Akamai

POWERING A BETTER INTERNET SINCE 1998
CELEBRATING X YEARS

DNS Authority Spreading

David C Lawrence
2 February 2009

Overview

- DNS Authority Spreading directs resolvers to a greater number of nameserver addresses than can fit in a normal DNS delegation reply.
- Improves performance.
- Improves attack resilience.
- Possible to be misconstrued as malicious use of the DNS.

Background

- Authorities for a zone normally determined by delegation from parent zone.
- A delegation response puts records in the Authority and Additional sections.
- Normal, non-delegating responses can also put records in the Authority and Additional sections.
- Resolvers traditionally opportunistic about caching all information in a response packet.
    - Used to be extremely trusting and really take ***all*** records from the packet.
    - Modern resolvers only trust "in-bailiwick" records; those that are for names for which the server being asked is either authoritative or the parent.

Background, Continued

- Delegation records from parent zone can disagree with those in child zone.
- Child is presumed correct.
- Child asserts its own authority information by including Authority and Additional with normal answers.
- In the absence of authority information from the child, caching resolvers just continue to use the parent's records.
- Authority records are normally not asked for operationally.

Typical DNS Reply

```
; <<>> DiG <<>> icann.org @ns.icann.org
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57098
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 7

;; QUESTION SECTION:
;icann.org.                     IN      A

;; ANSWER SECTION:
icann.org.              21600   IN      A       208.77.188.103

;; AUTHORITY SECTION:
icann.org.              86400   IN      NS      b.iana-servers.org.
icann.org.              86400   IN      NS      c.iana-servers.net.
icann.org.              86400   IN      NS      d.iana-servers.net.
icann.org.              86400   IN      NS      ns.icann.org.
icann.org.              86400   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     21600   IN      A       192.0.34.43
b.iana-servers.org.     21600   IN      A       193.0.0.236
c.iana-servers.net.     21600   IN      A       139.91.1.10
c.iana-servers.net.     21600   IN      AAAA    2001:648:2c30::1:10
d.iana-servers.net.     21600   IN      A       208.77.188.44
d.iana-servers.net.     21600   IN      AAAA    2620:0:2d0:1::44
ns.icann.org.           21600   IN      A       192.0.34.126
```

Akamai Authority Spreading

- Frequently change authorities for zone.
  - Use short time-to-live periods on authority records, 5-10 minutes.
  - Rotate names as well as addresses to refresh caches.
- Eligible authorities determined based on constant monitoring of the state of the network.
- Active resolvers rarely need to go back to parent (GTLD) servers.

Pros

- Performance Improvement
  - Handle requests by thousands of authorities.
  - Direct resolvers to closer nameservers on network edge.
  - Redirect away from congested links.
  - Remove unresponsive servers.
- Attack Resilience
  - All of the above, plus…
  - Increase tolerance of failure by parents.
  - Reduce impact to other zones when one is attacked.

Cons

- Can be misconstrued as malicious
  - “Fast Flux” or “Double Flux” Hosting
    - Essentially same technique as double flux.
    - http://st.icann.org/pdp-wg-ff/
    - draft-bambenek-doubleflux (expired)
    - Challenge presented by double flux demonstrates the usefulness of the technique.
  - Kaminsky cache poisoning vulnerability
    - http://doxpara.com/DMK_BO2K8.ppt
  - Some proposals for stopping malicious use could also stop beneficial use.
- Larger packet size than just returning answer
  - Commonly already done.
  - Not quite so bad with compression.
- Sensitive to cache implementations
  - Tested many different caching resolvers.
  - Subtle differences amongst all of them.

Questions?

David C Lawrence <tale@akamai.com>