SEGURIDAD DE PROTOCOLO DE INTERNET: ESTADO DEL ARTE

ABSTRACT

IPSec is a united protocol of security which adding encrypted and authentication to communications IP. While the encrypted can avoid a not authorized user as typically known as a hacker to read a message, the authenticated can avoid the attacks to a site, originated from externa! not desired or even places from within of the own net of the site.

Sorne of the most relevant works about the conceptual and operational area of this research and the theories underlying these themes are being developed and then forming a state of art in constant evolution.

KEYWORDS

lpv6, IPSec, Security in networks

PALABRAS CLAVES

lpv6, lpsec, seguridad en redes

RESUMEN

IPSec es un conjunto de protocolos de seguridad que permite agregar encriptado y autenticación a las comunicaciones IP. Mientras el encriptado puede evitar que un usuario no autorizado como típicamente un hacker pueda leer un mensaje, el autenticado puede evitar los ataques a un sitio originados de sitios externos no deseados o hasta de dentro de la propia red del sitio.

Algunos de los trabajos más relevantes relacionados con el área conceptual y operacional de esta investigación y las teorías subyacentes a estos son las temáticas que se desarrollan a continuación y que conforman un estado del arte en permanente evolución.

INTRODUCCIÓN

El estado del arte es una de las primeras etapas que debe desarrollarse dentro de una investigación, puesto que su elaboración, que consiste en "ir tras las huellas" del tema que se pretende investigar,permite determinar cómo ha sido tratado el tema, cómo se encuentra en el momento de realizar la propuesta de investigación y cuáles son las tendencias [1] [2].

A Internet [3] de forma recurrente se le atribuye el hecho de ser un medio de comunicación inseguro. Este es un tema con muchas aristas y que debe ser examinado en cada una de sus partes. [4]

Sin embargo, el problema de seguridad en el nivel de red sigue sin ser tenido en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados y basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o dando la posibilidad de escudriñar (o desviar) la información a intrusos.[S]

Como respuesta surgen mecanismos de barrera como los cortafuegos, pero los protocolos siguen sin incorporar medidas específicas de seguridad. Pero esto es sólo una parte del problema. La seguridad integral [6] comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas criptográficas [7] que están sujetas a diferentes normativas de exportación y uso en determinados países, lo que hace complicado su uso generalizado en un medio que se tiene por libre (en cuanto a la naturaleza de la información intercambiada y su formato)y homogéneo (en cuanto al tipo de protocolos/aplicaciones empleados).[8]

DESARROLLO

La seguridad es una de las grandes ventajas que presenta 1Pv6 (Internet Protocol Version 6). El nuevo protocolo de comunicación incluye, de forma obligatoria e intrínseca en su núcleo, la especificación de seguridad IPSec [9].

IPv6 recoge a través de la experiencia de 1Pv4, tanto lo bueno como lo malo, y lo mejora. En el caso de la seguridad, el nuevo protocolo utiliza también IPSec como lo hace 1Pv4, pero con la diferencia de que en este deja de ser algo opcional para pasar a ser obligatorio. Con 1Pv6 todo el tráfico de la red va a ser autenticado, vamos a saber quién es el origen, quién el destino, realizando un mejor y más exhaustivo seguimiento de la información y su envío.

IPV6

IPv6 es una actualización del Protocolo de Internet, el cual es clave para el funcionamiento de la Red. Un aspecto muy importante desde que se inició el diseño de 1Pv6 fue el reconocimiento de que tendría que coexistir en la red con IPv4 durante un largo período de tiempo. [1O]

Esto es debido a que ya existen millones de dispositivos, aplicaciones y servicios, los cuales no pueden ser desconectados ni tan siquiera por un momento. Internet ha llegado a ser una infraestructura crítica y no hay modo alguno de pararla, ni tan siquiera por una noche, realizar una actualización y tener 1Pv6 funcionando en toda la Red.

Es también fácil entender que aún cuando fuéramos capaces de hacerlo así, todavía habría dispositivos que no podrían ser actualizados para soportar 1Pv6, por ejemplo en aquellos casos en los cuales el fabricante ha desaparecido y posiblemente no se tiene el acceso al código existente en su interior para actualizarlo nosotros mismos.

Por este motivo, IPv6 ha sido diseñado junto a un conjunto de mecanismos de transición, los cuales permiten la coexistencia de ambos protocolos, IPv4 eIPv6, tanto tiempo como sea preciso como se muestra en la figura 1, lo cual dependerá de innumerables factores, escenarios de red, sectores de negocio, etc. Además, estos mecanismos de transición facilitan la integración de IPv6 en la red Internet existente hoy con IPv4. [11]

Figura 1.Calendario de Transición [12]

Técnicamente hablando, se puede decir que IPv6 está maduro: Hoy es posible hacer con IPv6 todo lo que se puede hacer con IPv4 y mucho más. Claramente se puede prever un mayor desarrollo de nuevos servicios y aplicaciones gracias a la implantación de IPv6. IPv6 traerá de nuevo la innovación a Internet, la innovación que el despliegue de NAT con IPv4 llegó a detener.

Un par de años atrás, muchas redes tan sólo soportaban IPv4 y muy pocas IPv6. Hoy la situación ha cambiado radicalmente y más y más redes comerciales ya soportan IPv6. En un futuro próximo, veremos toda la red Internet soportando tanto IPv4 como IPv6, e incluso llegaremos al punto en que algunas redes dejarán de soportar lpv4.

Por supuesto, la comunicación extremo-a-extremo con IPv4 seguirá siendo posible, porque se utilizarán mecanismos de transición, pero en sentido inverso al que se hace ahora cuando deseamos utilizar IPv6 en redes que solo soportan IPv4.

Estado del arte

Diversas instituciones públicas y privadas están fuertemente vinculadas con el compromiso de impulsar el despliegue de IPv6, incluyendo la Comisión Europea, el Departamento de Defensa Norteamericano, etc.

A nivel internacional, fue México el pionero en la investigación y realización de pruebas con el protocolo IPv6, seguido de países como España, Chile, Argentina, Uruguay, Brasil, entre otros. En Colombia apenas se está comenzando a incursionar en la temática de IPv6: UniNet, una Red Universitaria, sin ánimo de lucro cuyo fin es integrar servicios proporcionados a través de Internet, para ofrecerlos a comunidades virtuales, creadas por personas y organizaciones, lidera un proyecto de implementación de redes basadas en este protocolo, del cual ya forman parte la Universidad de Magdalena y la del Cauca, mencionando también a la Universidad de Pamplona con la implementación del túnel con la Universidad Nacional Autónoma de México.

Fuentes Primarias -Trabajos Relacionados - Internacional

UNAM
Entre las instituciones latinoamericanas están:
Instituto de Informática de la Universidad Austral de Chile y las universidades UBio-Bio, UFRO y UDLA; RETINA, y las universidades LINTI-UNLP, UBA de Argentina; EAFIT y las universidades UdeA, UniCauca y UniPamplona

REDIRIS
Demostrador de movilidad 1Pv6 para redes móviles de 4G.[15]
Catálogo de requisitos de prueba para la transición de 1Pv6. Olvera, C. [16]
Nuevo modelo de punto de intercambio de tráfico en 1Pv6. García, J.A. [17]

Desarrollo de ambientes interactivos tridimensionales para la educación [18]

Estado del Arte de lpv6 Módulo lpplan V6. [19]

Diseño y simulación de la implementación de tecnologías y procedimientos de transición del protocolo IPv6 en INTRANETS usando un IPv6 test bed. [20]

Modelo de migración de lpv4 a lpv6 para la red del sistema ITESM (21]

Presenta el trabajo de investigación, configuración y transición del nuevo protocolo que regirá la Internet en un futuro cercano, este es 1Pv6 (Protocolo Internet versión 6). A través del presente trabajo se pretenden mostrar básicamente dos cosas: por una parte el proceso de transición recomendado que debe seguir el ITESM para migrar a 1Pv6 y por un lado, ver todo lo referente a configuración de equipos Linux (22], encaminadores Cisco y la configuración clientes Windows (23] para formar parte de una red LAN y WAN sobre 1Pv6.[24]

Impactos de implementación del protocolo ipv6 para un proveedor de servicios de telecomunicaciones un enfoque comparativo entre el desempeño de ipv6 e ipv4. (25]

El enfoque del presente trabajo es el de evaluar de manera cuantitativa el desempeño de 1Pv6 y compararlo con el desempeño de 1Pv4, con objeto de establecer un marco de referencia para el análisis de su posible introducción.

Limitando el alcance de este enfoque y de manera muy concreta, la investigación que prosigue plantea la posibilidad para un proveedor de servicios de telecomunicaciones, de implementar el protocolo 1Pv6 e intenta proveer la información suficiente para que el ISP pueda determinar los impactos que dicha implementación pudiera representar dentro de su infraestructura, tecnologías, procedimientos, etc.

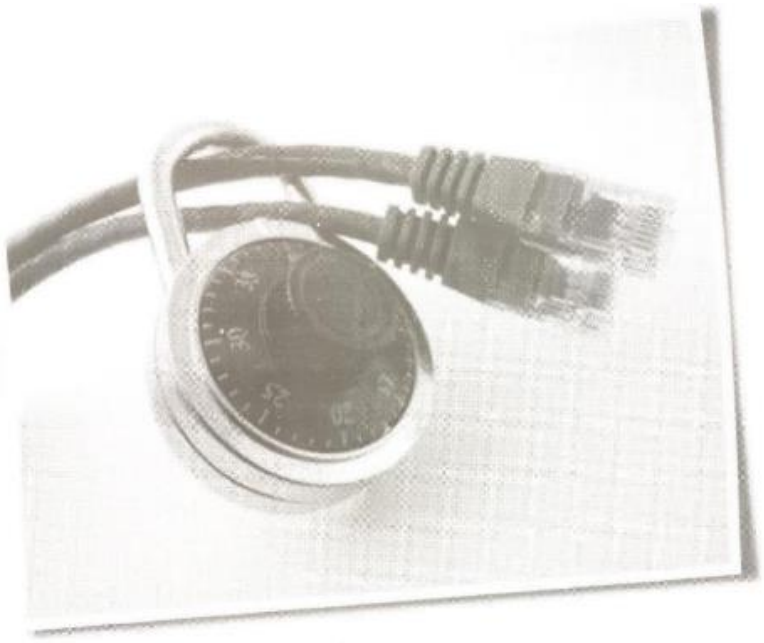
Fuentes Primarias -Trabajos Relacionados - Nacional

- Diseño e implementación de una arquitectura para la transmisión de video de alta calidad sobre redes IP 2006 - Actual [26]
- Prueba de conectividad y tiempo de respuesta del protocolo IPV6 en redes LAN (27]

Grupo Ciencias Coputacionales (CICOM) Universidad de Pamplona, Norte de Santander.

Seguridad en redes

Debido al carácter científico que en un principio tuvo Internet, la seguridad no fue contemplada históricamente en ninguna de las capas que forman la estructura TCP/IP. Con el auge de las tecnologías s de la información y el aumento de personas y empresas conectadas a Internet, la escasez de seguridad se fue convirtiendo en una necesidad. Además la proliferación de noticias sobre personas sin escrúpulos dedicadas a la piratería en Internet, creó un gran malestar social debido a la sensación de inseguridad por los ataques que sufrían tanto las empresas (bancos, universidades e incluso instituciones como ataques que sufrían tanto las empresas (bancos, universidades) e incluso instituciones como la NASA) como los usuarios (utilización ilícita de números de tarjetas de crédito entre otras). [28] [29]



La tardía reacción de las instituciones encargadas de la creación y mod1ficaoon de los protocolos de Internet, propició la aparición de diferentes soluciones comerciales (SSL [31], SET...) para que los usuarios pudieran disfrutar de una seguridad de internet no proporcionaba.

Aprovechando la necesidad de adaptar los diferentes protocolos al crecimiento de Internet, se optó por introducir una serie de especificaciones para garantizar la seguridad como parte implícita de las nuevas especificaciones de los protocolos. Estas especificaciones se conocen como IP Security o IPSec.

Una vez que se había consensuado la necesidad de introducir especificaciones de seguridad como parte intrínseca de los protocolos y no como simples extensiones voluntarias para los fabricantes de software, se planteó un duro debate sobre que capa sería la idónea para proporcionar esta seguridad. Esta decisión era crítica, ya que en el mercado ya existían diferentes soluciones comerciales (SSL, SET...) que proporcionaban distintos grados de seguridad en la capa de usuario.[32]

Finalmente para evitar duplicidades y asegurar un sistema seguro y autentico en todas las capas, se optó por incluir las especificaciones en el nivel más bajo de la pila (Stack) de protocolos, en la especificación del protocolo IP versión 6.

A nivel internacional

Seguridad en redes y criptografía [33]

El presente es una investigación referente al problema que existe de seguridad en redes e Internet. Se presentan los resultados de comparar el algoritmo de encripción de llave privada implementado en MAPLE basado en DES, un algoritmo Blowfish, un algoritmo de uso exclusivo de CES Encryption Utility, y un algoritmo de llave pública implementado en MAPLE basado en el RSA.

Arquitectura y protocolo de seguridad para redes activas [34]

En esta tesis se presenta ASRAEL, una arquitectura y protocolo de seguridad para la carga remota de módulos en un nodo activo. La arquitectura se compone de cuatro controles que son: autenticación del usuario que se conecta remotamente al nodo activo, la encriptación de las comunicaciones entre el nodo activo y el usuario remoto, la utilización del resumen del mensaje para verificar la integridad del módulo a cargar, así como también una firma digital para autenticar el creador del módulo y autorizar la carga del módulo en el nodo active.

SEGURIDAD EN INTERNET [35]

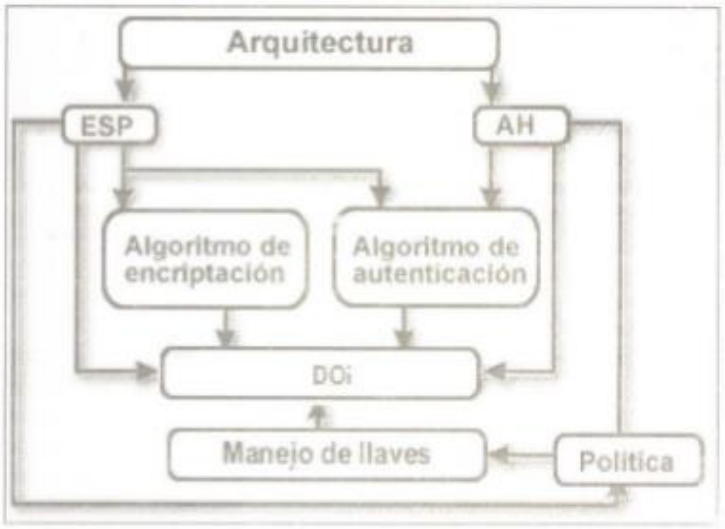
El objetivo de esta tesis es ofrecer un marco teórico sobre seguridad en internet, teniendo como base una exhaustiva investigación bibliográfica, y a la vez conocer el estado actual en que se encuentra el área de seguridad instituciones bursátiles más prestigiadas de la nación.

Mitigación de ataques en la capa de enlace de datos mediante detección y monitoreo de la red [36]

Seguridad es un tema primordial para los administradores de red de cualquier corporación. En la actualidad existen muchas herramientas que previenen y monitorean las redes en busca de taques. Sin embargo, la mayoría de estas herramientas protegen los dispositivos contra amenazas que van desde la capa 3 (red) hasta la capa 7 (aplicación) del modelo OSI, dejando las capas inferiores al descubierto.

IPSec

Una de las características importantes y requisito de 1Pv6, es la integración de seguridad en la capa de red utilizando el protocolo IPSec. IPSec (Internet Protocol Security) [37] es un conjunto de extensiones al protocolo IP. IPSec es un estándar de la IETF (Internet Engineering Task



Force) definido en el RFC 2401 [38].

Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) (39] y el Encapsulating Security Payload (ESP) [40J, protocolos y procedimientos para el manejo de llaves encriptadas.

AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra respuesta. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado. [41]

En la figura 3 se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también algoritmos de encriptacion.

Hoy en día a nivel mundial, regional y local se encuentran trabajando una gran cantidad de organizaciones, universidades y personas en diversos proyectos que involucran la seguridad del protocolo de nueva generación (1Pv6) y sus extensiones de seguridad (IPSec). [42]

A nivel mundial son varios los proyectos que se han realizado referentes a la seguridad en IPv6 (IPSec6).

A nivel internacional

A nivel mundial son varios los proyectos que se han realizado referentes a la seguridad en IPv6 (IPSec6).

IPsec en Ambientes IPv4 e IPv6 [43]

En este trabajo Hugo Adrian Francisconi de nacionalidad argentina proporciona un análisis exhaustivo sobre seguridad en internet en la capa IP (IPsec), basándose en estándares internacionales (RFC). Esto 1ncluve los serv1oos de autentificación, integridad, ocultación del contenido (confidencialidad}, control de acceso, etc. y el conjunto de protocolos por el cual esto es llevado a cabo (AH, ESP. IKE [44), ISAKMP, etc). Como así también se profundiza sobre los conceptos y algoritmos cnptográt1cos para poder entender y desarrollar esa tecnología.

Pv6 Interoperabilidad y robustez [45]

En esta investigación se presenta la evaluación del Protocolo de Internet versión 6 (1Pv6) en relac1on a su 1nteroperabilidad con plataformas tales como Windows XP Solaris 9, Linux Red Hat (versiones 8.0 y 9.0) y Mac OS Y 10.2 ,1O.3, también con protocolos ta1es como el Protocolo Ligero de Acceso a Directorio (LDAPl y 'I Protocolo dL Seguridad > '.IP::>E c' y sus mecanismos de transición como son los Tuneles 6to4, el doble Stack y el Tunnel brokPr Ademcis se proporoon2 una guía a través de ejemplos para configurar 1Pv6 sobre I<t • plataformas Windows XP Solaris (versiones 8.0 y 9.0), Linux RedHat \versiones 8.0 y 9.0) y Mac OS X ,('versión 10.2" Jaguar") y sobre los enrutadores CISCO 2620 XM.

Corporación Universitaria para el Desarrollo de internet. Comité para el desarrollo de la Red Memoria técnica del Laboratorio de interoperabilidad instalado en la Reunión de otoño de CUDI [46]

Este trabajo se baso en investigación sobre la Seguridad para el Protocolo IP (IPSec), se propuso la implementación de una VPN, se experimentó con implementaciones del tipo BITS (Bump InThe Stack),en sistemas operativos. Se eligieron dos sistemas diferentes, populares y utilizados en el entorno de lnternet2: MSWindows2000 para probar conexiones seguras con IPSec para 1Pv6 y Linux en su distribución Slackware 8 para la VPN con 1Pv4.

Protocolos de seguridad e instrumentación de IPSec en escenarios experimentales de internet 2 en México [47]

La seguridad es un aspecto de gran relevancia en las redes de la actualidad, se considera un requisito en los planes de diseño e instrumentación de nuevas redes, por lo que, dentro del contexto de contribución del CICESE a Internet 2 en México, se desarrolló este trabajo de tesis para experimentar con las nuevas tecnologías de seguridad que plantean el uso de protocolos para brindar seguridad directamente al nivel de la capa de red, en particular al protocolo IP, proporcionando una opción para solucionar el problema de seguridad en la capa de tránsito.

Utilización de VPNS (virtual prívate networks) como mecanismo de transferencia de información seguro en instituciones educativas. [48]

Este trabajo evalúa y analiza la seguridad ofrecida por un nuevo mecanismo de Acceso Remoto conocido como Virtual Prívate Network (VPN) que proporciona aspectos de seguridad [49] como encripción, autenticación de los datos [SO], autenticac1on de usuarios y control de acceso, con respecto a la ofrecida por los métodos tradicionales RADIUS y TACACS. Esta tecnología se basa en el establecimiento de un túnel entre los sitios involucrados mediante el uso de los protocolos IPSecurity (IPSec), Point to Point Tunneling Protocol (PPTP) y LayerTwo Tunneling Protocol (L2TP).

A nivel Nacional

Análisis del protocolo PSEC en ambiente ipv6

Por medio de este trabajo se logra un objetivo del proyecto Red IPv6 UP el cual se está llevando a cabo en el grupo de Investigación Ciencias Computacionales (CICOM), Programa de Ingeniería de Sistemas, con el fin de implantar el protocolo de red 1Pv6 bajo la arquitectura IPSec a modo de prueba en un segmento de la red de datos de la Universidad de Pamplona, de esta forma se estudiarán características generales de 1Pv6 y su extensión de seguridad IPSec.

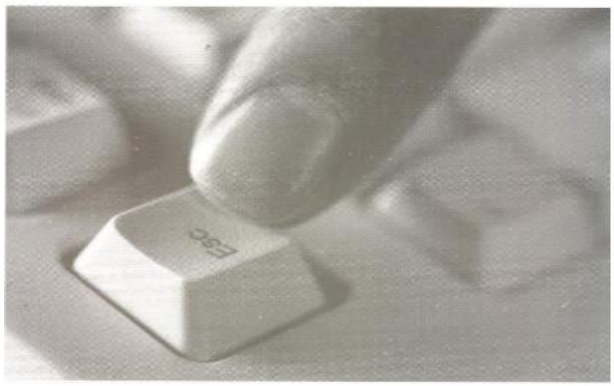
CONCLUSIONES

La seguridad en Internet siempre ha sido una de las principales preocupaciones para todos aquellos que están conscientes de los peligros que puede ocasionar una intrusión de alguien no deseado en nuestra propia computadora o en los archivos más secretos. No solo se debe cuidarse de aquellos quienes están fuera de nuestra casa u oficina sino también de quienes son compañeros de trabajo.

Un aspecto importante es comentar y fomentar sobre la cultura de seguridad en las compañías, puesto que existe un área de oportunidad que debe de aprovecharse y mejorarse.

Otro factor importante es la del establecimiento de políticas de seguridad, ya que las compañías no tienen bien definidas y establecidas las políticas de seguridad en el área de informática.

No olvidar la plataforma en que se encuentra instalado el firewall, ya sea Windows, Solaris, o Linux [51], ya que se deben conocer sus debilidades y fortalezas, y de realizar la configuración correcta para evitar posibles huecos que podrían utilizar los hackers para tener acceso a la información confidencial y relevante para la compañía.



BIBLIOGRAFÍA

[1] VILLALÓN, Antonio. Se9uridad en unix y redes Julio, 2002. [citado agosto 02, 2009]. Disponible en: http//lucas.hispalinux.es/Manuales -LuCAS/SEGUNIX/unixsec -2.1-html/

[2] [citado agosto 02, 2009]. Disponible en: docencia .udea.edu.co/bibliotecologia/seminario-estudiosusuario/unidad4/estado_arte.html

[3] Corporación universitaria para el desarrollo de internet A.C. Internet 2 Mexico.[citado agosto 02, 2009]. Disponible en: http://www.cudi.edu.mx/

[4] Delitos Informatico.Marzo, 2001. [citado agosto 02, 2009]. Disponible en World WideWeb:http://www.dehtosinformaticos.com/seguridad/clasifkacion.shtml

[5] ERNESTO, Axel. [citado agosto 02, 2009]. Disponible en World Wide Web: http://www.cs.cinvestav.mx/Estudiantes/TesisGraduados/2004/tesisAxelEmesto.pdf

[6] kriptopolis.[citado agosto 02, 2009]. Disponible en: http://www.kriptopolis.org/

[7] Criptonomicon. Susurros de la cripta. [citado agosto 02, 2009]. Disponible en World Wide Web: http://www.iec.csic.es/criptonomicon/susurros/susurros11.html

[8] The Twenty Most Critical Internet Security Vulnerabilities (Updated) – The Experts is consensus. [citado agosto 02, 2009]. Disponible en http:http://www.sans.org/top20/

[9] INTEL. IP Security: Building Block for the Trusted Virtual Network. [citado agosto 02, 2009]. Disponible en World Wide Web: http://www.intel.com/connectivity/resources/doc_library/white_papers/products/ipsecurity/npd_white paper.pdf

[10] Welcome to the IPv6 information Page. [citado agosto 03, 2009]. Disponible en World Wide Web: http://www.ipv6.org

[11] Palet, Jordi ipv4 exhaustion or transition to ipv6. [citado agosto 03, 2009]. Disponible en: www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf

[12][Citado agosto 03, 2009]. Disponible en : www.inictel.gob.pe/ipv6/Final-IPv6%20y%e20Seguridad.ppt

[13] ipv6 Mexico. [citado agosto 03, 2009]. Disponible en: http://www.ipv6.unam.mx

[14] Dialnet es un portal de difusión de la producción científica hispana. [citado agosto 03, 2009]. Disponible en World Wide Web: dianlet.unirioja.es/

[15] Boletín de la red nacional del I+D, RedIris, 2002 DIC. [Citado agosto 03, 2009]. Disponible en : www.ucm.es/BUCM/compludoc/S/10201/11335408_html

[16] Boletín de la red nacional del I+D, RedIris, 2002 DIC. [Citado agosto 03, 2009]. Disponible en : www.ucm.es/BUCM/compludoc/S/10704/1139207X_html

[17] Boletín de la red nacional del I+D, RedIris, 2002 DIC. [Citado agosto 03, 2009]. Disponible en : www.ucm.es/BUCM/compludoc/S/10502/11335408_html

[18] [citado agosto 3, 2009]. Disponible en World Wide Web: http//:www.isabel.dit.upm.es/component/otion.com_docman/task.doc_view/gid.407/.

[19][citado agosto 03, 2009]. Disponible en World Wide Web: http//:www.universitario.edu.uy/Proyectos/Proyectos/2005/Estado%20del%2Qarte%20de%20IPV6%20y%20modulo%201PV6%20para%20IPPlan.pdf

[20] [citado agosto 03, 2009].Disponible en: www.ing.unp.edu.ar/wicc2007/traba¡os/ARSO.pdf

[21] [citado agosto 03, 2009]. Disponible en World Wide Web: http://copernic:o.mty.itesm.mx/phronesí.s/mty/tmp/TTE SMMTY2006629.pdf

[22] [citado agosto 03, 2009]. Disponible en http://www.gulic.org/comos/lARTC/html/c440.html

[23] [citado agosto 03, 2009]. Disponible en World Wide Web; http://research.microsocom/en-us/projects/msripv6/

[24] [citado agosto 03, 2009]. Disponible en World Wide Web: http://lanic.utexas.edu/la/regt0n/network.ing/clac.soman .html

[25] [citado agosto 03, 20091. Disponible en World Wide Web: http://copernico.mty.ilesm.mx/phronesis/mty/1mp/ITTSMMTY20066 59.pdf

[26] [citado agosto 04, 2009]. Disponible en World Wide Web:scienti.colciencias.gov.co:8081/ciencia.war/search/EnProductoGr/xmllnfo.do?nroid grupo:00696098l55418&seqproducao- 83&codrh cvc-0000050458&seq.producao_cv=29120

[27] (citado agosto 04, 2009]. Disponible en World Wide Web: www.uninorte.edu.co/publicaóones/upload/pdWingenieria_n11.pdf

[28] [citado agosto 04, 2009]. Disponible en World Wide Web: http://www.rediris.es/cert/doc/unix.sec/node3l.html

[29] VlllALÓN, Antonio. Seguridad en unix y redes [En lineal Julio, 2002. [citado agosto 02, 2009]. Disponible en World Wide Web; httpJ/lucas.hispalinux.es/Manuales-LuCAS/SEGUNIX/unixsec·2.1-htmV

[30] [citado agosto 04, 2009]. Disponible en World Wide Web;http://sds200511667.files.wordpress..com/2008/08/malware1.jpg

[31] [citado agosto 04, 2009]. Disponible en World Wide Web:

[32] [citado agosto 04, 2009]. Disponible en: http://seguridad.internet2.ulsa.mx

[33] [citado agosto 04, 2009]. Disponible en World Wide Web: http://copernico.rnty,itesm.mx/phronesis/mty/tmp/JTESMMTY2004492.pdf

[34] [citado agosto 04, 2009]- Disponible en World Wide Web: http://copernico.mtyitesm.mx/phronesis/mty/tmp/ITESMMTY2C04483pdf

[35] [citado agosto 04. 2009]. Disponible en World Wide Web: http://copernicomty.itesmmxJphronesis/mty/lmp/ITESMMTY2002199.pdf

[36] [citado agosto 05, 2009]. Disponible en World Wide Web: http://copem1Co.rnty.1tesm.mxJphronesi rnty/tnl1>11TESMMTY2004493.pdf

[37] S. Deering, R Hinden. Internet Protocol, Ver5ion6 (1Pv6) Specifteation lnternet.Oraft, Rf-C 1752. Fnero 1995.

[38] [citado agosto05, 2009]. Disponible en World WideWeb: http://www.ietf.org/rfc/rfc2401.txt

[39] S. Kent, and R. Atkinson. IP Authentication Header (AH). RFC

[40] S. Kent, and R Atkinson. Protocol Erx:apsulating Security Payload (ESP). RFC 2406 Noviembre de 1998

[41] Ladid. Security and Privacity with 1Pv6. European Task Fork Communication. 2004

[42] S. Kent, R. Atkinson. Security Archltecture for the Internet Protocol RFC /401 November 1998.

[43] [citado agosto 05, 2009]. Disponible en World Wide Web: http://www.rfc·es.org/rfc/rfc24 l0-es.txt

[44] D. Harkins and D. Carrel.The Internet Key Exchange. RrC 2409, Noviembre de 1998.

[45] [citado agosto 05, 2009]. Disponible en World Wide Web:http://www.cs.c1nvestav.mx/EstudiantesJTesisGraduados/2004/tesisAxclErnesto.pdf

[46] [citado agosto 06, 2009). Disponible en World Wide Web:http://seguridad1ntemet2.ulsa mx/congresos/2001 /cudi2/maqueta.pdf

[47] [citado agosto 06, 20091. Disponible en World Wide http://seguridad.intemet2.ulsa.mx/publicat1ons/tesis_comedi pdf

[48] [citado agosto 06, 2009]. Disponible en World Wide http://coperrnco_mty.itesm.mx/phronesis/mty/tmp/lTESMMTY2002159.Jxlf

[49] [citado agosto 06, 2009]. Disponible en World Wide http://www.enterasys.com/company/li terature.aspx

[50] [citado agosto 06, 2009]. Disponible en World Wide https://wwwcertisur.com/legal/Docs/lntroCertDigitales.html

[51] Kame Project. (citado agosto 06, 2009}. Disponible en World Wide: www.kame.net[

BIBLIOGRAFÍA RECOMENDADA

[1] Barbera J. Retazos de una década prodigiosa."Boletin de Red IRIS:44, 1998, pp. 21-24

(2] Jose M. Femena.1Pv6 practico, May 2001. htt:/l/www.recfüis.es/red/reuniones/1Pv6practico.pdf

[3] Hunt CTCP/IP Network Admmistration, Th1rd EditlOn, 2002

[4] Krol E Hoffman C RFC 1462 FYI on'What is the lnternetr Request For Comments. May 1993.

[5] Lopez Ramón ¡10años! ¿Solo 10aflos?.BoletínRed IRIS:44, 1998.

[6] S. Deering and R. Hinden. RFC 2460: Internet Protocol,Version 6 (1Pv6) specicat1on, Obsoletes RFC 1883. Status: DRAFT STANDARD. December 1998

[7] Sanz M. A. Fundamentos históricos de la Internet en Europa y en España. Boletin de Red IR1S': 45, 1998

[8] Tanenbaum."Redes de computadoras: Tercera edición. En. Pearson, 1997.