Sexta Conferencia de Directores de Tecnología de Información, TICAL 2016
Gestión de las TICs para la Investigación y la Colaboración
Buenos Aires, 13 al 15 de septiembre de 2016

Incorporación de RAICES[1] a servicio Nrenum.net y DNSSEC dentro de Proyecto Magic

Wilfredo Antonio Bolaños Calderón

Universidad Católica de El Salvador
Santa Ana, El Salvador, Centroamérica
wilfredo@catolica.edu.sv

Resumen. El presente trabajo describe la experiencia en la incorporación de RAICES (Red Avanzada de Investigación, Ciencia y Educación Salvadoreña) al servicio Nrenum.net y DNSSEC del Proyecto Magic de la Unión Europea, del cual red CLARA y otras instituciones lideran. Nrenum es un servicio Enum de usuario mantenido por la red europea GEANT y en la que participan diferentes NRENs. Enum es utilizado para construir infraestructuras de marcación para redes VoIP y de Videoconferencia a nivel mundial, utilizando la infraestructura DNS.

En este marco RAICES se incorpora a este importante proyecto de comunicación global en el que investigadores y académicos alrededor del mundo mejoren su trabajo colaborativo. Luego de un proceso coordinado con red CLARA, en donde se intercambiaron experiencias y competencias. En septiembre de 2015 se delega a El Salvador por medio de RAICES el código nacional 503, siendo el país número 38 en obtenerlo a nivel mundial y el sexto a nivel Latinoamericano.

Posteriormente se asegura en RAICES el servicio de NRENUM por medio del protocolo DNSSEC (DNS Security Extensions), siendo el décimo país a nivel mundial en lograr este objetivo. DNSSEC incorpora firmas criptográficas a las consultas y respuestas y permite a los usuarios detectar información falsa, verifica la integridad y previene diversos ataques o problemas de seguridad relacionados al DNS.

Palabras Clave: NRENUM VoIP DNSSEC DNS MAGIC SEGURIDAD

1 Introducción

El Proyecto Magic financiado por la Unión Europea es un proyecto iniciado en mayo de 2015 y que finalizará en abril de 2017. Magic es liderado por varias instituciones a nivel mundial, entre ellas Red Clara. Su objetivo general es beneficiar las comunidades de ciencia a nivel global mediante servicios y aplicaciones “real-time”.

[1] Red Avanzada de Investigación, Ciencia y Educación Salvadoreña

Uno de los servicios ofrecidos por el proyecto es el NRENUM, el cual es administrado por la red europea GEANT y consiste en un Enum para la academia, el cual es mantenido por la red europea GEANT y en la que participan diferentes RNEIs[2]. Cada RNEI obtiene la delegación de una zona asociada al código del país que representa, en el caso de RAICES de El Salvador, el código asociado es: 503.

ENUM es utilizado para construir infraestructuras de marcación para redes VoIP y de Videoconferencia a nivel mundial, utilizando la infraestructura DNS.

Con Nrenum cada NRENs lleva acabo la asignación de los registros numéricos asociados a los dispositivos de comunicación (VoIP, Videoconferencia) de las instituciones académicas lo que permite tener un directorio telefónico global para el establecimiento de las comunicaciones en done investigadores y académicos alrededor del mundo mejoren su trabajo colaborativo.

2 NRENUM.NET

Cabe señalar que la incorporación de RAICES al proyecto nrenum.net tiene su base y motivación en la previa implementación del servicio de Voz sobre IP (VoIP) en la red, lo que ha permitido la comunicación VoIP entre sus miembros y con otras NRENs de la red CLARA: RNP de Brasil e Innovared de Argentina, con las que se implementó un servicio de comunición de VoIP punto a punto. Posteriormente se participó en el proyecto de CLARA PIT VoIP (Punto de Intercambio de tráfico de Voz sobre IP).

NRENUM es un servicio Enum de usuario mantenido por la red europea GEANT y en la que participan diferentes NRENs. Enum es utilizado para construir infraestructuras de marcación para redes VoIP y de Videoconferencia a nivel mundial, utilizando la infraestructura DNS.

En este marco RAICES se incorpora a este importante proyecto de comunicación global en el que investigadores y académicos alrededor del mundo mejoren su trabajo colaborativo. La incorporación de RAICES se realiza mediante un proceso coordinado con red CLARA, por medio de la RNEI Colombiana: RENATA, en donde se intercambiaron experiencias y competencias.

NRENUM utiliza la recomendación ITU E.164 la cual define las normas y estructuras de un número telefónico utilizado a nivel global, definiendo un código de país + Prefijo de la zona + número de terminal. Por ejemplo: +36 52 512901 en donde Código de país: 36 (Hungria); Código de zona: 52; Número de terminal o dispositivo: 512901.

ENUM (E.164 numbering mapping) es un protocolo estándar desarrollado por "Telephone Number Mapping working group" el cual utiliza los sistema de resolución inversa de nombres de los sistemas DNS para traducir los número telefónicos a direcciones URI.

ENUM es compatible con los protocolos de comunicación en tiempo real H.323 y SIP, en cual interactúa con el server ENUM y con el server DNS. El proceso puede

[2] Red Nacional de Educación e Investigación.

observarse en la figura 1.

Fig. 1 Establecimiento de llamada VoIP con NRENUM

En el proceso para establecer una llamada o una videoconferencia, utilizando el servicio NRENUM, ya sea utilizando el protocolo SIP o H.323 se realizan los siguientes pasos:

1. Se realiza la llamada al número +56 52 123456
2. El Gateway SIP o H.323 consulta al servidor NRENUM.NET
3. El Server NRENUM responde oon el URI asociado al número marcado
4. El Gateway SIP o H.323 consulta al DNS el URI
5. El server DNS responde al Gateway con el nombre de dominio y puerto responsable de la conexión SIP o H.323
6. Se realiza la señalización de la llamada y búsqueda del equipo o terminal entre los Gateways
7. Se realiza la comunicación entre los terminales o dispositivos utilizando el protocolo RTP (Real Time Protocol).

2.1 Pasos de Implementación de NRENUM.NET

- Implementar servidores DNS primario y secundario. Se configuran estos servidores para proveer la ENUM para el servicio NRENUM.NET. Es necesario que las IPs de los servidores DNS tengan resolución inversa.
- Crear zona de país. La zona debe estar en el formato X.X.nrenum.net, en donde X.X es el código de país en forma inversa. En el caso de El Salvador, se procede a crear la zona 3.0.5.nrenum.net con los registros necesarios: A, NS, MX, NAPTR (Name Authority Pointer, el cual convierte un número E.164 a una dirección URI).
- Registro de números (dispositivos). Consiste en agregar en el archivo de la zona los registros NAPTR (Name Authority Pointer). Se necesita agregar manualmente un registro NAPTR por cada dispositivo o terminal (por ejemplo teléfono IP o equipo de videoconferencia). Se procede entonces a agregar los registros al archivo /etc/bind/3.0.5.nrenum.net de esta forma:

Para dispositivos protocolo SIP:

```
0.6.6.0.4.8.4.2.3.0.5.nrenum.net. NAPTR 10 101 "u" "E2U+sip"
"!^.*$!sip:50324840660@catolica.edu.sv!" .
```

El anterior registro equivale a: +50324840660 en la URI: sip:50324840660@catolica.edu.sv

Para dispositivos protocolo H.323:

```
9.4.6.0.4.8.4.1.3.0.5.nrenum.net. NAPTR 10 101 "u" "E2U+h323sip"
"!^.*$!h323:50324840660@catolica.edu.sv!" .
```

El anterior registro equivale a: +50324840649 en la URI: h323:50324840649@catolica.edu.sv

- Probar funcionamiento de la zona creada a ser delegada.
- Solicitar a GEANT la delegación de la zona NRENUM.NET, llenando el formulario respectivo y enviándolo a delegations@nrenum.net. Este proceso se hace en coordinación con RENATA.
- Configuración de Gateway SIP/H.323. Luego de la aprobación de la zona delegada, se procede a la configuración del servidor Gateway SIP y/o del Gateway H.323.

Esta configuración incluye la configuración de las políticas de enrutamiento en el Gateway SIP Asterisk por medio del archivo /etc/asterisk/extensions.conf (Ver figura 2)

```
;Política de enrutamiento sistema NRENUM.NET
exten => _+.,1,Set(Sipuri=${ENUMLOOKUP(${EXTEN},sip,1,,e164.arpa)})
exten => _+.,n,GotoIf($["${Sipuri}" != ""]?dial)
exten => _+.,n,Set(Sipuri=${ENUMLOOKUP(${EXTEN},sip,1,,nrenum.net)})
exten => _+.,n,GotoIf($["${Sipuri}" = ""]?lookupfailed)
exten => _+.,n(dial),Dial(SIP/${Sipuri},60,r)
exten => _+.,n(lookupfailed),Hangup()
```

Fig. 2 Política de enrutamiento

- Realización de pruebas de llamadas utilizando número ENUM. Entre los números de prueba se tienen dispositivos SIP y H.323 ubicados en Australia, Hungría, UK, U.S.A.

2.2 Incorporación de RAICES a servicio NRENUM.NET

Luego de haber realizado exitosamente todos los pasos del punto anterior, en septiembre de 2015, NRENUM.NET delega a El Salvador por medio de RAICES el código nacional 503, siendo el país número 38 en obtenerlo a nivel mundial y el sexto a nivel Latinoamericano.

Este proceso fue publicado tanto en el sitio oficial de red CLARA, www.redclara.net, (ver Figura 3) como en el sitio del proyecto MAGIC, http://www.magic-project.eu, (Ver Figura 4).

Fig. 3 Noticia en sitio web de CLARA: Incorporación de RAICES a NRENUM.NET.

Fig. 4 Noticia en sitio web de Proyecto Magic: Incorporación de RAICES a NRENUM.NET.

Ranking en crawler.nrenum.net Como siguiente etapa es muy importante agregar cada uno de los dispositivos o equipos SIP/H.323 que se tienen en la red académico, para que cada uno de ellos tengan el acceso a la red nrenum.net.

Para monitoreo y verificación la red NRENUM tiene un sitio que basado en DNS que escanea y detecta los dispositivos de todo el árbol de nrenum.net, buscando los respectivos registros NAPTR y mostrándolos en el sitio web: HYPERLINK "http://crawler.nrenum.net" http://crawler.nrenum.net

Esta herramienta para realizar un escaneo completo de la red puede tardar hasta una semana para actualizar la tabla.

Este sitio HYPERLINK "http://crawler.nrenum.net" http://crawler.nrenum.net muestra los sitios top de los países con zonas

delegadas así como el número de registros NAPTR o ENUMs detectados (ver figura 5).

top country codes

#	country name	E.164	ENUMs
1.)	Hungary	+36	79711
2.)	Norway	+47	67859
3.)	Portugal	+351	52237
4.)	Brazil	+55	10048
5.)	Spain	+34	6904
6.)	North American Numbering Plan	+1	5034
7.)	Argentina	+54	3462
8.)	Australia	+61	1956
9.)	Italy	+39	932
10.)	Greece	+30	911
11.)	El Salvador	+503	103
12.)	United Kingdom	+44	49
13.)	Netherlands	+31	22
14.)	India	+91	22
15.)	Latvia	+371	21
16.)	Czech Republic	+420	20
17.)	Hong Kong	+852	20
18.)	Belgium	+32	11
19.)	Sri Lanka	+94	10
20.)	New Zealand	+64	10
21.)	France	+33	8
22.)	Colombia	+57	2
23.)	Chile	+56	1
24.)	Romania	+40	1
25.)	Poland	+48	1

Credits: Alexander Mayrhofer - enum.at GmbH

Fig. 5 Sitios Top en base a registros NAPTR (ENUMs) detectados por http://crawler.nrenum.net.

En la figura anterior se puede apreciar que El Salvador, con la zona delegada +503, se encuentra en la posición 11 con 103 registros NAPTR.

3 DNSSEC

Luego de tener asignada la zona (503) en RAICES así como los respectivos registros ENUMs, se procede a asegurarla utilizando protocolo DNSSEC (DNS Security Extensions). En este proceso RAICES se convierte en el décimo país a nivel mundial en lograr este objetivo.

DNS no es un protocolo seguro y en el transcurso de los años se han detectado algunas vulnerabilidades, como por ejemplo la #800113 o conocida como "Kaminsky bug" en honor al investigador que la descubrió y está relacionada al "envenenamiento de caché".

DNSSEC incorpora firmas criptográficas a las consultas y respuestas y permite a los usuarios detectar información falsa, verifica la integridad y previene diversos ataques o problemas de seguridad relacionados al DNS, ya que comprueba que los datos DNS no hayan sido modificados durante su transferencia.

Con DNSSEC se tienen dos tipos de llaves: Key Signing Keys (KSK) y Zone Signing Keys (ZSK) y diferentes algoritmos entre ellos RS/SHA-256.

3.1 Pasos para asegurar la zona con DNSSEC

Se considera asegurar la zona nrenum.net utilizando el sistema operativo GNU/Linux Debian , OpenDNSSEC y BIND:

- Instalar los paquetes y/o dependencias:

```
# apt-get install softhsm opendnssec
```

El comando anterior le instalará adicionalmente los paquetes necesarios como : sqlite3, opendenssec-enforcer, opendnssec-signer, system, libc-bin.

- Copiar el archivo de configuración de la zona

```
# cp /etc/bind/db.3.0.5.nrenum.net /var/lib/opendnssec/unsigned
```

- Inicializar el token

```
# softhsm --init-token --slot 0 --label "OpenDNSSEC"
```

El comando anterior pedirá un PIN el cual se utilizará en el paso posterior.

- Editar el archivo: /etc/opendnssec/conf.xml en donde se incluirá el PIN definido en el paso anterior.
- Editar el archivo "zonelist"

nano /etc/opendnssec/zonelist.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<ZoneList>
  <Zone name="db.3.0.5.nrenum.net">
    <Policy>default</Policy>
<SignerConfiguration>/var/lib/opendnssec/signconf/db.3.0.5.nrenu
m.net.xml</SignerConfiguration>
    <Adapters>
      <Input>
<File>/var/lib/opendnssec/unsigned/3.0.5.nrenum.net.</File>
      </Input>
      <Output>
<File>/var/lib/opendnssec/signed/3.0.5.nrenum.net.</File>
      </Output>
    </Adapters>
```

```
  </Zone>
</ZoneList>
```

En el código anterior se define la ubicación de los archivos: xml, y los de configuración de la zona, tanto sin firmar (unsigned) como el archivo ya firmado (signed).

- Actualizar la "zonelist"

```
# ods-ksmutil update zonelist
```

- Añadir la zona "5.0.3" a la "zonelist"

```
# ods-ksmutil zone add –zone db.3.0.5.nrenum.net
```

- Firmar la zona

```
# ods-signer sign db.3.0.5.nrenum.net
```

- Listar el estado de las llaves, en donde se muestran las llaves KSK y ZSK (Ver figura 6)

```
# ods-ksmutil key list –v
```

Ó si hubieran varias zonas:

```
# ods-ksmutil key list –v –zone db.3.0.5.nrenum.net
```

Fig. 6 Estado de las llaves de la zona db.3.0.5.nrenum.net

- En la figura anterior se observa que la llave KSK se encuentra en estado "ready" y necesita estar en estado "ready" por lo que es necesario notificar al opendnssec-enforcer con el siguiente el comando (ver figura 7):

```
# ods-ksmutil key ds-seen --zone db.3.0.5.nrenum.net --
keytag 6865
```

En donde 6865 corresponde al keytag de la llave KSK.

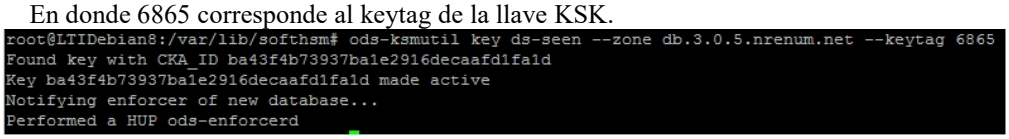

Fig. 7 Notificación a opendnssec-enforcer para activar llave 6885

Luego del anterior comando la llave KSK aparecerá en estado "activa".

- Verificar que se ha creado el archivo de zona "firmado", el cual contiene registros RRSIG, DNSKEY.
- Luego asegurarse de apuntar en el archivo de configuración de BIND (/etc/bind/named.conf.local) hacia la nueva zona firmada:

```
#nano /etc/bind/named.conf.local
 zone "3.0.5.nrenum.net" in {
      type master;
      file "/var/lib/opendnssec/signed/3.0.5.nrenum.net";
 }
```

- - Luego que se ha verificado el procedimiento anterior se exportan las llaves y se envían por un medio seguro hacia la zona superior (parent):

```
#ods-ksmutil key export --ds
```

3.2 Pruebas y monitoreo de la zona asegurada con DNSSEC

Existen pruebas a nivel de consola como en sitios web especializados para verificar

que la configuración esté correcta. Por ejemplo:

```
# dig 127.0.0.0 -t NAPTR 3.0.5.nrenum.net +dnssec
```

Con el comando anterior se apreciará que la zona está configurada con DNSSEC, mostrando los registros RRSIG.

Vía web, el sitio http://dnsviz.net/, posee una herramienta desarrollada originalmente en Sandia National Laboratories y mantenido actualmente por Verisign Labs, realiza un análisis visual de una zona DNSSEC, verificando el árbol completo de ella. Para el caso de la zona de RAICES la uri es: http://dnsviz.net/d/3.0.5.nrenum.net/dnssec/, en donde muestra de forma gráfica las zonas o islas de confianza existentes en el árbol (ver figura 8), incluyendo la zona 3.0.5.nrenum.net con sus registros en estatus "secure" (ver figura 9), detectando y mostrando cualquier error en los registros de las zonas mencionadas.

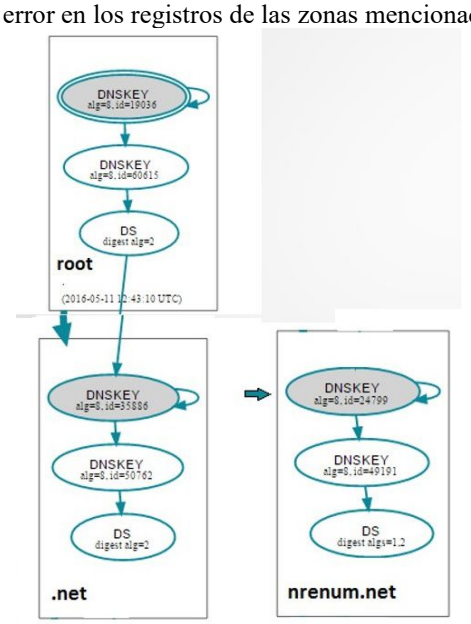

Fig. 8 Zonas "parents" : root ; -- .net ; -- .nrenum.net

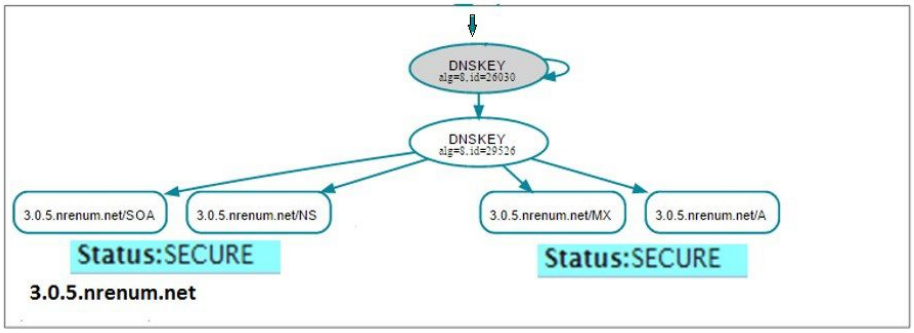

Fig. 9 Zona 3.0.5.nrenum.net de El Salvador (RAICES) asegurada, incluye los registros en estatus "Secure": SOA, NS, MX y A.

Existe otro sitio web que realiza una verificación de zonas DNSSEC: http://portfolio.sidnlabs.nl:8080/ el cual verifica la zona solicitad con sus respectivos registros, mostrando un breve mensaje si la zona está "secure" o si algún tipo de error (ver figura 10).

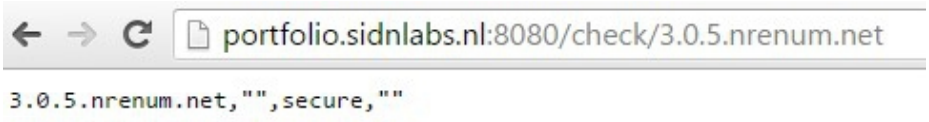

Fig. 10 Verificación de la zona 5.0.3.nrenum.net en el sitio portfolio.sidnlabs.nl

Actualmente están utilizando el servicio DNSSEC con NRENUM 10 países:

Tabla 1. Países utilizando DNSSEC dentrocon de servicio NRENUM.

ZONA	**PAIS**
EUROPA	Inglaterra, República Checa, Hungría, Noruega, Polonia
LATINOAMERICA	El Salvador (RAICES), Colombia (RENATA), PERU (RAAP)
NORTEAMERICA	U.S.A.
AUSTRALIA	Australia

Conclusiones

El servicio NRENUM es un importante proyecto de comunicación global en el que investigadores y académicos alrededor del mundo mejoran su trabajo colaborativo, por lo que es importante que todas las redes Nacionales (NREI) se incorporen a esta importante iniciativa. En el caso de muchas redes nacionales que ya forman parte de este proyecto es vital de que se vaya incrementando el número de dispositivos y terminales SIP/H.323 para lograr un mayor alcance e integración con este proyecto.

El proyecto MAGIC financiado por Unión Europea es una buena oportunidad para lograr incorporarse de la mejor manera, ya que ofrecen una colaboración y motivación por medio de sus miembros responsables.

Por otro lado el asegurar las zonas NRENUM por medio de DNSSEC es una buena práctica que permite a los usuarios del servicio detectar información falsa, verifica la integridad y prevenir diversos ataques o problemas de seguridad relacionados al DNS, garantizando la transparencia, estabilidad y seguridad del servicio.

Es importante que las redes nacionales que ya forman parte del servicio NRENUM incorporen DNSSEC en sus zonas delegadas.

Agradecimientos

Se agradece a la red Colombiana RENATA (Red coordinadora en CLARA de Projecto Magic) por el apoyo y seguimiento en la consecución del presente proyecto,

así como al proyecto Magic de la Unión Europea, a sus colaboradores técnicos, entre ellos a Mihály Mészáros de la red NIIF (http://niif.hu/).

Referencias

1. Corporación Latinoamericana de Redes Avanzadas. CLARA, http://www.redclara.net
2. Proyecto Magic, http://www.magic-project.eu
3. Servicio NRENUM, http://nrenum.net
4. Herramienta DNSVIZ, http://dnsviz.net/
5. SIDN Labs Portfolio Checker, http://portfolio.sidnlabs.nl
6. Vulnerabilidad DNS, http://www.kb.cert.org/vuls/id/800113
7. Algoritmos DNSSEC, https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml
8. Opendnssec Project, https://www.opendnssec.org/
9. Tools Guide Series on DNSSEC, https://net.educause.edu/ir/library/pdf/CSD5928.pdf