DNS Security (not DNSSEC)

Patrick W. Gilmore

Chief Network Architect, Akamai Technologies

DNS attacks – hard to mitigate

- Trivial to create an “intelligent” attack that is hard to mitigate

- DNS is UDP (duh)
  - Stateless
  - Easy to spoof
  - Trivial to create packets which are (nearly) indistinguishable from the real source

- So what do you do?

DNS attacks – not always “intelligent”

- There are other types of attacks

- Last attack we saw was purely volumetric
  - Large (10s of Gbps)
  - UDP packets stuff full of “A”
  - Some TCP SYNs thrown in for good measure

- Much easier to mitigate
  - Assuming you have the bandwidth
  - Or can get your upstream to filter properly

Mitigating intelligent attacks

- Several strategies to mitigate “intelligent” attacks on the receiving end
  - Anycast
  - Rate limiting

- Some ideas for mitigate with the help of the sending end
  - Ensure query-source is different from address handed to users
  - Dedicated node per large network

Receiving side mitigation – Anycast

- Obviously putting anycast nodes helps by having multiple locations to answer the same query
  - Spreads the load, adds redundancy, etc.
  - Added benefit of lowering resolution time

- While this helps in general, there is danger of flapping
  - Node A gets attacked, goes down, BGP withdrawn, attack moves to Node B, Node A comes back up, lather, rinse, repeat

- Possible optimization is using non-globally reachable anycast nodes
  - E.g. Install a node at an IX, announce only to peers

Receiving side mitigation – Rate limiting

- Multiple strategies to rate limit (e.g. RRL, discussed elsewhere)

- Danger of attacker using the rate limiting to DoS a specific client
  - Miscreant fires 1M qps at authority spoofing Comcast’s NS IP address, real queries from Comcast get limited

- Use more targeted rate limiting
  - E.g. Whatever the qps per source IP address, only start rate limiting if the total load is high
  - E.g. Watch for source addresses which violate TTL and rate limit more aggressively “out of TTL”

Sending side mitigation – Query source

- Request: For those running recursive name server, please use a different query source than the IP address you hand to end users
  - Harder to spoof
    - Not impossible, but every little bit helps
  - Makes filtering / rate limiting easier
  - Already in place for NSes behind NAT, load balancers, anycast, etc. (one would hope)

- This is a simple change with massive benefits

Sending side mitigation – Dedicated node

- Large authorities are willing to hand out anycast nodes to networks with large recursive server
- Lots of benefits
  - Faster resolution times
  - Attack resiliency – if attack takes out other authorities, you are safe
  - If attack is sourced from your network, other networks are protected (and your border is not impacted)
- No real downside
  - SO DO IT!

Questions

[Translation: Out of time…]