On the Time Value of Security Features in DNS

Paul Vixie, Farsight Security

November 2013, IEPG Vancouver

ca·nard

kəˈnär(d)/

noun

1.

an unfounded rumor or story.

Real S.A.V. Related Problems

- Indirect packet-bombing attacks
  - Triggering query looks like it came from victim
  - So, response (70x larger) goes to the victim
  - Solution: DNS RRL (Response Rate Limiting)
- Kaminsky-style cache poisoning
  - Cause or predict a cache-miss query
  - Flood the initiator with false responses
  - Solutions are: UDP SPR, DNSSEC

Not-so-real S.A.V. Problems

- Fragmentation related attacks
  - Predict/cause fragmented response
  - Flood initiator with false second fragments
  - Proposed solution: use TCP
- RRL slip=2 related attacks
  - Incite rate limiting by falsifying some queries
  - Use longer time window for Kaminsky-style attack
  - Proposed solution: use slip=1

Discussion: Use of TCP in DNS

- DNS (TCP/53) specifies that the client initiates close, or else the server uses a ~30s timeout
  - This makes channel exhaustion attack trivial
  - So if you can force an initiator to use TCP, you can force transaction failure
- TCP: 3xRTT, 7 packets, server side state
  - Slot occupancy time becomes the critical resource
  - Best case throughput is way lower than UDP

Discussion: Use of SLIP=1 in RRL

- In DNS RRL, a “slip” is a TC (truncation signal)
  - Default SLIP is 2, so, every other response
  - Everything that isn’t slipped, is dropped
- To a DDoS victim, SLIP=2 means 50% PPS drop
  - Many firewalls are PPS limited before bit limited
- To a real client, SLIP=2 means more retries
  - Retry with UDP on drops, or with TCP on slips
- Kaminsky attacks when SLIP=2 vs. SLIP=1
  - Hours vs. days of full 100Mbit/sec spoofed blast

Discussion of Qtype=ANY

- Many spoofed-source DNS attacks use QT ANY
  - This produces excellent amplification factors
- Many defenders therefore restrict QT ANY
  - This ignores QT NS, or QT TXT, or DNSSEC
- All security, like war, is really about economics
  - Attacker, defender, trying to drive other's cost up
  - Restricting QT ANY drives only one's own costs up
  - Suggestion: play at least one (!) move ahead

10,000 Foot View

- Source address validation, where deployed, prevents all known off-path DNS attacks
  - But it has to be done on attacker's network, and is therefore not under the defender's control
- DNSSEC, where deployed, prevents all known DNS poisoning attacks (including fragments)
  - But it has to be done by both producer and consumer, and is therefore not under defender's sole control

TANSTAAFL

- DNS performance (QPS) relies on statelessness
- DNS defense (DoS, poison) relies on state
- There is more than one kind of state
  - TCP, heavy weight
  - Eastlake cookies, medium weight
  - DNS RRL, light weight

Eastlake Cookies

- Clear text RN exchange, using DNS messages
- End state: each side knows the other’s RN
- Queries arriving without RN(i) are dropped
- Responses arriving without RN(r) are dropped
- No crypto, so no protection against on-path
- Proposed, 2007; Abandoned, “too complex”

Conclusion

- These are not examples of science:
  - “I’m not seeing that problem in my network.”
  - “I heard some expert say that fragments are bad.”
- Security is economics
  - We are in an information war
  - Goal: your(benefit/cost) > their(benefit/cost)
- Future > Present > Past
  - (area under the curve)