Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en la Universidad Nacional de Loja

Gabriela Espinoza Ami, Luis Chamba Eras[a]

[a] Carrera de Ingeniería en Sistemas, Universidad Nacional de Loja, Ciudad Universitaria Guillermo Falconí Espinosa "La Argelia" Loja, Ecuador
gpespinozaa@unl.edu.ec, lachamba@unl.edu.ec

Resumen. El presente artículo se basa en un estudio sobre las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) aplicado en comunidades virtuales de aprendizaje de la Universidad Nacional de Loja, para validar la autenticidad y la integridad de los datos del Sistema de Nombres de Dominio (DNS). Durante este estudio se efectuó un análisis del estado del arte del DNSSEC de las instituciones de educación superior a nivel internacional, nacional y local. Se desarrolló una virtualización de los servidores DNS de la universidad, en los que se realizó las configuraciones necesarias para el funcionamiento de DNSSEC, a través del proceso de firma de las zonas DNS mediante las claves públicas y privadas que establecen una cadena de confianza. Además se configuró un servidor de nombres recursivo que almacenó las claves públicas de los dominios firmados creando de esta forma anclas de confianza para validar las respuestas por parte de los usuarios. Como resultado de estos procedimientos se estableció una isla de confianza mediante los dominios firmados. Finalmente, se utilizó el complemento DNSSEC Validator que permitió comprobar que los dominios de la universidad a utilizar por las comunidades virtuales de aprendizaje están asegurados con DNSSEC y posteriormente replicar estos resultados a las universidades de ecuador.

Palabras Clave: DNSSEC, cadena de confianza, anclas de confianza, islas de confianza.

1 Introducción

Las instituciones de educación superior representan un microcosmos de la Internet como un todo, repleto de ataques cibernéticos, algunos de los cuales podrían ser impedidos por una combinación de firma y validación DNSSEC; en la parte académica, DNSSEC se suma a la autenticidad del producto del trabajo académico [1].

1.1 DNSSEC en comunidades virtuales de aprendizaje

Las comunidades virtuales de aprendizaje proporcionan el ambiente idóneo para que el alumno se inicie en la comunicación virtual con otros congéneres con los cuales comparte información [2], en donde la utilización de DNSSEC puede contribuir a combatir los ataques de suplantación de identidad, ataques contra la integridad de la información y el riesgo de que los usuarios sean redirigidos hacia cualquier sitio web inseguro o no deseado.

DNSSEC es un conjunto de especificaciones técnicas para salvaguardar ciertos tipos de información proporcionada por el DNS, que pretende proteger a los usuarios de las comunidades virtuales de aprendizaje contra cierto tipo de riesgos y ataques maliciosos mediante la firma digital de la información usando algoritmos de cifrado criptográficos de clave pública/privada, esto significa que la información es cifrada con la clave privada y validada con la clave pública, tal y como lo realizan los procesos de cifrado de clave pública/privada; con lo que el usuario puede tener certeza acerca de su validez [3].

Con la implementación de DNSSEC se señalará automáticamente que los usuarios han sido dirigidos a comunidades virtuales de aprendizaje reales que pretendían visitar, mitigando el riesgo de que sean inconscientemente raptados o erróneamente dirigidos a sitios falsos que pudieran poner en riesgo su seguridad; con lo que se podrá establecer una cadena de confianza en las comunidades virtuales de aprendizaje de cada institución de educación superior, en donde se podrá garantizar la procedencia de contenidos creados en este tipo de ambientes de aprendizaje [4].

1.2 Consecuencias en la educación superior

Los riesgos derivados del DNS y los beneficios de implementar DNSSEC tienen un significado especial para la educación superior. Se espera que las universidades sean "buenos ciudadanos de Internet" y den ejemplo en los esfuerzos para mejorar el bienestar público. Dado que los usuarios tienden a confiar en determinados ámbitos como el dominio *.edu*, más que otros, las expectativas para la fiabilidad de los sitios web de la universidad son altas. En la medida en que las instituciones de educación superior dependen de su reputación, DNSSEC es una vía para evitar algunos de los tipos de incidentes que pueden dañar el prestigio de una universidad.

En términos más concretos, las instituciones de educación superior almacenan enormes cantidades de información sensible (incluyendo la información personal y financiera para los estudiantes y otras personas, información médica y datos de investigación), y se mantienen activos en línea en las comunidades virtuales de aprendizaje cuyo acceso debe ser restringido efectivamente. Los ataques DNS resultan en contraseñas robadas, e-mail alterado (que a menudo es el canal para las comunicaciones oficiales), la exposición al malware, y otros problemas; por lo que DNSSEC puede ser una parte importante de una estrategia de seguridad cibernética de base amplia [5].

Razones por las cuales se ha realizado un estudio para la implementación de DNSSEC, utilizando un ambiente virtualizado donde se configura los servidores DNS de la universidad y se realiza el aseguramiento de las zonas DNS, así como también un servidor de nombres recursivo que valida las respuestas efectuadas por los usuarios; además se emplea como herramienta de validación el plugin DNSSEC Validator que comprueba la existencia de DNSSEC en las zonas aseguradas.

2 Métodos

Durante el desarrollo de esta investigación, se utilizó una metodología de resolución de problemas que se organiza en siete etapas descritas a continuación:

Etapa 1: Identificar el problema: en esta etapa se visualizó el problema de investigación, el mismo que se refiere a la comprobación de la seguridad en el protocolo DNS en cuanto a la validación de la autenticidad y la integridad de los datos transferidos en las comunidades virtuales de aprendizaje de la universidad.

Etapa 2: Explicar el problema: durante esta etapa se indagó el estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior, partiendo de la recogida de información tanto a nivel internacional, nacional y local, de forma específica en la Universidad Nacional de Loja y Universidad Técnica Particular de Loja; con el propósito de determinar las principales vulnerabilidades del DNS, lo que permitió avanzar en un consenso más firme y extendido sobre la naturaleza del problema.

Etapa 3: Idear las estrategias alternativas de intervención: en esta etapa se propuso las soluciones en cuanto a la manera de proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de la universidad, con lo cual se obtuvo las opciones factibles de aplicación.

Etapa 4: Decidir la estrategia: partiendo de las estrategias abordadas en la etapa anterior, esta fase afirmó la mejor solución que permitió analizar el estado del arte del Sistema de Nombres de Dominio de la universidad, y proteger los datos DNS que se transfieren en las comunidades virtuales de aprendizaje, con lo que se logró aportar seguridad en la autenticación y procedencia de datos en las comunidades virtuales de aprendizaje transferidos por el protocolo DNS.

Etapa 5: Diseñar la intervención: en esta etapa se estableció las acciones, plazos y recursos, para la realización de una serie de actividades y tareas concernientes al análisis del estado del arte del DNS y la protección de los datos DNS de las comunidades virtuales de aprendizaje de la universidad.

Etapa 6: Desarrollar la intervención: durante esta fase se realizó la revisión del estado del arte del sistema DNS en la universidad y las configuraciones y validaciones necesarias para la protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de la universidad.

Etapa 7: Evaluar los logros: Finalmente en esta etapa se analizó los resultados obtenidos durante el proceso de implementación, con lo que se determinó la eficiencia de los beneficios aportados por la tecnología DNSSEC en las comunidades virtuales de aprendizaje de la universidad, que se redactan en el apartado de discusión.

3 Resultados

3.1 Análisis del estado del arte del Sistema de Nombres de Dominio de las instituciones de educación superior

3.1.1 Recopilar información a nivel internacional

De acuerdo a la iniciativa DNSSEC Deployment [1], entre las principales instituciones de educación superior que han implementado DNSSEC, se encuentran:

- Colegio Técnico Acadiana (acadiana.edu)
- Colegio Baker (baker.edu)
- Universidad Berkeley de California (berkeley.edu)
- Universidad Bucknell (bucknell.edu)
- Colegio de Comunidad Técnica Central de Louisiana (cltc.edu)
- Universidad Carnegie Mellon (carnegiemellon.edu, cmu.edu)
- Universidad de Colorado Mesa (coloradomesa.edu, mesa.edu)
- Universidad Cal Poly Pomona (csupomona.edu)
- Universidad China de Hong Kong (cuhk.edu)
- Universidad DeSales (desales.edu)
- Universidad Estatal de Fort Hays (fhsu.edu)
- Colegio Técnico Flint Hills (fhtc.edu)
- Colegio Técnico Gateway (gtc.edu)
- Academia Nacional de Diseño de Karlsruhe (hfg.edu)
- Colegio Georgia Highlands (highlands.edu)
- Universidad de Indiana (indiana.edu, iu.edu)
- Colegio Técnico de Indiana (indianatech.edu)
- Universidad de Indiana Bloomington (iub.edu)
- Universidad de Indiana - Universidad de Purdue Indianápolis (iupui.edu)
- Laboratorio de Física Aplicada de la Universidad Johns Hopkins (jhuapl.edu)
- Instituto Kestrel (kestrel.edu)
- Comunidad de Luisiana y Sistema de Colegios Técnicos (lctcs.edu)
- Universidad Estatal de Luisiana (lsu.edu)
- Colegio Técnico de Luisiana (ltc.edu)
- Universidad Estatal de Westfield (ma.edu)
- Universidad de Millikin (millikin.edu)
- Comunidad Estatal de Minnesota y Colegio Técnico (minnesota.edu)
- Universidad de Monmouth (monmouth.edu)
- Universidad de Missouri de Ciencia y Tecnología (mst.edu)
- Universidad del Norte de Arizona (nau.edu)
- Colegio de Comunidad Técnica de Northshore (northshorecollege.edu)
- Colegio Técnico del Noroeste de Louisiana (nwltc.edu)
- Universidad de Oxford (oxford-university.edu)

- Universidad del Pacífico (pacificu.edu)
- Universidad de Pensilvania (penn.edu, upenn.edu)
- Centro de Supercomputación de Pittsburgh (psc.edu)
- Colegio Comunitario de Richland (richland.edu)
- Universidad Rockefeller (rockefeller.edu)
- Colegio Técnico Sur Central de Luisiana (scl.edu)
- Escuela de Minas y Tecnología de Dakota del Sur (sdsmt.edu)
- Universidad Adventista del Sur (southern.edu)
- Universidad del Sur de Utah (suu.edu)
- Universidad de Tilburg (tilburguniversity.edu)
- Instituto Tata de Ciencias Sociales (tiss.edu)
- Universidad Estatal de Truman (truman.edu)
- Universidad de Arkansas en Little Rock (ualr.edu)
- Corporación Universitaria para el Desarrollo de Internet Avanzado (ucaid.edu)
- Universidad Riverside de California (ucr.edu)
- Universidad de Iowa (uiowa.edu)
- Universidad del Condado de Maryland Baltimore (umbc.edu)
- Universidad de Stuttgart (uni-stuttgart.edu)
- Universidad Pompeu Fabra (upf.edu)
- Universidad de Valencia (valencia.edu)
- Colegio Washington & Jefferson (washjeff.edu)
- Universidad Estatal de Weber (weber.edu)

En Portugal, conforme a la asociación DNSSEC .PT [6] algunas instituciones de educación superior han firmado sus dominios con DNSSEC, mejorando así la seguridad de sus sitios mediante la aplicación de las mejores prácticas. Estas instituciones son:

- Instituto Politécnico de Bragança (www.ipb.pt)
- Instituto Politécnico de Cávado y Ave (www.ipca.pt)
- Instituto de Estudios Superiores de Fafe (www.iesfafe.pt)
- Instituto Tecnológico y Nuclear (www.itn.pt)
- Universidad Abierta (www.uaberta.pt)
- Universidad Autónoma de Lisboa (www.universidade-autonoma.pt)
- Universidad del Atlántico (www.uatlantica.pt)
- Universidad de Évora (www.uevora.pt)
- Universidad de Madeira (www.uma.pt)
- Universidad de Lisboa (www.ul.pt)

Resaltando como casos de éxito a la Universidad de Pensilvania [7] y la Universidad Pompeu Fabra [8].

3.1.2 Recopilar información a nivel nacional

Actualmente en el Ecuador ninguna institución de educación superior ha realizado el firmado de las zonas DNS con DNSSEC, con lo cual podrían enfrentarse a los riesgos derivados del DNS, debido a que las instituciones de educación superior almacenan enormes cantidades de información sensible y se mantienen activos en línea en las comunidades virtuales de aprendizaje cuyo acceso debe ser restringido efectivamente.

3.1.2.1 Recopilar información sobre TELCONET S.A.

La empresa privada TELCONET, operadora de comunicaciones corporativas y proveedora de servicios de internet en Ecuador, según los reportes de los laboratorios del Registro Regional de Internet para la región de Asia Pacífico (APNIC), no provee resolutores de validación DNSSEC [9]; es decir que no ha habilitado DNSSEC en sus servidores de nombres recursivos por lo que no permite que sus usuarios puedan verificar la autenticidad de las respuestas que otorga la zona.

3.1.3 Recopilar información a nivel local

3.1.3.1 Recopilar información en la Universidad Nacional de Loja

En la Universidad Nacional de Loja no se ha realizado la implementación de la tecnología DNSSEC, mecanismo que resulta conveniente desarrollar, ya que los usuarios del dominio de la universidad que se encuentran fuera de la ciudad como en Zapotepamba y la Quinta Experimental "El Padmi" podrían intercambiar información confidencial teniendo seguridad de que es la real; además en el caso de la Modalidad de Estudios a Distancia (MED) se tendrá la confianza de la información en cuanto a pagos bancarios que deben realizar.

3.1.3.2 Recopilar información en la Universidad Técnica Particular de Loja

En la Universidad Técnica Particular de Loja no se ha efectuado el despliegue de la tecnología DNSSEC, procedimiento que es beneficioso implementar, porque permitiría dar una solución integral a los ataques concernientes al DNS, y podría formar parte del proyecto de seguridad perimetral que se está llevando a cabo en la universidad.

3.2 Protección de los datos DNS que se transfieren en las comunidades virtuales de aprendizaje de la universidad

3.2.1 Instalación y configuración de los servidores DNS maestros

La instalación de los servidores DNS se realizó en máquinas virtuales mediante la utilización del servidor DNS de código abierto BIND9 [10] y sus paquetes dependientes, lo cual se efectuó a través de la consola del sistema operativo Debian 7.

La configuración de los servidores DNS se efectuó de forma virtualizada debido a que el dominio de la Universidad Nacional de Loja se encuentra almacenado en los servidores DNS de TELCONET, pero este proveedor aún no ha desplegado DNSSEC en sus zonas, por lo que no podría almacenar los registros DNSKEY de la universidad y de esta manera los usuarios que realicen una consulta DNS sobre este dominio no tendrán la seguridad de que la información se encuentra autenticada.

Las configuraciones que se establecieron para los servidores de la universidad se muestran de forma gráfica en la Figura 1, las mismas que son las siguientes:

- **Sitio web**
  - Dirección IP del servidor: **192.168.1.30**
  - Nombre del servidor: **unl**
  - Dominio a crear: **unl.edu.ec**
- **Comunidad virtual de aprendizaje**
  - Dirección IP del servidor: **192.168.1.35**
  - Nombre del servidor: **cvaunl**
  - Dominio a crear: **cva.unl.edu.ec**

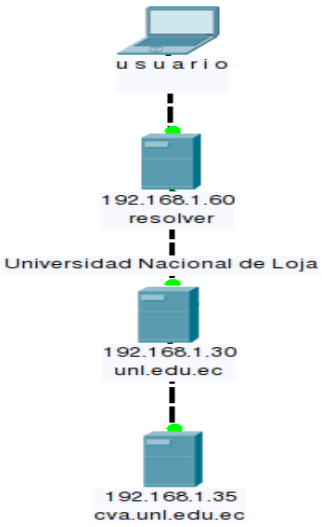

Fig. 1. Esquema DNS.

Para el esquema de la Figura 1, se efectuó los siguientes pasos:

1. Instalar el servidor DNS Bind9.
2. Modificar el archivo */etc/resolv.conf* para que el servidor resuelva las peticiones DNS.
3. Editar el archivo */etc/bind/named.conf.local* donde se asigna las zonas y el fichero en el que se encuentran.
4. Crear el archivo */etc/bind/db.unl.edu.ec* donde se configura la zona directa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs.
5. Crear el archivo */etc/bind/db.192.168.1* donde se configura la zona inversa agregándole los tiempos de espera, refrescar, reintentar, expirar, de vida y las traducciones de los nombres de equipo y las IPs.
6. Reiniciar el servicio.

3.2.2 Aseguramiento de la zona DNS

Las zonas *unl.edu.ec* y *cva.unl.edu.ec* han sido firmadas y su clave se ha configurado en un servidor de nombres recursivo validador, formándose una "isla" de confianza.

Debido a que las zonas *ec.* y *edu.ec.,* aún no están firmadas, cualquier dominio que tenga como su zona padre a uno de ellos y despliegue DNSSEC formará una isla de confianza como se muestra en la Figura 2.

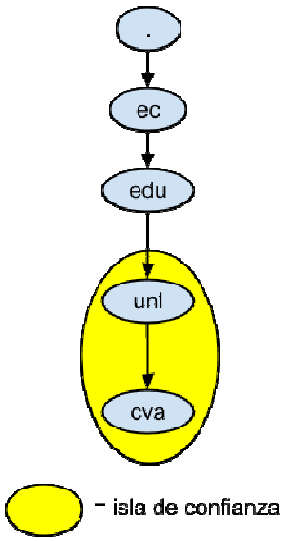

Fig. 2. Isla de confianza.

Para crear una "isla" de confianza se firmó las zonas y se distribuyó los "puntos de entrada seguros" al servidor de nombres recursivo [11]. Después de la creación de los

pares de claves utilizados para la firma y validación se firmó los datos de la zona para la universidad y se configuró el promotor de almacenamiento en caché en la red de la institución para validar los datos con la clave pública de la misma.

Es así que el aseguramiento de las zonas DNS de la universidad se ilustra de forma gráfica en la Figura 3.

Fig. 3. Esquema del aseguramiento de las zonas DNS.

Para el esquema de la Figura 3, se realizó el siguiente procedimiento:

1. *Configurar servidor autoritativo:* el servidor autoritativo se configuró para soportar DNSSEC.
2. *Crear pares de claves:* se creó una KSK (Key Signing Key) inicial y ZSK (Zone Signing Key) para cada zona para estar asegurado. Estas claves no tienen tiempo de expiración, y pueden ser usadas por el tiempo que se desee. Las partes privadas deben mantenerse en privado y seguras [12].
3. *Insertar las claves de la zona:* al crear pares de claves, estas se las incluyó en el archivo de zona.
4. *Firmar la zona:* una vez que las claves han sido incluidas en el archivo de zona, se prosigue a firmar la zona, para lo cual se utilizó la herramienta dnssec-signzone.

3.2.3 Configuración de un servidor de nombres recursivo para validar las respuestas

Se configuró un servidor de nombres recursivo para validar los datos que el mismo recibe. Los usuarios que utilizan este servidor de nombres recursivo como su resolvedor, sólo recibirán los datos que son ya sea seguros y validados o inseguros. Como resultado, la información segura que no supere la validación, no va a encontrar su camino a los usuarios; ya que al tener un servidor de nombres recursivo validador protege a todos aquellos que lo utilizan como un promotor contra la recepción de datos DNS falsificados.

Mediante la configuración de una clave pública para una zona específica, se le dice al promotor de almacenamiento en caché que todos los datos procedentes de esa zona deben estar firmados con la clave privada correspondiente. La zona actúa como un punto de entrada seguro en el árbol DNS y la clave configurada en el servidor de nombres recursivos actúa como el inicio de una cadena de confianza [11].

En el servidor de nombres recursivo se almacenó las claves KSK (claves públicas) de las zonas firmadas con DNSSEC como se muestra en la Figura 4, para de esta manera crear anclas de confianza.

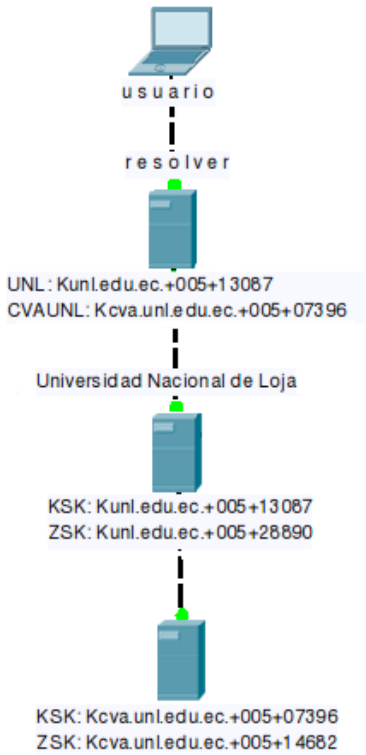

Fig. 4. Esquema del servidor de nombres recursivo con claves KSK.

Para el esquema de la Figura 4, se desarrolló los siguientes pasos:

1. *Configuración del promotor de almacenamiento en caché:* el promotor de almacenamiento en caché se configuró para soportar DNSSEC.
2. *Configurar un ancla de confianza:* un ancla de confianza es una clave pública que se configura como el punto de entrada para una cadena de autoridad [11]. Pero debido a que las zonas padres (*ec.*, *edu.ec.*) aún no están firmadas se configuró múltiples anclas de confianza.
3. *Configurar el registro:* es importante comprobar que la validación está funcionando correctamente, esto se hizo mediante el uso de las facilidades del registro de BIND en la máquina que está configurada como servidor de nombres recursivo validador.

3.3 Validación de DNSSEC

3.3.1 DNSSEC Validator

Es un complemento para navegadores Web que permite comprobar la existencia y validez de los registros de las extensiones de seguridad del DNS (DNSSEC) relativos a los nombres de dominio en la barra de direcciones del navegador. Los resultados de estas comprobaciones se muestran con iconos y textos de información en la barra de direcciones o barra de herramientas de la página [13]. Para la verificación de DNSSEC se instaló este complemento en el navegador Web Mozilla Firefox.

En los servidores de la universidad se comprobó que los dominios *unl.edu.ec* y *cva.unl.edu.ec* están asegurados mediante DNSSEC, como se muestra en las Figuras 5 y 6 respectivamente.

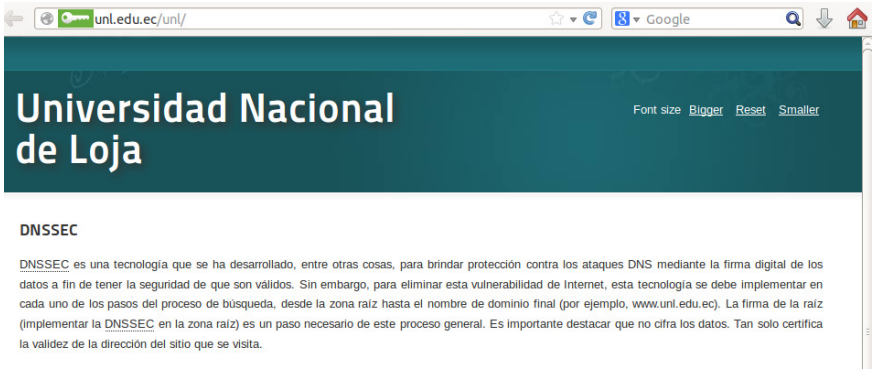

Fig. 5. Validación del dominio unl.edu.ec.

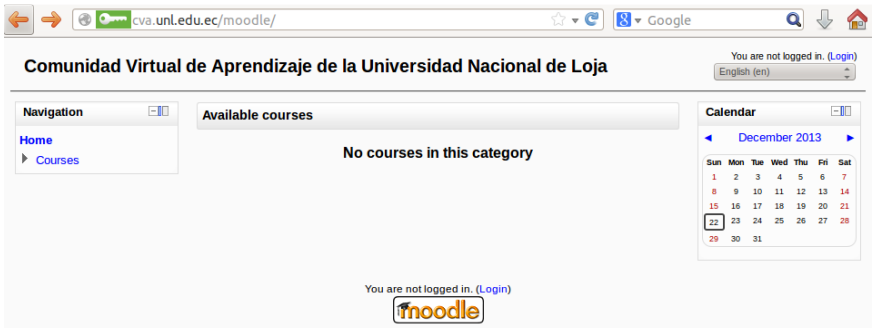

Fig. 6. Validación del dominio cva.unl.edu.ec.

Como se puede observar en las Figuras 5 y 6, el complemento permite saber si el dominio se encuentra firmado con DNSSEC al mostrar un icono en color verde, como es el caso de los dominios *unl.edu.ec* y *cva.unl.edu.ec*, en caso contrario el icono se mostraría con un símbolo en color rojo.

4 Discusión

La implementación de DNSSEC en las universidades fortalece la infraestructura de ambientes de aprendizaje autenticando el origen de los datos y verificando su integridad, así mismo ofrece protección contra los datos provenientes de DNS falsos usando criptografía de clave pública/privada para firmar digitalmente información de dominio; mediante lo cual la suplantación de identidad resulta más difícil y el envenenamiento de caché deja de ser una amenaza.

Mediante el proceso de firma digital, DNSSEC ofrece respuestas autenticadas a las consultas DNS recibidas, es decir que un servidor de almacenamiento de caché de nombres de dominio o incluso un cliente puede validar las respuestas recibidas por el servidor DNS, comprobando la firma de la respuesta recibida contra la clave pública apropiada y de esta forma verificar que los datos DNS no han sido alterados durante su transferencia.

La implementación de DNSSEC en máquinas virtuales que emulan los servidores DNS de la Universidad Nacional de Loja, ha permitido verificar el aseguramiento de los datos DNS que se transfieren en comunidades virtuales de aprendizaje de la misma; para ello se llevó a cabo el aseguramiento de las zonas DNS a través de la generación de pares de claves KSK y ZSK y la configuración de un servidor de nombres recursivo que almacena las claves KSK (claves públicas) de los dominios firmados creando de esta forma anclas de confianza para validar las respuestas por parte de los usuarios. A partir de estos procedimientos realizados se ha establecido una isla de confianza formada por los dominios de la universidad.

Como medio de comprobación, en el navegador Mozilla Firefox de la máquina virtualizada del usuario se ha instalado el plugin DNSSEC Validator que ha permitido demostrar que los dominios están asegurados con DNSSEC.

5 Conclusiones y Trabajos Futuros

El despliegue de DNSSEC en la comunidad virtual de aprendizaje de la universidad garantiza la procedencia de contenidos creados en este tipo de ambientes de aprendizaje y permite mantener comunicaciones digitales fidedignas y confiables para el aprendizaje y la investigación.

Referente al despliegue de las extensiones de seguridad en los dominios .ec y .edu.ec no se registra información de un plan para ser firmados, por lo que, las instituciones que deseen implementar DNSSEC en sus entornos DNS pueden hacer uso del DLV provisto por la Internet Systems Consortium.

La implementación de DNSSEC en todos los dominios de las instituciones de educación superior que pertenezcan al CEDIA permitirá tener islas y archipiélagos de confianza que permitirá autenticar y verificar la información que se genere en sus comunidades virtuales tanto en la academia como en la investigación.

Agradecimientos

La presente investigación forma parte del Trabajo de Titulación de Grado en la Universidad Nacional de Loja: "*Extensiones de Seguridad para el Sistema de Nombres de Dominio aplicadas en comunidades virtuales de aprendizaje de las instituciones de Educación Superior*" y de apoyo del proyecto de Tesis Doctoral en la Universidad del País Vasco: "*Propuesta de un Modelo de Confianza para Comunidades Virtuales de Aprendizaje*".

Los autores desean expresar su agradecimiento a las autoridades de la Universidad Nacional de Loja y el Área de Energía, las Industrias y los Recursos Naturales No Renovables; al personal técnico de la Unidad de Telecomunicaciones e Información y a la planta docente de la Carrera de Ingeniería en Sistemas.

Referencias

1. DNSSEC Deployment: DNSSEC in Higher Education - 1% is not enough. [En línea] link: https://www.dnssec-deployment.org/index.php/2012/03/dnssec-in-higher-education-1-isnt-enough/. Consulta realizada 11-Feb-2014.
2. Edilia Bautista Acosta, Rodolfo Sánchez Reyes: Las comunidades virtuales de aprendizaje en la educación presencial como medio para fomentar el uso de las TIC en los estudiantes de nivel medio superior (Propuesta). [En línea] link: http://www.comie.org.mx/congreso/memoriaelectronica/v10/pdf/area_tematica_07/ponencias/1101-F.pdf. Consulta realizada 11-Feb-2014.
3. Miguel Morillo Iruela: DNSSEC (DNS Security Extensions). Universidad de Castilla-La Mancha. [En línea] link: http://www.dns-sec.es/wp-content/uploads/2010/12/DNSSEC_mmi.pdf. Consulta realizada 11-Feb-2014.
4. .CO Internet S.A.S: Una introducción a DNSSEC. [En línea] link: http://www.cointernet.com.co/sites/default/files/documents/DNSSEC_Informacion_Mar2012_ES.pdf. Consulta realizada 11-Feb-2014.

5. Educause: Things you should know about DNSSEC. [En línea] link: http://net.educause.edu/ir/library/pdf/est1001.pdf. Consulta realizada 11-Feb-2014.
6. DNSSEC.PT: Higher education institutions and R&D sign their domains with DNSSEC. [En línea] link: http://www.dnssec.pt/index.php?lang=en. Consulta realizada 11-Feb-2014.
7. Shirley Ross: University of Pennsylvania Becomes First U.S. University to Deploy DNSSEC (DNS Security). Information Systems and Computing. [En línea] link: http://www.upenn.edu/computing/home/news/2009/1101dnssec.html. Consulta realizada 11-Feb-2014.
8. Joao Damas, José. M Femenia, Antoni Santos Cutando, Silvia Onsurbe Martínez: Despliegues DNSSEC. Information Systems and Computing, Universidad de Valencia, Universidad Pompeu Fabra. [En línea] link: http://www.rediris.es/difusion/publicaciones/boletin/90/ponencia11.A.pdf. Consulta realizada 11-Feb-2014.
9. APNIC: Resolvers by as. Laboratorios APNIC. [En línea] link: http://labs.apnic.net/dnssec/resolvers_by_as.txt. Consulta realizada 28-Oct-2013.
10. Internet Systems Consortium: BIND 9 Administrator Reference Manual. [En línea] link: http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.pdf. Consulta realizada 11-Feb-2014.
11. Olaf Kolkman: DNSSEC HOWTO, a tutorial in disguise. [En línea] link: http://www.nlnetlabs.nl/publications/dnssec_howto/dnssec_howto.pdf. Consulta realizada 11-Feb-2014.
12. Internet Systems Consortium: DNSSEC Look-aside Validation Registry. [En línea] link: https://dlv.isc.org/about/using. Consulta realizada 11-Feb-2014.
13. Martin Straka, Karel Slaný, Ondřej Surý, Ondřej Filip: DNSSEC Validator. CZ.NIC. [En línea] link: https://www.dnssec-validator.cz/. Consulta realizada 11-Feb-2014.