PREGUNTAS FRECUENTES SOBRE DNSSEC

¿Qué es DNS?

La identificación de equipos o máquinas en Internet se realiza a través de direcciones IP o nombres, que deben ser únicos para que el funcionamiento sea correcto. El sistema DNS (en español, *Sistema de nombre de dominio*), es el encargado establecer la correspondencia entre nombres (www.ejemplo.es) y direcciones IPs (192.168.2.15).

El DNS original no incluye métodos de seguridad, lo que se puso de manifiesto especialmente en 2008, cuando Dan Kaminsky publicó el documento "*Multiple DNS implementations vulnerable to cache poisoning*" (http://www.kb.cert.org/vuls/id/800113). A partir de ese momento organizaciones como ICANN promueven la implantación masiva de **DNSSEC**, cuyas especificaciones se habían establecido en 1995.

¿Qué es DNSSEC?

DNSSEC es un conjunto de extensiones de seguridad que utiliza cifrado asimétrico desarrollado para el servicio de DNS, que aporta los siguientes beneficios:

- Autentificar el origen de los datos de un servidor DNS
- Mantener la integridad de los datos entre servidores DNS
- Denegación de existencia autentificada

¿Qué no es DNSSEC?

- DNSSEC no es un nuevo protocolo que sustituya a DNS.
- No sirve como protección contra ataques de denegación de servicio.
- No proporciona confidencialidad a los datos del DNS: las respuestas proporcionadas por DNSSEC están autenticadas pero no cifradas.

¿Cómo se consigue autentificar y mantener la integridad de los datos?

DNSSEC utiliza criptografía asimétrica de clave pública de tal manera que la autoría de lo que se firma con una clave se puede comprobar con la otra. Va a existir una clave pública por cada dominio, que se distribuyen (Registros DS y Trust-Anchor) y se publican utilizando DNS (Registro DNSKEY) en la zona del dominio asegurado. Los registros son autentificados comprobando las firmas digitales con las claves públicas distribuidas, podemos encontrar una explicación más detallada de cómo funciona la firma digital en http://www.cert.fnmt.es/index.php?cha=cit&sec=3&page=219&lang=es.

Para que el sistema sea confiable es necesario que la clave privada se custodie adecuadamente, puesto que si esta se ve comprometida un atacante puede utilizarlo para falsificar los datos del dominio.

¿Qué son las claves KSK y ZSK?

KSK *(Key Signing Keys)* se corresponde a clave de firma de clave (una clave de términos larga) y **ZSK** *(Zone Signing Keys)* se corresponde a clave de firma de zona (una clave de términos corta).

DNSSEC obstaculiza los intentos de amenaza mediante una clave de términos corta (ZSK) para calcular de forma rutinaria las firmas de los registros del DNS, y una clave de términos larga (KSK) para calcular una firma en la ZSK para permitir la validación. La clave ZSK se cambia o renueva con frecuencia para que el atacante tenga mayor dificultad a la hora de encontrarla, mientras que la clave KSK más larga se cambia a intervalos mucho más largos (las mejores prácticas vigentes colocan este plazo en el término de un año).

En la zona se almacenan las dos claves KSK y ZSK. La clave ZKS firma todos los registros de la zona y la KSK firma las claves de la zona. Para poder resolver adecuadamente será necesario contar con ambas.

¿Qué son las extensiones de seguridad?

Estas extensiones de seguridad consisten en un nuevo conjunto de registros y modificaciones del actual protocolo DNS.

Los nuevos registros son:

- DNSKEY (DNS Public Key): Clave pública del DNS
- RRSIG (Resource Record Signature): Firma digital de un registro.
- DS (Delegation Signer): Hash de una DNSKEY
- NSEC/NSEC3 (Next Secure): Se utiliza para la denegación de existencia
- NSEC3PARAM: Parametros de configuración de NSEC3

En cuanto a las modificaciones del protocolo, se incluyen nuevas llamadas y peticiones de registros por cada consulta DNS que se realiza, para posibilitar la autenticación de los dominios.

¿Qué es la cadena de confianza?

La cadena de confianza consiste en una relación de registros **DNSKEY** (Claves públicas) y registros DS (Delegation Signer) que permite crear relaciones de confianza entre los dominios. De esta forma se pueda validar cualquier dominio que esté integrado en dicha cadena con una sola clave pública. Para conseguirlo, el registro DS, que es un hash (una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro o archivo) generado a partir de un registro DNSKEY, se publica en el dominio padre. Por ejemplo si tenemos el dominio red.es con su clave asociada, generamos el registro DS de la misma y lo publicamos en el dominio .es, de esta forma podemos autentificar el dominio red.es con la clave pública del dominio .es.

¿Cómo usuario final qué es necesario para poder protegerme con DNSSEC?

Para utilizar la validación de registros en DNSSEC, es necesario disponer de un equipo compatible con este sistema y contratar el servicio con un proveedor de DNS que cuente con un servidor DNS recursivo con la validación activada.

Este servidor DNS recursivo debe contener las claves públicas de los dominios que se quieran validar. También es posible utilizar alguno de los servidores recursivos con DNSSEC que algunas organizaciones como OARC's (https://www.dns-oarc.net) ponen a disposición de todo el mundo.

¿Qué ocurre si se consulta un registro DNS y falla la validación DNSSEC?

Cuando un servidor recursivo con la validación **DNSSEC** activada recibe una respuesta del DNS manipulada o falsificada, el cliente que solicitó dicha resolución de nombres no obtiene ningún registro y se le devuelve un código de error (RCODE) SERVFAIL que significa que se ha producido un error contestando a la consulta.

Como propietario de un dominio, ¿Qué pasos he de seguir para que el dominio utilice DNSSEC?

Para que el dominio esté asegurado con DNSSEC es necesario que los servidores DNS autoritativos de los que se dispone, publiquen el dominio firmado. Si los servidores DNS son BIND puedes utilizar OpenDNSSEC (http://www.opendnssec.org), que a partir de un fichero de zona (con formato BIND) sin firmar genera su equivalente firmado (con formato BIND); o las herramientas que BIND proporciona como dnssec-signzone. Para más información consulte http://www.nlnetlabs.nl/publications/dnssec_howto/.

¿Cuáles son las principales dificultades que nos podemos encontrar en un despliegue de DNSSEC?

Los principales problemas a solucionar son:

- Es necesario que el hardware de red soporte **EDNS0** (Soporte de mensajes DNS de mayor tamaño).
- Incremento de los recursos hardware (El incremento de recursos dependerá del volumen de información a gestionar):
    - en los servidores recursivos se necesitara más ancho de banda y CPU
    - en los servidores autoritativos se necesitara más memoria, ancho de banda y CPU
- Existe una carga adicional de trabajo a nivel de operación, ya que la implantación de DNSSEC conlleva una serie de procedimientos como son: la renovación de las claves o la monitorización del sistema de firma.
- Es muy recomendable conocer con detalle cómo funciona DNSSEC y tener conocimientos de criptografía, cualquier fallo o error puede provocar que todo un dominio sea inaccesible.

¿Dónde puedo buscar más información de DNSSEC?

En los **RFCs** (estándar en Internet) de la Internet Engineering Task Force se puede obtener información técnica:

- RFC 2535 Domain Name System Security Extensions
- RFC 3833 A Threat Analysis of the Domain Name System
- RFC 4033 DNS Security Introduction and Requirements (*DNSSEC-bis*)
- RFC 4034 Resource Records for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4035 Protocol Modifications for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4398 Storing Certificates in the Domain Name System (DNS)
- RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 4641 DNSSEC Operational Practices