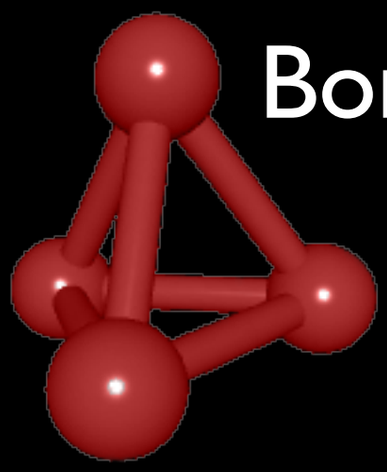


Bond Internet Systems

Evitando que tu servidor DNS sea un arma de destrucción masiva

João Damas

Hace algunos años,
en un lugar cercano...

Hace algunos años, en un lugar cercano...

El DNS era algo de lo más inofensivo

Hace algunos años, en un lugar cercano...

El DNS era algo de lo más inofensivo

Nadie le prestaba atención

Hace algunos años, en un lugar cercano...

El DNS era algo de lo más inofensivo

Nadie le prestaba atención

El servicio estaba en una esquina del servidor que sobraba

Hace algunos años, en un lugar cercano...

El DNS era algo de lo más inofensivo

Nadie le prestaba atención

El servicio estaba en una esquina del servidor que sobraba

Hoy

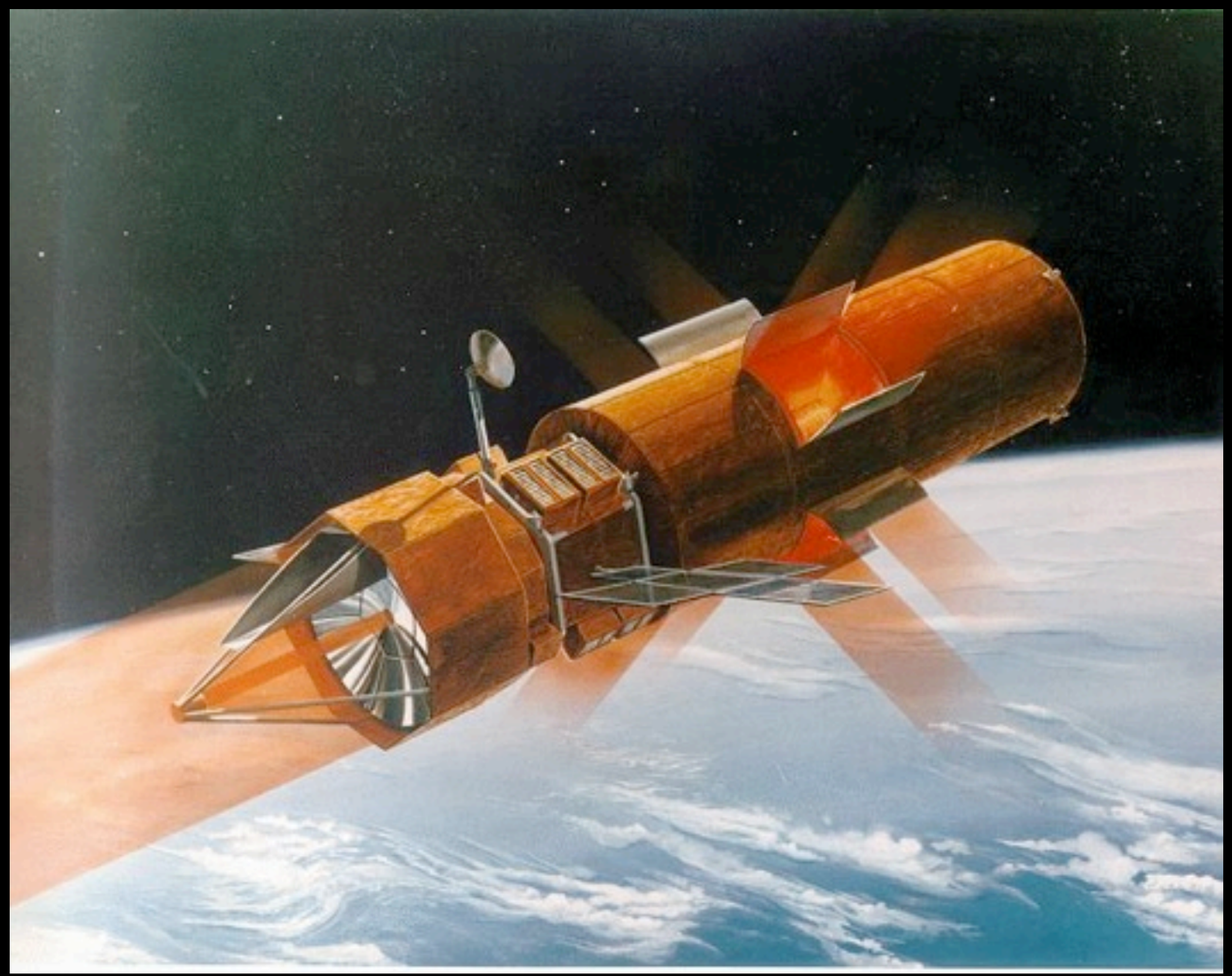
- Está claro lo crítico que es el DNS
- pero sigue estando al final de la lista
- y se le dedica poca atención

Amplificación

dig nic.nl any +dnssec (35 bytes)

la respuesta tiene 2899 bytes

El DNS hoy



¿Cómo evitarlo?

- DNS recursivo
- DNS autoritativo

DNS recursivo

DNS recursivo

Access

DNS recursivo

Access

Control

DNS recursivo

En el servidor de nombres

ACLs

Access

Control

DNS recursivo

En el servidor de nombres

ACLs

Access

Control

En la red

uRPF en interfaces de cliente

DNS recursivo

En el servidor de nombres

ACLs

Access

Control

En la red

uRPF en interfaces de cliente

http://www.bcp38.info/index.php/Main_Page
http://www.ripe.net/ripe/docs/ripe-431
http://www.ripe.net/ripe/docs/ripe-432

DNS recursivo

- RPZ: Response Policy Zones
  - Se recibe una zona de DNS en la que se especifican acciones a tomar para responder a preguntas sobre determinados dominios

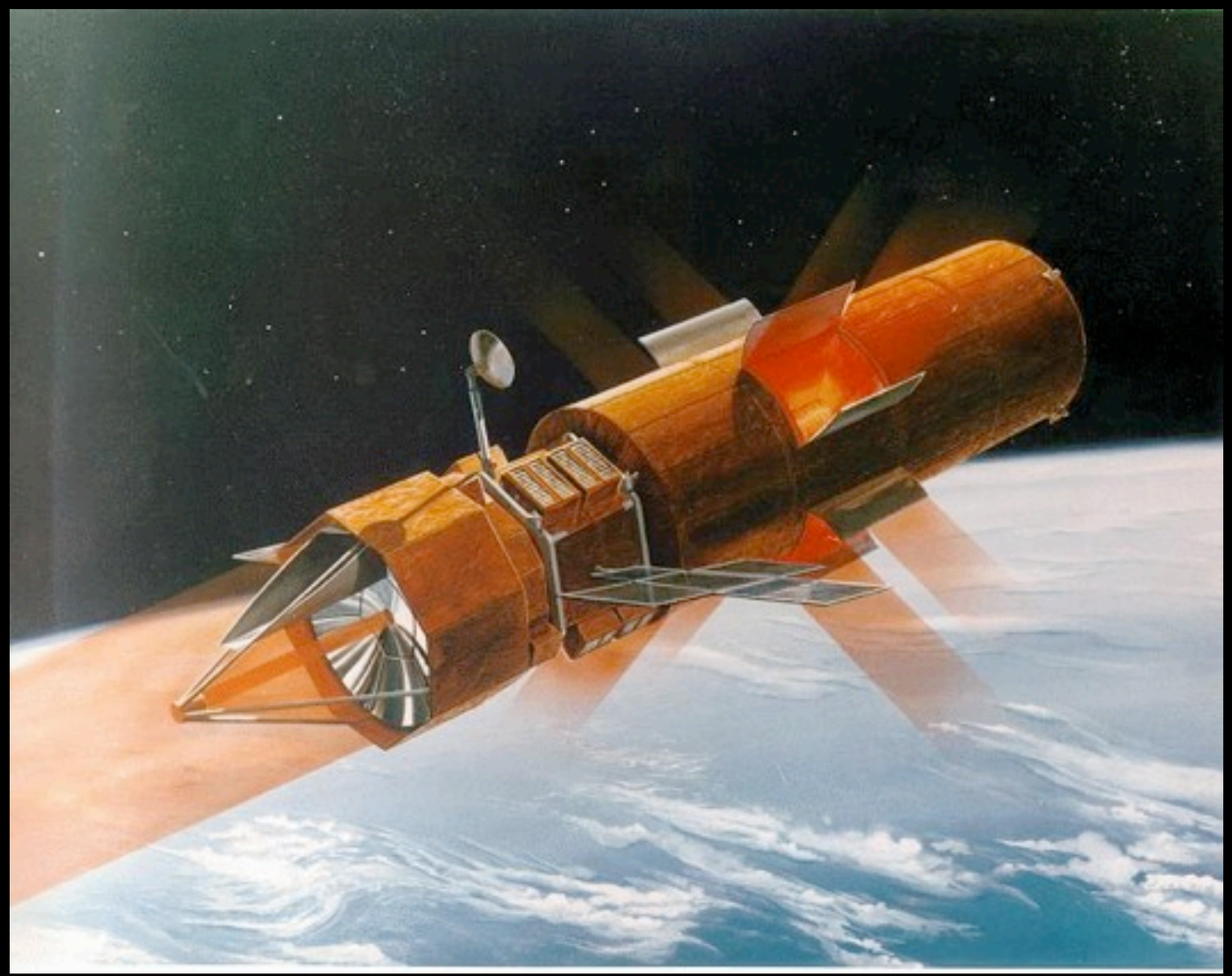
DNS recursivo

- RPZ: Response Policy Zones
  - lo que diga la zona
  - sólo log
  - nxdomain|nodata|cname

DNS autoritativo

- Durante años se procuró filtrar las preguntas de DNS entrantes
- pero esto nunca funciona
  - demasiados falsos positivos
  - pagan justos por pecadores
  - la linea de acceso sigue saturada

DNS autoritativo



DNS autoritativo

La idea que si funciona es

no responder

DNS autoritativo

Response Rate Limiting

RRL

Se instala el parche en BIND (9.9.4)
    Viene de *fábrica* con Knot DNS y NSD
Se controla a través de 3 parámetros
    responses-per-second
    window
    slip

http://www.redbarn.org/dns/ratelimits

Preguntas?