DNSSEC

Equipo 2

Alberto Boughton Reyes A01178500
Valeria Garcia Hernandez A01742811
Facundo Bautista Barbera A01066843
Emiliano Ruiz López A01659693
Daniel Garnelo Martinez A00573086

Que es

DNSSEC (Domain Name System Security Extensions):

Capa adicional de seguridad a uno o varios servidores DNS de un dominio.

Funcionamiento

En si, extiende DNS con autenticación e integridad mediante firmas digitales.

RFC

RFC (Request for Comments) es un documento oficial publicado por el IETF (Internet Engineering Task Force)

Son el mecanismo mediante el cual se definen y actualizan las tecnologías que hacen funcionar Internet.

RFCs fundamentales para DNSSEC

1. RFC 4033 (conceptos)
2. RFC 4034 (registros)
3. RFC 4035 (validación)
4. RFC 6840 y 9364 (actualizaciones).

Registros DNSSEC

DNSKEY – claves

Almacena claves públicas, utilizadas por las KSK (Key Signing Key) y ZSK (Zone Signing Key)

RRSIG – firmas

Contiene las firmas digitales de los RRsets

DS – cadena de confianza

Enlaza la clave del dominio hijo con la zona padre, creando la cadena de confianza

NSEC/NSEC3 – negación autenticada.

Oculta la estructura de la zona mediante hashing

Algoritmos

Uso:
Los algoritmos en DNSSEC se usan para firmar, validar, encadenar y proteger la información del DNS usando criptografía.

RSA/SHA-256 (más utilizado globalmente)

ECDSA P-256 (más pequeño, mejor procesamiento)

Ed25519 (moderno y eficiente).

Diferencias con DNS

DNS tradicional: No tiene autenticación.

DNSSEC: Incluye firmas, validación, cadenas de confianza, requiere instalar EDNSo, bits DO / AD / CD.

Evolución

RFC

2065 y 2535

DNSSEC-bis
(4033/4034/4035)

9364

Primeras versiones obsoletas.

2005

2023

Tiempo

Adopción Mundial

TLDs firmados >90% globalmente

Significa que el TLD forma parte de la cadena de confianza de DNSSEC en 90% del mundo.

Alta validación: Europa <=60%

Baja validación: América y LATAM =>30

Ataques Mitigados

Protege de:
Cache poisoning, spoofing, Kaminsky.

No ofrece protección contra:
Ataques volumétricos, amplificación, túneles DNS o secuestros que ocurren fuera del proceso de resolución.

Ventajas

Autenticación e integridad.
Base para DANE, SSHFP, etc.

Desventajas

Complejidad operativa.
Paquetes DNS más grandes.
Gestión y rotación de claves.

Documentacion a mayor detalle

https://docs.google.com/document/d/1ajFnMatg0fBL_ZlYHqogYOkz4OzWAzrTFgIohFZ90bE/edit?usp=sharing