Tecnología DNSSEC,
la navegación más segura

Calle San Rafael, 14
28108 Alcobendas (Madrid)
902 90 10 20
www.acens.com

Cuando un usuario navega por la red, lo que suele hacer es escribir en el navegador la url que quiere visitar y automáticamente, ante nosotros aparece la información correspondiente a la dirección que hemos indicado en la barra de direcciones. ¿Pero cómo sabe el navegador la información que debe mostrarnos? La información que se maneja por la red, no son letras y números, tal y como se nos presenta cuando nosotros la vemos, sino que está compuesta de números. Por lo que debe haber algo que haga la conversión de la dirección que nosotros escribimos a números, que indicará donde está la información que nosotros hemos solicitado.

Esta transformación es realizada por los denominados **Servidores de nombres de dominios, más conocidos como DNS**. Lo que hacen los DNS es transformar la dirección que hemos tecleado en el navegador en una dirección única, compuesta por números. Es lo que se denomina direcciones IP, y que todo aquel que tenga algún dominio y aplicación web en la red, ha tenido que escuchar alguna vez, ya que para que se muestre, al dominio le debe de haber indicado las DNS de la máquina en la que se encuentra alojada su aplicación.

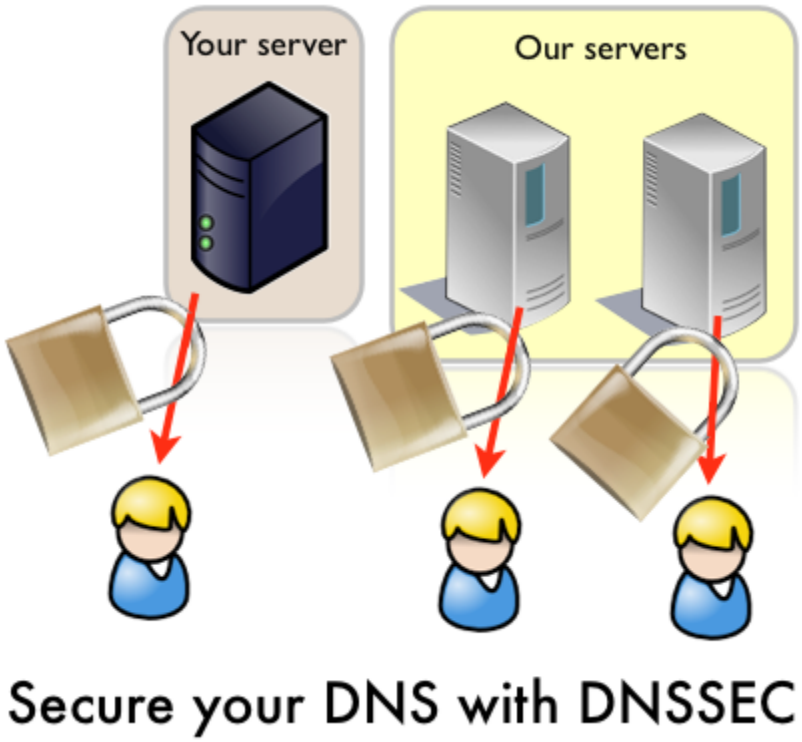
Hace tiempo se detectó un problema de seguridad con las DNS por el cual, un atacante podría forzar la situación para tomar el control de la sesión y enviar al usuario al propio sitio web fraudulento del atacante, con el fin de obtener sus credenciales o bien hacer cualquier otro tipo de cosas.

Ante estos problemas de seguridad con las DNS se plantea la utilización del DNSSEC.

¿Qué es DNSSEC?

DNSSEC es una tecnología que se ha desarrollado, entre otras cosas, para blindar contra este tipo de ataques mediante la firma digital de los datos a fin de tener la seguridad de que son válidos. Sin embargo, para eliminar esta vulnerabilidad de Internet, esta tecnología se debe implementar en cada uno de los pasos del proceso de búsqueda, desde la zona raíz hasta el nombre de dominio final (por ejemplo, www.acens.com). La firma de la raíz (implementar la DNSSEC en la zona raíz) es un paso necesario de este proceso. Es importante destacar que no cifra los datos, tan solo certifica la validez de la dirección del sitio que se visita, para evitar suplantación de direcciones que pueda causar los problemas.

Beneficios para el usuario



La información que sale ahora de los servidores tiene la certificación de que no está falseada y así llega replicada a los servidores más cercanos al usuario, que puede navegar de forma más segura y evita caer en tácticas de suplantación de páginas mucho más poderosas que las actuales y que, en la mayoría de los casos, son estafas.

Si en los casos de Phising basta con ser cautos y tomar una serie de medidas como leer bien la dirección URL a la que remite el delincuente o no contestar correos sospechosos, de haberse explotado la vulnerabilidad, habría sido muy difícil distinguir entre una página falsa y otra real. Aunque no se tiene conocimiento de que se hubiera explotado, se cree que algunos delincuentes podrían saber de ella.

El usuario puede hacer una navegación más segura y evitar caer en tácticas de suplantación de páginas mucho más poderosas que las actuales.

Por otro lado Dnssec refuerza los protocolos y niveles de seguridad SSL, utilizados para cifrar la información confidencial que se envía o se recibe, tanto como para proteger la almacenada en los servidores públicos o corporativos.

¿Cómo extiende DNSSEC a DNS?

La tecnología DNSSEC se basa en sistemas de encriptación, donde es necesario claves públicas y privadas para verificar que la información es correcta. Para conseguir esto, DNSSEC añade cuatro nuevos registros.

- **DNSKEY**: Es donde se guarda la clave pública con la que se firman las zonas.
- **RRSIG**: Guarda un hash encriptado del RRSet, encriptado con la clave privada de la zona.
- **NSEC**: Guarda una respuesta para los casos en los que el nombre requerido o el RR no existan en el archivo de Zona.
- **DS**: Contiene el Hash de la clave pública de la zona hija firmado por la clave privada del padre.