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 Ingeniera, División de ingeniera eléctrica departamento de computación, 2009
- Tanenbaum, Andrew. "SISTEMAS OPERATIVOS MODERNOS", Editorial Prentice Hall, México, 1ª edición, 1993.

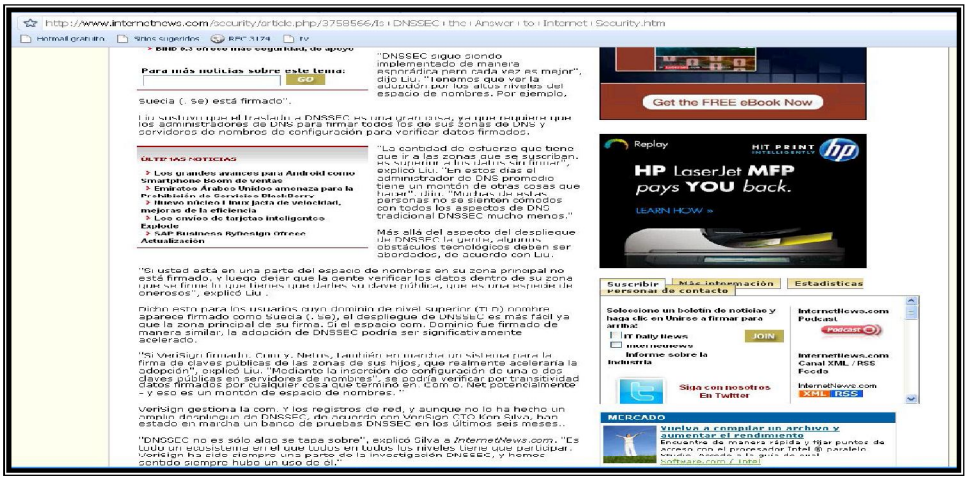
LISTA DE FIGURAS

- 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

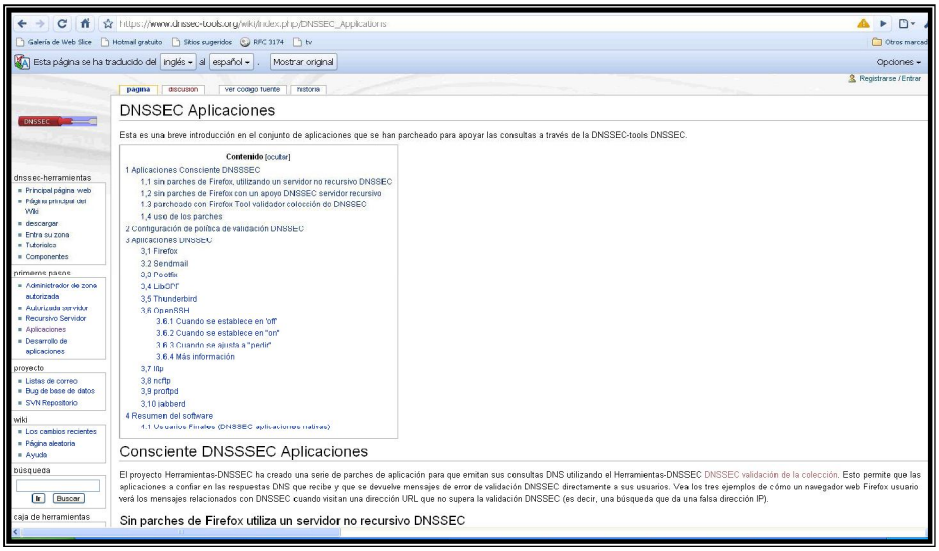
MESOGRAFÍA

Fuente 8 de Junio del 2010

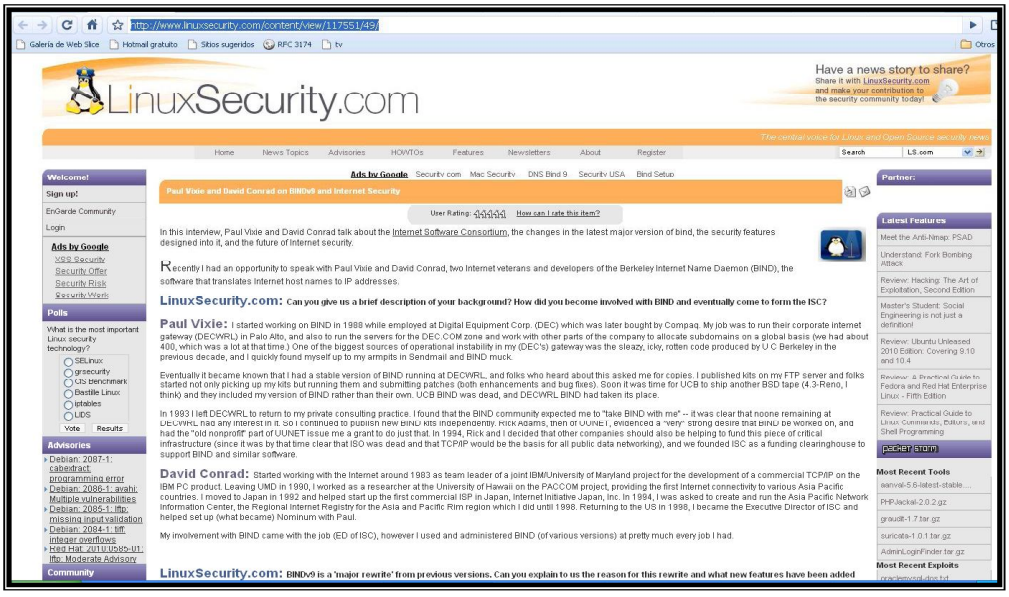
http://www.internetnews.com/security/article.php/3758566/Is+DNSSEC+the+Answer+to+Internet+Security.htm



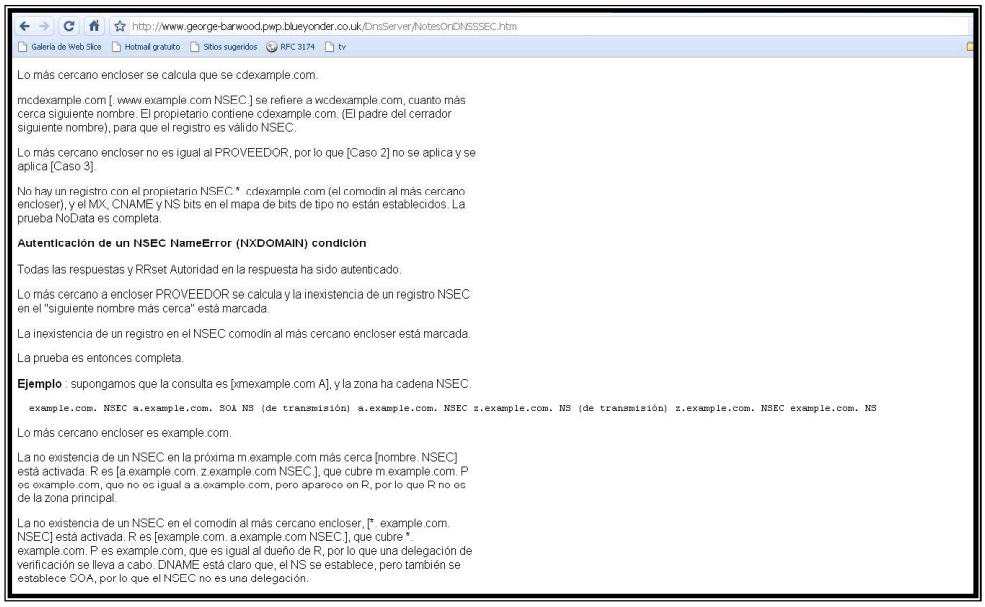
https://www.dnssec-tools.org/wiki/index.php/DNSSEC_Applications



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



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



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

mcdexample.com [. www.example.com NSEC] se refiere a wcdexample.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 el 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 [xmexample.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 os example.com, que no os igual a a.example.com, pero aparoce en R, por lo que R no os 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-dnsext...] [Diff1] [Diff2]

PROPOSED STANDARD

Network Working Group — B. Laurie
Request for Comments: 5155 — G. Sisson
Category: Standards Track — R. Arends
Nominet
D. Blacka
VeriSign, Inc.
February 2008

DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

Status of This Memo

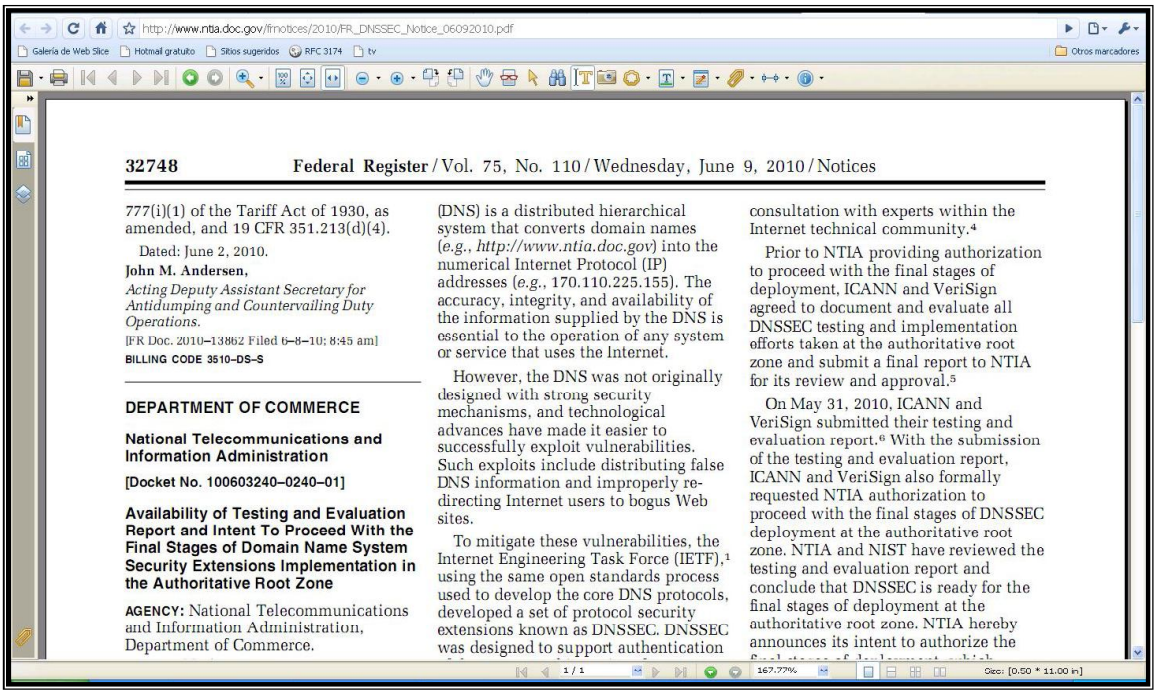
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution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

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. 2010–13862 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.

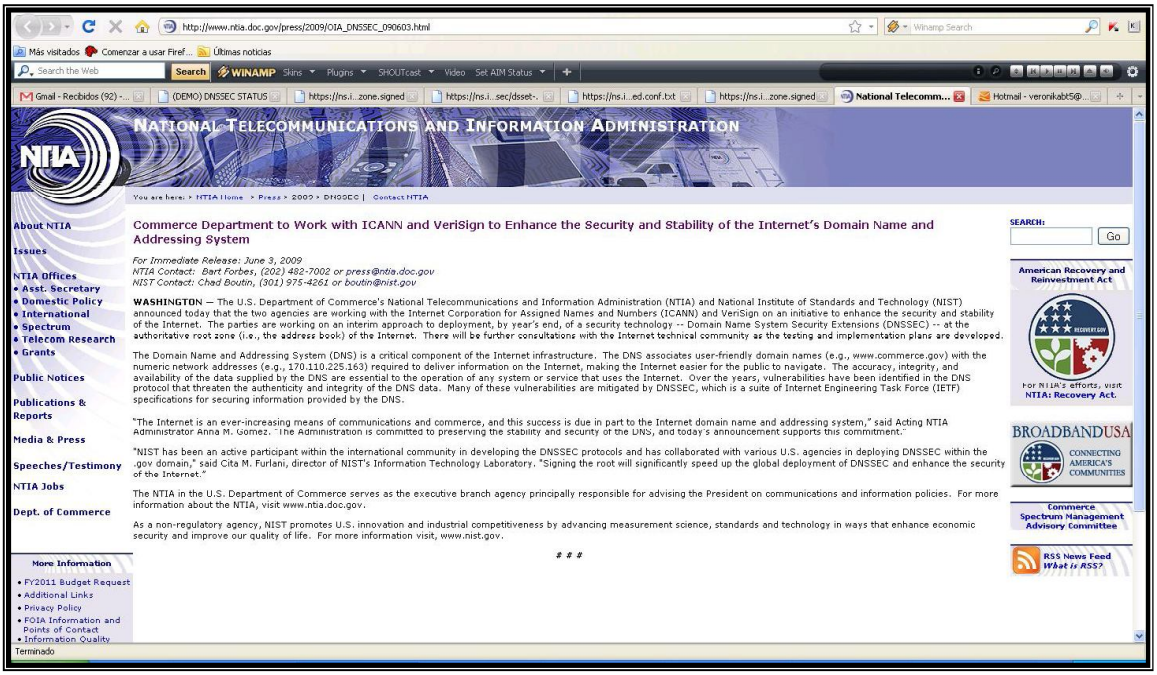
To mitigate these vulnerabilities, the Internet Engineering Task Force (IETF),[1] using the same open standards process used to develop the core DNS protocols, developed a set of protocol security extensions known as DNSSEC. DNSSEC was designed to support authentication

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

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.

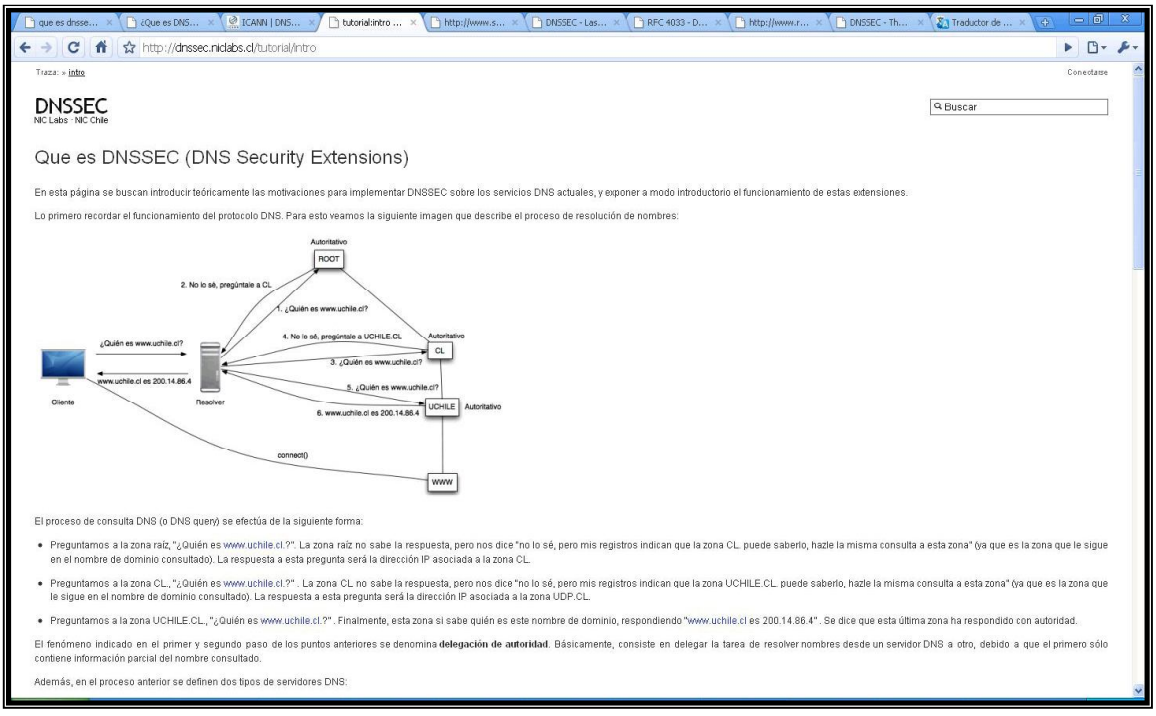
As a non-regulatory agency, NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. For more information visit, www.nist.gov.

# # #

13 de julio del 2010

Descritpcion breve de que es dnssec http://teleobjetivo.org/blog/que-es-dnssec.html

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

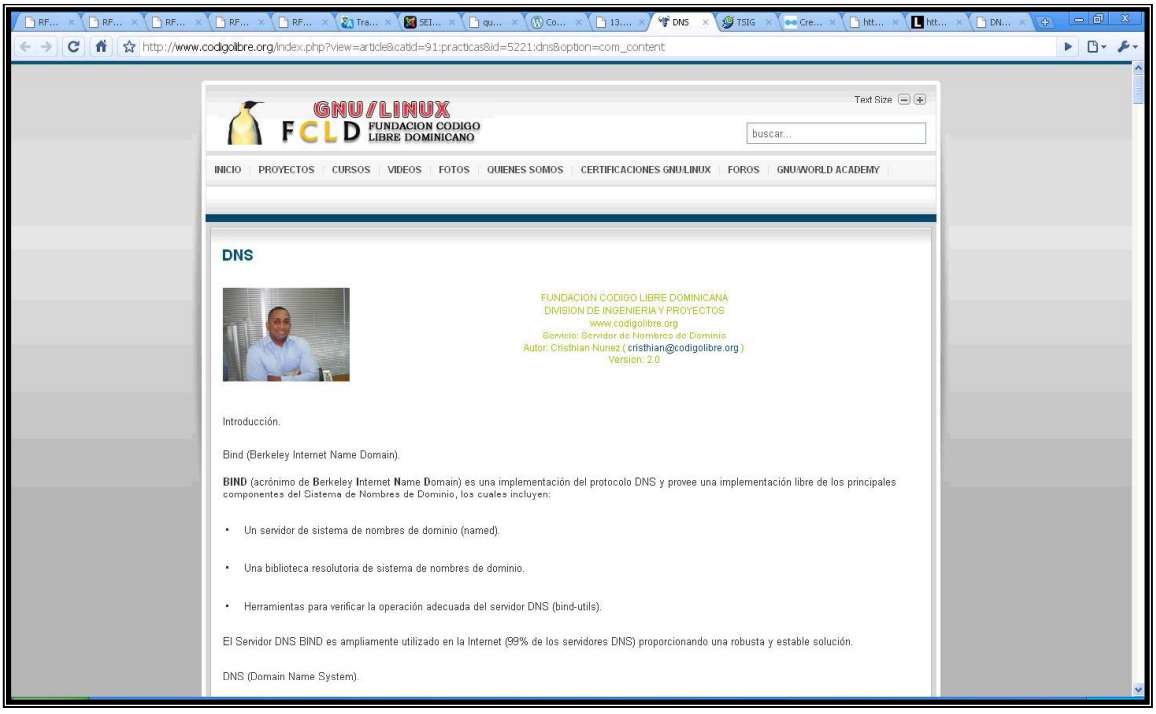


http://www.saulo.net/des/DNSSEC-pre.pdf

Descripción de dnssesc con la implementación explicada paso a paso

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

Como configurar un dns y los componentes que tiene



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

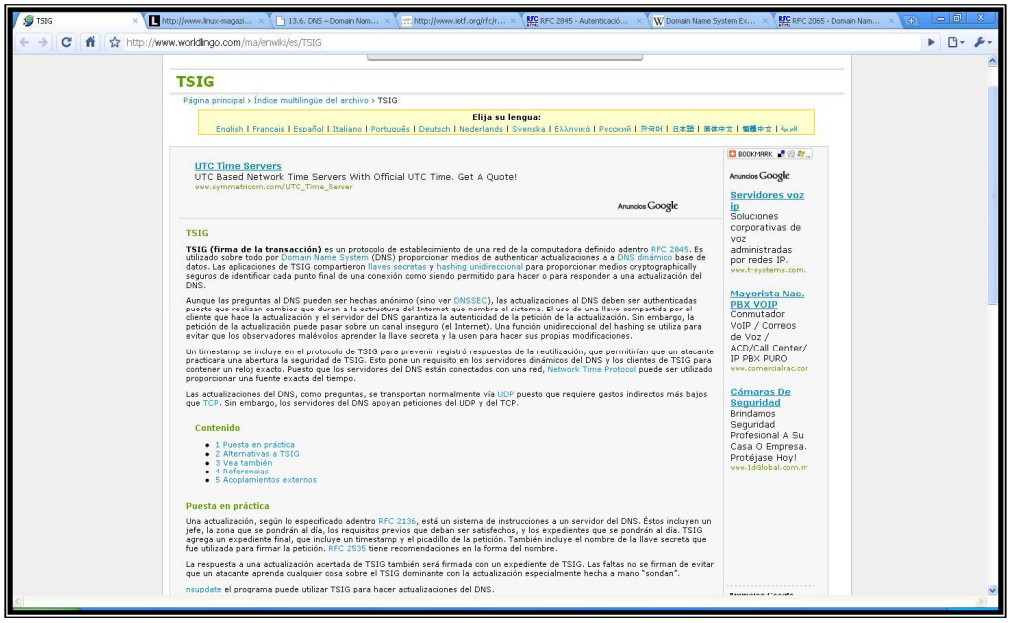
http://www.eluniversal.com.mx/articulos/59265.html

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

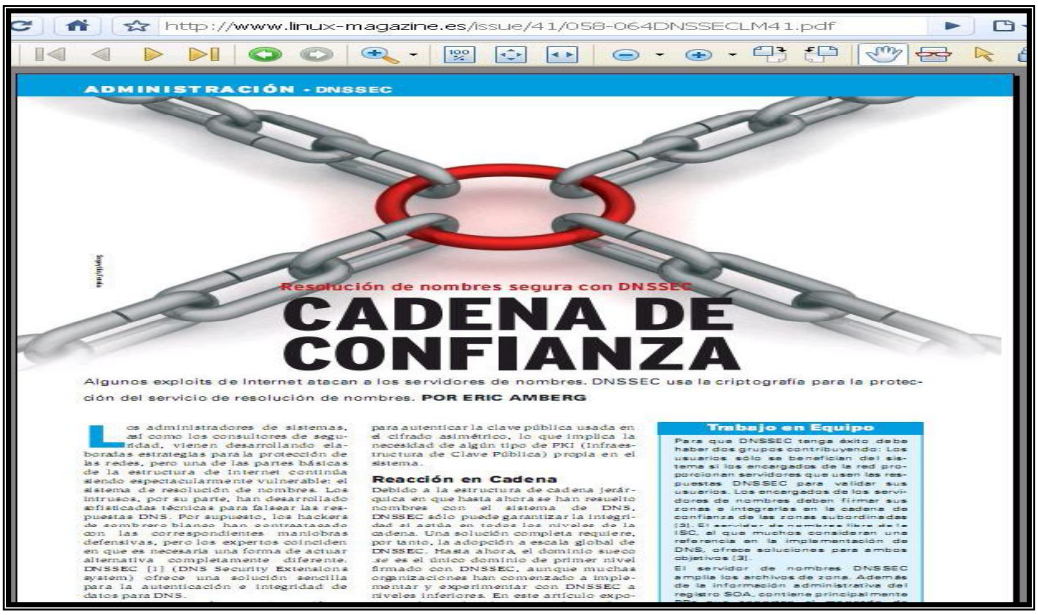
Descripción del protocolo TSIG http://www.worldlingo.com/ma/enwiki/es/TSIG



DNSSEC cadenas de confianza publicación que presenta el cómo funciona DNSSEC

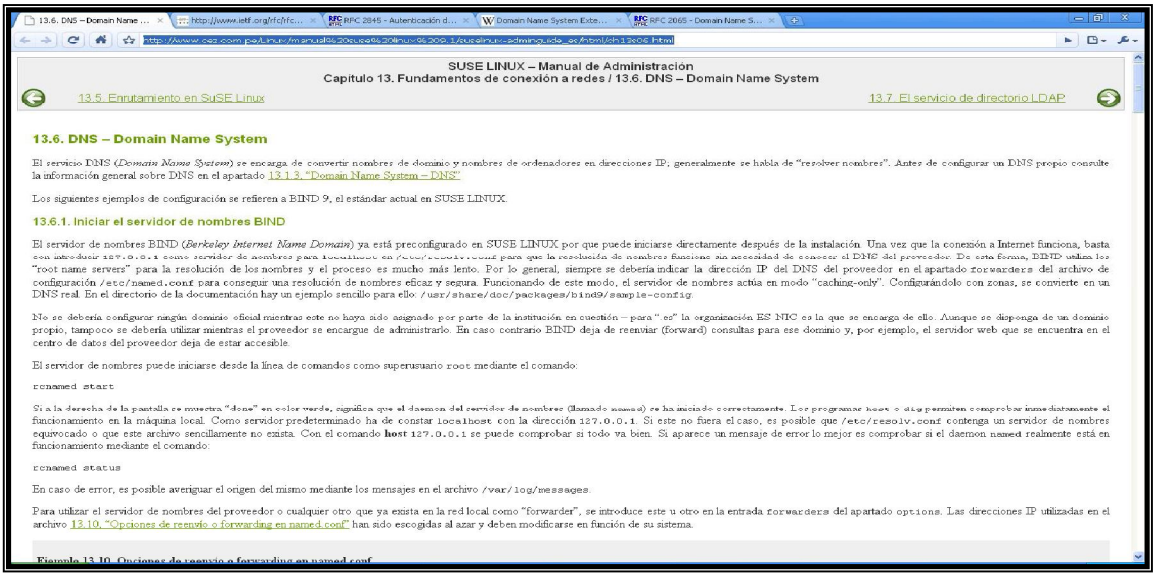
http://www.linux-magazine.es/issue/41/058-064DNSSECLM41.pdf

2 de julio del 20 10



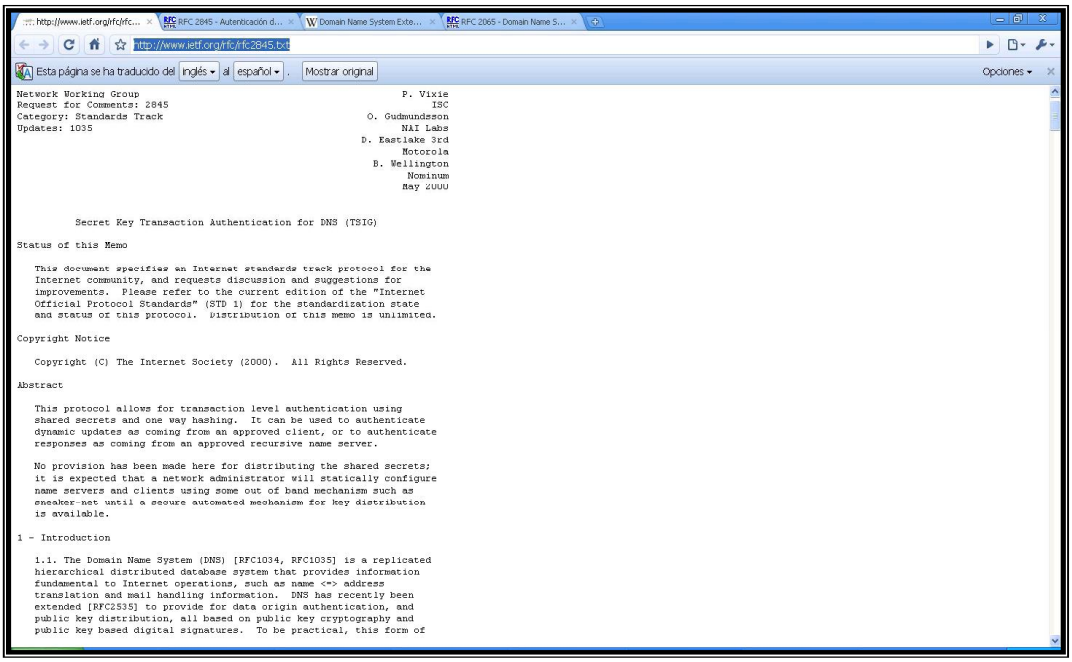
Descripción del DNS

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



RFC 2845 descripción del protocolo RNDSIG

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



Network Working Group P. Vixie
Request for Comments: 2845 ISC
Category: Standards Track O. Gudmundsson
Updates: 1035 NAI Labs
D. Eastlake 3rd
Motorola
B. Wellington
Nominum
May 2000

Secret Key Transaction Authentication for DNS (TSIG)

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 or this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

This protocol allows for transaction level authentication using shared secrets and one way hashing. It can be used to authenticate dynamic updates as coming from an approved client, or to authenticate responses as coming from an approved recursive name server.

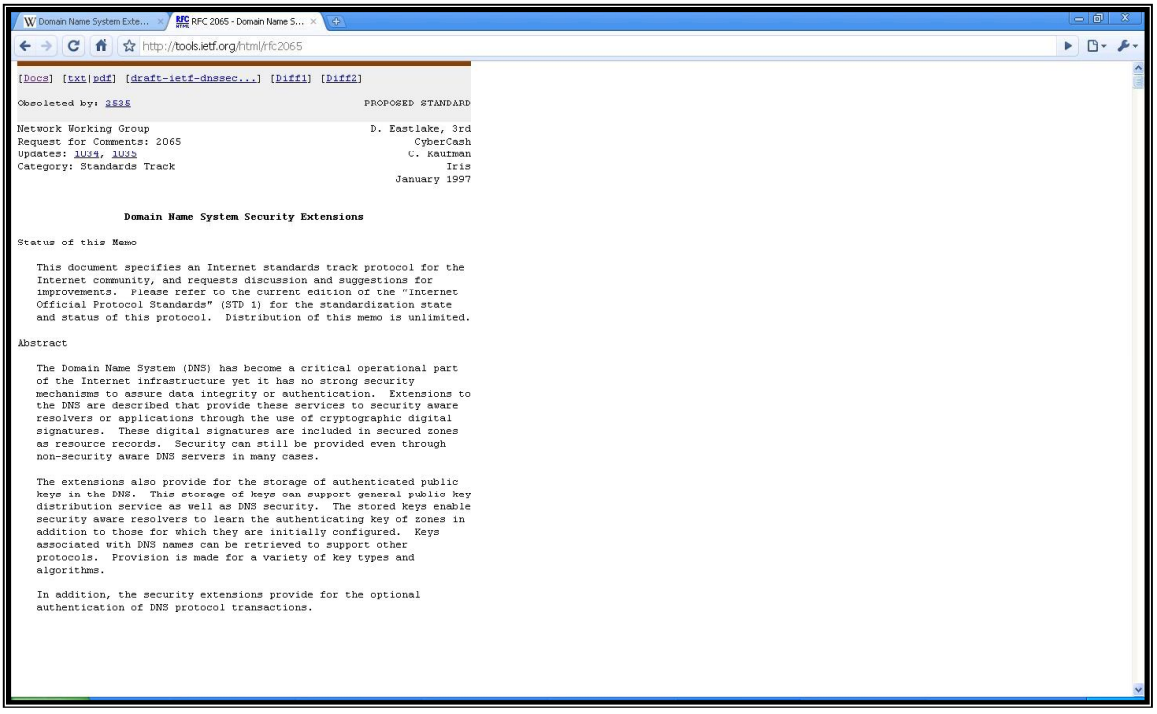
No provision has been made here for distributing the shared secrets; it is expected that a network administrator will statically configure name servers and clients using some out of band mechanism such as sneaker-net until a secure automated mechanism for key distribution is available.

1 - Introduction

1.1. The Domain Name System (DNS) [RFC1034, RFC1035] is a replicated hierarchical distributed database system that provides information fundamental to Internet operations, such as name <=> address translation and mail handling information. DNS has recently been extended [RFC2535] to provide for data origin authentication, and public key distribution, all based on public key cryptography and public key based digital signatures. To be practical, this form of

Primera publicación del protocolo DNSSEC en el RFC 2065

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



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

Obsoleted by: 2535 PROPOSED STANDARD

Network Working Group D. Eastlake, 3rd
Request for Comments: 2065 CyberCash
Updates: 1034, 1035 C. Kaufman
Category: Standards Track Iris
January 1997

Domain Name System Security Extensions

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 (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication. Extensions to the DNS are described that provide these services to security aware resolvers or applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can still be provided even through non-security aware DNS servers in many cases.

The extensions also provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution service as well as DNS security. The stored keys enable security aware resolvers to learn the authenticating key of zones in addition to those for which they are initially configured. Keys associated with DNS names can be retrieved to support other protocols. Provision is made for a variety of key types and algorithms.

In addition, the security extensions provide for the optional authentication of DNS protocol transactions.

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/alac-docs/index.cgi?problemas_de_seguridad_del_sistema_de_nombres_de_dominio_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/