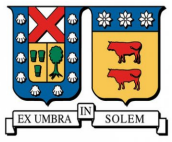


UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE ELECTRÓNICA

Proyecto de Redes de Computadores

DNSCrypt

Presentado por	Alan Bitterlich Alfredo Montenegro Galvarino Sotomayor Enzo Tapia
Fecha	28-09-2015

DNSCrypt

1. Introducción

DNSCrypt es un protocolo que autentica la comunicación entre un cliente DNS y una resolución DNS. Sirve para prevenir la suplantación de la DNS y el espionaje. Usa la técnicas de encriptado para asegurarse que la respuesta proviene desde el *DNS resolver* elegido y que no ha sido manipulada.

Es posible utilizar este protocolo en sistemas operativos tales como Windows, OSX, Android, iOS, BSD y Linux como veremos en este proyecto.

Es importante resaltar que DNSCrypt es un Protocolo de codigo abierto, el cual no está asociado a ninguna compañía ni organización.

DNSCrypt sirve por sobre todo a hacer el Internet un lugar más seguro para sus usuarios.

2. Instalación y Configuración en Linux

Para poder utlizar DNSCrypt en Linux, es necesario seguir los siguientes pasos:

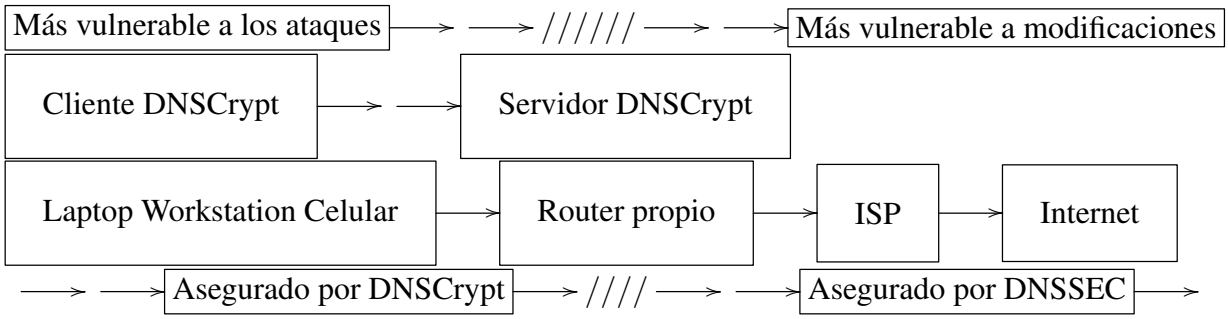
1. Instalar dnscrypt-proxy.

DNSCrypt se implementa típicamente usando un par de Proxies (Cliente y Servidor). En el lado del cliente, DNSCrypt se comporta como un proxy para que los clientes se conecten a él. En vez de utilizar la propia configuración DNS del ISP (Internet Service Provider), es posible utilizar por ejemplo 127.0.0.1 o alguna otra IP para que que el cliente DNSCrypt pueda contactar. El cliente proxy transcribe las consultas normales del DNS en consultas encriptadas del DNS, luego las envía a un servidor proxy DNS el cual verifica las respuestas. Si las respuestas son genuinas, el servidor proxy DNS reenvía las respuestas al cliente DNS.

Een el lado del servidor de DNSCrypt recibe las consultas DNS enviadas por el cliente proxy, los reenvía a una resolución de DNS que sea de confianza, y firma las respuestas que ha recibido antes de reenviarlos al cliente proxy.

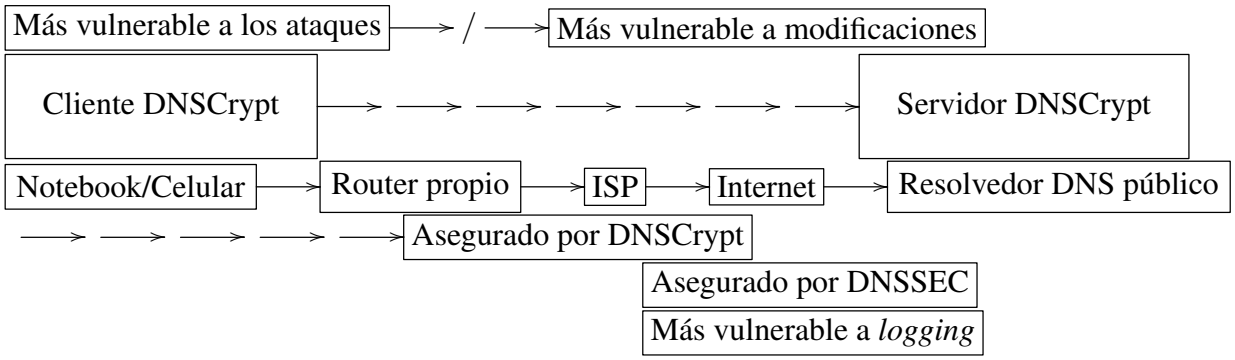
El protocolo DNSCrypt utiliza los puertos 443 del UDP y TCP, los cuales son menos propensos a ser filtrados por routers y ISPs que el puerto estándar DNS.

Usualmente la red local es la mas vulnerable cuando se trata de una suplantación de DNS. El servidor DNSCrypt puede ejecutarse en el router junto con un resolvedor DNS moderno. Entonces los clientes pueden ejecutar el código del DNSCrypt aprovechando el router resolver DNS.

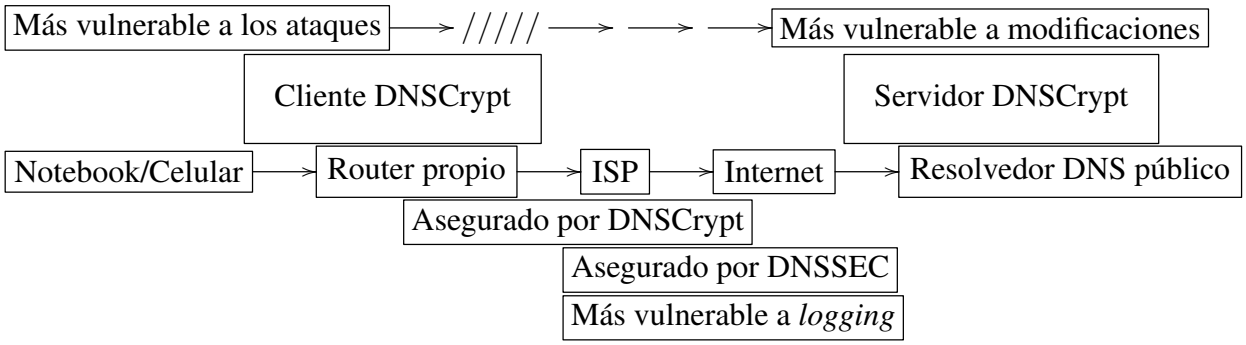


Por otro lado, las organizaciones y personas ejecutan resolvedores públicos de DNS que apoyan al protocolo DNSCrypt. Estos pueden ser usados para ejecutar un Server DNSCrypt o un Resolvedor DNS en el router.

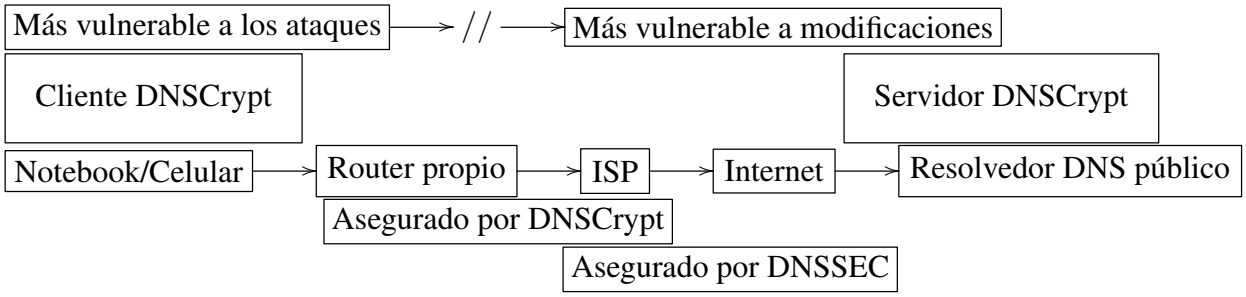
Para máxima protección se ejecuta el Cliente DNSCrypt en cada dispositivo cliente.



Si se confía plenamente en la red local, el cliente DNSCrypt puede ejecutarse en el router:



Finalmente se puede ejecutar un server DNSCrypt propio en una red de confianza remota para tener un control completo sobre lo que está haciendo el resolver y qué actividad de usuario está guardando el resolver (o *logging* como se denomina en inglés).



3. Servidor DNSCrypt

Si se está ejecutando un servidor DNS recursivo privado o público, añadiendo soporte para el protocolo DNSCrypt, esto requiere instalar DNSCrypt-Wrapper, la cual es el proxy DNSCrypt del lado del servidor.

El DNSCrypt-Wrapper se puede compilar desde el código fuente.

En OSX también se puede usar Homebrew para la instalación:

```
brew install dnscrypt-wrapper
```

4. Conclusiones

Internet puede ser un lugar aveces peligroso con respecto a nuestra información personal, tales como identidad, contraseñas, cuentas bancarias, entre otras.

Como pudimos aprender a lo largo de este curso no es de gran complejidad rastrear una dirección de IP para saber la ubicación final o cercana al usuario. Es por esto y también para proteger la información a la que accedemos diariamente es que se puede usar herramientas como DNSCrypt.

Si se sospecha que alguien está espiando los paquetes que se envían o que se reciben, se puede instalar DNSCrypt en el servidor cliente.

Tal como se especificó en este proyecto, es posible instalar DNSCrypt dentro de la red periférica tanto en cualquier dispositivo cliente o en el Router.

Las encriptaciones hechas en este caso, solo se aplican a la DNS. Es decir que los demás protocolos no se alteran mantienen su operación normal.

Referencias

[1] Henry, Alan. *How to Boost Your Internet Security with DNSCrypt*. `http://lifehacker.com/how-to-boost-your-internet-security-with-dnscrypt-510386189`, consultado el 27 de septiembre del 2015.

[2] *Slackware-14.1-DnsCrypt Proxy 1.4.3*. `https://www.linuxquestions.org/questions/blog/arniekat-436077/slackware-14-1-dnscrypt-proxy-1-4-3-36406/`, consultado el 27 de septiembre del 2015.

[3] *Introducing DNSCrypt*. `https://www.opendns.com/about/innovations/dnscrypt/`, consultado el 27 de septiembre del 2015.

[4] *Securing DNS Communication: dnscrypt-proxy*. `https://n0where.net/securing-dns-communication-dnscrypt-proxy/`, consultado el 27 de septiembre del 2015.

[5] *DNSCrypt + DNSMasq en ArchLinux - Encripta tus peticiones DNS y saltate cualquier restrincion de tu ISP*. `http://blog.jam.net.ve/2014/02/16/dnscrypt-dnsmasq-en-archlinux/`, consultado el 27 de septiembre del 2015.