



BIBLIOGRAFÍA



BIBLIOGRAFÍA

LIBROS

- ⦿ Albitz, Paul, Liu, Cricket. “*DNS AND BIND*”, Editorial O’Reilly, Estados Unidos, 4ª edición, 2001.
- ⦿ Albitz, Paul, Liu, Cricket. “*DNS AND BIND*”, Editorial O’Reilly, Estados Unidos, 3ª edición, 1998.
- ⦿ Kabelova Alena “*DNS IN ACTION A DETAILED AND PRACTICAL GUIDE TO DNS IMPLEMENTATION, CONFIGURATION AND ADMINISTRATION*” Editorial Packt publishing Birmingham- Mumbai
- ⦿ López Barrientos Ma. Jaquelina “*CRIPTOGRAFÍA*”, Universidad Nacional Autónoma de México, Facultad de Ingeniería, División de Ingeniería eléctrica departamento de computación, 2009
- ⦿ Tanenbaum, Andrew. “*SISTEMAS OPERATIVOS MODERNOS*”, Editorial Prentice Hall, México, 1ª edición, 1993.

LISTA DE FIGURAS

- ⦿ Figura 1 Fuente: [19 de mayo del 2010
<http://inza.wordpress.com/2008/10/page/2/>
- ⦿ Figura 2 Fuente: [19 de mayo del 2010
<http://www.andymeneely.com/blog/science/computer-security/public-key-cryptography/#more-95>
- ⦿ Figura 1.3 Fuente: [04 de Abril 2010
<http://www.outono.net/elentir/?p=606>]
- ⦿ Figura 1.6 Fuente: [04 de Abril 2010
http://library.thinkquest.org/07aug/01676/spanish/downtheages_wars_too_lsanddevices_jeffersonswheel.html]
- ⦿ Figura 1.7 Fuente http://redyseguridad.fi-p.unam.mx/pp/aldo/criptografia/notasclase/tema_4.pdf



- ✦ Figura 1.10 Fuente http://redyseguridad.fi-p.unam.mx/pp/aldo/criptografia/notasclase/tema_4.pdf
- ✦ Figura 1.11 Fuente: <http://www.inf.utfsm.cl/~rmonge/seguridad/cripto-03-bn.pdf> 16 de junio del 2010
- ✦ Figura 1.15 Imagen tomada de Criptografía por Ing Ma. Jaquelina López Barrientos página 233
- ✦ Figura 1.16 Imagen tomada de Criptografía por Ing Ma. Jaquelina López Barrientos página 238

MESOGRAFÍA

Fuente 8 de Junio del 2010

<http://www.internetnews.com/security/article.php/3758566/Is+DNSSEC+the+Answer+to+Internet+Security.htm>





https://www.dnssec-tools.org/wiki/index.php/DNSSEC_Applications

The screenshot shows a web browser displaying the 'DNSSEC Applications' page on the DNSSEC-tools.org wiki. The page title is 'DNSSEC Aplicaciones'. Below the title, there is a brief introduction in Spanish: 'Esta es una breve introducción en el conjunto de aplicaciones que se han parcheado para apoyar las consultas a través de la DNSSEC-tools DNSSEC.' The main content is a table of contents with the following items:

- 1 Aplicaciones Consiente DNSSEC
 - 1.1 sin parches de Firefox, utilizando un servidor no recursivo DNSSEC
 - 1.2 sin parches de Firefox con un agente DNSSEC servidor recursivo
 - 1.3 parcheado con Firefox Tool validador colección de DNSSEC
 - 1.4 uso de los parches
- 2 Configuración de política de validación DNSSEC
 - 2.1 Firefox
 - 2.2 Sendmail
 - 2.3 Puente
 - 2.4 LinCIT
 - 2.5 Thunderbird
 - 2.6 OpenSSH
 - 2.6.1 Cuando se establece en "off"
 - 2.6.2 Cuando se establece en "on"
 - 2.6.3 Cuando se ajusta a "partial"
 - 2.6.4 Más información
- 3.7 IIS
- 3.8 nntp
- 3.9 proftpd
- 3.10 sabdard
- 4 Resumen del software
 - 4.1 Usuarios Firefox (DNSSEC aplicaciones ratificadas)

Below the table of contents, there is a section titled 'Consiente DNSSEC Aplicaciones' which explains that the project creates a series of patches for applications to emit DNS queries using the DNSSEC validation tool. It also includes a note: 'Sin parches de Firefox utiliza un servidor no recursivo DNSSEC'.

http://www.linuxsecurity.com/content/view/117551/49/

The screenshot shows the LinuxSecurity.com website with an article titled 'Paul Vixie and David Conrad on BIND9 and Internet Security'. The article text includes:

LinuxSecurity.com: Can you give us a brief description of your background? How did you become involved with BIND and eventually come to form the ISC?

Paul Vixie: I started working on BIND in 1988 while employed at Digital Equipment Corp. (DEC) which was later bought by Compaq. My job was to run their corporate internet gateway (DECWRL) in Palo Alto, and also to run the servers for the DEC.COM zone and work with other parts of the company to allocate subdomains on a global basis (we had about 400, which was a lot at that time). One of the biggest sources of operational instability in my (DEC's) gateway was the sleazy, icky, rotten code produced by U.C. Berkeley in the previous decade, and I quickly found myself up to my armpits in Sendmail and BIND muck.

Eventually it became known that I had a stable version of BIND running at DECWRL, and folks who heard about this asked me for copies. I published kits on my FTP server and folks started not only picking up my kits but running them and submitting patches (both enhancements and bug fixes). Soon it was time for UCB to ship another BSD type (4.3-Rel), I think) and they included my version of BIND rather than their own. UCB BIND was dead, and DECWRL BIND had taken its place.

In 1993 I left DECWRL to return to my private consulting practice. I found that the BIND community expected me to "take BIND with me" -- it was clear that noone remaining at DECWRL had any interest in it, so I commuised to publish new BIND kits independently, reick Adams, then or UUNET, I envisioned a "very" strong desire that BIND be worked on, and had the "old non-profit" part of UUNET issue me a grant to do just that. In 1994, Rick and I decided that other companies should also be helping to fund this piece of critical infrastructure (since it was by that time clear that ISO was dead and that TCP/IP would be the basis for all public data networking), and we founded ISC as a funding clearinghouse to support BIND and similar software.

David Conrad: started working with the Internet around 1983 as team leader of a joint IBM/University of Maryland project for the development of a commercial TCP/IP on the IBM PC product. Leaving UMD in 1990, I worked as a researcher at the University of Hawaii on the PACCOM project, providing the first Internet connectivity to various Asia Pacific countries. I moved to Japan in 1992 and helped start up the first commercial ISP in Japan, Internet Initiative Japan, Inc. In 1994, I was asked to create and run the Asia Pacific Network Information Center, the Regional Internet Registry for the Asia and Pacific Rim region which I did until 1998. Returning to the US in 1998, I became the Executive Director of ISC and helped set up (what became) Nominum with Paul.

My involvement with BIND came with the job (ED of ISC), however I used and administered BIND (of various versions) at pretty much every job I had.

LinuxSecurity.com: BIND9 is a "major rewrite" from previous versions. Can you explain to us the reason for this rewrite and what new features have been added



http://www.george-barwood.pwp.blueyonder.co.uk/DnsServer/NotesOnDNSSEC.htm

Lo más cercano encloser se calcula que se cdexample.com.

mcexample.com [www.example.com NSEC] se refiere a wcexample.com, cuanto más cerca siguiente nombre. El propietario contiene cdexample.com. (El padre del cerrador siguiente nombre), para que el registro es válido NSEC.

Lo más cercano encloser no es igual al PROVEEDOR, por lo que [Caso 2] no se aplica y se aplica [Caso 3].

No hay un registro con el propietario NSEC * cdexample.com (el comodín al más cercano encloser), y al MX, CNAME y NS bits en el mapa de bits de tipo no están establecidos. La prueba NoData es completa.

Autenticación de un NSEC NameError (NXDOMAIN) condición

Todas las respuestas y RRset Autoridad en la respuesta ha sido autenticado.

Lo más cercano a encloser PROVEEDOR se calcula y la inexistencia de un registro NSEC en el "siguiente nombre más cerca" está marcada.

La inexistencia de un registro en el NSEC comodín al más cercano encloser está marcada.

La prueba es entonces completa.

Ejemplo: supongamos que la consulta es [mexample.com A], y la zona ha cadena NSEC.
 example.com. NSEC a.example.com. SOA NS (de transmisión) a.example.com. NSEC z.example.com. NS (de transmisión) z.example.com. NSEC example.com. NS

Lo más cercano encloser es example.com.

La no existencia de un NSEC en la próxima m example.com más cerca [nombre NSEC] está activada. R es [a.example.com. z.example.com NSEC], que cubre m example.com. P es example.com, que no es igual a a.example.com, pero aparece on R, por lo que R no es de la zona principal.

La no existencia de un NSEC en el comodín al más cercano encloser, [* example.com. NSEC] está activada. R es [example.com. a.example.com NSEC], que cubre * example.com. P es example.com, que es igual al dueño de R, por lo que una delegación de verificación se lleva a cabo. DNAME está claro que, el NS se establece, pero también se establece SOA, por lo que el NSEC no es una delegación.

http://tools.ietf.org/search/rfc5155

[Docs] [txt/pdf] [draft-ietf-dnssec...] [Diff1] [Diff2]

PROPOSED STANDARD

Network Working Group
 Request for Comments: 5155
 Category: Standards Track

E. Laurie
 G. Sisson
 R. Arends
 Nominet
 D. Blacka
 VeriSign, Inc.
 February 2008

DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

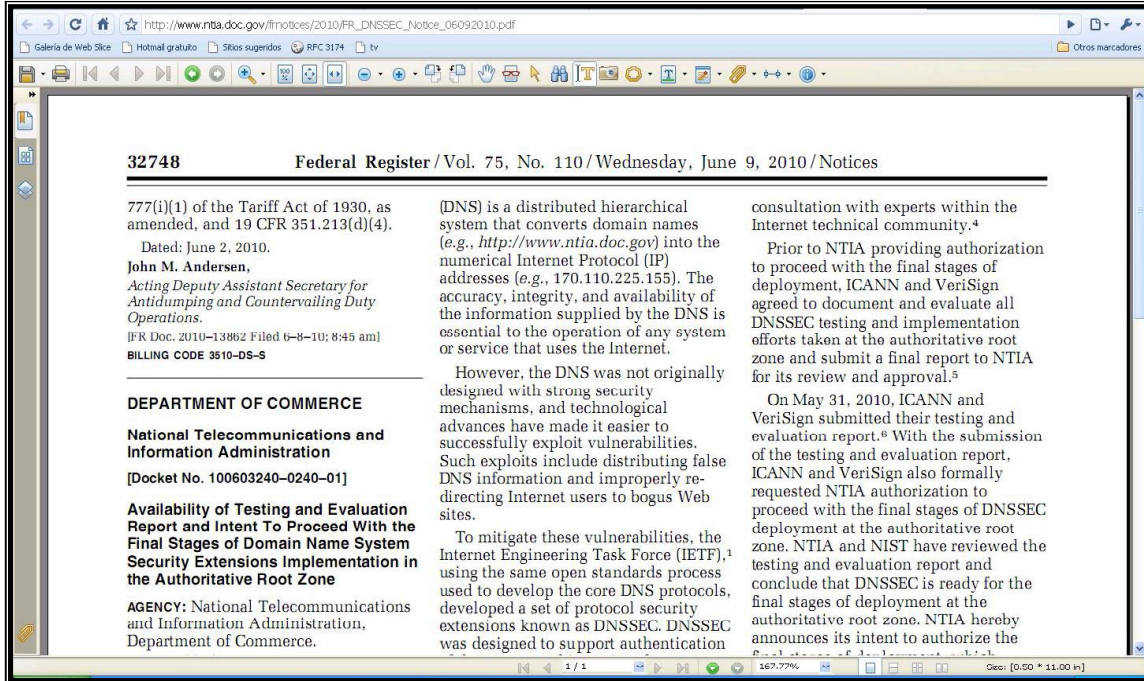
The Domain Name System Security (DNSSEC) Extensions introduced the NSEC resource record (RR) for authenticated denial of existence. This document introduces an alternative resource record, NSEC3, which similarly provides authenticated denial of existence. However, it also provides measures against zone enumeration and permits gradual expansion of delegation-centric zones.

Table of Contents

1.	Introduction	4
1.1.	Rationales	4
1.2.	Requirements	4
1.3.	Terminology	5
2.	Backwards Compatibility	6
3.	The NSEC3 Resource Record	7
3.1.	RDATA Fields	8
3.1.1.	Hash Algorithm	8
3.1.2.	Flags	8
3.1.3.	Iterations	8
3.1.4.	Salt Length	8
3.1.5.	Salt	8
3.1.6.	Hash Length	9
3.1.7.	Next Hashed Owner Name	9



http://www.ntia.doc.gov/frnotices/2010/FR_DNSSEC_Notice_06092010.pdf



32748 Federal Register / Vol. 75, No. 110 / Wednesday, June 9, 2010 / Notices

777(i)(1) of the Tariff Act of 1930, as amended, and 19 CFR 351.213(d)(4).
 Dated: June 2, 2010.
John M. Andersen,
Acting Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.
 [FR Doc. 2010-13882 Filed 6-8-10; 8:45 am]
BILLING CODE 3510-DS-S

DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
[Docket No. 100603240-0240-01]

Availability of Testing and Evaluation Report and Intent To Proceed With the Final Stages of Domain Name System Security Extensions Implementation in the Authoritative Root Zone

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

(DNS) is a distributed hierarchical system that converts domain names (e.g., <http://www.ntia.doc.gov>) into the numerical Internet Protocol (IP) addresses (e.g., 170.110.225.155). The accuracy, integrity, and availability of the information supplied by the DNS is essential to the operation of any system or service that uses the Internet.

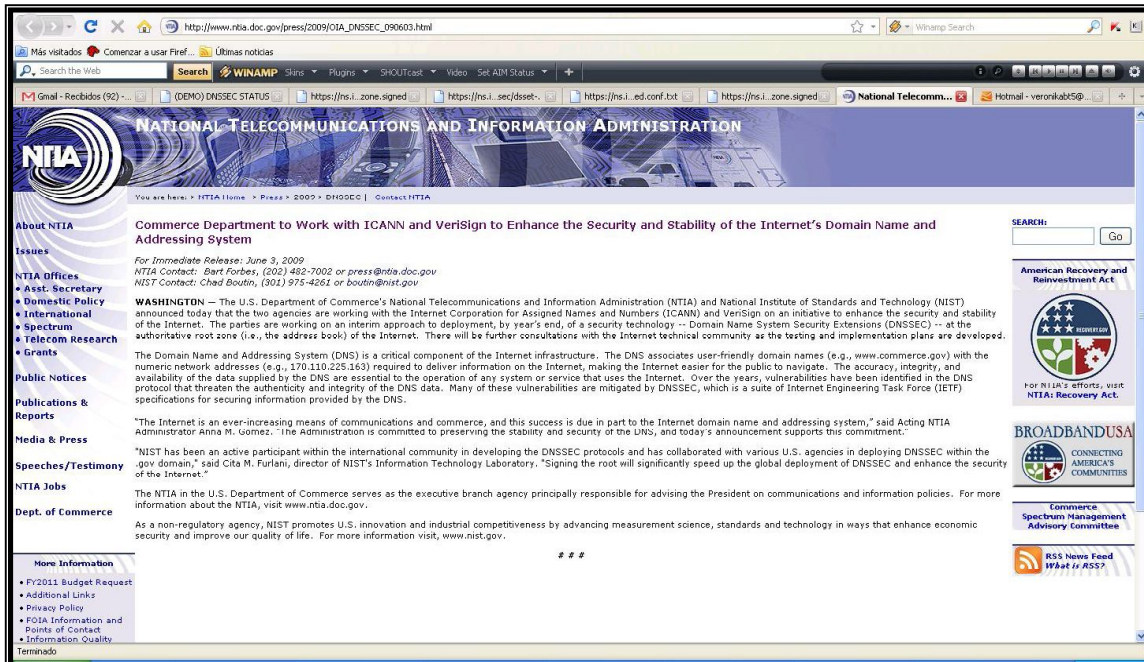
However, the DNS was not originally designed with strong security mechanisms, and technological advances have made it easier to successfully exploit vulnerabilities. Such exploits include distributing false DNS information and improperly re-directing Internet users to bogus Web sites.

To mitigate these vulnerabilities, the Internet Engineering Task Force (IETF),¹ using the same open standards process used to develop the core DNS protocols, developed a set of protocol security extensions known as DNSSEC. DNSSEC was designed to support authentication consultation with experts within the Internet technical community.⁴

Prior to NTIA providing authorization to proceed with the final stages of deployment, ICANN and VeriSign agreed to document and evaluate all DNSSEC testing and implementation efforts taken at the authoritative root zone and submit a final report to NTIA for its review and approval.⁵

On May 31, 2010, ICANN and VeriSign submitted their testing and evaluation report.⁶ With the submission of the testing and evaluation report, ICANN and VeriSign also formally requested NTIA authorization to proceed with the final stages of DNSSEC deployment at the authoritative root zone. NTIA and NIST have reviewed the testing and evaluation report and conclude that DNSSEC is ready for the final stages of deployment at the authoritative root zone. NTIA hereby announces its intent to authorize the

http://www.ntia.doc.gov/press/2009/OIA_DNSSEC_090603.html



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

You are here: [NTIA Home](#) > [Press](#) > 2009 > [DHGSEC](#) | [Contact NTIA](#)

Commerce Department to Work with ICANN and VeriSign to Enhance the Security and Stability of the Internet's Domain Name and Addressing System

For Immediate Release: June 3, 2009
 NTIA Contact: Bart Forbes, (202) 482-7002 or press@ntia.doc.gov
 NIST Contact: Chad Boutin, (301) 975-4261 or boutin@nist.gov

WASHINGTON — The U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) and National Institute of Standards and Technology (NIST) announced today that the two agencies are working with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign on an initiative to enhance the security and stability of the Internet. The parties are working on an interim approach to deployment, by year's end, of a security technology -- Domain Name System Security Extensions (DNSSEC) -- at the authoritative root zone (i.e., the address book) of the Internet. There will be further consultations with the Internet technical community as the testing and implementation plans are developed.

The Domain Name and Addressing System (DNS) is a critical component of the Internet infrastructure. The DNS associates user-friendly domain names (e.g., www.commerce.gov) with the numeric network addresses (e.g., 170.110.225.163) required to deliver information on the Internet, making the Internet easier for the public to navigate. The accuracy, integrity, and availability of the data supplied by the DNS are essential to the operation of any system or service that uses the Internet. Over the years, vulnerabilities have been identified in the DNS protocol that threaten the authenticity and integrity of the DNS data. Many of these vulnerabilities are mitigated by DNSSEC, which is a suite of Internet Engineering Task Force (IETF) specifications for securing information provided by the DNS.

"The Internet is an ever-increasing means of communications and commerce, and this success is due in part to the Internet domain name and addressing system," said Acting NTIA Administrator Anna M. Gomez. "The Administration is committed to preserving the stability and security of the DNS, and today's announcement supports this commitment."

"NIST has been an active participant within the international community in developing the DNSSEC protocols and has collaborated with various U.S. agencies in deploying DNSSEC within the gov domain," said Cita M. Furlani, director of NIST's Information Technology Laboratory. "Signing the root will significantly speed up the global deployment of DNSSEC and enhance the security of the Internet."

The NTIA in the U.S. Department of Commerce serves as the executive branch agency principally responsible for advising the President on communications and information policies. For more information about the NTIA, visit www.ntia.doc.gov.

As a non-regulatory agency, NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. For more information visit, www.nist.gov.

###

More Information

- FY2011 Budget Request
- Additional Links
- Privacy Policy
- FOIA Information and Points of Contact
- Information Quality

Terminado

SEARCH:

American Recovery and Reinvestment Act
 For NITIA's efforts, visit [NTIA: Recovery Act](#).

BROADBAND USA
 CONNECTING AMERICA'S COMMUNITIES

Commerce Spectrum Management Advisory Committee

RSS News Feed
 RSS for RSS



13 de julio del 2010

Descripción breve de que es dnssec <http://teleobjetivo.org/blog/que-es-dnssec.html>

¿Que es DNSSEC y para que sirve?
3 de Junio de 2009 · Sin comentarios

Leo en IDG que la entidad que gestiona el dominio .org ha decidido activar el protocolo DNSSEC, con lo que todos los dominios terminados en .org (por ejemplo, teleobjetivo.org), también podrán activar este sistema de seguridad.

Las páginas web y las direcciones email se identifican mediante nombres, pero en Internet los servidores se identifican mediante direcciones IP; para la conversión de uno a otro se utiliza el protocolo DNS, que consiste básicamente en enviar una consulta pidiendo la dirección IP que corresponde a un determinado nombre. El proceso para convertir un nombre en una dirección IP es el siguiente:

- Nuestro ordenador envía la consulta al servidor/servidores DNS que tiene configurados; normalmente, son los servidores de nuestro proveedor de acceso a Internet.
- El servidor DNS al que enviamos la pregunta extrae la raíz del nombre pedido, que para "teleobjetivo.org" sería "org", y pregunta a los servidores raíz (una lista de servidores conocida y que se configura de forma estática en todos los servidores DNS) que servidores DNS gestionan el ".org", que los servidores raíz responderán con una lista de direcciones IP.
- El servidor DNS envía a los servidores de los dominios ".org" una consulta pidiendo la dirección IP del servidor DNS que gestiona el dominio "teleobjetivo.org".

<http://dnssec.niclabs.cl/tutorial/intro>

Que es DNSSEC (DNS Security Extensions)

En esta página se buscan introducir teóricamente las motivaciones para implementar DNSSEC sobre los servicios DNS actuales, y exponer a modo introductorio el funcionamiento de estas extensiones.

Lo primero recordar el funcionamiento del protocolo DNS. Para esto veamos la siguiente imagen que describe el proceso de resolución de nombres:

El proceso de consulta DNS (o DNS query) se efectúa de la siguiente forma:

- Preguntamos a la zona raíz, "¿Quién es www.uchile.cl?". La zona raíz no sabe la respuesta, pero nos dice "no lo sé, pero mis registros indican que la zona CL puede saberlo, hazle la misma consulta a esta zona" (ya que es la zona que le sigue en el nombre de dominio consultado). La respuesta a esta pregunta será la dirección IP asociada a la zona CL.
- Preguntamos a la zona CL, "¿Quién es www.uchile.cl?". La zona CL no sabe la respuesta, pero nos dice "no lo sé, pero mis registros indican que la zona UCHILE.CL puede saberlo, hazle la misma consulta a esta zona" (ya que es la zona que le sigue en el nombre de dominio consultado). La respuesta a esta pregunta será la dirección IP asociada a la zona UDP.CL.
- Preguntamos a la zona UCHILE.CL, "¿Quién es www.uchile.cl?". Finalmente, esta zona sí sabe quién es este nombre de dominio, respondiendo "www.uchile.cl es 200.14.86.4". Se dice que esta última zona ha respondido con autoridad.

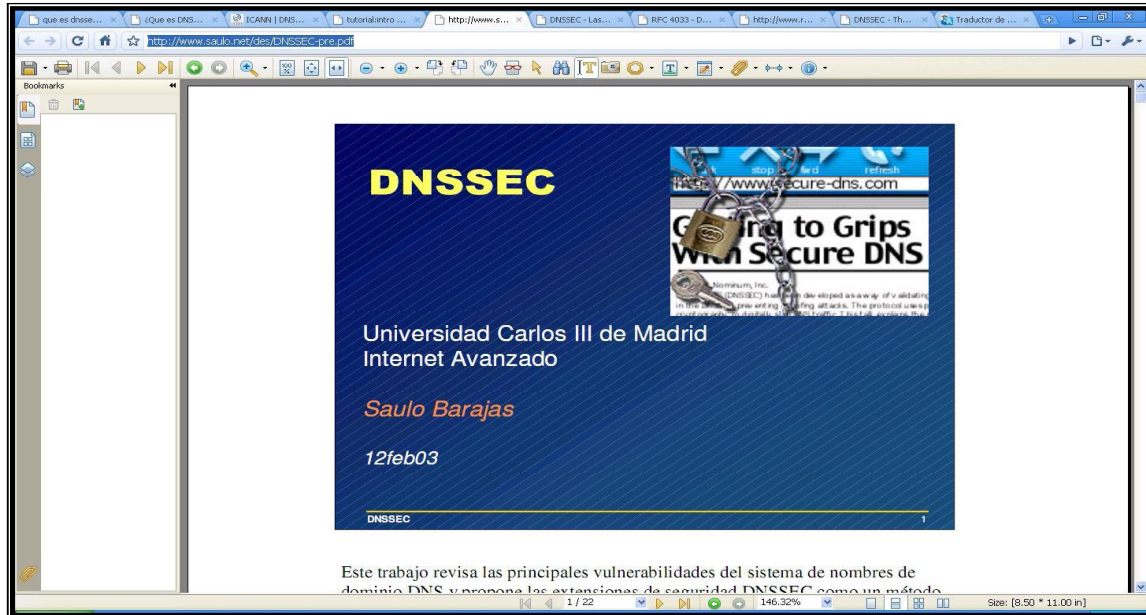
El fenómeno indicado en el primer y segundo paso de los puntos anteriores se denomina **delegación de autoridad**. Básicamente, consiste en delegar la tarea de resolver nombres desde un servidor DNS a otro, debido a que el primero sólo contiene información parcial del nombre consultado.

Además, en el proceso anterior se definen dos tipos de servidores DNS:



<http://www.saulo.net/des/DNSSEC-pre.pdf>

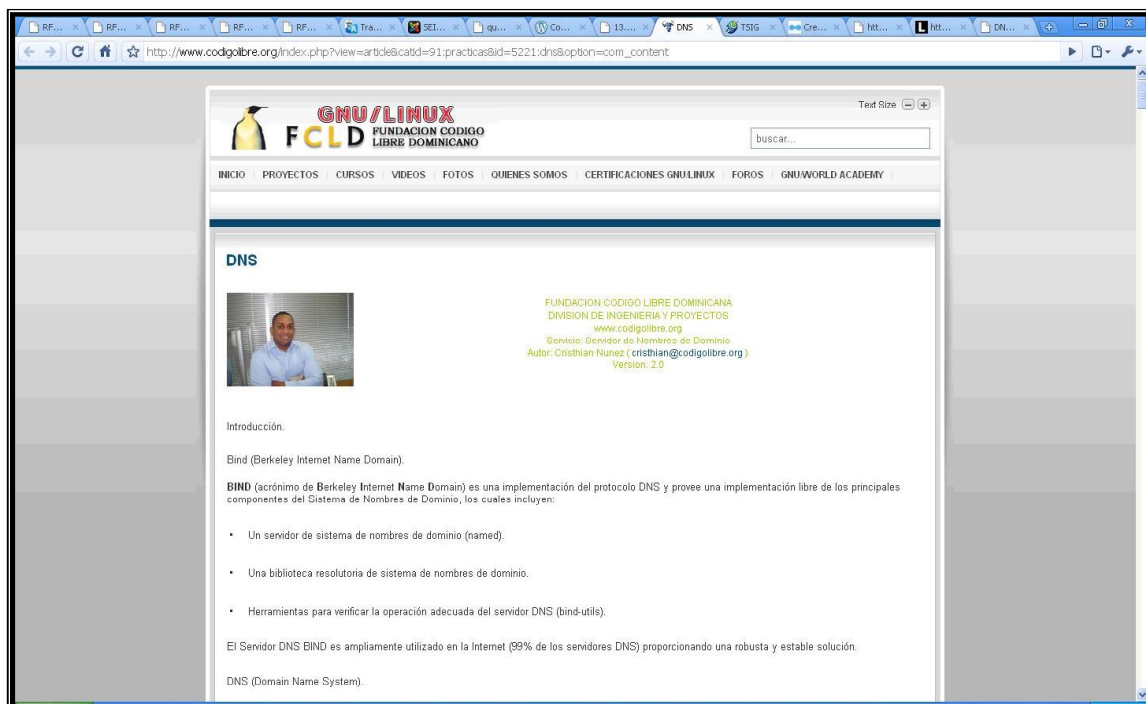
Descripción de dnssesc con la implementación explicada paso a paso



http://www.codigolibre.org/index.php?view=article&catid=91:practicass&id=5221:dns&option=com_content

Como configurar un dns y los componentes que tiene

Como configurar un dns y los componentes que tiene





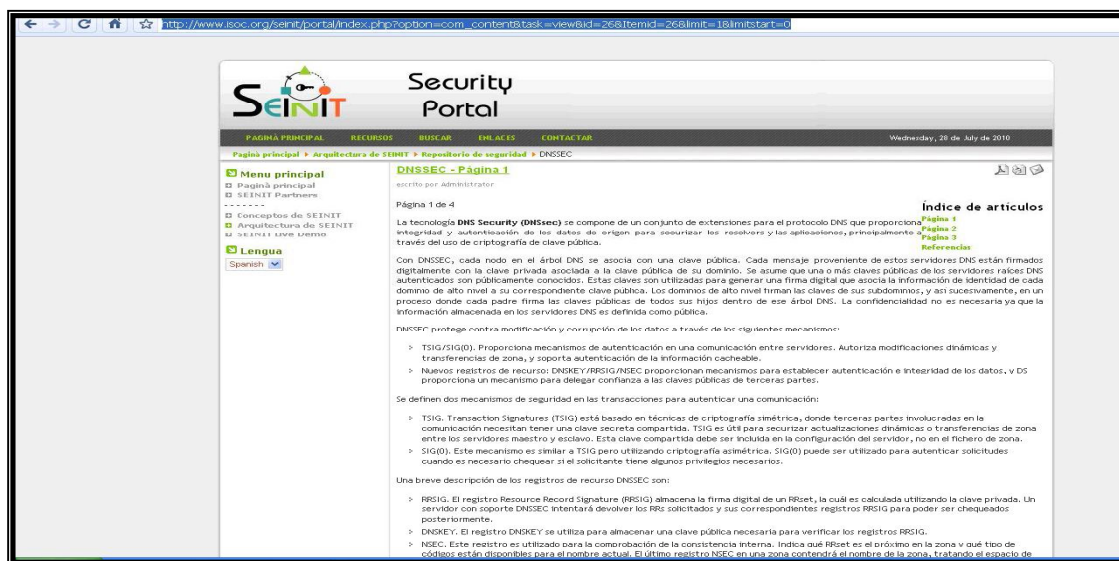
Periódico el universal se da de alta la zona .eu y .org

http://www.eluniversal.com.mx/articulos/59265.html



Descripción de DNSSEC 27 de julio del 2010

http://www.isoc.org/seinit/portal/index.php?option=com_content&task=view&id=26&Itemid=26&limit=1&limitstart=0





TSIG descripción del protocolo

<https://www.czechpoint.cz/nps/portal/modules/dhcp/help/es/DHCPCreateTSIG.html>

La imagen muestra una captura de pantalla de un navegador web que muestra la página de ayuda "Crear clave TSIG". El navegador muestra la URL <https://www.czechpoint.cz/nps/portal/modules/dhcp/help/es/DHCPCreateTSIG.html>. El contenido de la página incluye:

- Ayuda**
- Crear clave TSIG**
- La clave TSIG proporciona una forma de autenticar actualizaciones en una base de datos DNS dinámica.
- Para crear una clave TSIG:
 1. Especifique el nombre de la clave TSIG.
 2. Especifique el nombre del algoritmo. Este algoritmo se utiliza para generar una clave TSIG.
 3. Especifique la clave secreta que se utilizará para descifrar la clave TSIG.
 4. Seleccione un servicio en la lista. La clave TSIG se creará en el servicio que se especifique.
 5. Haga clic en Crear.
- Enlaces relacionados:
 - [Acercar de la utilidad de gestión de DHCP](#)
 - [Gestión de claves TSIG](#)
- Los símbolos de marca comercial (®, ™, etc.) indican una marca comercial de Novell. El asterisco (*) indica una marca comercial de otro fabricante. Si desea obtener más información, consulte [información legal](#).

Descripción del protocolo TSIG

<http://www.worldlingo.com/ma/enwiki/es/TSIG>

La imagen muestra una captura de pantalla de la página de descripción del protocolo TSIG en WorldLingo. El navegador muestra la URL <http://www.worldlingo.com/ma/enwiki/es/TSIG>. El contenido de la página incluye:

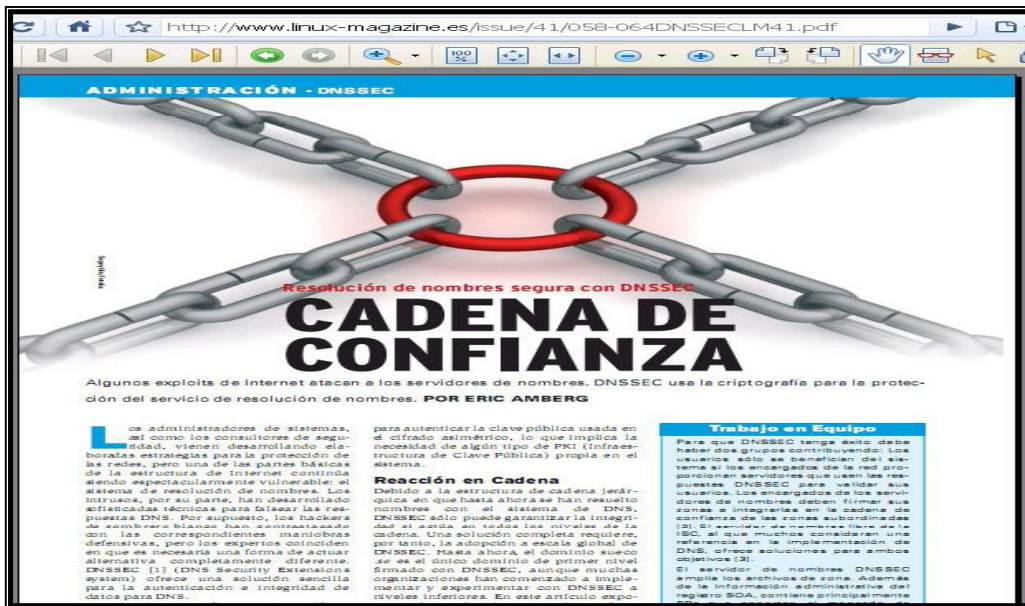
- TSIG**
- UTC Time Servers**
UTC Based Network Time Servers With Official UTC Time. Get A Quote!
www.symmetric.com/UTC_Time_Server
- TSIG (firma de la transacción)** es un protocolo de establecimiento de una red de la computadora definido adentro RFC 2845. Es utilizado sobre todo por **Domain Name System (DNS)** proporcionar medios de autenticar actualizaciones a a **DNS** dinámico base de datos. Las aplicaciones de TSIG compartenon claves secretas y hashing unidireccional para proporcionar medios cryptographically seguros de identificar cada punto final de una conexión como siendo permitido para hacer o para responder a una actualización del DNS.
- Aunque las preguntas al DNS pueden ser hechas anónimo (sino ver **DNSSEC**), las actualizaciones al DNS deben ser autenticadas a través que realizan cambios que duran a la estructura del Internet que sobrevive al sistema. El uso de una clave secreta para el cliente que hace la actualización y el servidor del DNS garantiza la autenticidad de la petición de la actualización. Sin embargo, la petición de la actualización puede pasar sobre un canal inseguro (el Internet). Una función unidireccional del hashing se utiliza para evitar que los observadores malévulos aprender la llave secreta y la usen para hacer sus propias modificaciones.
- Un **timestamp** se incluye en el protocolo de TSIG para prevenir registros respuestas de la reutilización que permitirían que un atacante practicara una abertura la seguridad de TSIG. Esto pone un requisito en los servidores dinámico del DNS y los clientes de TSIG para contener un reloj exacto. Puesto que los servidores del DNS están conectados con una red, **Network Time Protocol** puede ser utilizado proporcionar una fuente exacta del tiempo.
- Las actualizaciones del DNS, como preguntas, se transportan normalmente vía **UDP** puesto que requiere gastos indirectos más bajos que **TCP**. Sin embargo, los servidores del DNS soportan peticiones del **UDP** y del **TCP**.
- Contenido**
 - 1 Puesta en práctica
 - 2 Alternativas a TSIG
 - 3 Vea también
 - 4 Referencias
 - 5 Acoplamientos externos
- Puesta en práctica**
- Una actualización, según lo especificado adentro RFC 2136, está un sistema de instrucciones a un servidor del DNS. Éstos incluyen un jefe, la zona que se pondrán al día, los requisitos previos que deban ser satisfechos, y los expedientes que se pondrán al día. TSIG agrega un expediente final, que incluye un **timestamp** y el picadillo de la petición. También incluye el nombre de la llave secreta que fue utilizada para firmar la petición. RFC 2136 tiene recomendaciones en la forma del nombre.
- La respuesta a una actualización acertada de TSIG también será firmada con un expediente de TSIG. Las faltas no se firman de evitar que un atacante aprenda cualquier cosa sobre el TSIG dominante con la actualización especialmente hecha a mano "sondan".
- nsupdate** el programa puede utilizar TSIG para hacer actualizaciones del DNS.



DNSSEC cadenas de confianza publicación que presenta el cómo funciona DNSSEC

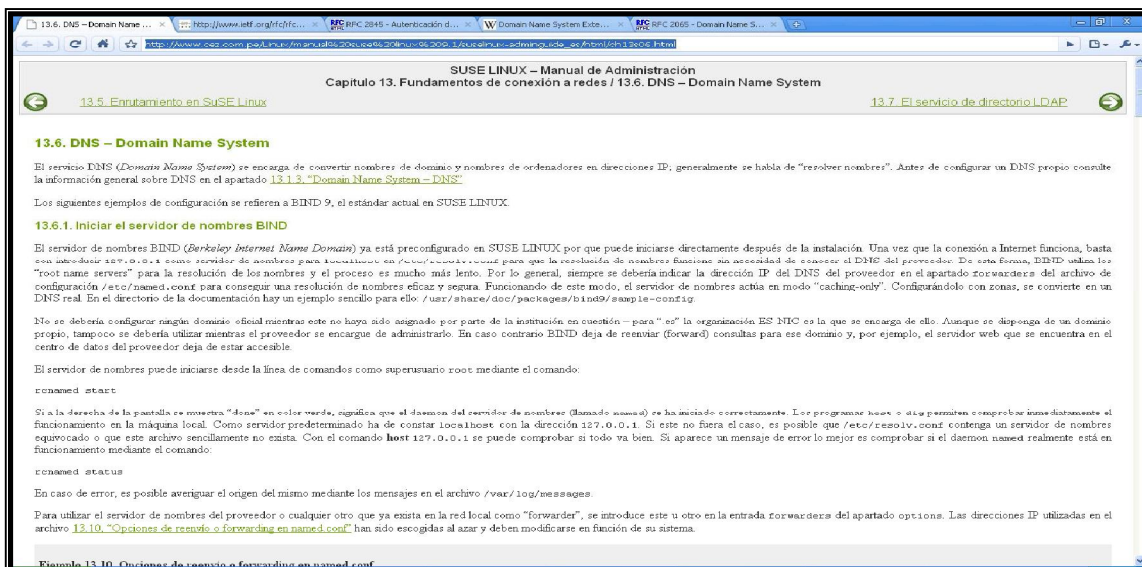
<http://www.linux-magazine.es/issue/41/058-064DNSSECLM41.pdf>

2 de julio del 2010



Descripción del DNS

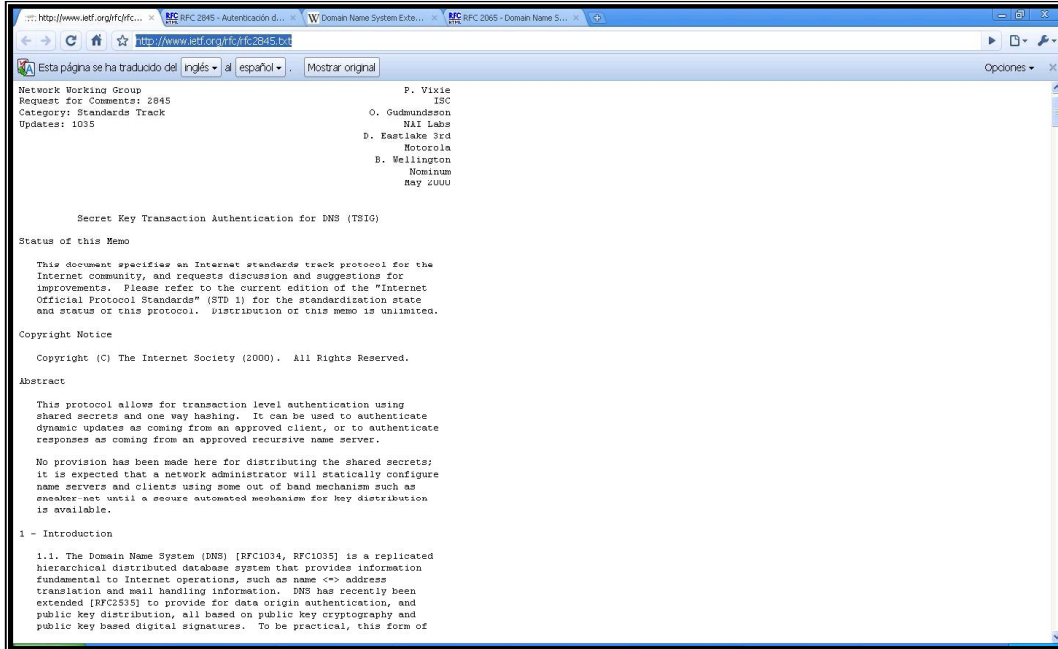
http://www.cez.com.pe/Linux/manual%20suse%20linux%209.1/suselinux-adminguide_es/html/ch13s06.html





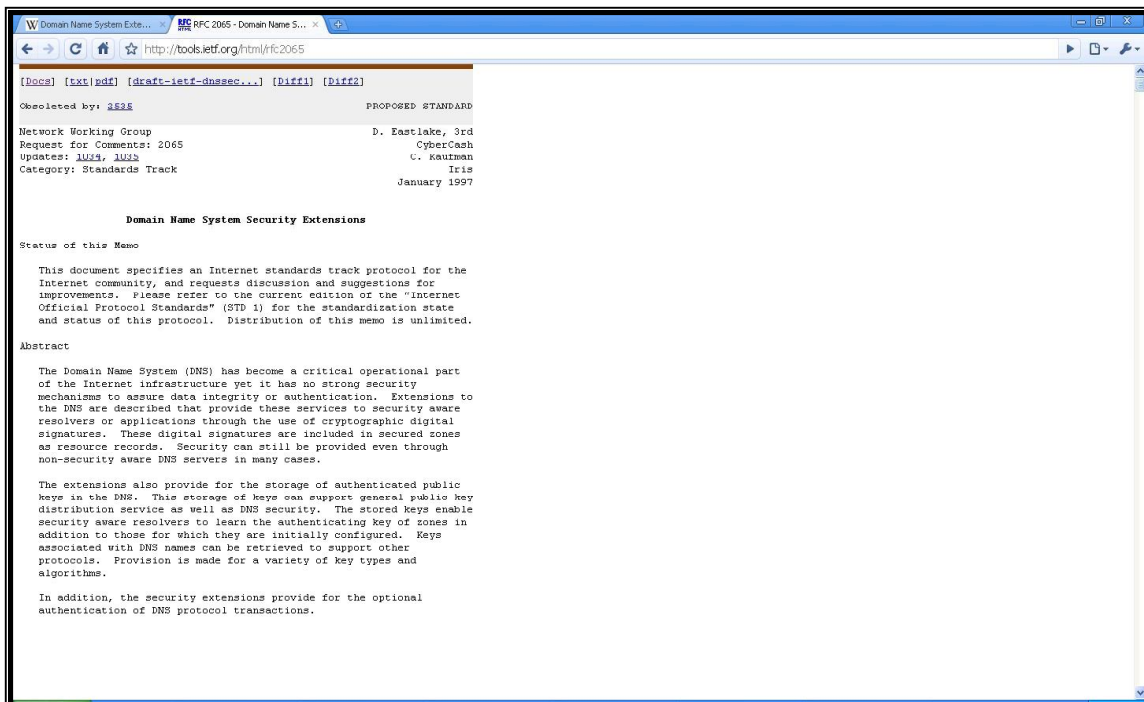
RFC 2845 descripción del protocolo RND SIG

<http://www.ietf.org/rfc/rfc2845.txt>



Primera publicación del protocolo DNSSEC en el RFC 2065

<http://tools.ietf.org/html/rfc2065>





<http://www.cs.jhu.edu/~ateniese/papers/dnssec.pdf>
<http://net.educause.edu/ir/library/pdf/EST1001.pdf>
<http://www.ripe.net/training/dnssec/material/dnssec.pdf>
<http://www.dnssec.net/links>
http://ws.edu.isoc.org/workshops/2008/cctld-ams/Documentation/DNSSEC_Key_maintenance.pdf
<http://www.infoweapons.com/content/why-do-you-need-dnssec>
<http://computerworld.nl/article/11819/wat-is-dnssec.html>
https://st.icann.org/alach-docs/index.cgi?problemas_de_seguridad_del_sistema_de_nombres_de_domino_dns_dentro_del_ambito_de_competencia_de_la_icann_al_alac_st_0309_5_es
http://pedrollo.com.co/pdf/SIC_68_Riesgos%20en%20el%20Sistema%20de%20DNS.pdf
<http://www.intgovforum.org/cms/2010/Background/Spanish-IGF-Background-Funcionamiento de DNS>
<http://www ldc.usb.ve/~yudith/docencia/ci-4821/PRESENTACION-DNS.pdf>
<http://www.icann.com/es/public-comment/public-comment-201012-es.htm>
<http://www.ripe.net/training/dnssec/material/dnssec.pdf>
ROOT dnssec
<http://www.root-dnssec.org/>
http://www.iis.se/pdf/Routertester_en.pdf
http://www.cert.uy/historico/pdf/DNSSEC_-_parte1_-_CERTificate.pdf
<https://www.iana.org/dnssec/>
