DNSSEC

Una breve introduzione

Marco d'Itri
<md@seeweb.it>

Seeweb s.r.l.

Peering workshop NaMeX - 9 luglio 2010

DNSSEC

Che cosa è?

Permette di **garantire** l'autenticità di un record DNS grazie a crittografia a chiave pubblica e firme digitali.

A cosa serve?

Protegge i client impedendo di accettare record DNS falsificati.

seeweb

Perché?

Il corretto funzionamento del DNS è alla base di quasi ogni altro protocollo. Senza DNSSEC il protocollo è intrinsecamente vulnerabile a diversi tipi di attacco (es: Kaminsky).

DNSSEC è un enabler

Ancora non conosciamo tutti i modi in cui sarà usato!

seeweb

Cosa non è

- Non fornisce confidenzialità dei dati nel DNS.
- Non impedisce attacchi DoS all’infrastruttura DNS.
- Non crea un canale sicuro tra client e resolver.

seeweb

Storia

Prima versione - 1997

RFC 2065: non scala (il parent doveva firmare ogni record del figlio).

Aggiunti record DS (KSK/ZSK) - 2005

RFC 4033: permette lo zone walking.

Aggiunto record NSEC3 - 2008

RFC 5155: ce l'abbiamo fatta!

seeweb

Le novità del protocollo

Nuovi resource record

DNSKEY, RRSIG, NSEC e DS.

Nuovi bit

Checking Disabled (CD) e Authenticated Data (AD), uso di EDNS.

seeweb

In breve, come funziona?

Risposta positiva

Il record richiesto è accompagnato dal suo RRSIG.

Risposta negativa

Un record NSEC è accompagnato dal suo RRSIG.

Ogni zona è firmata dal proprio amministratore

I RRSIG sono verificati con le chiavi dei DNSKEY, le chiavi sono confermate dai record DS nella zona superiore.

seeweb

Turtles all the way down

Dove trovo le chiavi?

Si procede ricorsivamente a validare una zona cercando la sua chiave nella zona superiore o finché non si arriva a una trust anchor nota.

Quindi?

Aspettiamo la pubblicazione della trust anchor per la root.

seeweb

Perché non lo usa nessuno?

- Non funzionerà mai...
- Non sarà mai standardizzato...
- .com non sarà mai firmata...
- La root non sarà mai firmata...

seeweb

Possibili svantaggi

DNSSEC non perdona gli errori!

Occorre automatizzare le operazioni ed automatizzare i controlli.

Servono più risorse

- CPU per firmare e verificare i record.
- RAM per zone più grandi.
- Banda per trasmettere le risposte più grandi (con EDNS o TCP).
- Software moderno.

seeweb

Possibili problemi

- Slave con software troppo vecchio.
- TCP bloccato.
- Problemi di path MTU discovery.
- Indispensabile NTP!
- Alcuni CPE hanno proxy DNS pieni di bug.
- Registrar che non supportano (davvero) DNSSEC.

seeweb

Verificare o no?

Se una zona è firmata male non sarà visibile ai soli resolver che verificano. Ai propri clienti non importa di chi è la colpa.

Domande?

`http://www.linux.it/~md/text/dnssec.pdf`

(google . . . Marco d'Itri . . . I feel lucky)

seeweb