DNSSEC a escala de Internet

Felipe Tribaldos, CISSP

felipe@cloudflare.com

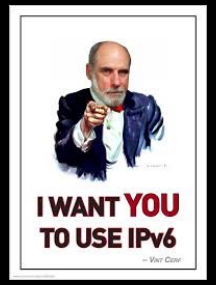
lacnic25
2/6 mayo - la habana, cuba

CloudFlare

- CDN + DNS Autoritativo (incluyendo DNSSEC gratis)
- >4M+ de dominios
- 40+ mil millones consultas/día
- 79 PoPs en 40 países (en crecimiento)

CLOUDFLARE

Innovaciones



- IPv6 Gateway
- Universal SSL
- Universal DNSSEC
- HTTP/2 (+Server Push)
- Websockets

DNSSEC a escala de Internet

1. Introducción a DNSSEC
2. Curvas Elípticas
3. Respuestas Negativas
4. Respuestas ‘Any’
5. Apoyo de Regitrars y Registry

CLOUDFLARE

Introducción DNSSEC

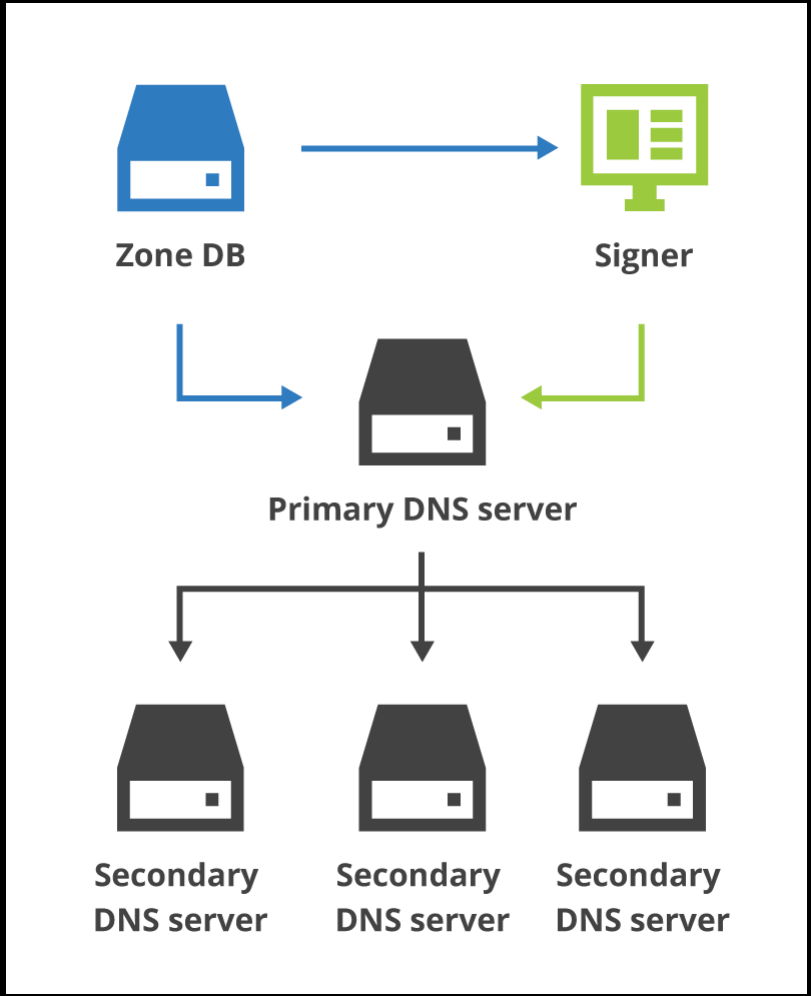
¿ Porque DNSSEC ?

- Proteger las repuestas contra interceptación y envenenamiento de cache

- Habilitar nuevas funciones como DANE, y otros protocolos de llaves.

DNSSEC: Como

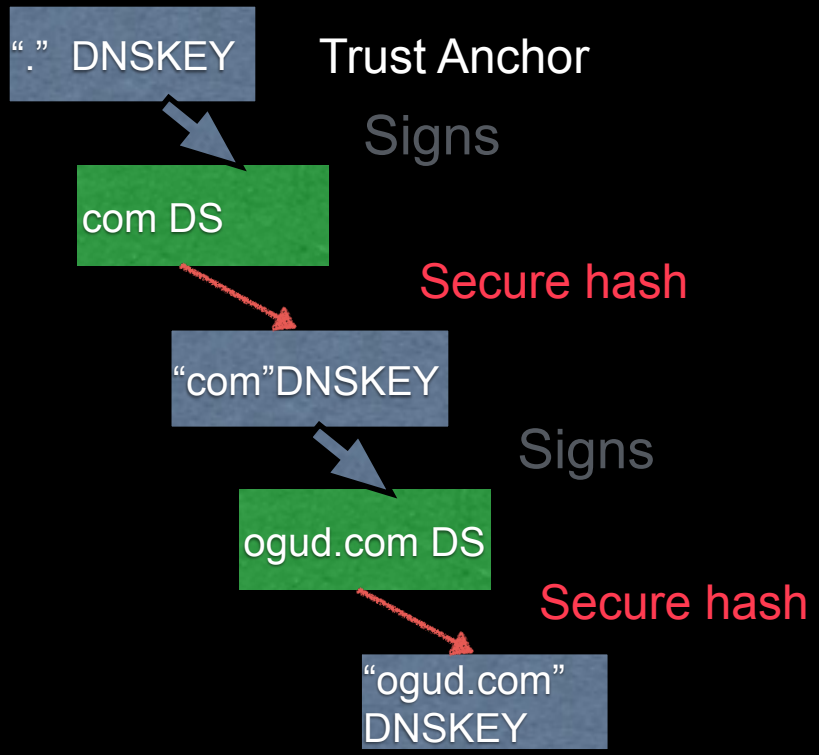
- Firmas Digitales
  - Llaves RSA y ECDSA
  - Las zonas son firmadas en un punto central y distribuido a servidores DNS
- Respuestas
  - Siempre hay una respuesta firmada o una prueba firmada que la respuesta no existe
  - Prueba negativa puede probar que no existe el tipo o el nombre



CLOUDFLARE

DNSSEC ==> DNS-Autenticación

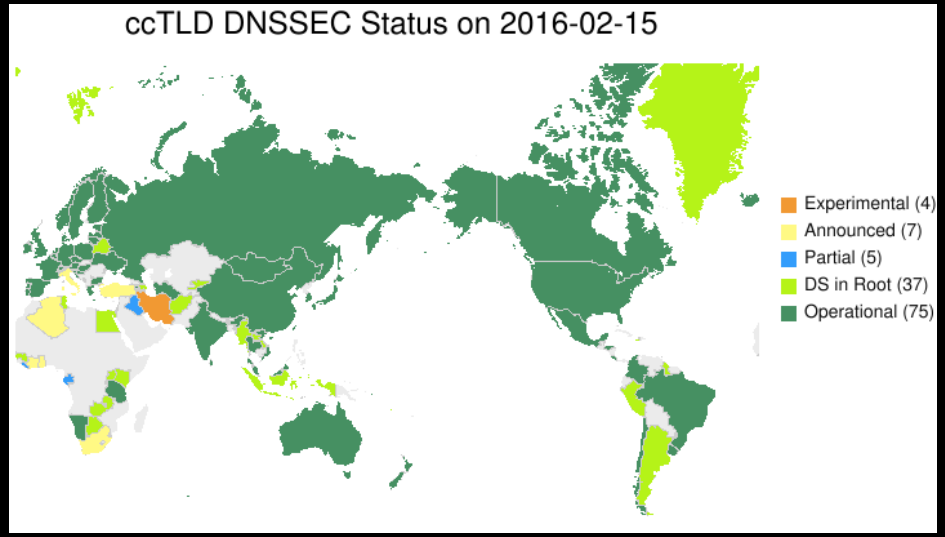
- Objetivo: Respuestas a prueba de interceptación
- Firmas Digitales agregadas al RRSet
- Jerarquía de confianza establecida por una serie de registros DNSKEY y DS
  - DNSKEY == Public KEY
  - DS == Hash (domain name | DNSKEY)
- Negación de existencia explicita



CLOUDFLARE

ccTLD estatus Global DNSSEC

- Software
  - La Mayoría de los servidores DNS soporta
  - La mayoría de los DNS Resolvers soporta
- Publicación
  - Raíz esta firmado
  - 70% de los TLD's están firmados
  - millones de dominios están firmados



CLOUDFLARE

Estatus en área de LACNIC

- ccTLD’s firmado en área LACNIC
- 11 Firmados
- 18 Sin Firmar

- No todos los registradores/TLD's aceptan todos los registros DS.

Fuente: https://www.lactld.org/wp-content/uploads/2015/03/Statplanet/StatPlanet.html

Curvas Elípticas

Tamaño v Velocidad

Trasfondo

- CloudFlare mitiga grandes ataques de DDoS (regularmente >400M+ pps). Ataques de noviembre/2015 contra L-Root (~5M pps)
- DDoS de Amplificación de DNS (queries pequeños, respuestas grandes). Reporte de Akamai 2/2016
- Zonas firmadas con firmas grandes son preferidas por los atacantes para lanzar ataques de amplificación.

Curvas Elípticas: Paquetes pequeños

- CloudFlare utiliza ECDSA para mantener la llave y las firmas pequeñas
- Casi todas las repuestas de DNS de CloudFlare es menor a <512 bytes incluyendo DNSSEC

¿Porque ECDSA tienes llaves pequeñas ?

Energía necesaria para romper una llave de 228 bit RSA vs. 228 bit ECDSA.

RSA:

Energía necesaria para hervir una cucharada de agua

CLOUDFLARE

Ref: Arjen Lestra

Energía necesaria para romper una llave de 228 bit RSA vs. 228 bit ECDSA.

RSA:
Energía necesaria para hervir una cucharada de agua

ECDSA:
hervir toda el agua en el planeta

CLOUDFLARE

Ref: Arjen Lestra

Comparando respuestas DNSKey

```
ietf.org.                1800    IN      DNSKEY  256 3 5 AwEAAdDECajHaTjfSoNTY58WcBah1BxPKVIHBz4IfLjfqMvium4lgKtK ZLe97DgJ5/NQrNEGGQmr6fKv
Uj67cfrZUojZ2cGRizVhgkOqZ9scaTVX NuXLM5Tw7VWOVIceeXAuuH2mPIiEV6MhJYUsW6dvmNsJ4XwCgNgroAmX hoMEiWEjBB+wjYZQ5GtZHBFKVXACSWTiCtddHcueOeSVPi5
WH94Vlubh HfiytNPZLrObhUCHT6kOtNE6phLoHnXWU+6vpsYpz6GhMw/R9BFxW5Pd PFIWBgoWk2/XFVRSKG9Lr61b2z1R126xeUwvw46RVy3hanV3vNO7LM5H niqaYclBbhk=
ietf.org.                1800    IN      DNSKEY  [illegible] xz9p/sZ+8AByqyFHLdZc HoOGF7CgB5OKYMvGOgysuYQl
oPlwbq7Ws5WywbutbXyG24lMWy4jijlJ UsaFrS5EvUu4[illegible]j1cKr2nX1NrmMRowIu3DIVtGbQJmzpukpDVZaYMMAm8M5
vz4U2vRCV ETLgDoQ7rhsiD127J8gVExjO8B0113jCajb[illegible]ykHR7rlPqqmw58nIELJUFoMcb/BdRLg byTeurFlnxs=
ietf.org.                1800    IN      RRSIG [illegible] 45586 ietf.org. dpOO1u/mE0ZmcergtT4RA5DdV8E
i3nTYvsuTFKqEou4Smku5UpO1giVp sOpdDRwvei5g2HC8vK/nKHDhcotNRZunawRvA5ynNgNrGAGSpXh5R6H2 Io/7yDr2TK529YHee0MTVeHqk6YeyyiFvCL1XMLt3jj4/G3pjo
z7mS8M NLgysKQMEZqJHfZhARZeSNIuK/QpRJhBX9UQYrv6IJ/2l5WqdL6C6aeB fYe+bhn3G2s9apnUQFiq0xo3ybyQJmO6UEPjuEnn8uLXnXTlRdthZbnY g5yZReSWb4jVYQKC
yX4Pnm09TtrpduZQqzl20v+8nMITf4HJnSj7EvPN AxmCXg==
```

```
filippo.io.              3600    IN      DNSKEY  257 3 13 DGpDkudNu/XQT1Km
QkXFtKCfZPxHGV07qSTIcDXS33/WtT8UUG7LvxAg KznsRSFEhiOVR53E69/E57IFm8b6Zw==
filippo.io.              [illegible]  IN      [illegible] koPbw9wmYZ7ggcjn
Q6ayHyhHaDNMYELKTqT+q[illegible]0PYFkH1ruxLhe5g==
filippo.io.              3600    IN      RRSIG   DNSKEY 13 2 3600 20150523
162528 20150422162528 42 filippo.io. KGjopS+z5rsK++grfGMuA2al/vQ9S5tBXOJq
ZbeTOYB0hfHG7Sl6hqR1 xfoibSJA1BiX5r9Ujo5YVU/NE1H0TQ==
```

RSA: 1181 BYTES

ECDSA: 305 BYTES

CLOUDFLARE

ECDSA es rápido

…importante cuando se computan 56.9 mil millones (*‘billions’*) firmas por día

Optimizando ECDSA en Go

- Implantación nativa en assembler (Vlad Krasnov)
- 21x mejora en velocidad
- Ahora pate del Go crypto library (Go 1.6)
- Toma a CloudFlare 0.0001 segundos firmar un registro DNS

	Antes	Despues	Mejora
ECDSA Sign	1,015,006 ns/op	48,741 ns/op	**20.8x**
ECDSA Verify	3,086,282 ns/op	146,991 ns/op	**21.0x**

CLOUDFLARE

Respuestas Negativas

Ahorro de Computo

Problemas de las respuestas negativas

1. Requiere que el servidor autoritativo responda con el nombre anterior y el siguiente
2. 2 NSEC + 2 NSEC RRSIG para decir una sola respuesta

¿ Cual es el problema con el nombre anterior y el próximo ?

Arquitectura de DNS de CloudFlare

- DNS server escrito 100% en Go, llamado RRDNS
- No hay concepto de un “zone file”, en ves es una BD SQL de registros DNS.
- Lógica del DNS, generamos dinámicamente las repuestas al momento

El problema con el anterior + el próximo nombre

1. No hay “zone file”, así que necesita una búsqueda indexada de la BD
2. Respuestas dinámicas hacen que el anterior + el próximo sea difícil
3. NSEC expone el información sobre la zona (y NSEC3 puede ser vulnerable a dictionary attack)

RFC4470 Mentiras Blancas “White Lies”

- Genera aleatoriamente el anterior y el próximo nombre para NSEC
- Ayuda a prevenir ”zone walking” y consultas adicionales de BD

El problema con 2 NSEC para decir solo una cosa

RFC4470 Mentiras Blanca “White Lies”

- Aun utiliza dos registros firmados NSEC para decir una cosa

CloudFlare “Black Lies” para NXDOMAIN

- El proximo nombre es siempre \000.[themissingname]
- Un NSEC por repuesta

```
cloudflare.com.         1799  IN    SOA   ns3.cloudflare.com. dns.cloudflare.com. 2020905521 10000 2400
  604800 3600
  bogus.cloudflare.com. 3599  IN    NSEC  \000.bogus.cloudflare.com. RRSIG NSEC
  cloudflare.com.       1799  IN    RRSIG SOA 13 2 86400 20160309213638 20160307193638 35273
  cloudflare.com. mgx1FncjVdOpWhMOqm6+kcPBi/6zC8LF00ccG3DA1RNiI6hXmrqnFiUg
  dsngBT3VYo0+8AsZ1l0vJiopCdNoTw==
  bogus.cloudflare.com. 3599  IN    RRSIG NSEC 13 3 3600 20160309213638 20160307193638 35273
  cloudflare.com. 8nbevvyI/RsSjunQzjlPkIHphiAOu5gti+aj2ucBx3Nhc7cnaHtJbJ5C
  dFrOF7eoZuPeiegf0KTtMyhAYp3tWQ==
```

CLOUDFLARE

Comparando respuestas negativas

```
ietf.org.          1799    IN      SOA     ns0.amsl.com. glen.amsl.com. 1200000317 1800 1800 604800 1800
    ietf.org.      1799    IN      RRSIG   SOA 5 2 1800 20170213210533 20160214200831 40452 ietf.org. P8XoJx+SK5nUZAV/IqiJrsoKtP1c+GXmp3FvEOUZPFn1VwW33242LVrJ
    GMI5HHjMEX07EzOXZyLnQeEvlf2QLxRIQm1wAnE6W4SUp7TgKUZ7NJHP dgLr2gqKYim4CI7ikYj3vK7NgcaSE5jqIZUm7oFxxYO9/YPz4Mx7COw6 XBOMYS2v8VY3DICeJdZsHJnVKlgl8L7/yqrL8qhkSW1yDo3YtB9cZEjB
    OVk8uRDxK7aHkEnMRz0LODOJ10AngJpg9LrkZ1CO444RhZGgTbwzN9Vq rDyH47Cn3h8ofEOJtYCJvuX5CCzaZDInBsjq9wNAiNBgIQatPkNriR77 hCEHhQ==
    ietf.org.      1799    IN      NSEC    ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY SPF
    ietf.org.      1799    IN      RRSIG   NSEC                                                    f.org. B9z/JJs30tkn0DyxVz0zaRlm4HkeNY1TqYmr9rx8rH7kC32PWZ1Fooy6 16qmB33/
    cvD2wtOCKMnNQPdTG2qUs/RuVxqRPZaQojlVZsy/GYONmlap Bp                                          RCXwUOzZnW bdttjsmbAqONuPQURaGz8ZgGztFmQt5dNeNRaq5Uqdzw738vQjYwppfU
    9GSLkT7RCh3kgbNcSaXeuWfFnxG1R2SdlRoDICos+RqdDM+23B                                          2NOA9mexa7yTuXH+x o/rzRA==
    www.apps.ietf.org. 1799    IN      NSEC    cloudflare-verify.ietf.org. A RRSIG NSEC
    www.apps.ietf.org. 1799    IN      RRSIG   NSEC 5 4 1800 20170213210614 20160214200831 40452 ietf.org. U+hEHcTps2lC8VKS61rU3MDZq+U0KG4/oJjIHVYbrWufQ7NdMdnY6hCL
    OmQtsvuZVRQjWHmowRhMj83JMUagxoZuWTg6GuLPin3c7PkRimfBx7jI wjqORwcuvpBh92A/s/2HXBma3PtDZl2UDLy4z7wdO62rbxGU/LX1jTqY FoJJLJfJ/C+ngVMIE/QVneXSJkAjHV96FSEnreF81V62x9azv3AHo4tl qnoYvRDtK
    +cR072A5smtWMKDfcIr2fI11TAGIyhR55yAiolIPDEz5koj BfMstC/JXVURJMM+1vCPjxvwYzTZN8ilCf1AupyyR8BNWxgic5yh1IjH 1AuAVQ==

cloudflare.com.                1799    IN      SOA                                                2400 604800 3600
    blog.cloudflare.com. 3599  IN      NSEC    \000.
    cloudflare.com.            1799    IN      RRSI                                                cloudflare.com. kgjtJDuuNC/yX8yWQpol4ZUUr8s8yAXZi26KWBI6S3HDtry2t6LnP1ou
    QK10Ut7DXO/XhyZddRBVj3pIpWYdBQ==
    blog.cloudflare.com. 3599  IN      RRSIG   NSEC 13 3 3600 20160220230013 20160218210013 35273 cloudflare.com. 8BKAAS8EXNJbm8DxEI1OOBba8KaiimIuB47mPlteiZf3sVLGN1edsrXE +q
    +pHaSHEfYG5mHfCBJrbi6b3EoXOw==
```

NSEC: 1094 bytes

Black Lies: 357 bytes

CLOUDFLARE

Problemas con NODATA:

- Tendríamos que buscar en la base de datos para los tipos existentes (consumo de CPU)
- No siempre es posible por respuestas dinámicas

CloudFlare “Black Lies” para NODATA

- Se muestran todos los tipos excepto los que estan buscando
- Cuando preguntas por TXT:

```
blog.cloudflare.com.  3599 IN  NSEC \000.blog.cloudflare.com. A WKS HINFO MX
  TXT AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG NSEC TLSA HIP OPENPGPKEY SPF
```

- Cuando preguntas por MX:

```
blog.cloudflare.com.  3599 IN  NSEC \000.blog.cloudflare.com. A WKS HINFO MX
  TXT AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG NSEC TLSA HIP OPENPGPKEY SPF
```

CLOUDFLARE

Respuestas ANY

- `Draft RFC` draft-ietf-dnsop-refuse-any

$ dig ANY cloudflare.com

;; ANSWER SECTION:

cloudflare.com. 5 IN RRSIG HINFO 13 2 3789 20160507144352 20160505124352 35273 cloudflare.com. 6eUptMCSjjzoJO1e8kovavv+KmQFv0ir3txhRjyx48go2tbQbpB3Lh5E D6+d3eVRfpbVuWRTIqLOzwusRwNCOQ==cloudflare.com. 5 IN HINFO "Please stop asking for ANY" "See draft-ietf-dnsop-refuse-any"

CLOUDFLARE

Soporte de Registros y Registradores

La ultima milla

Apoyo en Registros y Registradores

- Gran diferencia entre ser un estandar de Internet y adopción en la practica
- DNSSEC es requerido por el acuerdo de registrar
- DNSSEC Algoritmo 13 (ECDSA) ha sido un estándar por años
- Aun así muchos registrars + registries no lo soportan

"In order ***to enable the DNSSEC, the domain name must be under [the registrar's] DNS management*** *which means the domain will need to be moved to our servers. The changes [i.e. adding the DS] have not been completed and this request has been closed."*

CLOUDFLARE

“I talked to support at the registrar and they said that I would need to ***enter the DS record with you since my DNS is hosted here****.”*

Registrar Support: “The DNSSEC option is not yet operational, we still don’t provide support for it. ”

Registrant: “So if I add my DS record and ***it says ‘DNSSEC Active’, DNSSEC won’t really be active****?”*

Registrar Support: “Exactly.”

Muchos ccTLD's y Registradores han agregado ECDSA:

- Norid (.no)
- SIDN (.nl)
- Eurid (.eu)
- eNic (.eu)
- NZRS (.nz)
- NIC.br (.br)
- DNSimple
- Hover
- Internet.bs
- OVH
- Metaname

https://www.ietf.org/id/draft-latour-dnsoperator-to-rrr-protocol-00.txt

```
Network Working Group                                          J. Latour
Internet-Draft                                                     CIRA
Intended status: Informational                              O. Gudmundsson
Expires: April 21, 2016                                   Cloudflare, Inc.
                                                               P. Wouters
                                                                  Red Hat
                                                             M. Pounsett
                                                               Rightside
                                                          October 19, 2015


       Third Party DNS operator to Registrars/Registries Protocol
            draft-latour-dnsoperator-to-rrr-protocol-00.txt

Abstract

   There are several problems that arise in the standard
   Registrant/Registrar/Registry model when the operator of a zone is
   neither the Registrant nor the Registrar for the delegation.
   Historically the issues have been minor, and limited to difficulty
   guiding the Registrant through the initial changes to the NS records
   for the delegation.  As this is usually a one time activity when the
   operator first takes charge of the zone it has not been treated as a
   serious issue.
```

CLOUDFLARE

dnssec-integration@cloudflare.com

Gracias

Felipe Tribaldos
felipe@cloudflare.com
@ftribaldos