proceso no sincronizado y no se utiliza para datos reales hasta que el vínculo se confirma operativamente con la recepción del reconocimiento.

[0026] Figura 2 es un diagrama ejemplar que muestra el flujo de trabajo entre el servidor de dominio fuente y un colega potencial (por ejemplo, un computador que es el dominio objetivo) de acuerdo con el invento. Inicialmente, un anuncio que incluye una dirección administrativa, una ficha de emplazamiento y una fecha de vencimiento se envía del servidor al colega. Cuando el colega reconoce el anuncio, el colega envía una invitación de vuelta a la dirección administrativa del servidor que es parte de la asociación. La invitación del colega incluye una dirección administrativa del colega, la fecha de vencimiento, un certificado y la ficha de emplazamiento. En respuesta, el servidor envía a la dirección administrativa del colega una aceptación de la dirección administrativa de servidor que incluye en la aceptación la fecha de vencimiento, el certificado, la ficha de emplazamiento y una firma. Luego de que se recibe la aceptación, del colega le pasa una invitación al servidor y la



indicación la reconoce el servidor para establecer la conexión. Si el mensaje de invitación no se puede verificar utilizando la política de confiabilidad como se mostró en la figura 2 y entonces la petición se puede poner en cola en espera de una aprobación manual.

[0027] En referencia a la figura 3, un diagrama de bloque ejemplar muestra una administradora de mensajes segura de acuerdo con el invento. La aceptación de la invitación por el colega crea unos certificados cruzados en el agente administrativo SMM que luego se envía a los agentes trabajadores SMM que codifican el certificado. La certificación cruzada restringe el conjunto de nombres que la nueva confiabilidad acepta y la restricción a la comunicación de dominio del servidor limítrofe. Para facilitar una ejecución mejorada, el SMM que envía asigna una llave de sesión y reutiliza ésta llave a través de mensajes múltiples a un recipiente SMM. La llave de la sesión también se puede distribuir en este caso del administrador SMM al trabajador SMM de tal manera que todos los trabajadores utilicen la misma llave para reducir el tamaño de la memoria cache. Para permitir el escalamiento, la llave privada de decodificación correspondiente para el certificado codificado debe estar disponible en todo el Internet enfrenteado a los servidores limítrofes para permitir la decodificación de correo entrante. Esto se puede generar en un solo sitio, por ejemplo, el agente administrativo y distribuido a todos los trabajadores de servidor. Una vez que se establece una relación confiable, se debe mantener. Por ejemplo, el certificado original se puede retener y una solicitud de renovación enviarse a otro SMM antes de que el certificado expire.

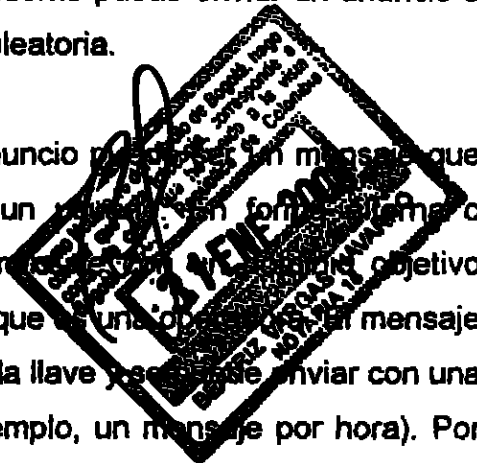
[0028] Desde la perspectiva del servidor, el sistema de acuerdo a este invento establece un vínculo entre el dominio fuente y el dominio objetivo. Inicialmente un servidor fuente transmite un anuncio a un dominio objetivo potencial. El aviso incluye un elemento de datos tales como se mencionó o



una ficha u otro secreto que está asignado específicamente al dominio objetivo. Adicionalmente, el anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el servidor dominio fuente y el computador objetivo. El servidor dominio fuente recibe una invitación del dominio objetivo cuya invitación está dirigida a la dirección del dominio fuente que suministró previamente. La invitación incluye un elemento de datos en el anuncio o un elemento de datos que corresponde al elemento de datos en el anuncio. Esto permite que el servidor fuente inicie un proceso para establecer un vínculo entre el servidor de dominio objetivo y el servidor de dominio fuente tan pronto recibe el servidor de dominio fuente la invitación del servidor de dominio objetivo. Como se anotó en la figura 2, el servidor de dominio fuente transmite al servidor de dominio objetivo una aceptación para establecer el vínculo entre ellos.

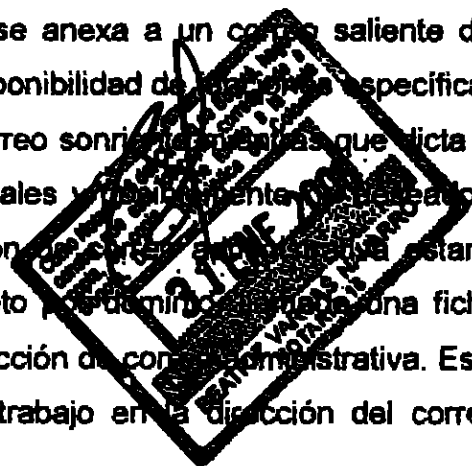
[0029] En una implementación, el dominio fuente transmite en forma selectiva el anuncio al dominio objetivo de donde el dominio fuente ha recibido el mensaje en forma alterna o adicionalmente, el dominio fuente puede enviar un anuncio al dominio objetivo que se ha identificado específicamente. En forma alterna o adicionalmente, el dominio fuente puede enviar un anuncio a dominios objetivos seleccionados en forma aleatoria.

[0030] En una implementación, el anuncio puede ser un mensaje que se genera en respuesta a la acción de un usuario. En forma alterna o adicionalmente el anuncio puede ser un mensaje a un dominio objetivo único y/o un mensaje a un dominio objetivo que es una operación. El mensaje único al dominio objetivo puede ser para cada llave y se puede enviar con una determinación basada en el tiempo (por ejemplo, un mensaje por hora). Por ejemplo, la acción del usuario puede ser un NDR o recibos de vuelta.



[0031] En una implementación del invento, un servidor de email ocasionalmente añade un encabezado adicional (como un "x-header") a un mensaje que se entrega a otro dominio email. Los datos en el encabezado incluyen un secreto que es específico al dominio objetivo y la dirección de correo adonde el mensaje administrativo del dominio objetivo se puede dirigir de vuelta al servidor de correo. Si el correo en el dominio objetivo también se dirige a través del servidor que implementa esta implementación del invento, entonces detectara el encabezado adicional y determinara que debe haber un servidor compatible en el dominio de origen. El dominio objetivo luego dirige el tráfico administrativo, tal como las peticiones para establecer una conexión segura, a la dirección de correo administrativa contenida. Como se anotó anteriormente, tales mensajes administrativos deben contener el secreto que le fue suministrado al dominio objetivo. El que acepta el correo administrativo en el dominio de origen puede entonces descartar cualquier correo que pretenda ser del dominio objetivo pero que no contiene el secreto correspondiente al dominio objetivo. Aunque esto no suministra una seguridad absoluta de que el correo administrativo recibido es del dominio que origina, minimiza la vulnerabilidad al SPAM

[0032] En una implementación, el invento se implementa utilizando un encabezado, llamado una mención, que se anexa a un correo saliente del dominio fuente. Esta mención revela la disponibilidad de direcciones específicas en el servidor de correo que origina en correo sonriente en las que dicta la necesidad para generar mensajes adicionales y posiblemente los reenvíos. Como se anotó anteriormente, la dirección de correo administrativa estaría incluida en la mención y habría un secreto por dominio que sería una ficha para mitigar los riesgos del SPAM a la dirección de correo administrativa. Esto da soporte a los mensajes del flujo de trabajo en la dirección del correo administrativo



92

[0033] La ficha (o secreto) se puede generar de un dominio objetivo y una semilla de secreto que se mantiene en el servidor que origina. Esto permite que una semilla única se comparta a través de múltiples servidores, de tal manera que cada servidor va a generar la misma ficha única para cualquier dominio objetivo. Cuando un mensaje administrativo se recibe en el servidor que origina (porque está dirigido a la dirección administrativa incluida en la mención), la ficha suministrada en el mensaje administrativo la chequea el servidor que origina. Para chequear la ficha, el servidor de e-mail genera una ficha para el dominio que envió el mensaje administrativo utilizando la semilla interna actual. Si la ficha generada es la misma que la que se utilizó en el mensaje administrativo, entonces ese mensaje tiene la ficha correcta y pasa al destino apropiado para mensajes administrativos. Si la ficha no concuerda, se aplica el mismo proceso que a fichas previas (hasta un número límite.) Si ninguna de las semillas válidas actuales se puede utilizar para generar una ficha que concuerda con la ficha en el mensaje entrante, entonces el mensaje no se considera válido y se descarta o se rechaza, y no se pasa al destino eventual para mensajes administrativos. Esto previene ataques no autorizados de SPAM contra el receptor del mensaje administrativo, que puede no ser capaz de enfrentar un gran volumen de e-mail. Adicionalmente, para prevenir la negación de ataques a los servicios de un dominio que recibió una ficha válida, el proceso de verificación es capaz de seguir la pista de cuantos mensajes pasaron recientemente al destino administrativo de un dominio particular o utilizando una ficha particular. Cuando ese número excede un límite permitido, los mensajes administrativos adicionales utilizando esa ficha se descartan o se rechazan.

[0034] La figura 4 es un diagrama de flujo que registra las operaciones de búsqueda de ruta administrativas del SMM de acuerdo con este invento. La verificación de firmas y decodificación deben suceder antes que cualquier proceso anti-SPAM por qué la salida de la verificación es necesaria para fijar

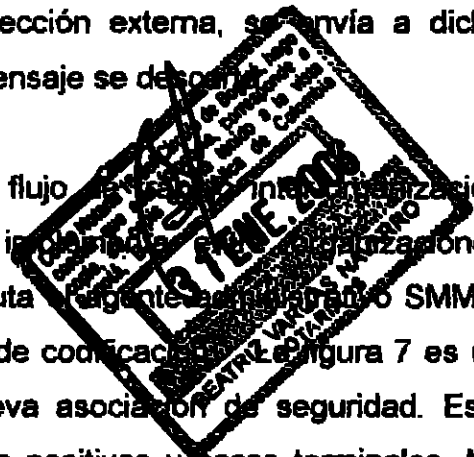
13

93

las banderas de propiedad del mensaje utilizadas por el agente anti-SPAM. La verificación de firma debe suceder luego del RLB y otras funciones en el nivel de la dirección IP. De esta manera, el proceso comienza con la recepción de mensajes en la dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje en 402. Si se determina en 404 que la ficha no es válida para la dirección del remitente, el mensaje se abandona en 406 y el proceso de búsqueda de ruta termina. Si la ficha es válida, el proceso procede a 408 para determinar si el dominio tiene una cuenta máxima que se ha excedido. Si el máximo se excedió, el mensaje se abandona en 406; de lo contrario, si la firma es válida en 410 el mensaje se envía al agente administrador local.

[0035] La figura 5 es un diagrama de flujo que muestra las operaciones de búsqueda de ruta de un trabajador SMM de acuerdo con el invento. La firma y codificación SMM es generalmente la última función. Este componente también inserta el encabezado que contienen la dirección efímera actual SMM para todo el correo que va para dominios sin relación de seguridad. Como se muestra en la figura 5, el dominio busca una firma válida en 502 y una dirección externa en 504 luego de haber encontrado una ficha válida. Si la firma es válida y no hay dirección externa, el mensaje se envía al agente trabajador local en 506. Si hay una dirección externa, se envía a dicha dirección. Si no hay una firma válida el mensaje se descarta.

[0036] En una implementación, el flujo de trabajo de implementación como se muestra en la figura 6 se implementa en las organizaciones administrativas. El flujo de trabajo lo ejecuta el agente administrador SMM y puede incluir el intercambio de una llave de codificación. La figura 7 es un diagrama de estado que muestra la nueva asociación de seguridad. Este diagrama únicamente considera los casos positivos y casos terminales. No incluye otros aspectos tales como la re-transmisión de mensajes anteriores al

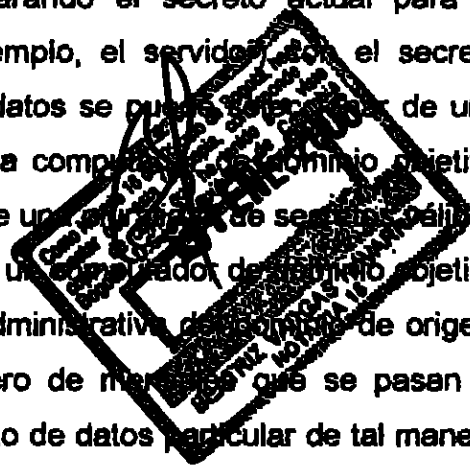


94

94

límite de re-transmisión. En general, los dominios que buscan la aprobación se marcan y si la marca se ha recibido el dominio se aprueba. Los dominios que buscan aceptación se manejan en forma similar.

[0037] Otros rasgos opcionales del invento incluyen lo siguiente que se puede incrementar en forma separada o en combinación. El anuncio puede incluir una fecha de vencimiento y en tal caso el servidor fuente no inicia el proceso para establecer un vínculo con el computador dominio objetivo (por ejemplo, el servidor) cuando el servidor de dominio fuente recibe la invitación luego de la fecha de vencimiento. El elemento de datos puede ser uno de los siguientes: un secreto por dominio incluyendo un número pseudo-aleatorio para cada computador de dominio objetivo (por ejemplo, el servidor), un secreto generado a través de selecciones del computador de dominio objetivo (por ejemplo, el servidor) y una semilla secreta que se utiliza para generar los secretos por dominio para más de un dominio; y un secreto por dominio generado codificando el computador de dominio objetivo (por ejemplo el servidor) y una fecha de terminación para el secreto. Los el elemento de datos puede incluir un secreto y en tal caso el servidor de dominio fuente verifica el secreto recibido del computador de dominio objetivo (por ejemplo, el servidor) re computando y luego comparando el secreto actual para el computador de dominio objetivo (por ejemplo, el servidor) con el secreto incluido en el anuncio. El elemento de datos se puede seleccionar de una pluralidad de secretos múltiples para cada computador de dominio objetivo (por ejemplo, el servidor) de tal manera que una serie de secretos válidos se pueden utilizar para la comunicación de un computador de dominio objetivo (por ejemplo, el servidor) a la dirección administrativa de dominio de origen. Se puede imponer un límite en el número de mensajes que se pasan al servidor de dominio fuente con un elemento de datos particular de tal manera que negaciones de ataques de servicio utilizando un elemento de datos correcto se minimizan. El servidor de dominio fuente puede incluir la habilidad

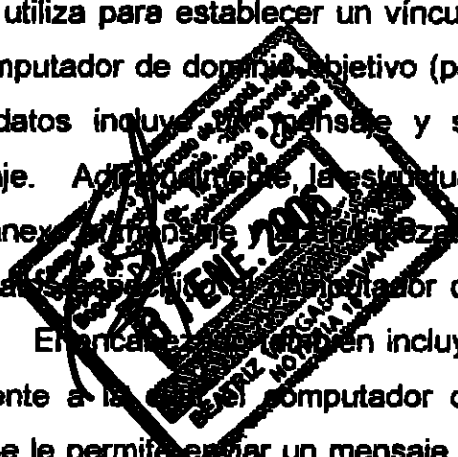


22

95

para sobrepasar los requerimientos para un elemento de datos para el computador de dominio objetivo dado (por ejemplo, el servidor) para permitir una autorización fuera-de-banda para enviar mensajes de invitación de un dominio particular. El elemento de datos puede ser una ficha en el mensaje de anuncio en un encabezado de correo o incrustada en el cuerpo de un mensaje o el elemento de datos puede ser una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando pasa a través del servidor de correo. El servidor de dominio fuente puede dar soporte a múltiples fichas válidas simultáneamente para el mismo dominio y verificar los mensajes de invitación de sub-dominios del computador de dominio objetivo (por ejemplo, el servidor) verificando la ficha de entrada contra las fichas para el computador de dominio objetivo (por ejemplo, el servidor). El elemento de datos puede ser una mención e incluir en la mención información de la versión para el servidor de dominio fuente e incluir en la mención funciones apoyadas por el servidor de dominio fuente.

[0038] En una implementación el invento comprende una estructura de datos para que el aviso se pueda transmitir del servidor de dominio fuente al computador de dominio objetivo (por ejemplo, el servidor). Como se anotó anteriormente, esta estructura de datos se utiliza para establecer un vínculo entre el servidor de dominio fuente y el computador de dominio objetivo (por ejemplo, el servidor). La estructura de datos incluye un mensaje y su encabezado usual relacionado con él mensaje. Además, la estructura de datos incluye un encabezado adicional anexo al mensaje y al encabezado del mensaje que incluye un elemento de datos asociado al computador de dominio objetivo (por ejemplo, el servidor). En el encabezado también incluye una dirección del servidor de dominio fuente a la que el computador de dominio objetivo (por ejemplo, el servidor, se le permite enviar un mensaje al servidor de dominio fuente para establecer un vínculo entre el servidor de dominio fuente y el computador de dominio objetivo (por ejemplo, el servidor).



:

96

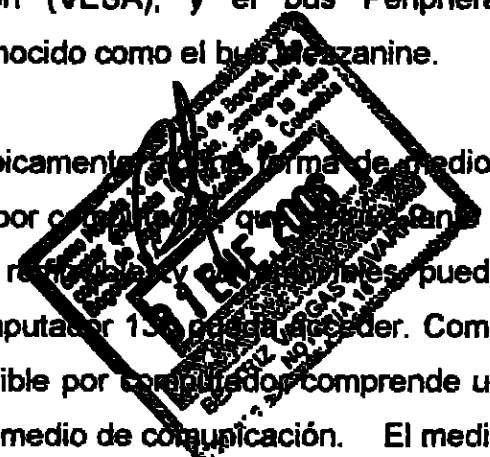
96

Como se anotó anteriormente, el encabezado adicional debe incluir una fecha de vencimiento, aunque esto es opcional.

[0039] Una implementación operativa ejemplar:

[0040] La figura 8 muestra un ejemplo de un dispositivo de cómputo de propósito general en la forma de un computador 130. En una implementación del invento, un computador tal como el computador 130 es adecuado para uso en las otras figuras que se muestran y se describen acá. El computador 130 tiene uno o más procesadores o unidades procesadoras 132 y una memoria de sistema 134. Tiene en la implementación que se muestra, un bus de sistema 136 que acopla los componentes varios del sistema incluyendo la memoria del sistema 134 con el procesador 132. El bus 136 representa uno o más de varios tipos de estructuras de bus, incluyendo un bus de memoria o controladora de memoria, un bus periférico, un puerto de gráficos acelerado, y un procesador de bus local utilizando cualquiera de varias arquitecturas de bus. Como ejemplo, y no como limitante, estas arquitecturas incluyen el bus Industry Standard Architecture (ISA), el bus Micro Channel Architecture (MCA), el bus Enhanced ISA (EISA), el bus local Video Electronics Standards Association (VESA), y el bus Peripheral Component Interconnect (PCI) también conocido como el bus Mezzanine.

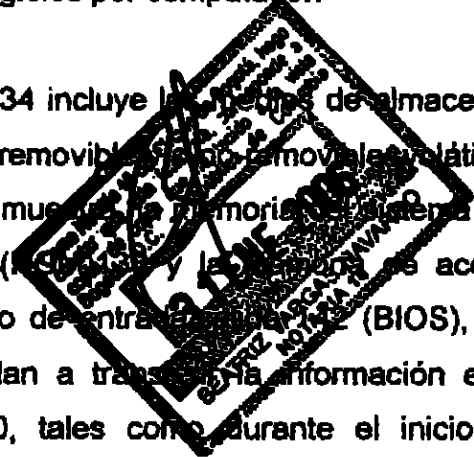
[0041] El computador 130 tiene típicamente en la forma de medios legibles por computador. El medio legible por computador que comprende a los medios volátiles y no-volátiles, medios removibles y no-removibles, puede ser cualquier medio disponible que el computador 130 pueda acceder. Como ejemplo y no como limitante, el medio legible por computador comprende un medio de almacenaje de computador y un medio de comunicación. El medio legible por computador incluye los medios volátiles y no-volátiles, removibles y no-removibles implementados en cualquier método o tecnologías para



97

almacenar información tal como instrucciones legibles por computador, estructuras de datos, modo los del programa o cualquier otro tipo de datos. por ejemplo, los medios legibles por computador incluyen RAM, ROM, EPPROM, memoria flash o cualquier otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) o cualquier otro almacenaje en disco óptico, casetes magnéticos, cintas magnéticas, almacenaje en discos magnéticos o cualquier otro dispositivo de almacenaje magnético, o cualquier otro medio que se pueda utilizar para almacenar la información deseada que el computador 130 pueda acceder. Los medios de comunicación encarnan instrucciones legibles por computador, estructuras de datos, módulos de programa, u otros tipos de datos en señal de datos modulada tales como ondas transportadoras y otros mecanismos de transporte e incluyen cualquier medio de suministro de información. Aquellos diestros en el arte están familiarizados con las señales de datos moduladas, que tienen una o más de sus características fijas o alteradas de tal manera que codifican la información en la señal. Medios alambrados, tales como redes alambradas o conexiones alambradas directas, y medios inalámbricos, tales como acústicos, RF, infrarrojos y otros medios inalámbricos, son ejemplos de medios de comunicación. Combinaciones de cualquier tipo de los anteriores también se incluyen dentro del alcance de medios legibles por computador.

[0042] La memoria del sistema 134 incluye los tipos de almacenaje en computador en la forma de memoria removible y/o no-removible, volátil y/o no-volátil. En la implementación que se muestra, la memoria del sistema 134 incluye a la memoria de sólo lectura (ROM) 138 y la memoria de acceso aleatorio (RAM) 140. Un sistema básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir la información entre elementos dentro del computador 130, tales como durante el inicio, se almacenan en forma típica en ROM 138. La RAM 140 Contienen típicamente datos y/o módulos de programa que son accesibles inmediatamente y/o están

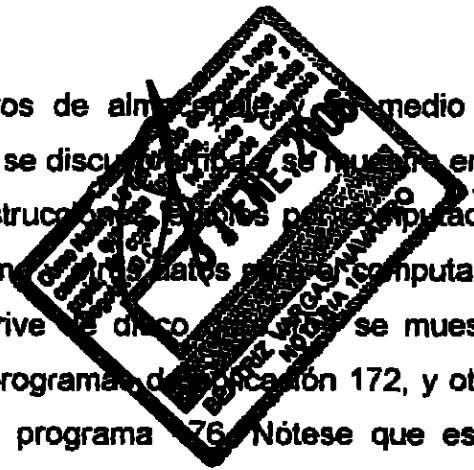


98

operados actualmente por la unidad de procesamiento 132. Como ejemplo, y no como limitante, la figura 8 muestra el sistema operativo 144, programas de aplicación 146, y otros módulos de programas 148, y datos de programas 150.

[0043] El computador 130 también puede incluir otros medios de almacenaje en computador removibles y/o no-removibles, volátiles y/o no-volátiles. Por ejemplo, la figura 8 muestra un drive de disco duro 154 que lee o escribe a medios magnéticos no-removibles y no-volátiles. La figura 8 también muestra un drive de disco magnético 156 que lee o escribe a el disco magnético removible, no-volátil 158, y un drive de disco óptico 160 que lee o escribe a el disco óptico removible, no-volátil 162 tal como un CD- ROM o cualquier otro medio óptico. Otros tipos de medios de almacenaje en computador removibles/no-removibles, portátiles/no-volátiles que se pueden utilizar en el ambiente operativo ejemplar incluyen, pero no están limitadas a, cassettes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cintas de videos digitales, RAM de estado sólido, ROM de estado sólido, y cosas parecidas. El drive de disco duro 154, y el drive de disco magnético 156 y el drive de disco óptico 160 están conectados en forma típica al bus del sistema 136 a través de una interfase de memoria no-volátil, tal como la interfase 166.

[0044] El drive u otros dispositivos de almacenaje, como medio de almacenaje en computador asociado que se discute típicamente en la figura 8, suministra el almacenaje de instrucciones, datos para el computador, estructuras de datos, módulos de programa, y otros datos para el computador 130. En la figura 8, por ejemplo, el drive de disco duro se muestra almacenando el sistema operativo 170, programas de aplicación 172, y otros módulos de programa 174, y datos de programa 176. Nótese que estos componentes pueden ser iguales o diferentes al sistema operativo 144,



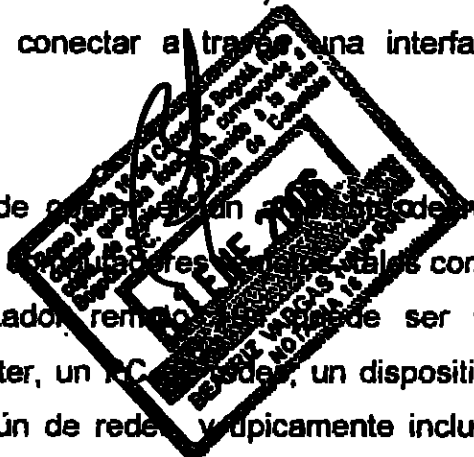
99

99

programas de aplicación 146, u otros módulos de programa 148, y datos de programa 150, al sistema operativo 170, programas de aplicación 172, otros módulos de programas 174 y datos de programas 176 se les dan distintos números para mostrar que, por lo menos, son copias diferentes.

[0045] Un usuario puede ingresar un comando de información al computador 130 a través de dispositivos de entrada o dispositivos de selección en la interfase del usuario tales como un teclado 180 y un dispositivo de señalamiento 182 (por ejemplo, un ratón, un trackball, una pluma o una almohadilla táctil). Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, un joystick, un panel de juegos, un disco satelital, escáner, y demás. Éstos y otros dispositivos de entrada se conectan a la unidad procesadora 132 a través de una interfase de usuario de entrada 184 que se acopla al bus del sistema 136, pero que puede estar conectada por otras interfases o estructuras de bus, tales como puertos paralelos, puertos de juego, o el Bus Serial Universal (USB). Un monitor 188 u otro tipo de dispositivo de visualización también se conecta al bus del sistema 136 a través de una interfase, tal como la interfase de vídeo 190. Adicionalmente al monitor 188, los computadores frecuentemente incluyen otros dispositivos de salida periféricos (que no se muestran) tales como una impresora y parlantes, que se pueden conectar a través de una interfase periférica de salida (que no se muestran).

[0046] El computador de 130 puede estar en un ambiente de red utilizando conexiones lógicas a uno o más computadores, tales como el computador remoto 194. El computador remoto puede ser un computador personal, un servidor, un router, un PC, un nodo, un dispositivo de un colega o cualquier otro nodo común de red, y típicamente incluye muchos o todos de los elementos descritos arriba relativos al computador 130. Las conexiones lógicas que se muestran en la figura 8 incluyen una red de



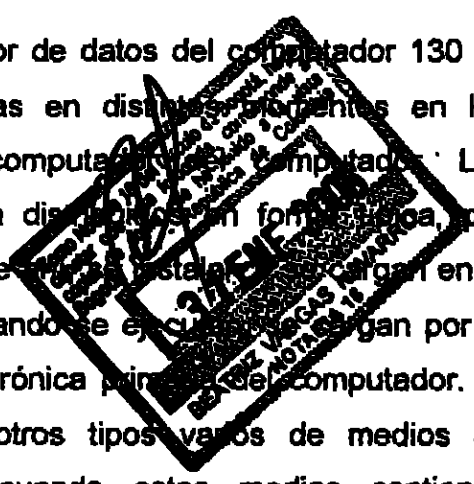
100

100

área local (LAN) 196 y una red de área amplia (WAN) 198, pero también pueden incluir otras redes. La LAN 136 y/o la WAN 138 pueden ser una red alamburada, una red inalámbrica, o una combinación, y demás. Estos ambientes de redes son comunes en oficinas, redes de computadores de negocios, intranets, y redes globales de computadores (por ejemplo, Internet).

[0047] Cuando se utilizan en un ambiente de red local, el computador 130 está conectado a la LAN 196 a través de una interfase de red o adaptador 186. Cuando se utiliza en un ambiente de red de área amplia, el computador 130 incluye típicamente un modem 178 u otros medios para establecer comunicación con la WAN 198, tal como Internet. El modem 178, que puede ser interno o externo, se conecta al bus del sistema 136 a través de una interfase de entrada del usuario 184, u otros mecanismos apropiados. En un ambiente de red, los módulos de programa que se muestran relativos al computador 130, o porciones de él, se pueden almacenar en un dispositivo de almacenaje de memoria remoto (que no se muestran). Como ejemplo, y no como limitante, la figura 8 muestra programas de aplicación remotos 192 como residiendo en el dispositivo de memoria. Las conexiones de red que se muestran son ejemplares y otros medios para establecer un vínculo de comunicación entre computadores se puede utilizar.

[0048] Generalmente, el procesador de datos del computador 130 se programa con instrucciones almacenadas en distintos elementos en los medios de almacenaje legibles por computador. Los programas y el sistema operativo están distribuidos en forma física, por ejemplo, en discos floppy o CD ROMs. Dichos programas se cargan en la memoria secundaria del computador. Cuando se ejecutan, se cargan por lo menos parcialmente en la memoria electrónica primaria del computador. El invento descrito acá incluye estos y otros tipos varios de medios de almacenaje legibles por computador cuando estos medios contienen



[a]

101

instrucciones o programas para implementar los pasos descritos más abajo en conjunto con un micro procesador u otro procesador de datos. El invento también incluye al computador en sí mismo cuando se programa de acuerdo a los métodos y técnicas descritos acá.

[0049] Con un propósito ilustrativo, los programas y otros componentes de programas ejecutables, tales como el sistema operativo, se muestran como bloques discretos. Se reconoce, sin embargo, que tales programas y componentes residen, en varios momentos, en distintos componentes de almacenaje del computador, y los ejecuta el procesador(es) del computador.

[0050] Aunque se describe en relación con el ambiente de sistema de computación ejemplar, incluyendo a los computadores 130, el invento es funcional con otros ambientes de sistema de computación de propósito general o especial y otras combinaciones. El ambiente de sistema de computación no tiene la intención de sugerir ninguna limitación en cuanto al alcance, uso o funcionalidad del invento. Aún más, el ambiente de sistema de computación no se debe interpretar como teniendo algunas dependencias o requerimiento relacionado con uno o varios componentes o combinación de ellos ilustrados en el ambiente operativo ejemplar. Ejemplos de sistemas de cómputo, ambientes, y/o configuraciones que son adecuadas para uso con el invento incluyen, pero no están limitados a, computadores personales, computadores servidores, dispositivos de mano, computadores multi-procesadores, teléfonos móviles, Pcs de red, máquinas portátiles, estaciones de trabajo, ambientes de cómputo distribuidos que incluya cualquiera de los sistemas anteriores o dispositivos mencionados, y otros parecidos.

[0051] El invento se puede describir en el contexto general de las instrucciones ejecutables por computador, tales como módulos de programa, ejecutados por uno o más computadores u otros dispositivos. Generalmente.

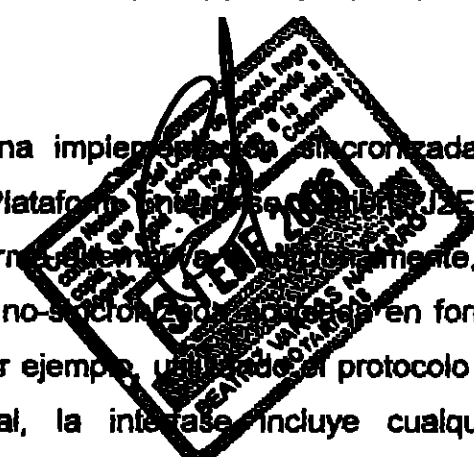
102

102

los módulos de programa incluyen, pero no están limitados a, rutinas, programas, objetos, componentes, estructuras de datos que ejecutan tareas particulares o implementan tipos de datos abstractos particulares. El invento también se puede practicar en ambientes de cómputo distribuidos donde las tareas las ejecuta un procesador remoto que está vinculado a través de una red de comunicaciones. En un ambiente de cómputo distribuido, los módulos de programa pueden estar localizados tanto en los medios de almacenaje del computador local y en el computador remoto incluyendo a los dispositivos de almacenaje de memoria.

[0052] Una interfase en el contexto de la arquitectura de software incluye módulos de software, componentes, porciones de código, u otras secuencias de instrucciones ejecutables por computador. La interfase incluye, por ejemplo, un primer módulo que accede a un segundo módulo para ejecutar tareas de cómputo en beneficio del primer módulo. El primero y segundo módulo incluyen, en un ejemplo, aplicaciones de interfases de programación (API) tales como las suministradas por el sistema operativo, interfaces de modelo de objetos (COM) (por ejemplo, para aplicaciones de comunicación colega-colega), y las interfaces de formato de intercambio de meta datos del lenguaje de marcación extensible (XML)(por ejemplo, para la comunicación entre servicios de red).

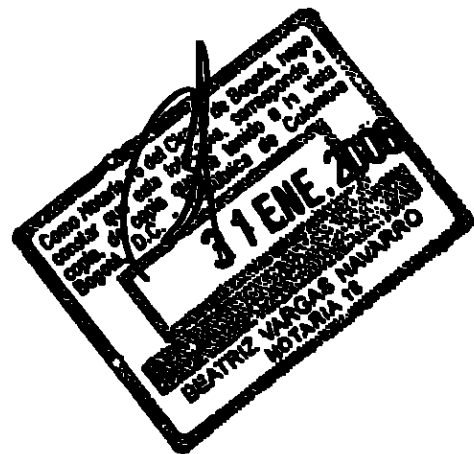
[0053] La interfase puede ser una implementación sincronizada y acoplada fuertemente como la Java 2 Plataforma Interfaz de Objetos (J2EE), COM, o COM distribuido (DCOM). En forma alternativa, no fuertemente, la interfase puede ser una implementación no-sincronizada, acoplada en forma suelta tal como en un servicio de red (por ejemplo, utilizando el protocolo de acceso a objetos simple). En general, la interfase incluye cualquier combinación de las siguientes características: acoplada fuertemente, acoplada suelta, sincronizada, y no-sincronizada. Aún más, la interfase se



103

104

[0059] Como se pueden hacer varios cambios en la construcción mencionada, productos, y métodos sin alejarse del alcance del inventó, se pretende que todo el material contenido en la anterior descripción y que se muestra en los dibujos acompañantes se debe interpretar como ilustrativa y no limitante en ningún sentido.



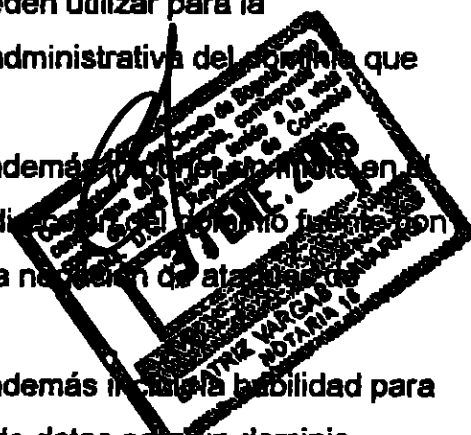
105

LO QUE SE REIVINDICA ES:

1. Un método para establecer un vínculo entre un dominio fuente y un dominio objetivo que comprende:
transmitir un anuncio del dominio fuente al dominio objetivo donde el anuncio incluye un elemento de datos específico para el dominio objetivo y donde el aviso incluye una dirección del dominio fuente a la cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo; y
recibir por el dominio fuente, a través de la dirección del dominio fuente una invitación del dominio objetivo donde la invitación incluye un elemento de datos o un elemento de datos correspondiente al elemento de datos donde el dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo tan pronto recibe el dominio fuente la invitación.
2. El método de la reivindicación 1 comprende además la transmisión de una aceptación del dominio fuente al dominio objetivo para establecer el vínculo entre ellos.
3. El método de la reivindicación 1 donde el anuncio se transmite en forma selectiva a por lo menos uno de los siguientes:
dominios objetivos de donde el dominio fuente ha recibido un mensaje;
dominios objetivo específicamente identificados anteriormente;
dominios objetivos seleccionados en forma aleatoria.
4. El método de la reivindicación 1 donde el anuncio es un mensaje que genera en respuesta a una acción de usuario; donde el anuncio es un mensaje con un dominio objetivo único; donde el anuncio es un mensaje para un dominio objetivo que es un operador; donde el anuncio es un mensaje único al dominio objetivo para cada llave; o donde el anuncio es un mensaje enviado con una determinación basada en el tiempo.
5. El método de la reivindicación 1 donde el anuncio comprende un encabezado adicional que incluye los elementos de datos y la dirección del dominio fuente.



6. El método de la reivindicación 1 donde el aviso comprende una fecha de vencimiento y donde el dominio fuente no inicia el proceso para establecer un vínculo con el dominio objetivo cuando el dominio fuente recibe la invitación luego de la fecha de vencimiento.
7. El método de la reivindicación 1 donde el elemento de datos es por lo menos uno de los siguientes: un secreto por dominio que incluye un número pseudo-aleatorio para cada dominio objetivo; un secreto generado a través del dominio objetivo y una semilla de secreto que se utiliza para generar un secreto por dominio para más de un dominio; y un secreto por dominio generado codificando el dominio objetivo y una fecha de vencimiento del secreto.
8. El método de la reivindicación 1 donde el elemento de datos comprende un secreto y donde el dominio fuente verifica el secreto recibido del dominio objetivo re-computando y luego comparando el secreto actual para el dominio objetivo con el secreto incluido en el aviso.
9. El método de la reivindicación 1, donde el elemento de datos se selecciona de una pluralidad de secretos múltiples para cada dominio objetivo de tal manera que hay una pluralidad de secretos validos que se pueden utilizar para la comunicación del dominio objetivo a la dirección administrativa del dominio que origina.
10. El método de la reivindicación 1, comprende además proporcionar en el número de mensajes que se pueden pasar de la dirección del dominio fuente con un elemento de datos particular donde se mitiga la necesidad de ataques al servicio utilizando un elemento de datos correcto.
11. El método de la reivindicación 1, comprende además incluir la habilidad para sobrepasar los requerimientos para un elemento de datos para un dominio objetivo dado y de esta manera habilitar la autorización fuera de banda para enviar el mensaje de invitación de un dominio particular.
12. El método de la reivindicación 1, donde el elemento de datos es una ficha en el mensaje de aviso en un encabezado de correo o incrustado en el cuerpo del



10x

mensaje o donde el elemento de datos es una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando se pasa a través del servidor de correo.

13. El método de la reivindicación 1 comprende además el soporte de múltiples fichas válidas para el mismo dominio y la verificación de mensajes de invitación de sub-dominios del dominio fuente verificando las fichas de entrada contra fichas para el dominio objetivo.

14. El método de la reivindicación 1 donde el elemento de datos es una mención y comprende además incluir en la mención información sobre la versión para el dominio fuente e incluir en la mención funciones soportadas por el dominio fuente.

15. Una estructura de datos para un anuncio se transmite de un dominio fuente a un dominio objetivo para establecer un vínculo entre el dominio fuente y el dominio objetivo que comprende:

Un mensaje;

Un encabezado relacionado con el mensaje; y

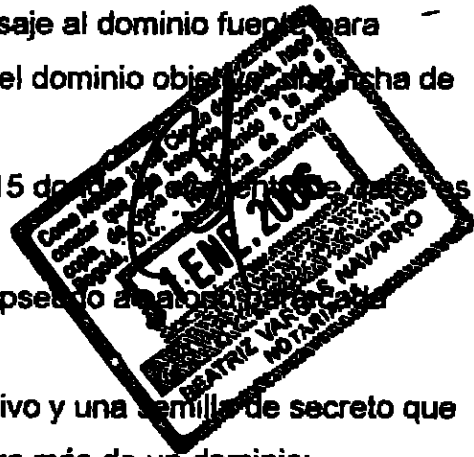
Un encabezado adicional anexo al mensaje y que incluye un elementos de datos específico al dominio objetivo que incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje al dominio fuente para establecer un vínculo entre el dominio fuente y el dominio objetivo, una ficha de emplazamiento y una fecha de vencimiento.

16. La estructura de datos de la reivindicación 15 donde el elemento de datos es por lo menos uno de los siguientes:

Un secreto por dominio que incluye un número pseudo aleatorio para el dominio objetivo,

Un secreto generado a través del dominio objetivo y una semilla de secreto que se utiliza para generar secretos por-dominio para más de un dominio;

un secreto por dominio generado codificando el dominio objetivo y una ficha de vencimiento del secreto;



108

Un secreto donde el dominio objetivo verifica el secreto recibido del dominio objetivo re-calculando y luego comparando el secreto actual para el dominio objetivo con el secreto incluido en el anuncio;

Un elemento de datos se selecciona de una pluralidad de secretos múltiples que se sobreponen para cada dominio objetivo de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación del dominio objetivo a la dirección administrativa del dominio que origina;

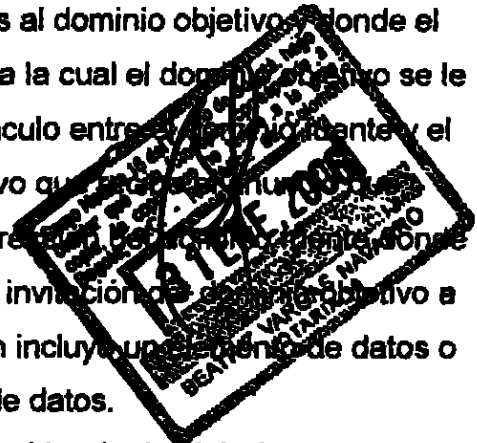
Una ficha en el mensaje de anuncio, en el encabezado del correo o incrustado en el cuerpo del mensaje o donde el elemento de datos es una ficha en el encabezado del correo y el cuerpo del mensaje permanece codificado cuando pasa a través del servidor de correo; y

Una mención que incluye además incluir en la mención información sobre la versión para el dominio fuente e incluye en la mención funciones soportadas por el dominio fuente.

17. Un sistema para establecer un vínculo entre un dominio fuente y un dominio objetivo que comprende:

Un servidor de dominio fuente transmitiendo un anuncio al dominio objetivo donde el anuncio incluye elementos de datos específicos al dominio objetivo; donde el anuncio incluye una dirección del dominio fuente a la cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo; y un computador dominio objetivo que recibe el anuncio y que incluye la recepción del elemento de datos y la dirección del dominio fuente donde el computador del dominio objetivo transmite una invitación del dominio objetivo a la dirección del dominio fuente donde la invitación incluye un elemento de datos o elemento de datos correspondiente al elemento de datos.

18. El sistema de la reivindicación 17 donde el servidor de dominio fuente transmite una aceptación del dominio fuente al dominio objetivo para establecer el vínculo entre ellos y donde el servidor de dominio fuente inicia un proceso para establecer un vínculo con el computador de dominio objetivo tan pronto recibe del servidor de dominio fuente la invitación; y



Comprende adicionalmente uno de los siguientes:

Imponer un límite en el número de mensajes que se pueden pasar a la dirección del dominio fuente con un elemento de datos particular donde se mitiga la negación de ataques de Servicio utilizando un elemento de datos correcto.

Sobrepasando los requerimientos para un elemento de datos para un dominio objetivo dado para permitir las autorizaciones fuera de banda para enviar un mensaje de invitación de un dominio particular; y soportando simultáneamente fichas múltiples válidas para el mismo dominio y verificando el mensaje de invitación de sub-dominios del dominio objetivo verificando la ficha entrante contra fichas para el dominio objetivo.

19. El sistema de la reivindicación 17 donde un anuncio transmitido por un servidor dominio fuente comprende por lo menos uno de los siguientes:

Un anuncio transmitido en forma selectiva al dominio objetivo de donde el dominio fuente ha recibido un mensaje;

Un anuncio transmitido en forma selectiva al dominio objetivo específicamente identificado anteriormente o seleccionado en forma pseudo-aleatoria del dominio objetivo;

Un mensaje que se genera en respuesta a una acción de usuario (por ejemplo, ndrs, recibos);

Un mensaje con un dominio objetivo único;

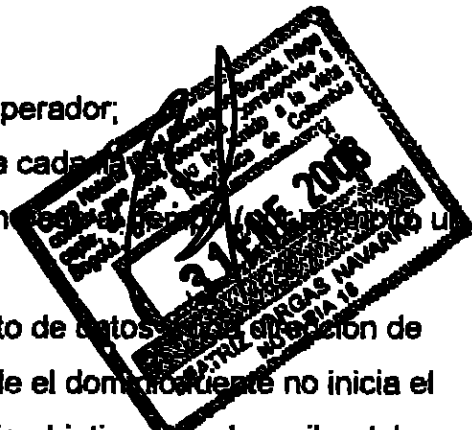
Un mensaje para el dominio objetivo que es un operador;

Un mensaje único para el dominio objetivo y para cada hora;

Un mensaje enviado en determinación hechas en los días de la semana (por ejemplo, mensaje cada hora);

Un encabezado adicional que incluye un elemento de datos de la dirección de dominio fuente; y una fecha de vencimiento donde el dominio fuente no inicia el proceso para establecer un vínculo con el dominio objetivo cuando recibe del dominio fuente una invitación luego de la fecha de vencimiento.

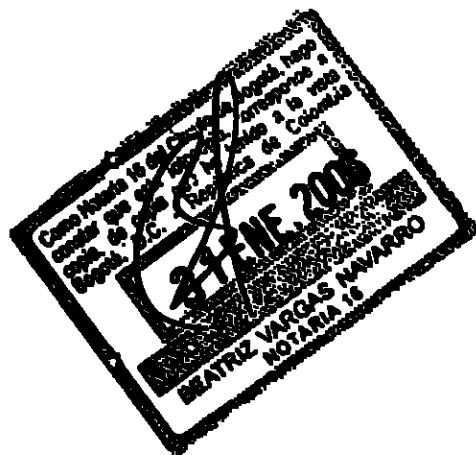
20. El sistema de la reivindicación 17 donde el elemento de datos es por lo menos uno de los siguientes: un secreto por dominio que incluye un número pseudo-



///

RESUMEN

Un anuncio se transmite de un dominio fuente a un dominio objetivo. El anuncio incluye elementos de datos específicos al dominio objetivo y. El anuncio incluye una dirección del dominio fuente al cual el dominio objetivo se le permite enviar un mensaje para establecer un vínculo entre el dominio fuente y el dominio objetivo. El anuncio lo recibe en dominio objetivo incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio objetivo a la dirección del dominio fuente. La invitación incluye el elemento de datos o elemento de datos correspondiente al elemento de datos. El dominio fuente inicia un proceso para establecer un vínculo con el dominio objetivo tan pronto recibe del dominio fuente la invitación.



112

FIG. 1

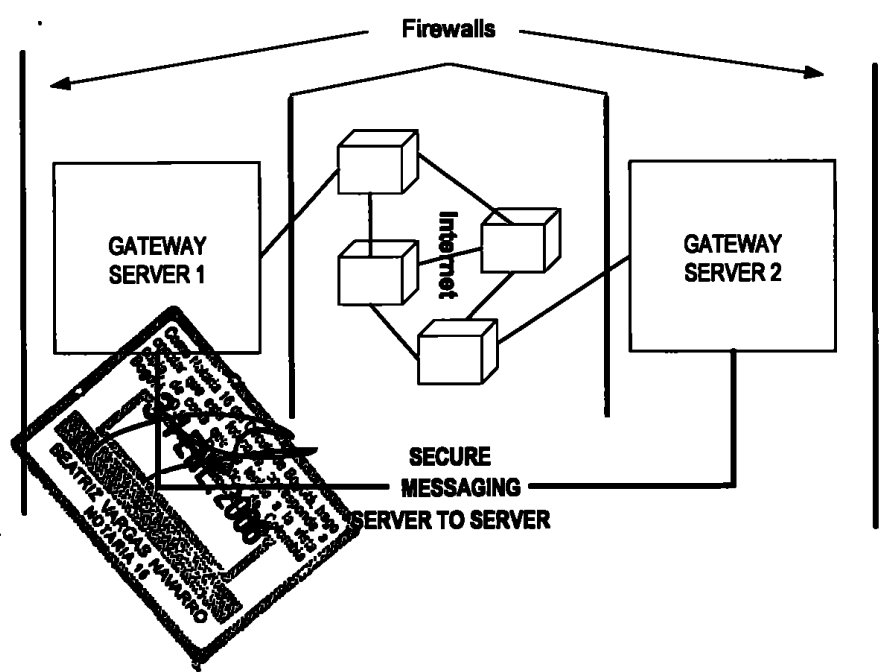
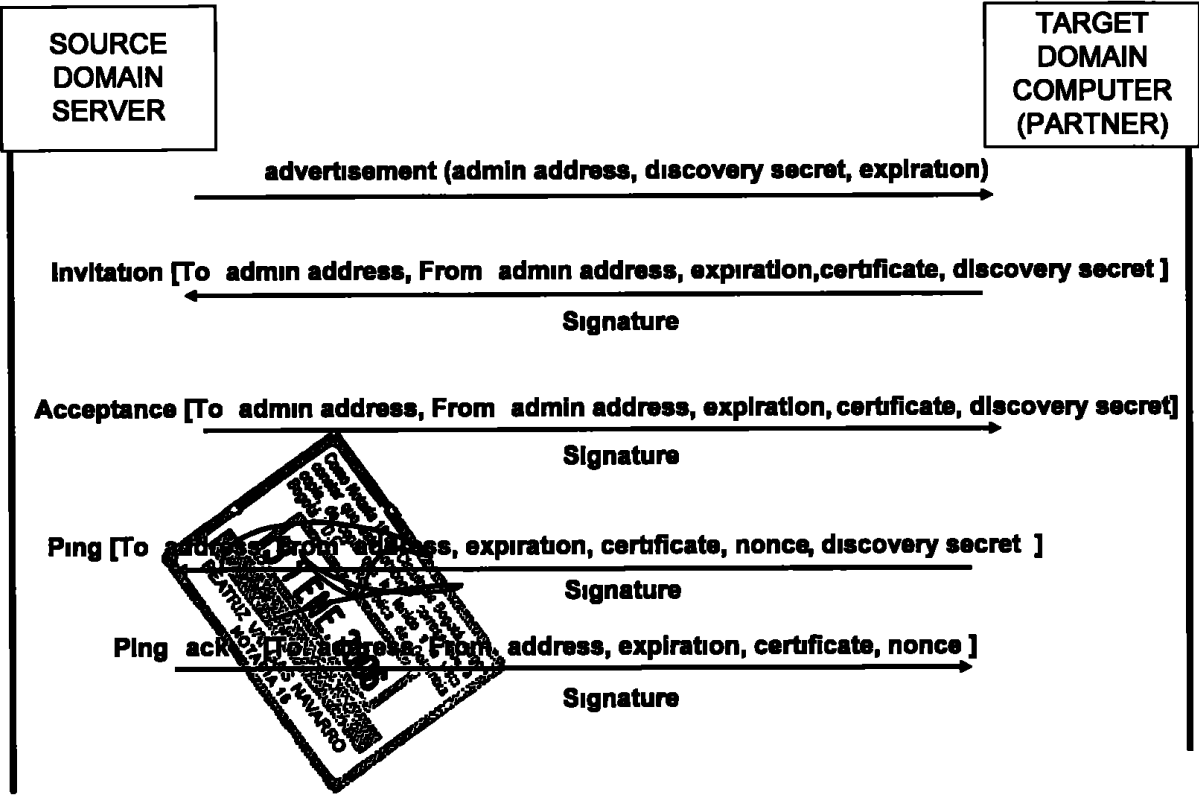
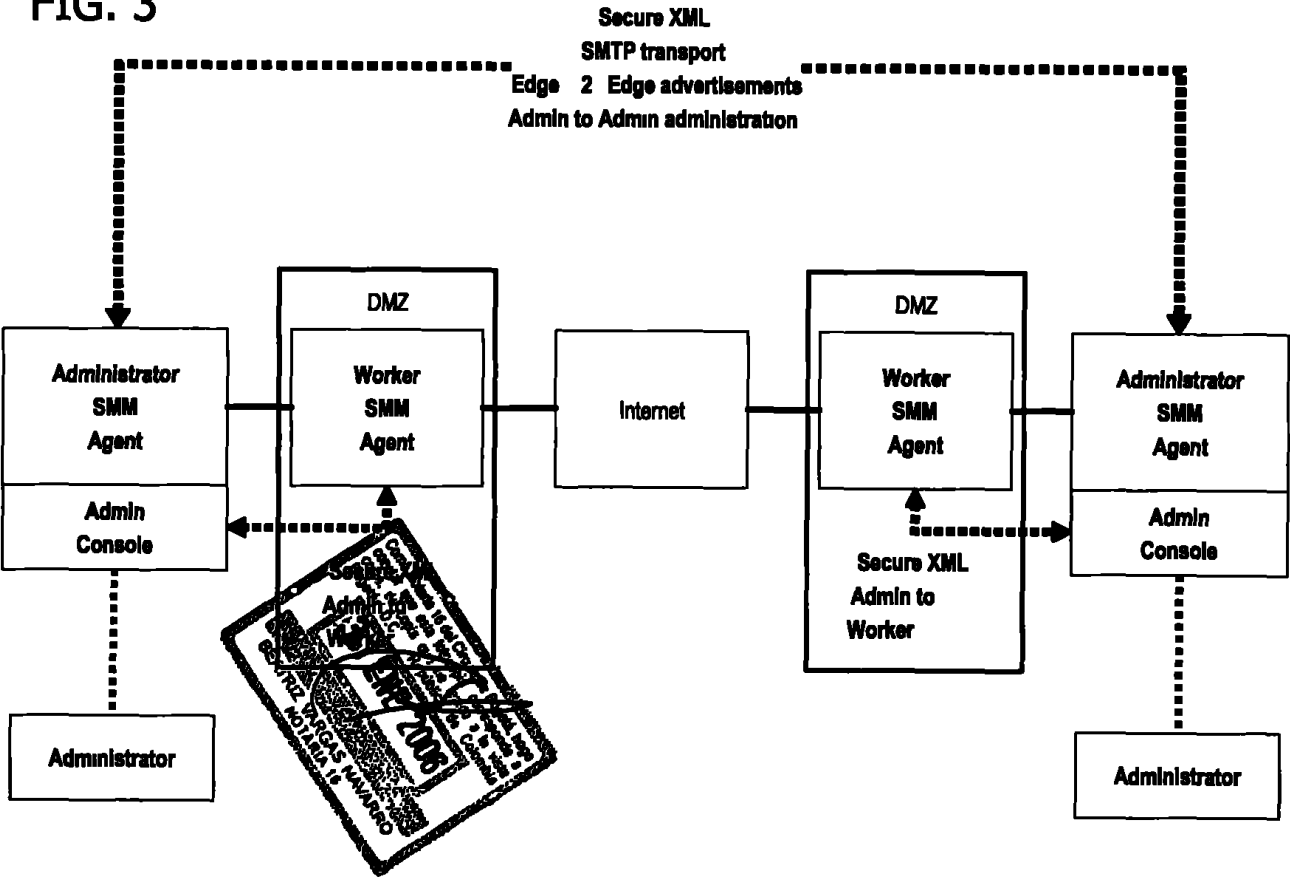


FIG. 2



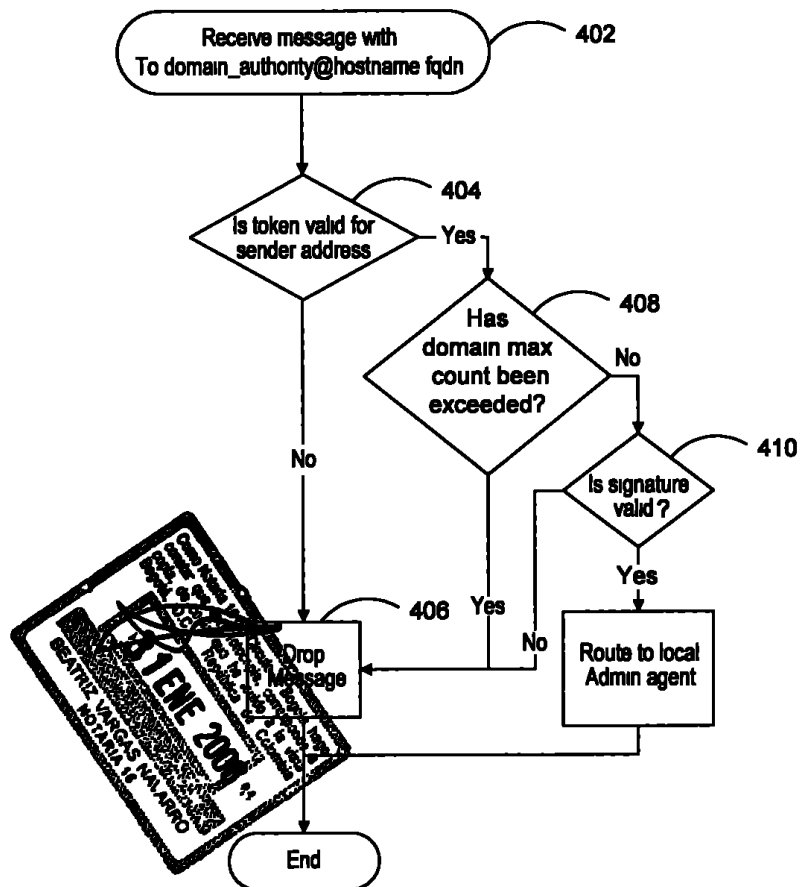
1/3

FIG. 3



115

FIG. 4



116

FIG. 5

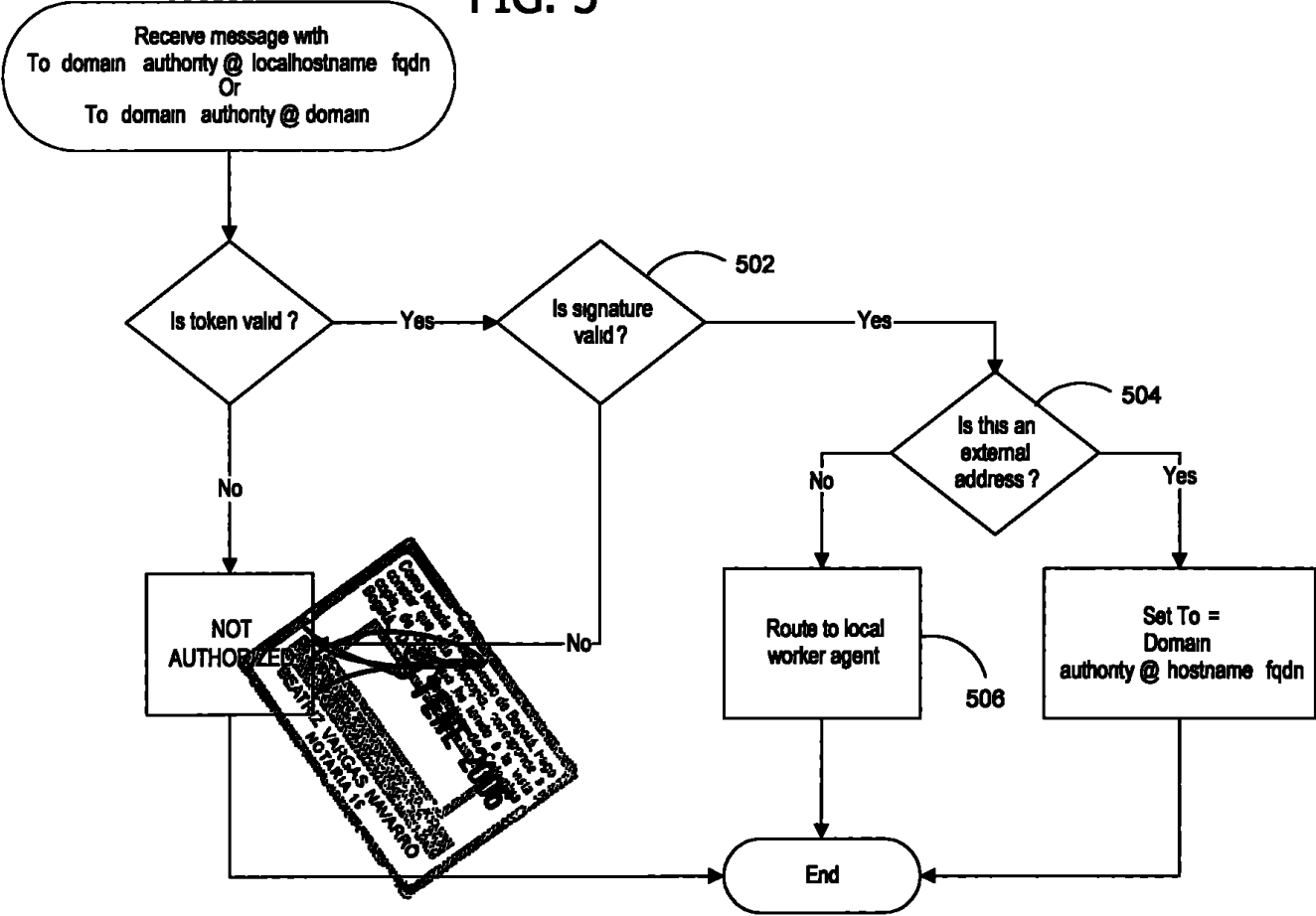


FIG. 6

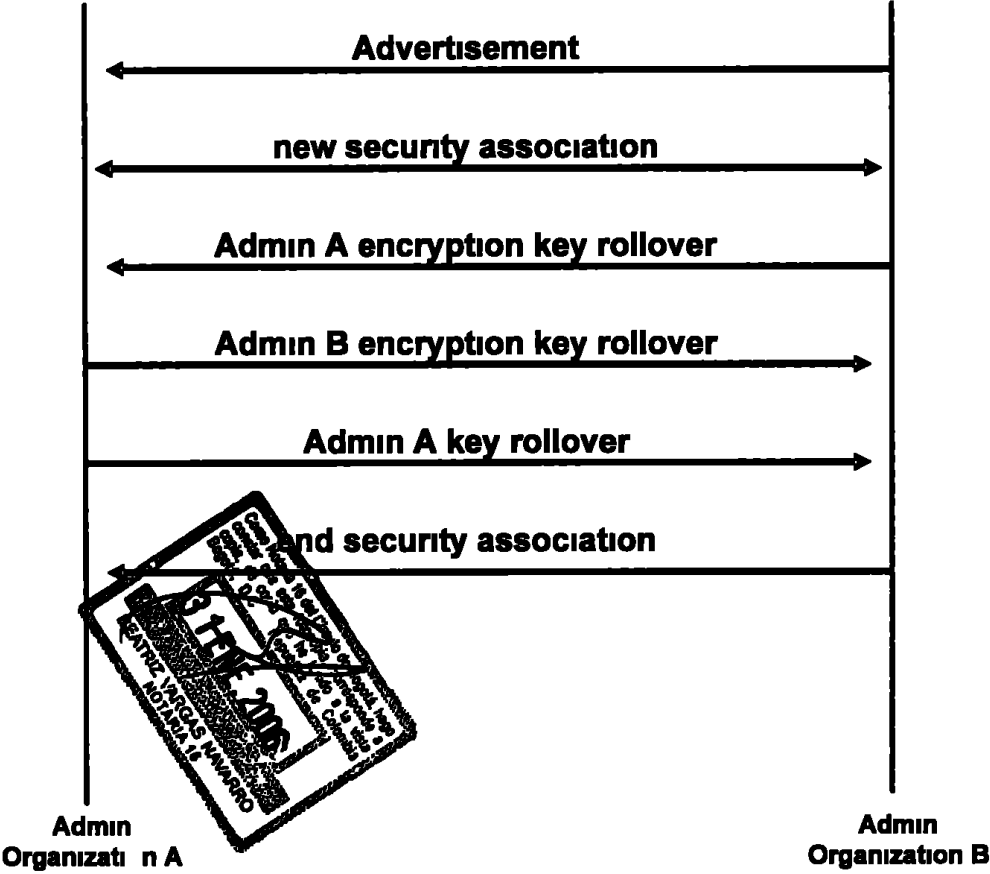
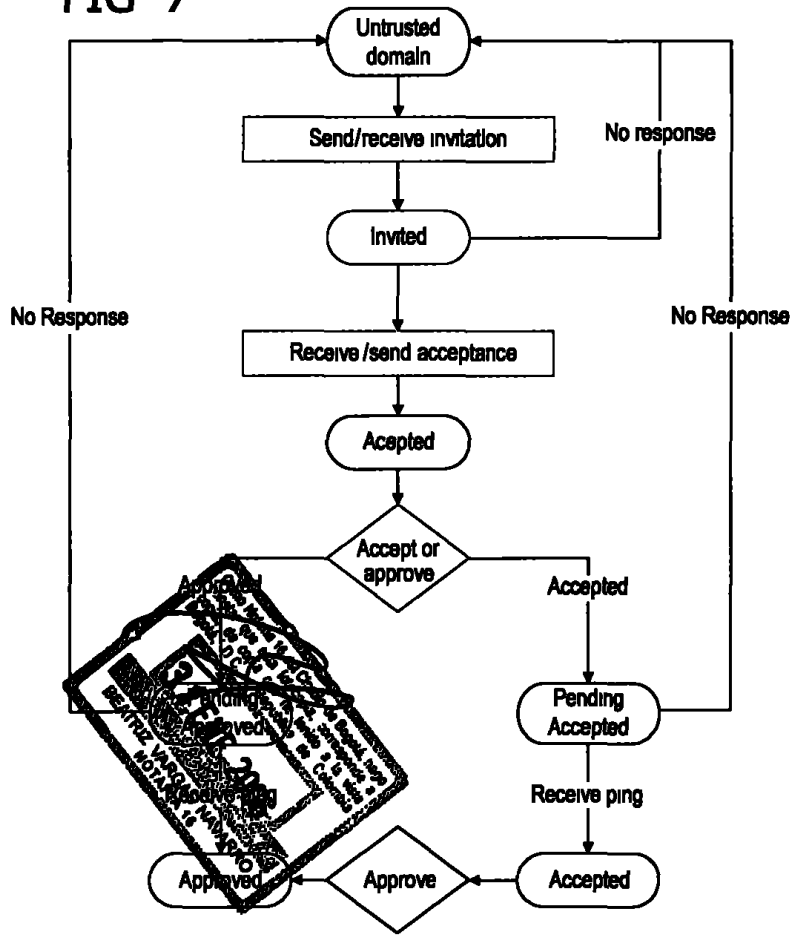


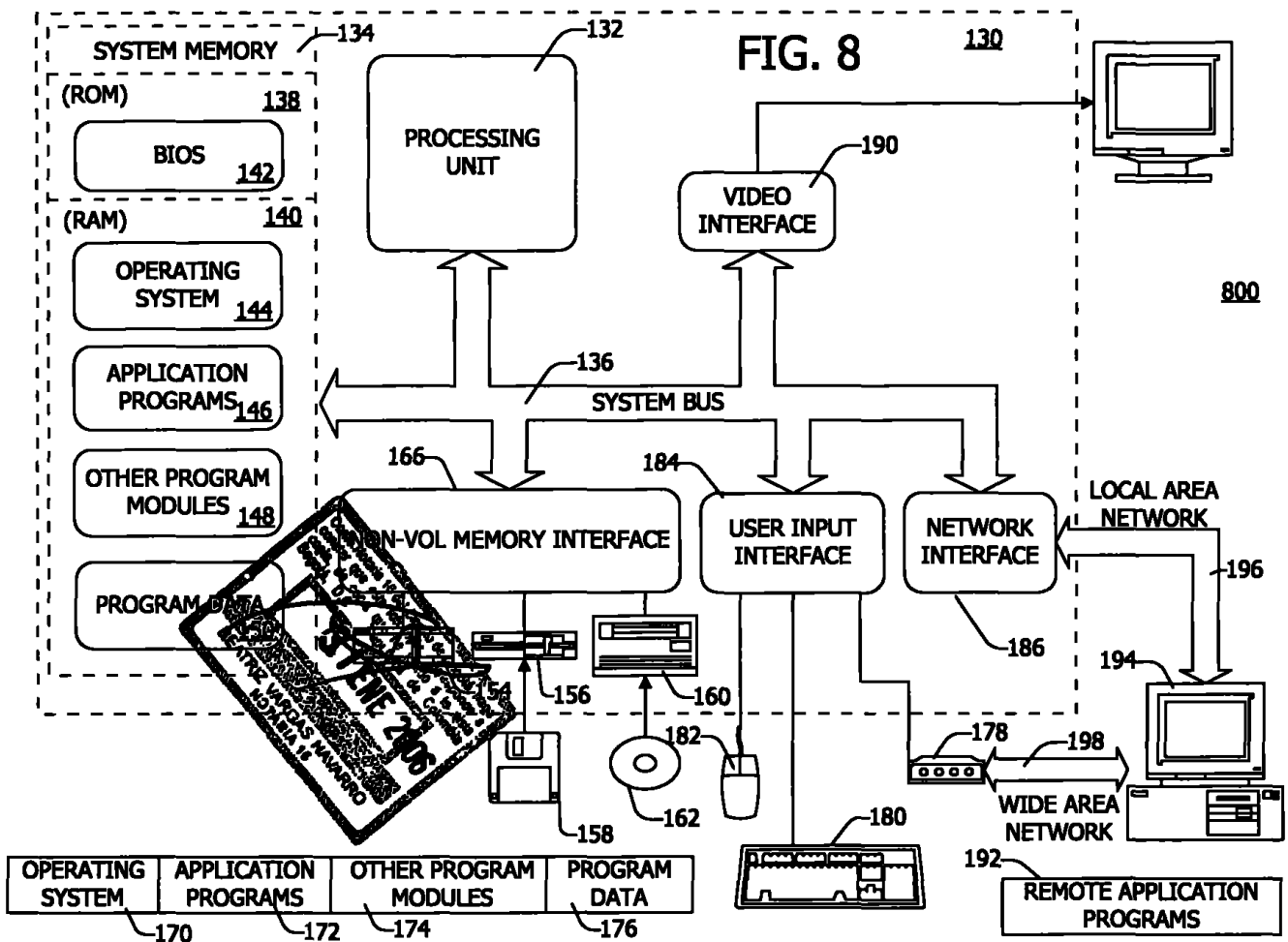
FIG 7

118



7/8

119



DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS

OFICINA DE PATENTE Y MARCA REGISTRADAS
SECRETARÍO Y COMISIONADO ASISTENTE DE
PATENTES Y MARCAS REGISTRADAS

PTAS

500034342AA

Junio 06, 2005
ROBERT M. BAIN /FRA
ONE METROPOLITAN SQUARE, 16 FLOOR
SENNIGER POWERS
ST. LOUIS MO 63102

OFICINA DE PATENTES Y MARCAS REGISTRADAS DE LOS ESTADOS UNIDOS
NOTIFICACION DEL RECORDATORIO DEL DOCUMENTO DE ASIGNACION

EL DOCUMENTO ADJUNTO HA SIDO GRABADO POR LA DIVISION DE LA OFICINA DE
PATENTES Y MARCAS REGISTRADAS DE E.U. UNA COPIA COMPLETA EN MICROFILME
ESTA DISPONIBLE EN EL CUARTO DE BÚSQUEDA DE LAS ASIGNACIONES EN LA CINTA
Y EL NUMERO DE CUADRO QUE SE CITAN ABAJO.

POR FAVOR REVISE TODA LA INFORMACIÓN CONTENIDA EN ESTA
NOTIFICACIÓN. LA INFORMACIÓN CONTENIDA EN ESTA NOTIFICACIÓN DE
ARCHIVO REFLEJA LOS DATOS PRESENTES EN EL SISTEMA DE ASIGNACIÓN DE
PATENTES Y MARCAS REGISTRADAS. SI USTED ENCUENTRA ALGUN ERROR O
TIENE ALGUNA PREGUNTA CONCERNIENTE A ESTA NOTIFICACION, PUEDE
LLAMAR AL EMPLEADO CUYO NOMBRE APARECE EN ESTA NOTIFICACIÓN AL
NÚMERO 703-308-9723. POR FAVOR ENVIE LAS SOLICITUDES PARA
CORRECCIÓN A: OFICINA DE PATENTES Y MARCAS REGISTRADAS DE E.U,
CORREO:ASSIGNMENT SERVICES DIVISION, P.O. BOX 1450, ALEXANDRIA,
VA 22313.

FECHA DE GRABACION: 06/06/2005

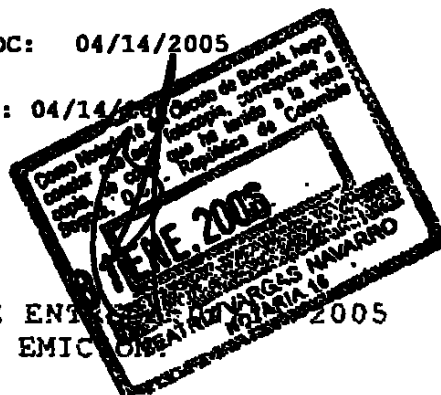
CINTA/CUADRO 01095/09307
NUMERO DE PAGINAS: 6

RESUMEN: ASIGNACION DE INTERÉS AL CESIONISTA (VER DOCUMENTO PARA
DETALLES)

CESIONISTA:
TRIBBLE, ERIC P.
CESIONISTA:
FREEMAN, TREVOR
, CESIONISTA:
MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMONT, WASHINGTON 96052

FECHA DOC: 04/14/2005

FECHA DOC: 04/14/2005



NUMERO DE SERIAL: 11107011
NUMERO DE PATENTE:

FECHA DE ENTREGA: 04/14/2005
FECHA DE EMISIÓN: 04/14/2005

TITULO: SISTEMA Y METODO PARA ESTABLECER QUE UN SERVIDOR Y UN
CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE

DIVISION DE ASIGNACIONES
OFICINA DE ARCHIVOS PUBLICOS

121

ASIGNACION DE PATENTE

Versión electrónica v1.1 06/06/2005
 Estilo de hoja versión v1.1 500034342

TIPOS DE SUMISIÓN: NUEVA ASIGNACIÓN

NATURALEZA DE LA ENTREGA: ASIGNACIÓN

DATOS DE LA PARTE QUE ENTREGA

Nombre	Fecha ejecución
Eric D Tribble	04/14/2005
Trevor W Freeman	04/14/2005

DATOS DE LA PARTE QUE RECIBE

Nombre:	Corporación Microsoft
Dirección:	One Microsoft Way
Ciudad	Redmont
Estado/pais:	WASHINGTON
C.P.:	98052

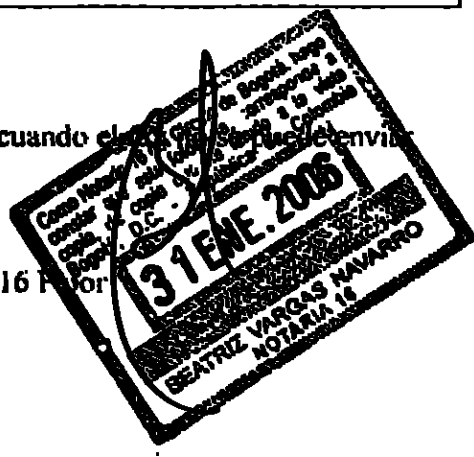
NÚMEROS DE PROPIEDAD total: 1

Tipo De Propiedad	Número
Solicitud Numero:	11107011

DATOS DE CORRESPONDENCIA

Fax: (314) 231-4342
 la correspondencia se enviará a través del correo de EU cuando el
 teléfono: 3142315400
 e-mail: uspatents@senniger.com
 nombre de correspondencia: Robert M. Bain
 Línea de Dirección 1 One Metropolitan Square, 16 Floor
 Línea de Dirección 2 Senniger Powers
 Línea de Dirección 4 St, MISSOURI 63102

Nombre del presentador Robert M. Bain
 Total anexos: 4
 Fuente = 00083383##pagina1.tif



122

Asignación de patente

Yo/nosotros, Eric D Tribble, Trevor W Freeman ("Cesionistas"), hemos inventado ("INVENTO") divulgado y/o reivindicado en la solicitud de patente llamada " SISTEMA Y METODO PARA DETERMINAR QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN CORREO COMPATIBLE Y SEGURO" ('solicitud'), que:

- ☒ Se archivará sin la patente de asignación ejecutada. Por medio de la presente, el cesionista autoriza, y solicita, al representante legal del cesionario, de SENNIGER POWERS, que están asociados con el número de cliente 000038779, para insertar aquí en paréntesis (U.S. No Serial. 11/107.011, archivado 04/15/2005)
No. serial de esta solicitud y fecha de entrega, si son conocidos;
☐ presentada el y se le dio el No. Serial:
☐ Se archiva en forma simultánea;

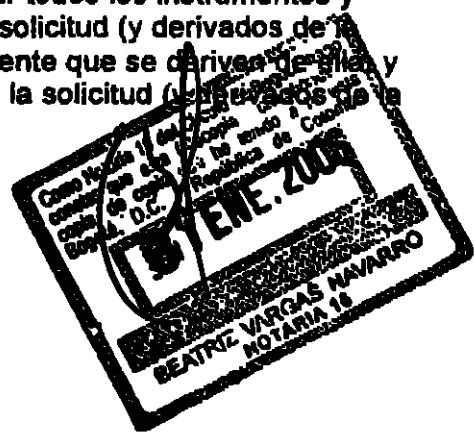
La corporación Microsoft, una corporación de Washington, en su propio nombre y el de sus sucesores y cesionarios, tiene derecho a, y está deseoso de adquirir la totalidad y exclusividad de los derechos, títulos e interés en el invento y la aplicación (y todas las demás aplicaciones de patentes que se deriven de esta, tales como aplicaciones de continuación, en y para los Estados Unidos y sus territorios, y todos los países extranjeros ("derivados de la solicitud");

En consideración buena y valiosa, en el recibo que el CESIONISTA reconoce por la presente, los CESIONISTA(S) venden, asignan y transfieren hacia el CESIONARIO, el derecho completo, título e interés en y dicho invento y la solicitud (y derivados de la solicitud);

El Cesionista se compromete a ejecutar todos los instrumentos y documentos requeridos para el procesamiento de la solicitud (y derivados de la solicitud), para el litigio en cuanto a las cartas de patente que se deriven de ella y con el propósito de proteger y perfeccionar el título a la solicitud (y derivados de la solicitud).

04/14/05
04/14/05

Eric D Tribble (Firma)
Trevor W Freeman (Firma)



Título: Sistema y Método para determinar que un Servidor y un Correspondiente tienen correo compatible y seguro
Clase Preliminar
713

124

LICENCIA PARA ENTREGA EXTRANJERA BAJO
Título 35, Código de los Estados Unidos, Sección 184
Título 37, Código de Reglamento Federal, 5.11 & 5.15

CONCEDIDA

Al solicitante se le ha concedido la licencia bajo 35 U.S.C. 184, si la frase "SI SE REQUIERE, LA LICENCIA DE ENTREGA EXTRANJERA SE CONCEDE" seguida de una fecha que aparece en este formato. Estas licencias se conceden para todas las solicitudes donde las condiciones que se requieren para una licencia se han cumplido, sin importar si la licencia se requiere o no tal como se expone en 37 CFR 5.15. El alcance y las limitaciones de estas licencias se exponen en 37 CFR 5.15(a) al menos de que una licencia anterior se haya remitido bajo 37 CFR 5.15(b). La licencia está sujeta a revocación con una notificación por escrito. La fecha que se indica en la fecha efectiva de la licencia, al menos de que una licencia anterior de alcance similar se haya concedido bajo 37 CFR 5.13 o 5.14.

El licenciado debe guardar esta licencia y la puede utilizar en cualquier momento en la fecha que se hace efectiva o luego al menos de que se revoque. Esta licencia se transfiere automáticamente a cualquier aplicación relacionada que se haya entregado bajo 37 CFR 1.53(d). Esta licencia no es retroactiva.

La concesión de una licencia no aminora la responsabilidad del licenciado para la seguridad del tema a tratar como lo impone cualquier contrato con el Gobierno o las prescripciones de leyes existentes relacionadas con el espionaje y la seguridad nacional o la exportación de datos técnicos. Los licenciados se deben informar sobre el reglamento vigente especialmente respecto a ciertos países, otras agencias, y particularmente la Oficina de Defensa de Controles de Comercio, departamento de estado (con respecto a Armas, Municiones e Implementos de Guerra (22 cfr 121-128)); la Oficina de Administración de Exportaciones, Departamento de Comercio (15 cfr 370.10(J)); la Oficina de Control de Activos, Departamento del Tesoro (31 CFR partes 500+) y el Departamento de Energía.

NO CONCEDIDA

Por el momento no se ha concedido la licencia bajo 35 U.S.C. 184, si la frase "SI SE REQUIERE, LA LICENCIA DE ENTREGA EXTRANJERA SE CONCEDE" NO APARECE en este formato. El solicitante puede todavía hacer una petición para una licencia bajo 37 CFR 5.15. La licencia se concede antes del vencimiento de seis meses a partir de la fecha entrega de los documentos. Si no se recibe una licencia antes del vencimiento de seis meses desde la fecha de entrega de esta solicitud y la licencia no ha recibido una notificación de una orden de secreto bajo 35 U.S.C. 181, el licenciado puede entregar la solicitud extranjera de acuerdo a 37 CFR 5.15(b).



125

125

SISTEMA Y METODO PARA ESTABLECER QUE UN SERVIDOR Y UN CORRESPONDIENTE TIENEN E-MAIL SEGURO Y COMPATIBLE

CAMPO TECNICO

[0001] Implementaciones del presente invento se relacionan con el campo de establecer una interconexión compatible entre dos dominios. En particular, implementaciones de este invento se relacionan con un sistema y método para revelar y descubrir servidores de correo con capacidades avanzadas.

ANTECEDENTES DEL INVENTO

[0002] Algunos sistemas anteriores intentaban identificar al potencial correspondiente comunicándose directamente. Sin embargo, estos sistemas se hacían vulnerables a atacantes cuando se comunicaban, y en particular, podían ser causa o ser vulnerables al SPAM y a ataques de negación de servicio.

[0003] De esta manera, se hace deseable un sistema que enfrente estas y otras desventajas identificando en forma discreta a un potencial correspondiente de tal manera que un vínculo seguro entre un servidor y el potencial correspondiente se pueda establecer.

RESUMEN DEL INVENTO

[0004] Implementaciones del invento incluyen un sistema de correo electrónico que ocasionalmente añade un encabezado adicional al mensaje que se envía a los dominios potenciales del correspondiente. Los datos en el encabezado adicional son un secreto que es específico al mensaje que se envía a un dominio correspondiente particular y una dirección de correo e-mail a la cual se pueden dirigir los mensajes administrativos de ese correspondiente al servidor. Si el correo en el dominio del correspondiente también se dirige a través de un servidor como el de esta

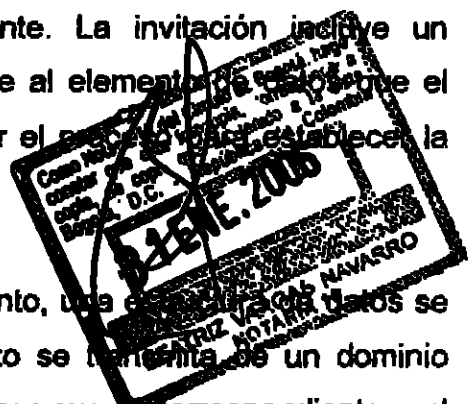


126

126

implementación, entonces detectara los encabezados adicionales y determinará que hay más servidores compatibles en el dominio que origina. Puede entonces dirigir el tráfico administrativo, tal como solicitudes para establecer una conexión segura, a la dirección administrativa contenida. Este mensaje administrativo también debe contener el secreto que le fue suministrado para ese dominio correspondiente. El aceptador para el correo administrativo en el dominio que origina puede entonces descartar cualquier correo que pretenda ser del dominio del correspondiente pero que no tiene el secreto asociado al dominio del correspondiente.

[0005] En una implementación, el invento incluye un método para determinar que un dominio correspondiente potencial tiene tecnología de e-mail compatible y segura para establecer un vínculo entre el dominio fuente y el dominio correspondiente. Un secreto de descubrimiento se trasmite del dominio fuente al dominio correspondiente. El Secreto de descubrimiento incluye un elemento de datos específico al dominio del correspondiente y una dirección del dominio fuente a la cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad entre el dominio fuente y el dominio correspondiente. El dominio fuente recibe a través de la dirección del dominio fuente una invitación del dominio correspondiente. La invitación incluye un elemento de datos o un elemento correspondiente al elemento de datos que el dominio correspondiente puede utilizar para iniciar el proceso de establecer la compatibilidad con el dominio correspondiente.



[0006] De acuerdo con un aspecto del invento, una invitación de datos se suministra para que un secreto de descubrimiento se transmita de un dominio fuente a un dominio correspondiente para establecer que el correspondiente y el dominio fuente tienen tecnologías de e-mail compatible y segura u otras tecnologías de e-mail o comunicaciones. El Secreto de descubrimiento incluye un mensaje; un encabezado que se relaciona con el mensaje; y un encabezado

127

adicional anexo al mensaje. El encabezado adicional incluye (1) un elemento de datos específico al dominio correspondiente e incluye una dirección del dominio fuente al cual se le permite al dominio correspondiente enviar un mensaje al dominio fuente para establecer que el dominio correspondiente y dominio fuente tienen tecnologías de e-mail seguras y compatibles, (2) un secreto de descubrimiento y (3) una fecha de vencimiento.

[0007] En otra forma, el inventó comprende un sistema para establecer que un correspondiente y un dominio fuente tienen tecnología de e-mail compatible y segura u otra tecnología de e-mail o comunicaciones. Un servidor dominio fuente transmite un secreto de descubrimiento al dominio del correspondiente. El secreto de descubrimiento incluye un elemento de datos específico al dominio del correspondiente y una dirección del dominio fuente a la cual al dominio del correspondiente se le permite enviar un mensaje para establecer que el correspondiente y el dominio fuente tienen tecnologías de e-mail compatibles y seguras. Un computador del dominio correspondiente recibe el secreto de descubrimiento incluido en el elemento de datos y la dirección del dominio fuente. El Computador del dominio correspondiente transmite una invitación del dominio del correspondiente a la dirección del dominio fuente. La invitación incluye en elemento de datos o un en elemento correspondiente al elemento de datos.

[0008] En forma alterna, el inventó puede comprender otros rasgos y aparatos varios.

[0009] Otros rasgos en parte serán aparentes y en parte serán obvios.



DESCRIPCIÓN BREVE DE LOS DIBUJOS

[0010] La figura 1 es un diagrama de bloque ejemplar de los servidores de entrada 1 y 2 con una mensajería segura entre ellos.

128

[0011] La figura 2 es un diagrama ejemplar que muestra el flujo de trabajo entre un servidor de dominio fuente y un correspondiente potencial (por ejemplo, un servidor de dominio correspondiente) de acuerdo con el invento.

[0012] La figura 3 es un diagrama de bloque ejemplar que muestra un administrador de mensajes seguro de acuerdo con el invento.

[0013] La figura 4 es un diagrama de flujo que muestra la operación de búsqueda de ruta de la administración de mensajes segura (SMM) de acuerdo con el invento.

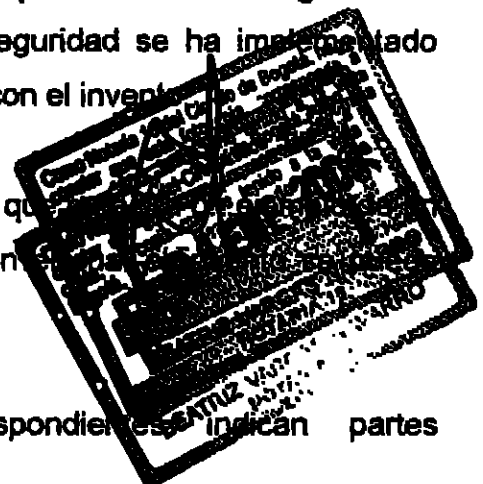
[0014] La figura 5 es un diagrama de flujo que muestra las operaciones de búsqueda de ruta de un trabajador SMM de acuerdo con el invento.

[0015] La figura 6 es un diagrama de bloque ejemplar que muestra un resumen del flujo de trabajo inter-organización entre un servidor (admin organizaciónA) y un correspondiente (admin organización B) de acuerdo con el invento.

[0016] La figura 7 es un diagrama de flujo que muestra un diagrama de estado luego de que una nueva asociación de seguridad se ha implementado entre un servidor y un correspondiente de acuerdo con el invento.

[0017] La figura 8 es un diagrama de bloque que muestra un ambiente de sistema de computación adecuado en el que se puede implementar.

[0018] Caracteres de referencia correspondientes indican partes correspondientes a través de todos los dibujos.

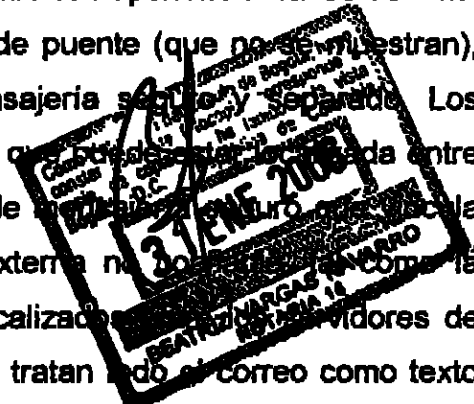


129

DESCRIPCIÓN DETALLADA DEL INVENTO

[0019] El invento se relaciona con un sistema y método para determinar que un correspondiente potencial tiene tecnología de e-mail compatible y segura para comenzar el proceso de establecer un vínculo entre el servidor y el correspondiente. En particular, el invento se relaciona con un sistema y método para iniciar el proceso de establecer un vínculo seguro para el despliegue de e-mail seguro. El invento le permite a un servidor determinar que un correspondiente potencial se puede establecer como un objetivo porque la tecnología de e-mail es compatible y segura. Como resultado, una vez se identifica al correspondiente potencial, el servidor puede intercambiar información de material clave con el correspondiente potencial para establecer un vínculo seguro.

[0020] El objetivo de la firma y codificación del dominio de acuerdo con el invento es suministrar un mecanismo de transporte independiente para intercambiar mensajes confidenciales y autenticados por el servidor entre los servidores. La figura 1 es un diagrama de bloque ejemplar de los servidores de entrada 1 y 2. Los servidores 1 y 2 tienen un vínculo de mensajería seguro entre ellos. El servidor puede estar separado por una firewall opcional a través del cual pueden estar conectados a servidores cabeza de puente (que no se muestran), que pueden ser parte de un sistema de mensajería seguro separado. Los servidores de entrada 1 y 2 forman una sub-red que puede estar separada entre una red interna confiable, tal como el sistema de mensajería seguro, y una red externa no confiable, tal como la Internet pública. Los firewalls también están localizados entre los servidores de entrada y la Internet. Los servidores de entrada tratan todo el correo como texto claro y codifican todo el correo puerta a puerta. Si los servidores de entrada y cabeza de puente no comparten las mismas llaves de codificación, el servidor de entrada no puede decodificar el correo codificado del servidor cabeza de puente.



130

[0021] Existe la necesidad para una administración de los datos autoritarios para todas las relaciones internas y externas. Opcionalmente, se implementa un modelo maestro único en vez de un modelo maestro múltiple porque es más sencillo y porque no tienen que resolver conflictos de réplicas. Las operaciones de administración segura de mensajes (SMM) son poco frecuentes y las demoras en las operaciones SMM no deben demorar la entrega, únicamente demoran la configuración de una nueva asociación segura. El tamaño de la base de datos es generalmente pequeño (por ejemplo, cientos de miles de records de unas pocas K; podría ascender a varios megabytes, pero probablemente no cientos de megabytes) entonces hay suficiente tiempo para reparar o cambiar hardware o hacer una restauración del sistema antes de que se pierda el servicio. En una implementación, operaciones con datos críticos se replican en otro servidor de entrada. Como no hay un punto único de administración, no todos los datos se replican y los datos replicados son únicamente de lectura.

[0022] Un servidor se pueden conectar con un número de dominios correspondientes para configurar vínculos de correo para un proyecto específico. Sin embargo, la coordinación de la administración de tal proyecto generalmente no escala. Para que la mensajería segura tenga un impacto, el correo seguro se habilita con la mayoría de los correspondientes de negocios de la organización. Esto requiere de la habilidad para descubrir que correspondientes tienen servidores de entrada instalados y tienen un flujo de correo organización-a-organización simple para determinar si hay negocios que establezcan un vínculo de correo seguro.

[0023] El invento permiten el descubrimiento de servidores de entrada instalados en la organización de un correspondiente de tal manera que se pueda establecer una conexión segura. Para facilitar el descubrimiento, el servidor indica (por ejemplo anuncia) su presencia con un correo saliente que tiene alguna indicación (o anuncio), al cual aquí se le llama un secreto de descubrimiento. Para

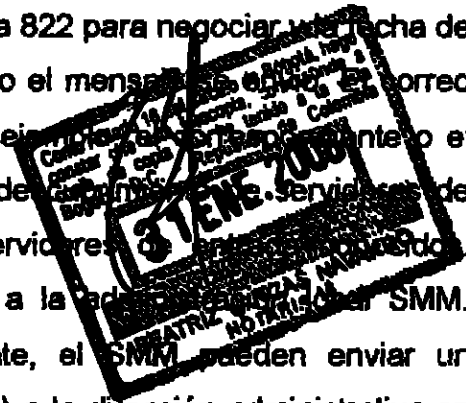


(31)

131

minimizar que el proceso del secreto de descubrimiento sea vulnerable a un ataque, el sistema y método del invento no utiliza una dirección codificada en duro en su secreto de descubrimiento. Sin embargo, se considera que en una implementación una dirección única se puede utilizar con el secreto de descubrimiento para que se incluya en cualquier e-mail para esa dirección. Como resultado, únicamente los mensajes de las partes que han visto el secreto de descubrimiento (que incluye el secreto de descubrimiento) pueden enviar a la dirección administrativa. Por lo tanto, en una implementación preferida, se utiliza una dirección única, y el secreto de descubrimiento se debe suministrar en todos los mensajes. En forma alterna, la dirección indicada es un nombre de casilla de correo aleatorio que puede rotar con un intervalo razonable, por ejemplo, semanalmente. Mientras que este enfoque aleatorio es una opción, es una implementación menos preferida. Para asegurar que la vulnerabilidad se minimiza, el secreto de descubrimiento está ligado al dominio que envía, por ejemplo, el dominio fuente, y al dominio al que le envía, por ejemplo el dominio correspondiente. En el evento de que el secreto de descubrimiento esté disponible para un tercer partido el único dominio que se afectaría es el dominio cuya dirección de invitación estaba comprometida.

[0024] De una manera, el secreto descubrimiento puede ser un encabezado 822 que contiene la dirección efímera 822 para negociar una fecha de vencimiento de la dirección 822 relativa a cuando el mensaje es enviado. El correo entrante lo escanea el servidor que recibe (por ejemplo, el servidor de correo entrante o el servidor del correspondiente) para secretos de descubrimiento. Se comparan los secretos de entrada y los compara contra una lista de servicios de entrada conocidos. Cualquier adición a esa lista se les comunica a la administración del SMM. Cuando se descubre un nuevo correspondiente, el SMM pueden enviar un mensaje de pruebas (por ejemplo, una invitación) a la dirección administrativa en el otro SMM para ofrecer un turno en la firma del dominio y la codificación u otro servicio. Cuando se recibe una invitación de otro administrador SMM, si el

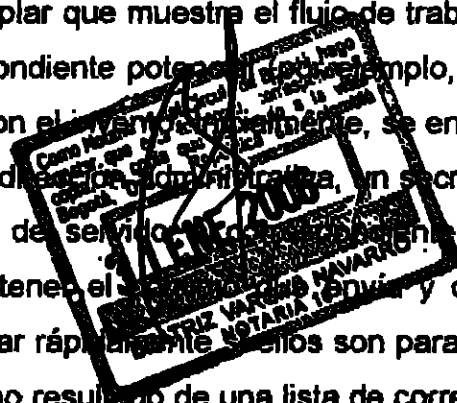


132

132

mensaje se puede verificar bajo la política de confiabilidad existente entonces el SMM local puede invocar una política para automáticamente aceptar la invitación. En forma alterna, el administrador SMM pueden requerir de una aprobación manual antes de aceptar la invitación. Tan pronto se recibe la aceptación de la invitación por el servidor, si el mensaje es intrínsecamente verificable, entonces el SMM que recibe podría invocar una política para automáticamente iniciar el uso de la firma y codificación del dominio. Primero, envía un mensaje de prueba codificado con un número aleatorio único, y espera un reconocimiento (que incluye al número aleatorio único) para asegurarse que el correo seguro se puede decodificar al otro lado. Nótese que la invitación y mensaje de aceptación están firmados con una llave autoritaria del SMM, mientras que en el mensaje de prueba y el reconocimiento están firmados con una llave de firmas (que es un hijo de la llave autoritaria). El proceso rutinario que firma y codifica el correo sólo tiene la autoridad de firmar con la llave de firmas (por seguridad). Por lo tanto, el correo de prueba y el reconocimiento también verifican que un correo seguro va a funcionar con la llave de firma, no únicamente con la llave autoritaria. La configuración de un nuevo dominio seguro es un proceso no sincronizado y no se utiliza para datos reales hasta que el vínculo se confirme operacional con la recepción del reconocimiento del mensaje de prueba antes de hacer anuncios administrativos.

[0025] La figura 2 es un diagrama ejemplar que muestra el flujo de trabajo entre un servidor dominio fuente y un correspondiente potencial (por ejemplo, un computador de dominio objetivo) de acuerdo con el invento. Inicialmente, se envía un secreto de descubrimiento que incluye una dirección de correo, un secreto de descubrimiento y una fecha de vencimiento de servicio. El secreto de descubrimiento también debe contener el dominio de correo y que recibe, de tal manera que uno puede determinar rápidamente si ellos son para su dominio (porque ellos pueden haber salido como resultado de una lista de correo). Cuando el correspondiente reconoce el secreto de descubrimiento, el correspondiente envía una invitación de vuelta al servidor a la dirección

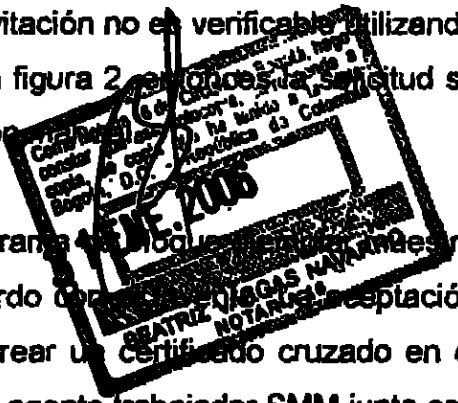


133

133

administrativa que era parte del secreto de descubrimiento. En una implementación, sólo responde al descubrimiento si también ha enviado correo "al" dominio. Por lo tanto un spammer no puede inducir al dominio fuente a que lo invite (porque usted, para comenzar, nunca les envió correo). La invitación del correspondiente incluye una dirección administrativa del correspondiente, una fecha de vencimiento, un certificado y el secreto de descubrimiento y otra información (por ejemplo, el Id del flujo de trabajo, información del contacto, dominios de envío y recibo, etc.). En respuesta, el servidor envía una aceptación a la dirección administrativa del correspondiente de la dirección administrativa del servidor e incluye en la aceptación la fecha de vencimiento, el certificado, el secreto de descubrimiento y una firma. Esta es una opción administrativa, aunque la política por defecto puede incluir una respuesta automática. En una implementación, se puede restringir a un funcionamiento manual, o únicamente responder si la certificación del que invita cumple cierta política de confiabilidad. Luego de que se recibe la aceptación, el correspondiente envía un mensaje de prueba al servidor y el mensaje de prueba lo reconoce el servidor para establecer la conexión que pone a la asociación en estado de alerta. Puede involucrar una acción administrativa automática para avanzar del estado de alerta al estado activo. Puede involucrar un paso adicional para pasar del estado activo (que utiliza la relación segura pero no la cree) al estado autenticado (que cree en la identidad que asegura el otro partido). Si el mensaje de invitación no es verificable utilizando la política de confiabilidad como se mostró en la figura 2, la solicitud se puede poner en cola en espera de una aprobación.

[0026] En referencia a la figura 3, un diagrama de flujo ilustra un administrador de mensajes seguros de acuerdo con la aceptación de la invitación por el correspondiente puede crear un certificado cruzado en el agente administrativo SMM que luego lo envía al agente trabajador SMM junto con el certificado de codificación. (El certificado cruzado se crea generalmente para asociaciones autenticadas (para poder definir lo que ellas pueden autenticar). Las

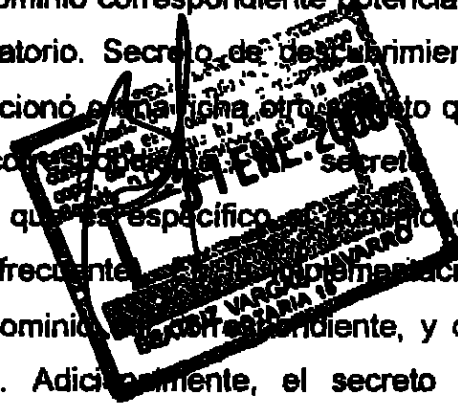


134

134

asociaciones activas lo tienen todo excepto el certificado cruzado. El certificado cruzado restringe el conjunto de nombres que la nueva confianza permite y la restricción de la comunicación con el dominio del servidor de entrada. En este punto, se distribuye a todos los trabajadores los certificados e información en cuanto a la nueva asociación. También se puede distribuir la llave de la sesión de la administración SMM a todos los trabajadores SMM de tal manera que todos los trabajadores utilicen la misma llave para reducir el tamaño de la memoria cache. Para permitir el escalamiento, la llave privada de de codificación correspondiente para el certificado de codificación debe estar disponible en todo el Internet de frente a los servidores de entrada para permitir la decodificación del correo entrante. Esto se genera en un solo sitio, por ejemplo, el agente administrador, y se distribuye a todos los trabajadores del servidor. Una vez que se establece una relación de confianza, se debe mantener. Por ejemplo, el certificado original se puede retener y una solicitud de renovación enviarse al otro SMM antes de que el certificado venza. El certificado hijo de firma y codificación también se puede actualizar frecuentemente.

[0027] Vez en la perspectiva del servidor, el método de acuerdo con el invento comienza el proceso para establecer un vínculo entre un dominio fuente y un dominio correspondiente. Inicialmente, un servidores de dominio fuente transmite un secreto de descubrimiento a un dominio correspondiente potencial a través de un mensaje aleatorio o pseudo aleatorio. Secreto de descubrimiento incluye un elemento de datos tal como se mencionó anteriormente, otro elemento que se asigna específicamente al dominio correspondiente. Secreto de descubrimiento incluye un secreto compartido que es específico al dominio del correspondiente (y posiblemente al dominio frecuente). La implementación preferida, es una porción de la semilla, del dominio correspondiente, y del dominio fuente (en algún orden específico). Adicionalmente, el secreto de descubrimiento incluye una dirección en el dominio fuente al cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad



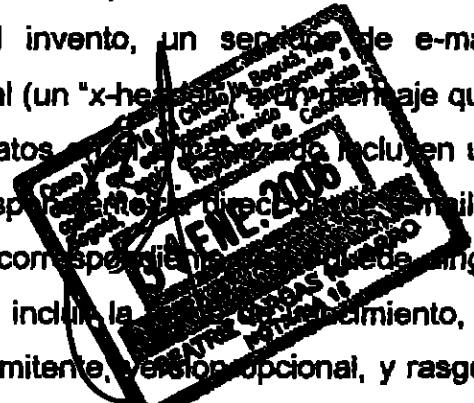
135

135

entre el servidor del dominio fuente y el computador objetivo. El servidor del dominio fuente recibe una invitación del dominio correspondiente, invitación que está dirigida a la dirección del dominio fuente que se había suministrado previamente. La invitación incluye un elemento de datos en el secreto de descubrimiento o un elemento correspondiente al elemento de datos en el secreto de descubrimiento. Esto permite que el servidor del dominio fuente inicie un proceso para establecer la compatibilidad entre el servidor del dominio correspondiente y el servidor del dominio fuente tan pronto recibe el servidor del dominio fuente una invitación del servidor del dominio correspondiente. Como se anotó en la figura 2, el servidor del dominio fuente transmite al servidor del dominio correspondiente una aceptación para establecer la compatibilidad entre los dos.

[0028] En una implementación, el dominio fuente transmite en forma selectiva el secreto de descubrimiento a dominios correspondientes de donde el dominio fuente ha enviado el mensaje. Forma alterna o adicionalmente, el dominio fuente puede enviar un secreto de descubrimiento a dominios correspondientes que sean identificado anteriormente.

[0029] En una implementación, el secreto de descubrimiento puede estar anexo al mensaje que se envió específicamente para llevar el secreto de descubrimiento. En una implementación del invento, un servidor de e-mail ocasionalmente añade un encabezado adicional (un "x-header") a un mensaje que se va a distribuir a otro dominio e-mail. Los datos en el encabezado incluyen un secreto que es específico al dominio del correspondiente al cual el mensaje administrativo del dominio correspondiente puede dirigirse de vuelta al servidor de e-mail, como también incluir la dirección de descubrimiento, el dominio del correspondiente, el dominio del remitente, versión opcional, y rasgos opcionales. Si el correo en el dominio del correspondiente también se dirige a través de un servidor que incrementa este invento, entonces podrá detectar el



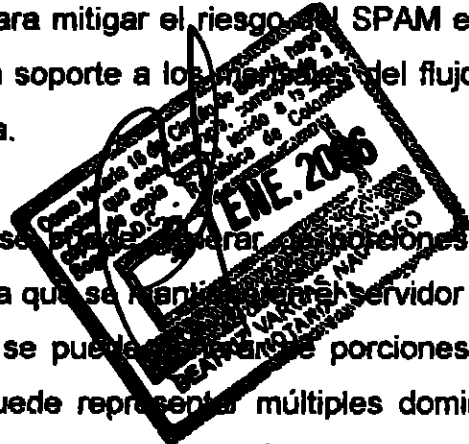
136

136

encabezado adicional y determinar que puede haber un servidor compatible en el dominio que origina. El dominio del correspondiente entonces dirige el tráfico administrativo tales como, la petición para establecer una conexión segura, a la dirección de e-mail administrativa contenida. El controlador de correo para el correo administrativo en el dominio que origina puede entonces descartar cualquier correo que pretende ser del dominio del correspondiente pero que no contiene el secreto correspondiente al dominio del correspondiente. Aunque esto no suministra una seguridad absoluta de que el correo administrativo que se recibe es del dominio que origina, si minimiza la vulnerabilidad al SPAM en la dirección administrativa y asegura que un atacante que puede ver los e-mails para el dominio correspondiente únicamente puede intentar imitar la dirección administrativa del dominio del correspondiente a diferencia de cualquier dominio.

[0030] En una implementación, el invento se incrementa utilizando un encabezado, llamado un secreto de descubrimiento (llamado a veces también una mención), que se anexa aun e-mail saliente del dominio fuente. Este secreto de descubrimiento revela la disponibilidad de una función especial en el servidor de correo que origina el e-mail saliente mientras evita la necesidad para generar mensajes adicionales y posiblemente no deseables. Como se anotó anteriormente, la dirección de e-mail administrativa estarían incluidas en la mención y habría una secreto por-dominio para mitigar el riesgo de SPAM en la dirección de e-mail administrativa. Esto daría soporte a los mensajes del flujo de trabajo en la dirección de e-mail administrativa.

[0031] El secreto de descubrimiento se puede generar a partir de porciones del dominio correspondiente y una semilla secreta que se mantiene en el servidor que origina. Secreto de descubrimiento también se puede generar a partir de porciones del dominio fuente, porque términos servidor puede representar múltiples dominios fuente. Una implementación podría potencialmente tener una "fuente" para todos los dominios en el servidor fuente. Esto permite en una semilla única se comparta



137

137

a través de múltiples servidores, de tal manera que cada servidor va a generar términos secreto de descubrimiento único a cualquier dominio correspondiente. Cuando un mensaje administrativo se recibe en el servidor que origina (porque está dirigido a la dirección administrativa incluida en la mención), el secreto de descubrimiento suministrado en el mensaje administrativo es chequeado por el servidor que origina. Para chequear el secreto de descubrimiento, el servidor de e-mail pueden generar (o almacenar) un secreto de descubrimiento para el dominio que envió el mensaje administrativo utilizando la semilla interna actual. Si el secreto de descubrimiento generado ese mismo que el secreto en el mensaje administrativo, entonces ese mensaje tiene el secreto de descubrimiento correcto y pasa a través a su destino apropiado para la negociación de mensajes. La negociación de los mensajes se pasa entre dominios. Si el secreto de descubrimiento no concuerda, entonces el mismo proceso se aplica a secretos de descubrimiento anteriores (hasta un número limitado). Sin ninguna de las semillas actuales válidas se puede utilizar para generar el secreto de descubrimiento que concuerda con el secreto de descubrimiento en el mensaje entrante, entonces el mensaje no se considera válido y se descarta o se rechaza, y no se pasa a su destino eventual para los mensajes administrativos. Esto previene ataques de SPAM no autorizados contra el receptor del mensaje administrativo, que puede no ser capaces de hacer frente a volúmenes grandes de e-mail. Adicionalmente, para prevenir ataques de negación de servicio de un dominio que ha recibido un secreto de descubrimiento válido, el proceso de verificación permite que el servidor mantenga la pista de cuantos mensajes pasaron recientemente al destino administrativo de un dominio particular o utilizando un secreto de descubrimiento particular. Cuando ese número excede un límite predefinido, se rechaza permitida con mensajes administrativos adicionales utilizar ese secreto de descubrimiento se descartan o se rechazan.



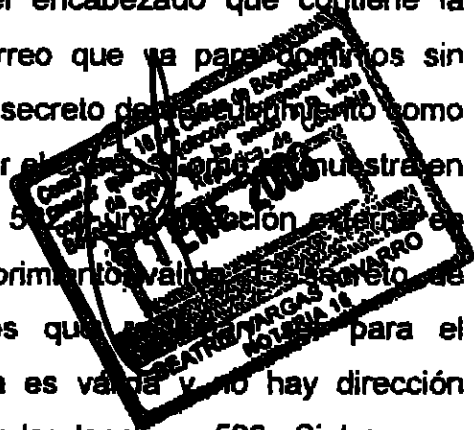
[0032] La figura 4 3 de drama de flujo se muestra las operaciones de búsqueda de ruta administrativa del SMM de acuerdo con el invento. La

138

138

verificación de firma y la decodificación debe suceder antes que el proceso anti-SPAM por qué la salida de la verificación es necesaria para fijar las banderas de propiedad del mensaje utilizadas por el agente anti-SPAM. La verificación de firmas de suceder después del estado de bloque y otras funciones a nivel del protocolo de dirección o IP. por lo tanto, el proceso comienza recibiendo mensajes en la dirección del dominio fuente al cual dominio correspondiente se le permite enviar un mensaje en 402. Si se determina en 404 el secreto de descubrimiento no es válido para el dominio que envía, el mensaje se abandona en 406 y la búsqueda de ruta termina. Si el secreto de descubrimiento es válido, el proceso procede a 408 para determinar si el dominio tiene una cantidad máxima o una tasa que se haya excedido. Si el máximo será excedido, el mensaje se descarta en 406; de lo contrario, si la firma es válidas en 410 el mensaje se envía al agente administrador local. Sin embargo, la verificación de firma no necesariamente sucede en el trabajador; generalmente sucede en el SMM.

[0033] La figura 5 es un diagrama del flujo que demuestra las operaciones de búsqueda de ruta de un trabajador SMM de acuerdo con el invento. El SMM es el Administrador de Mensajería Segura; los trabajadores son los servidores que el SMM administra/controla y que hacen el procesamiento del tráfico de correo. La firma y codificación del SMM es generalmente la última función. Cada mensaje que va a un dominio con una asociación de mensaje segura está firmado y codificado. Este componente también inserta el encabezado que contiene la dirección efímera actual SMM para todo el correo que va para dominios sin relación de seguridad. El trabajador le añadirá un secreto de descubrimiento como sea apropiado, pero no lo hace sólo para asegurar el correo. Como se muestra en la figura 5, el dominio busca una firma válida en 502. Si la dirección externa es 504 luego de encontrar un secreto de descubrimiento válido. El secreto de descubrimiento sólo se chequea en mensajes que van para el administrador, no en correo normal. si la firma es válida y no hay dirección externa, el mensaje se envía al agente trabajador local en 506. Si hay una



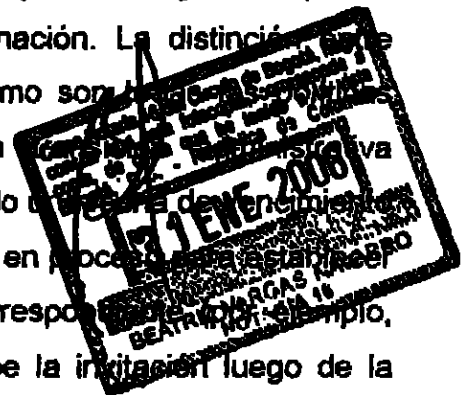
137

139

dirección externa se envía a ella. Si el mensaje aparece con el dominio asegurado, una firma inválida se trata en forma idéntica a como si la firma no estuviera presente. La fuente del mensaje no se autentica.

[0034] En una implementación, el flujo de trabajo inter-organización como se muestra en las figuras 6 esta implementado entre organizaciones administrativas que representan el ciclo de vida de la relación. Otros giros son posibles: las llaves tienen certificaciones asociadas a ellas. Las certificaciones pueden o para con más frecuencia que las llaves. Hay firmas, codificación, certificaciones de autoridad y llaves, todas las cuales rotan en forma independiente. También, puede haber más tarde secuencias de reconocimiento/pruebas. El flujo de trabajo lo ejecuta el agente administrativo SMM y puede tener un intercambio para lograr una rotación (la rotación es el término para la actualización a una nueva llave o certificado). La figura siguiente es un diagrama de estado que muestra la nueva asociación de seguridad. Este diagrama únicamente considera los casos positivos y terminales. No incluye otros aspectos tales como la re-transmisión de mensajes antes del límite de re-transmisión.

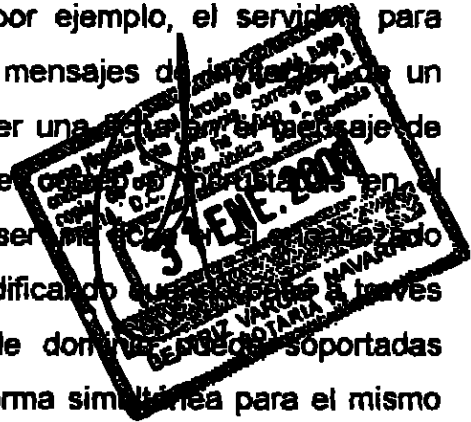
[0035] Otros rasgos opcionales del invento incluye en lo siguiente que se puede implementar en forma separada o en combinación. La distinción entre asociación activa y autenticada es "opcional", así como son los rasgos de asociación activa y autenticada que se pueden aplicar para hacer una asociación automática. El secreto de descubrimiento puede incluir una fecha de vencimiento y entre el caso de servidor del dominio fuente no inicia en proceso de descubrimiento la compatibilidad con el computador del dominio correspondiente (por ejemplo, servidor) cuando el servidor del dominio fuente recibe la invitación luego de la fecha de vencimiento de tal manera que el secreto compartido no se expone más y más sobre el tiempo. El elemento de datos puede ser uno de los siguientes: un secreto por dominio que incluye un número aleatorio o pseudo aleatorio para cada



140

140

computador del dominio correspondiente (por ejemplo, el servidor), un secreto generado con una porción del computador del dominio correspondiente (por ejemplo, el servidor) y una semilla de secreto que se utiliza para generar secretos por dominio para más de un dominio; y un secreto por dominio generado codificando el computador del dominio correspondiente (por ejemplo, el servidor) y una fecha de vencimiento del secreto. El elemento de datos puede incluir un secreto en cuyo caso el servidor del dominio fuente puede recordar el secreto o puede verificar el secreto recibido del computador del dominio del correspondiente (por ejemplo, el servidor) re computando y luego comparando el secreto actual para el computador del dominio correspondiente (por ejemplo, servidor) con el secreto incluido en el secreto de descubrimiento. El elemento de datos se puede seleccionar de una pluralidad de secretos múltiples que son válidos en tiempos que se sobreponen para cada computador del dominio del correspondiente (por ejemplo, el servidor) de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación de un computador de el dominio correspondiente (por ejemplo, el servidor) a la dirección administrativa del dominio que origina. Se puede imponer un límite en el número de mensajes que se le pasan a la dirección del servidor del dominio fuente con un elemento de datos particular del tal manera que la negación de ataques al servicio utilizando un elemento de datos correcto se mitiga. El servidor del dominio fuente puede incluir la habilidad de sobrepasar los requerimientos para un elemento de datos para un computador del dominio correspondiente dado (por ejemplo, el servidor) para permitir la autorización fuera-de-banda de enviar mensajes de invitación a un dominio particular. El elemento de datos puede ser una fecha actual para el mensaje de secreto de descubrimiento en un encabezado del mensaje o se inserta en el cuerpo del mensaje o el elemento de datos puede ser una fecha de vencimiento del correo y el cuerpo del mensaje permanece codificado que se descubre a través de un servidor de correo. El servidor fuente de dominio puede soportadas múltiples secretos de descubrimiento válidos en forma simultánea para el mismo dominio y verificar en mensaje de invitación de su-dominios del computadora del

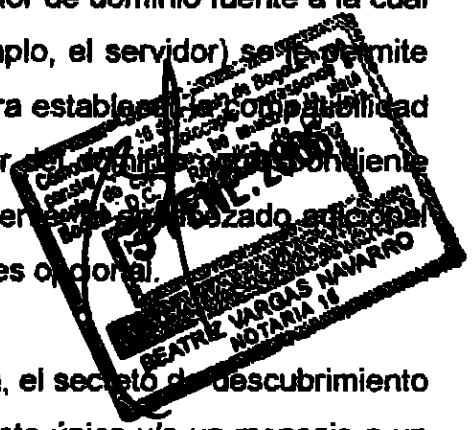


141

141

dominio correspondiente (por ejemplo, el servidor) verificando el secreto de descubrimiento entrante contra secreto de descubrimiento para el computador del dominio correspondiente (por ejemplo, el servidor). El elemento de datos puede ser un secreto de descubrimiento e incluir información de la versión para el servidor dominio fuente e incluir las funciones que el servidor dominio fuente soporta.

[0036] En una implementación el invento comprende una estructura de datos para qué secreto de descubrimiento se transmita de servidor dominio fuente al computadora del dominio correspondiente (por ejemplo, el servidor). Como se anotó anteriormente, este secreto de descubrimiento se utiliza para establecer la compatibilidad entre servidor de dominio fuente y en computadora de dominio correspondiente (por ejemplo, el servidor). En forma alterna, se podría utilizar para otros propósitos entre los dos dominios. Por ejemplo, se podría utilizar para qué se pusieran de acuerdo en enviar un formato propietario TNEF en niveles de texto o HTML que no tendría nada que ver con codificación o seguridad. La estructura de datos incluye un mensaje y su encabezado usual relacionado con el mensaje. Adicionalmente, la estructura de datos incluye un encabezado adicional anexo al mensaje y un encabezado de mensaje que incluye elementos de datos específico al computador del dominio correspondiente (por ejemplo, el servidor). el encabezado también incluye una dirección del servidor de dominio fuente a la cual computadora del dominio correspondiente (por ejemplo, el servidor) se le permite enviar un mensaje al servidor del dominio fuente para establecer la compatibilidad entre el servidor del dominio fuente y el computador del dominio correspondiente (por ejemplo, el servidor). Como se anotó anteriormente, el encabezado adicional debe incluir una fecha de vencimiento, aunque esto es opcional.



[0037] Adicionalmente como en forma alterna, el secreto de descubrimiento puede ser un mensaje con un dominio correspondiente único y/o un mensaje a un dominio correspondiente que es un operador. El mensaje único al dominio

142

142

correspondiente puede ser para cada llave se puede enviar con una determinación pasada en el tiempo (por ejemplo, un mensaje por hora). Por ejemplo, la acción del usuario puede ser un NDR o un recibo. En particular, la decisión de enviar un mensaje separado o de anexarlo a uno que se envía es independiente de si usted lo hace en cada mensaje u ocasionalmente. Un caso cruzado es esperar a un mensaje que tiene un receptor en un dominio único (el dominio correspondiente) en vez de anexar el secreto de descubrimiento a un mensaje que tiene receptores en dominios múltiples. En una implementación, el mensaje se divide de tal manera que las copias que va al receptor en el dominio correspondiente tiene el secreto de descubrimiento para ese dominio.

[0038] La figura 8 muestra un ejemplo de un dispositivo de cómputo de propósito general en la forma del computador 130. en una implementación del invento, un computador tal como el computador 130 es adecuado para utilizarse en otras figuras que se muestran y se describen acá. El computador 130 tiene uno más procesadores o unidades procesadoras 132 y una memoria de sistema 134. En la implementación que se muestra, un bus de sistema 136 acopla los componentes varios del sistema incluyendo a la memoria del sistema 134 al procesador 132. El bus 136 representa uno o más de varias tipos de estructuras de bus, incluyendo un bus de memoria o controlador de memoria, un bus periférico, puerto de gráficos acelerados, y un procesador o bus local utilizando cualquier tipo de arquitectura de bus. como ejemplo, y no como limitante estas arquitecturas incluyen el bus Industry Standard Architecture (ISA), el bus Micro Channel Architecture (MCA), el bus Enhanced ISA (EISA), el bus local Video Electronics Standards Association (VESA), y el bus Peripheral Component Interconnect (PCI) también conocido como el bus 1322.

[0039] El computador 130 tiene típicamente una o más unidades de medios legibles por computador. Los medios legibles por computador, que pueden incluir tanto a los medios volátiles como no-volátiles, removibles y no-removibles, pueden

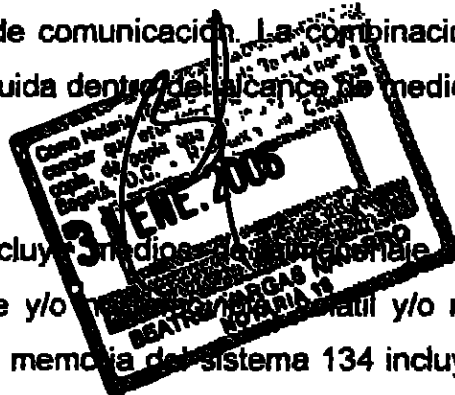


(4)

143

ser cualquier medio disponible que el computador 130 pueda acceder. Como ejemplo y no como limitante, el medio legible por computador comprende los medios de almacenaje en computador y medios de comunicación. Los medios de almacenaje en computadoras incluyen los volátiles y no-volátiles, removibles y no-removibles incrementados en cualquier tecnología o método para almacenar información tal como instrucciones legibles por computador, estructuras de datos, módulos de programa u otros datos, por ejemplo, los medios de almacenaje en computador incluyen RAM, ROM, EEPROM, memorias flash y otras tecnologías de memoria, CD-ROM, discos versátiles digitales(DVD) u otros medios de almacenaje en discos ópticos, cassettes magnéticos, cintas magnéticas, almacenaje en discos magnéticos u otros dispositivos de almacenaje magnético, u otros medios que se puedan utilizar para almacenar la información deseada y que el computador 130 pueda acceder. Los medios de comunicación típicamente constan de instrucciones legibles por computador, estructuras de datos, módulos de programas, u otros datos en señal de datos modulada tales como ondas transportadoras u otros medios de transporte mecánico e incluyen cualquier medio para distribuir información. Aquellos diestros en el arte están familiarizados con la señal de datos modulada, que tienen una o más de sus características fijas o alteradas de tal manera que codifican la información en la señal. Los medios alambrados, tales como redes alambradas o conexiones alambradas en forma directa, y medios inalámbricos, tales como acústicos, RF, infrarrojos, y otros medios inalámbricos son ejemplos de medios de comunicación. La combinación de cualquiera de los anteriores también está incluida dentro del alcance de los medios legibles por computador.

[0040] La memoria del sistema 134 incluye medios de almacenamiento en computador en la forma de memoria removible y/o memoria no removible, volátil y/o no volátil. en la implementación que se muestra, la memoria del sistema 134 incluye la memoria de sólo lectura (Roma) 138 y la memoria de acceso aleatorio (RAM) 140. Un sistema básico de entrada/salida 142 (BIOS), que contienen las rutinas



144

144

básicas que ayudan en la transferencia de la información entre los elementos dentro del computador 130, tales como durante el inicio, se almacenan en forma típicas en la ROM 138. La RAM 140 contiene típicamente datos y/o módulos de programa que son accesibles inmediatamente a y/o están operados en el presente por la unidad procesadora 132. Como ejemplo, y no como limitante, la figura 8 muestra un sistema operativo 144, programas de aplicación 146, y otros módulos de programa 148, y datos de programa 150.

[0041] El computador 130 también puede incluir otros medios de almacenaje en computador removibles/no removibles, volátiles/no volátiles. Por ejemplo, la figura 8 muestra un drive de disco duro 154 que lee y escribe a medios magnéticos no removibles, no volátiles. La figura 8 también muestra un drive de disco magnético 156 que lee y escribe a el disco magnético removible, no volátil 158, y un drive de disco óptico 160 que lee y escribe a el disco óptico no volátil removible 162 tal como un CD ROM u otros medios ópticos. Otros medios de almacenaje en computador removibles/no removibles, volátiles/no volátiles que se pueden utilizar en el ambiente operativo ejemplar incluyen, pero no están limitados a, cassettes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cintas de videos digital, RAM de estado sólido, ROM de estado sólido y cosas parecidas. El drive de disco duro 154, y el drive de disco magnético 156 y el drive de disco óptico 160 están típicamente conectados al bus del sistema 136 a través de una interfase de memoria, tal como la interfase 166.

[0042] Los drives y otros dispositivos de almacenaje en computador asociados y que se muestran en la figura 8, suministran el almacenaje de instrucciones legibles por computador, estructuras de datos, módulos de programas y otros datos para el computador 130. En la figura 8, por ejemplo, el drive de disco duro 154 se muestra almacenando el sistema operativo 170, programas de aplicación 172, otros



145

145

módulos de programa 174, y datos de programa 176. Nótese que estos componentes pueden ser iguales a o diferentes al sistema operativo 144, programas de aplicación 146, y otros módulos de programa 148, y datos de programa 150. El sistema operativo 170, los programas de aplicación 172, otros módulos de programa 174, y datos de programa 176 tienen distintos números para mostrar que, por lo menos, son copias distintas.

[0043] Un usuario puede entrar comandos e información en el computador 130 a través de dispositivos de entrada o dispositivos de selección en la interfase del usuario, tal como un teclado 180 y dispositivos de señalamiento 182 (por ejemplo ratón, trackball, un bolígrafo o una almohadilla táctil). Otros dispositivos de entrada (que no se muestran) pueden incluir un micrófono, un joystick, un panel de juegos, un disco satelital, un escáner, o cosas parecidas. Estos y otros dispositivos de entrada están conectados a la unidad procesadora 132 a través de la interfase de entrada 184 que esta acoplada al bus 136, pero puede estar conectada por otras interfases u estructuras de bus, tales como puertos paralelos, puertos de juego, o el Bus Serial Universal (USB). Un monitor 188 otros tipos de dispositivos de visualización también se conectan al bus del sistema 136 a través de una interfase, tal como la interfase de videos 190. Adicionalmente al monitor 188, el computador frecuentemente incluye otros dispositivos de salida periféricos (que no se muestran) tal como una impresora o parlantes, que se pueden conectar a través de una interfase periférica (que no se muestra).

[0044] El computador 130 pueden operarse en una o más redes utilizando conexiones lógicas a uno o más computadores, como es el computador remoto 194. El computador remoto 194 puede ser un computador personal, un servidor, un buscador de rutas, un Pc de mesa, el dispositivo de un colega u otro nodo de red común, y típicamente incluye muchos o todos de los elementos descritos anteriormente relativos al computador 130. Las conexiones lógicas que se muestran en la figura 8 incluye en una red de área local (LAN) 196



146

y una red de área amplia (WAN) 198, pero también puede incluir otras redes. La LAN 136 y/o la WAN 138 pueden ser redes alámbricas, redes inalámbricas, o una combinación. Estos ambientes de redes son comunes en oficinas, negocios, redes amplias de computadores, Internet es, y redes globales de computadores, por ejemplo, Internet.

[0045] Cuando se utilizan en un ambiente de redes de área local, el computador 130 estará conectado a la LAN 196 a través de una interfase de redes o adaptador 186. Cuando y se utilizan en un ambiente en un tender redes de área local, el computador 130 incluye típicamente una modem 178 u otros medios para establecer comunicación con la WAN 198, tal como Internet. El modem 178, que puede ser interno o externo, está conectado al pos del sistema 136 a través de una interfase de usuario de entrada 184, u otro mecanismo apropiado. En un ambiente de redes, los módulos de programa que se muestran relativos al computador 130, o porciones de, se pueden almacenar en un dispositivo de almacenaje de memoria remoto (que no se muestran). Como ejemplo, y no como limitante, la figura 8 muestra programas de aplicación remotos 192 como residiendo en el dispositivo de memoria. Las conexiones de redes que se muestran son ejemplares y otros medios para establecer un vínculo de comunicación entre computadores se puede utilizar.

[0046] Generalmente, el procesador de datos 132 del computador 130 es programable por medio de instrucciones almacenadas en varios de los componentes de almacenaje legibles por computador. Los programas y el sistema operativo están típicamente distribuidos, por ejemplo, en discos floppy o CD-ROMs. De ahí, se instalan o se cargan en la memoria secundaria del computador. En el momento de ejecución, se cargan por lo menos parcialmente en la memoria electrónica primaria del computador. El invento descrito acá incluye estos y otros tipos de medios de almacenaje legibles por computador cuando tales medios contienen instrucciones o programas para

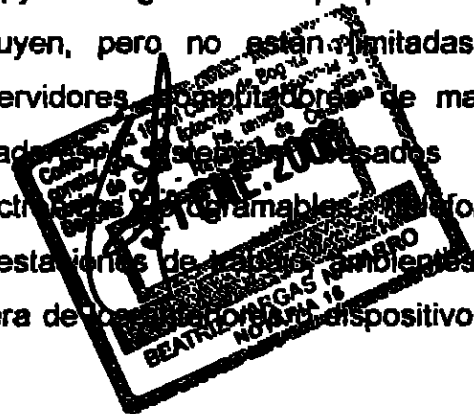


147

implementar los pasos descritos más abajo en conjunto con un microprocesador u otros procesadores de datos. El invento también incluye al computador en sí mismo cuando está programado de acuerdo a los métodos y técnicas descritos acá.

[0047] Con un propósito ilustrativo, los programas y otros componentes de programas ejecutables, tales como el sistema operativo, se muestran en bloques discretos. Se reconoce sin embargo, que estos programas y componentes residen en varios momentos en distintos componentes de almacenaje del computador, y son ejecutados por el procesador(es) del computador.

[0048] Aunque descrito en relación al ambiente de sistema de computación ejemplar, incluyendo el computador 130, el invento es funcional con muchos otros ambientes de sistema de computación de propósito general o especial y con otras configuraciones. El ambiente de sistema de computación no tiene la intención de sugerir ningún tipo de limitación en cuanto al alcance o funcionalidad del invento. Aún más, el ambiente de sistema de computación no se debe interpretar como teniendo ningún tipo de dependencia o requerimiento relacionado con uno o más combinaciones de los componentes ilustrados en el ambiente operativo ejemplar. Ejemplos de sistemas de cómputo, ambientes, y/o configuraciones que pueden ser adecuadas para uso con el invento incluyen, pero no están limitadas a, computadores personales, computadores servidores, computadores de mano, laptops, sistemas con multi procesadores, sistemas basados en microprocesadores, cajas, productos electrónicos programables, teléfonos móviles, PCs de red, mini- computadores, estaciones de trabajo, ambientes de cómputo distribuidos que incluyen cualesquiera de los dispositivos, y demás.



[0049] El invento se puede describir en el contexto general de instrucciones ejecutables por computador, tales como módulos de programa, ejecutados por uno

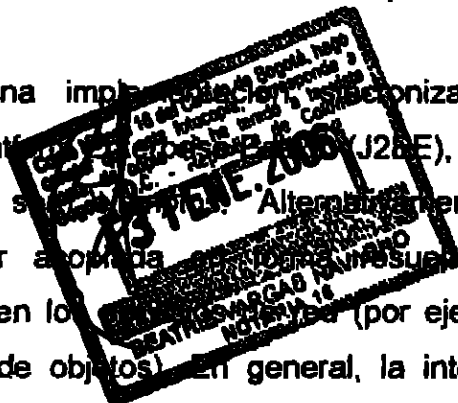
148

148

o más computadores o dispositivos. Generalmente, los módulos de programa incluyen, pero no están limitados a, rutinas, programas, objetos, componentes, y estructuras de datos que ejecutan tareas particulares o implementan tipos de datos abstractos particulares. El invento también se puede practicar en un ambiente de cómputo distribuido donde las tareas las ejecuta un dispositivo de procesamiento remoto que está ligado a través de una red de comunicaciones. En un ambiente de cómputo distribuido, los módulos de programa pueden estar localizados tanto en los medios de almacenaje locales como remotos incluyendo los dispositivos de almacenaje de la memoria.

[0050] Una interfase en el contexto de la arquitectura de software incluye módulos de software, componentes, porciones de código, y otras secuencias de instrucciones ejecutables por computador. La interfase incluye, por ejemplo, un primer módulo que accede a un segundo módulo para ejecutar tareas de cómputo en beneficio del primer módulo. El primero y segundo módulos incluyen, en un ejemplo, interfaces de aplicaciones de programación (APIs) tales como las suministradas por el sistema operativo, interfaces de modelo de componentes de objetos (COM) por ejemplo, Para aplicaciones de comunicación colega-colega), y el intercambio de meta datos en interfases con formato de lenguaje de marcación extensible (XML)(por ejemplo, para comunicación entre servicios de red).

[0051] La interfase puede ser una implementación sincronizada y fuertemente acoplada tal como la Java 2 Platform (J2SE), COM, o la distribuida COM (DCOM), estos sistemas. Alternativamente o adicionalmente, la interfase puede estar acoplada en formas sueltas, en implementaciones no sincronizadas como en los sistemas de objetos (por ejemplo, utilizando el protocolo de acceso simple de objetos). En general, la interfase incluye cualquier combinación de las siguientes características: acoplada fuertemente, acoplada en formas sueltas, sincronizadas, y no sincronizadas. Aún



149

149

más, la interfase se puede conformar a un protocolo estándar, un protocolo con propietario, o una combinación de protocolos estándar y con propietario.

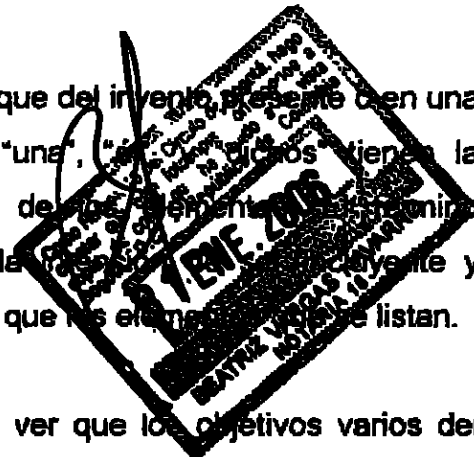
[0052] La interfase descrita hasta puede ser toda parte de una interfase única o puede estar implementada en interfases separadas o una combinación de ellas. Las interfases pueden ejecutarse localmente o en forma remota para suministrar la funcionalidad. Aún más, la interfase puede incluir más o menos funcionalidades que las ilustradas o descritas acá.

[0053] Cuando está en operación, el computador 130 funciona ya sea como el servidor de dominio fuente o el computador de dominio correspondiente (que puede ser una servidor) para ejecutar las instrucciones ejecutables por computador como se anotó anteriormente, y como se ilustró en las figuras 2-7.

[0054] El orden de ejecución de los métodos ilustrados y descritos acá no es esencial, al menos de que se especifique. Esto es, dos elementos y métodos se pueden ejecutar en cualquier orden, al menos de que se especifique lo contrario, y que los métodos pueden incluir más o menos elementos que aquellos que se presentan acá. Por ejemplo, se considera que ejecutar un elemento particular antes, contemporáneo con, o luego de otro elemento está dentro del alcance del invento

[0055] Cuando se introduce un elemento que del invento presente o en una de sus implementaciones, los artículos "un", "una", "uno", "una", "unos", "unas", "un", "una", "uno", "una", "unos", "unas", "comprende", "incluye", y "constará de" tiene la intención de significar que hay uno o más de los elementos que se mencionan. "comprende", "incluye", y "constará de" tiene la intención de significar que puede haber elementos adicionales que los elementos que se listan.

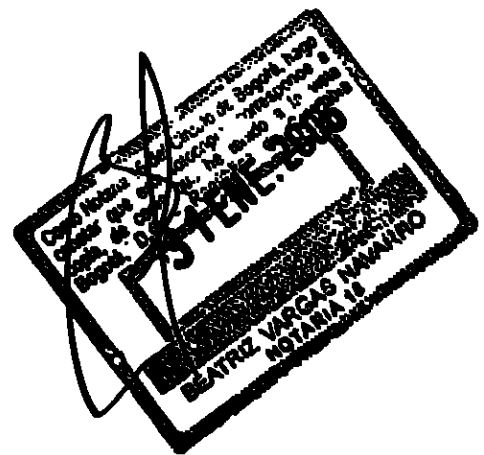
[0056] En vista de lo anterior, se puede ver que los objetivos varios del invento se logran y otros resultados ventajosos se alcanzan.



150

150

[0057] Como se pueden hacer varios cambios en la construcción anterior, productos, y métodos, sin alejarse del alcance del invento, se pretende que todo el material contenido en la descripción anterior y que se muestra en los dibujos que la acompañan se debe interpretar como ilustrativa y no limitante en ningún sentido.



151

151

Lo que se reivindica es:

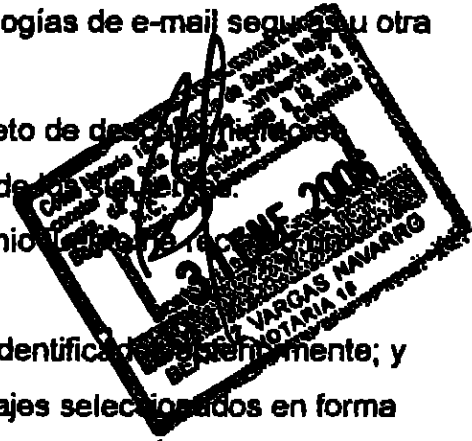
1. Un método para determinar que un dominio correspondiente potencial tiene tecnología de e-mail segura y compatible para establecer un vínculo entre el dominio fuente y un dominio correspondiente y que comprende:

Transmitir un secreto de descubrimiento de un dominio fuente a un dominio correspondiente donde el secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y donde el secreto de descubrimiento incluye una dirección del dominio fuente al cual el dominio correspondiente se le permite enviar un mensaje para establecer la compatibilidad entre el dominio fuente y el dominio correspondiente; y
Recibir del dominio fuente a través de la dirección del dominio fuente una invitación del dominio correspondiente donde la invitación incluye el elemento de datos o un elemento correspondiente al elemento de datos que el dominio correspondiente puede utilizar para iniciar un proceso para establecer la compatibilidad con el dominio correspondiente.

2. El método de la reivindicación 1 comprende además transmitir una aceptación del dominio fuente al dominio correspondiente para establecer que el correspondiente y el dominio fuente tienen tecnologías de e-mail seguras u otra tecnología de e-mail o de comunicaciones.

3. El método de la reivindicación 1 donde el secreto de descubrimiento se transmite en forma selectiva a por lo menos uno de los siguientes:
Dominios correspondientes de donde el dominio fuente recibe mensajes;
Dominios correspondientes específicamente identificados previamente; y
Dominios correspondientes a través de mensajes seleccionados en forma aleatoria.

4. El método de la reivindicación 1 donde el secreto de descubrimiento es un mensaje que se genera en respuesta a una acción de usuario; donde el secreto de



152

152

descubrimiento es un mensaje con un dominio correspondiente único; donde el secreto de descubrimiento es un mensaje a un dominio correspondiente que es un operador; donde el secreto de descubrimiento es un mensaje único a un dominio correspondiente para cada llave; o donde el secreto de descubrimiento es un mensaje enviado con una determinación basada en el tiempo.

5. El método de la reivindicación 1 donde el secreto de descubrimiento comprende un encabezado adicional que incluye el elemento de datos y la dirección del dominio fuente.

6. El método de la reivindicación 1 donde el secreto de descubrimiento comprende unas fechas de vencimiento y donde el dominio fuente no establece que los dominios correspondientes y fuente tienen tecnologías de e-mail segura y compatible cuando el dominio fuente recibe la invitación luego de la fecha de vencimiento.

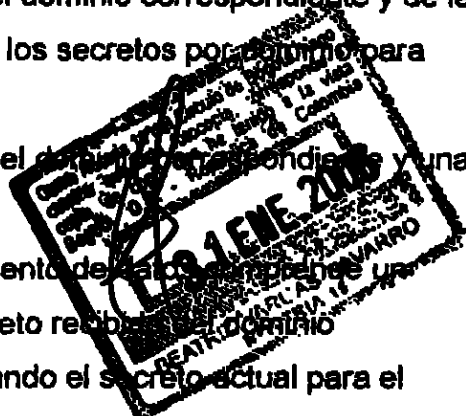
7. El método de la reivindicación 1 donde el elemento de datos es por lo menos uno de los siguientes:

un secreto por dominio que incluye un número aleatorio o pseudo aleatorio para cada dominio correspondiente;

un secreto generado a través de porciones del dominio correspondiente y de la semilla de secreto que se utilizó para generar los secretos por dominio para más de un dominio; y

un secreto por dominio generado codificando el dominio correspondiente y una fecha de vencimiento del secreto.

8. El método de la reivindicación 1 donde el elemento de datos comprende un secreto y donde el dominio fuente verifica el secreto recibido del dominio correspondiente re-computando y luego comparando el secreto actual para el dominio correspondiente con el secreto incluido en el secreto de descubrimiento a través del cual el dominio fuente únicamente correspondió con el dominio correspondiente potencial que suministró el secreto de tal manera que ataques de negación de servicio del dominio correspondiente se mitigan.



153

153

9. El método de la reivindicación 1 donde el elemento de datos se selecciona de una pluralidad de secretos múltiples simultáneos y válidos para cada dominio correspondiente de tal manera que hay una pluralidad de secretos válidos que se pueden utilizar para la comunicación de un dominio correspondiente a la dirección administrativa del dominio que origina.

10. El método de la reivindicación 1 comprende además la imposición de un límite en el número de mensajes que se pasan a la dirección del dominio fuente con un elemento de datos particular mediante el cual se mitigan los ataques de negación de servicio utilizando elementos de datos correcto.

11. El método de la reivindicación 1 comprende además incluir la habilidad de sobrepasar los requerimientos para un elemento de datos para un dominio correspondiente dado para permitir la autorización fuera de banda y enviar un mensaje de invitación de un dominio particular.

12. El método de la reivindicación 1 donde el elemento de datos es una ficha en el mensaje de secreto de descubrimiento en el encabezado de un correo o incrustado en el cuerpo del mensaje o donde el elemento de datos es una ficha en un encabezado de correo y el cuerpo del mensaje permanece codificado cuando pasa a través de servidor de correos.

13. El método de la reivindicación 1 comprende además el sorteo de fichas simultáneas válidas para el mismo dominio y la verificación de los mensajes de invitación de sub-dominios del dominio correspondiente contra la ficha de entrada contra fichas para el dominio correspondiente.

14. El método de la reivindicación 1 donde el elemento de datos incluye una versión para el dominio fuente e incluyendo en la mención funciones que el dominio fuente soporta.

15. Una estructura de datos para que un secreto de descubrimiento se trasmita de un dominio fuente a un dominio correspondiente para establecer que el dominio fuente y el dominio correspondiente tienen tecnologías de email segura y compatible y que comprende:



154

155

Una mención que comprende además incluye en la mención la información de versión para el dominio fuente y incluye en la mención funciones apoyadas por el dominio fuente.

17. Un sistema para establecer que los dominios correspondiente y fuente tienen tecnologías de email segura y compatible, y que comprende:

Un servidor dominio fuente transmitiendo un secreto de descubrimiento al dominio correspondiente donde el secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y donde el secreto de descubrimiento incluye una dirección del dominio fuente a la cual se le permite al dominio correspondiente enviar un mensaje para establecer que el correspondiente y el dominio fuente tienen tecnologías y de email segura y compatible; y

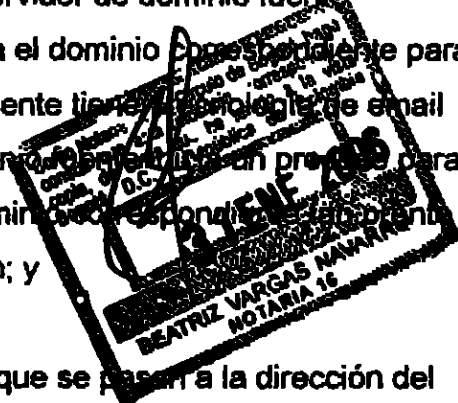
un computador del dominio correspondiente recibiendo e incluyendo el elemento de datos y la dirección del dominio fuente a donde el computador dominio correspondiente le transmite una invitación del dominio correspondiente a la dirección del dominio fuente donde la invitación incluye el elemento de datos o un elemento correspondiente al elemento de datos.

18. El sistema de la reivindicación 17 donde el servidor de dominio fuente transmite una aceptación del dominio fuente para el dominio correspondiente para establecer que los dominios fuente y correspondiente tienen tecnologías de email segura y compatible y donde el servidor del dominio fuente transmite un protocolo para establecer un vínculo con un computador del dominio correspondiente, el cual recibe de servidor del dominio fuente la invitación; y

Comprende además uno de los siguientes:

Imponer un límite en el número de mensajes que se pasan a la dirección del dominio fuente con un elemento de datos particular mediante el cual la negación de los ataques de servicio utilizando un elemento de datos correcto se mitigan;

Sobrepasar los requerimientos para un elemento de datos para un dominio correspondiente dado para permitir autorización fuera de banda para enviar



156

156

mensajes de invitación de un dominio particular y dar soporte a múltiples fichas válidas para el mismo dominio y verificar los mensajes de invitación de subdominios del dominio correspondiente verificando el secreto de descubrimiento entrante contra los secretos de descubrimiento para el dominio correspondiente.

19. El sistema de la reivindicación 17 donde el secreto de descubrimiento transmitido por el servicio del dominio fuente comprende por lo menos uno de los siguientes:

Un secreto de descubrimiento selectivo transmitido al dominio correspondiente de donde el dominio fuente ha recibido un mensaje;

Un secreto de descubrimiento transmitido en forma selectiva al dominio correspondiente identificado específicamente por adelantado o ser designado en forma aleatoria del dominio correspondiente;

Un mensaje que se genera en respuesta a una acción de usuario;

Un mensaje con un dominio correspondiente único;

Un mensaje a un dominio correspondiente que es la dirección de una operadora de servidor;

Un mensaje único al dominio correspondiente para cada llave;

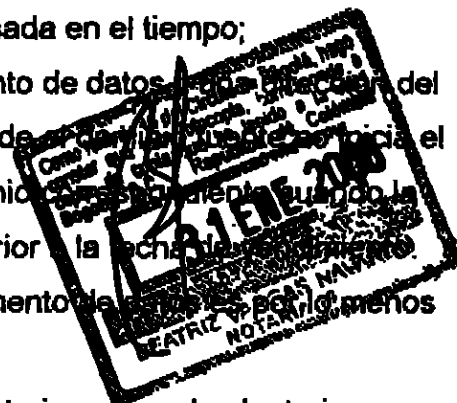
Un mensaje enviado con una determinación basada en el tiempo;

Un encabezado adicional que incluye un elemento de datos de la fecha de inicio del dominio fuente; y una fecha de vencimiento donde el elemento de datos de la fecha de inicio del dominio fuente es posterior a la fecha de vencimiento.

20. El sistema de la reivindicación 17 donde el elemento de datos de la fecha de inicio del dominio fuente es posterior a la fecha de vencimiento.

Un secreto por dominio que incluye un número aleatorio o pseudo aleatorio para cada dominio correspondiente,

Un secreto generado con porciones del dominio correspondiente y una semilla de secreto que se utiliza para generar el secreto por dominio para más de un dominio;

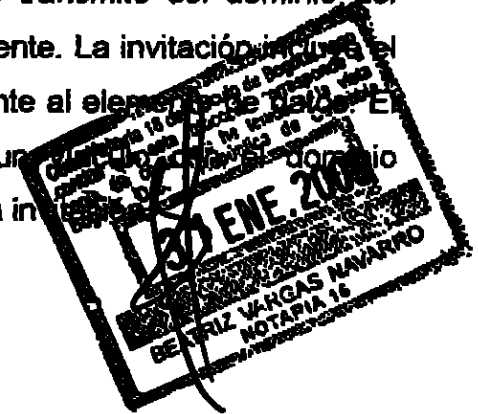


157

158

RESUMEN

Un secreto de descubrimiento se transmite de un dominio fuente a un dominio correspondiente. El secreto de descubrimiento incluye un elemento de datos específico al dominio correspondiente y punto el secreto de descubrimiento incluye una dirección del dominio fuente a la cual se permite al dominio correspondiente en días un mensaje para determinar que un correspondiente potencial en tienen tecnologías de e-mail segura incompatible para establecer un vínculo entre el dominio fuente y el dominio correspondiente. El secreto de descubrimiento no reside en dominio correspondiente incluyendo la recepción del elemento de datos y la dirección del dominio fuente. Una invitación se transmite del dominio del dominio correspondiente al la dirección del dominio fuente. La invitación incluye el elemento de datos o elemento de datos correspondiente al elemento de datos. El dominio fuente inicia un proceso para establecer un vínculo entre el dominio correspondiente tan pronto recibe del dominio fuente la invitación.



159



Industria y Comercio
SUPERINTENDENCIA

ADMINISTRACIÓN Y CONTROL
Radicación: 06010319 00000000 Folio: 159
Fecha (AMD): 2006-02-05 12:45:19
Trámite: 1. REGISTRO 2. AL PRESENTAR
Dependencia: 2000 DIVISION DE NUEVAS CREACIONES

159

Delegatura de Propiedad Industrial
División de Nuevas Creaciones

**REQUISITOS NECESARIOS PARA PRESENTACIÓN Y AGILIZACIÓN DEL
TRAMITE**

	USUARIO	RADICADOR
PATENTE DE INVENCION () MODELO DE UTILIDAD ()	()	()
Indicación de que se solicita la concesión de una patente.	()	()
-Datos de identificación del solicitante o de la persona que se presenta la solicitud	()	()
-Descripción de la invención	()	()
Dibujos de ser estos pertinentes	()	()
Comprobante de Pago de las tasas establecidas.	()	()
COMPLETA () INCOMPLETA ()	()	()

DISEÑO INDUSTRIAL ()

-Indicación de que se solicita el registro de Diseño Industrial	()	()
-Datos de identificación del solicitante o de la persona que se presenta la solicitud	()	()
Representación gráfica y fotográfica del Diseño Industrial o muestra del Material que incorpora el diseño	()	()
Comprobante de Pago de las tasas establecidas.	()	()
COMPLETA () INCOMPLETA ()	()	()

ESQUEMA DE TRAZADO ()

-Indicación de que se solicita el registro de Diseño Industrial	()	()
Datos de identificación del solicitante o de la persona que se presenta la solicitud	()	()
Representación gráfica del Esquema Trazado	()	()
Comprobante de Pago de las tasas establecidas	()	()
COMPLETA () INCOMPLETA ()	()	()

Firma Responsable

Fecha

PROTOCOLO

Expediente 06 - 10919

**SUPERINDUSTRIA Y COMERCIO
SISTEMA DE REGISTRO**

MANTENIMIENTO DE PROTOCOLOS

Numero : 18089

Fecha : 04/08/1995

Conferido: MICROSOFT CORPORATION

Pais : US ESTADOS UNIDOS DE AMERICA

Ciudad : 234 REDMOND, WASHINGTON

Represent: S Sustituir: S Desistir: S

No. Radicacion : 95 34920 Clase: 0 Seav: 0 Seac: 0

scncla	Codigo	Ctr	Nombre
1	77	A	CARDENAS NAVAS DARIO
2	3853		CARDENAS CABALLERO EDUARDO
3	5048		CARDENAS MARTINEZ BERNARDO

Encontrados (1/1) registro(s)

**Al contestar favor indique el número de
radicación consignado en el sticker**

**Sede Centro: Carrera 13 No. 27-00 Pisos 2, 5, 7 y 10
Commutador: 3 820840 Fax: 3 505220
Sede CAN: Tr. 40A No. 38-50 3153265 al 69
Fax: 3 505220. Línea 9800-910 165
Web: www.sic.gov.co e-mail: info@sic.gov.co
Bogotá D.C. - Colombia**

167
161

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Bogotá,
2020

Doctor(a)
CARDENAS NAVAS DARIO
Apoderado(a) y/o Representante de
MICROSOFT CORPORATION

REFERENCIA	Radicación No. 6 10919
	Trámite 2
	Evento 1
	Actuación 430
	Oficio No. 2113

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, se le comunica que:

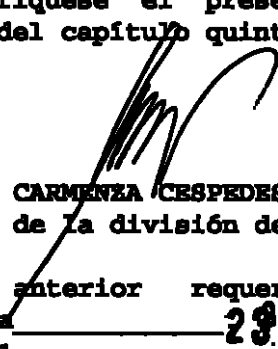
1. Debe allegar copia del documento en que consta la cesión del derecho a la patente otorgado por el(los) inventor(s) al(los) solicitante(s) o a su(s) causante(s) (art. 26-k, Dec 486/2000).

2. Los folios 126 a 159 se tomaran como solicitud nacional.

3. Para efectos de la publicación en la gaceta se recomienda allegar el extracto diligenciado.

En cumplimiento del artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos (2) meses siguientes ala fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.


ALIX CARMENZA CRESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 23 FEB. 2000
adpai

Se recuerda al interesado que debe presentar, dentro de los dieciséis meses siguientes contados a partir de la fecha de presentación de la solicitud cuya prioridad se invoca, copia de la misma certificada por la autoridad que la expidió y, en los casos en que haya lugar, la traducción simple del capítulo

Continúa en la página siguiente...

162/63

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Radicación No.: 6 10919

reivindicatorio. El incumplimiento de éste plazo, acarreará la pérdida de la prioridad invocada.