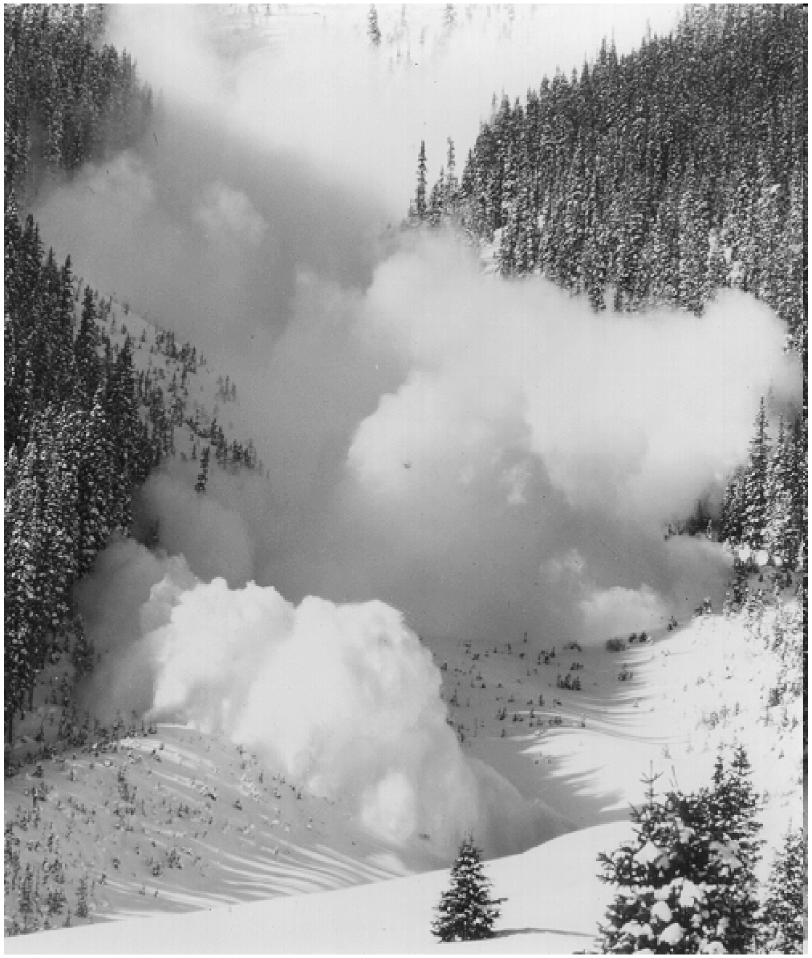
Forgery Resilience #2: Path forward

Olafur Gudmundsson

Andrew Sullivan

History

- draft-ietf-dnsext-forgery-resilience-00.txt
  - Adopted early 2007 now at IESG
  - Addresses how to add entropy to queries via non “standard-compliant” means
- Mid 2008 word of Kaminsky attack causes lots of mailing list traffic and panic.
  - DNSEXT starts process to figure out if/what to do for more FR measures



Call for ideas

- Chairs asked people to document suggestions and analysis for further work

- Drafts:
  - http://tools.ietf.org/id/draft-barwood-dnsext-fr-resolver-mitigations-08
  - http://tools.ietf.org/id/draft-reid-dnsext-aleatoric-00
  - http://tools.ietf.org/id/draft-weaver-dnsext-fr-comprehensive-00
  - http://tools.ietf.org/id/draft-wijngaards-dnsext-resolver-side-mitigation-00
  - http://tools.ietf.org/html/draft-hubert-ulevitch-edns-ping-00
  - http://tools.ietf.org/html/draft-vixie-dnsext-dns0x20-00

- Significant overlap among the drafts

Call for focus:

- Chairs asked the working group to comment on drafts and suggest what to work on.
  - Almost silence.
- Chairs invited people to join a “design” team to work on narrowing the focus of possible work and asked absent WG members to submit their suggestions.

“Design” team:

- Chairs
- Nicholas Weaver
- Antoin Verschuren
- Jim Reid
- Matt Larson
- Peter Koch
- David Blacka

We met for 2.5 hours on Monday and discussed number of ideas and tried to understand the implications of each idea as well as interaction of ideas

➔ in order to recommend a path forward

Topic: Additional Entropy

- Additional Entropy:
  - DNS Ping: ➔"just do it" helps when available, does not hurt in any case
  - Aleatoric: DNS Ping much better ➔ withdrawn
  - 0x20: helps in the case when DNS Ping is not available,
    - ➔ "Mostly harmless" the only standards actions: specify that server MUST copy QName unchanged into answer and resolver MUST strip 0x20 from answer.
  - "RTT Banding" or "Name server scatter":
    - Requires much more work before we can recommend on how to do this, at least a document on how to measure and maintain measures off Round Trip times should be written. i.e. a RTT BCP ➔ Discourage for now

Topic: Data Acceptance

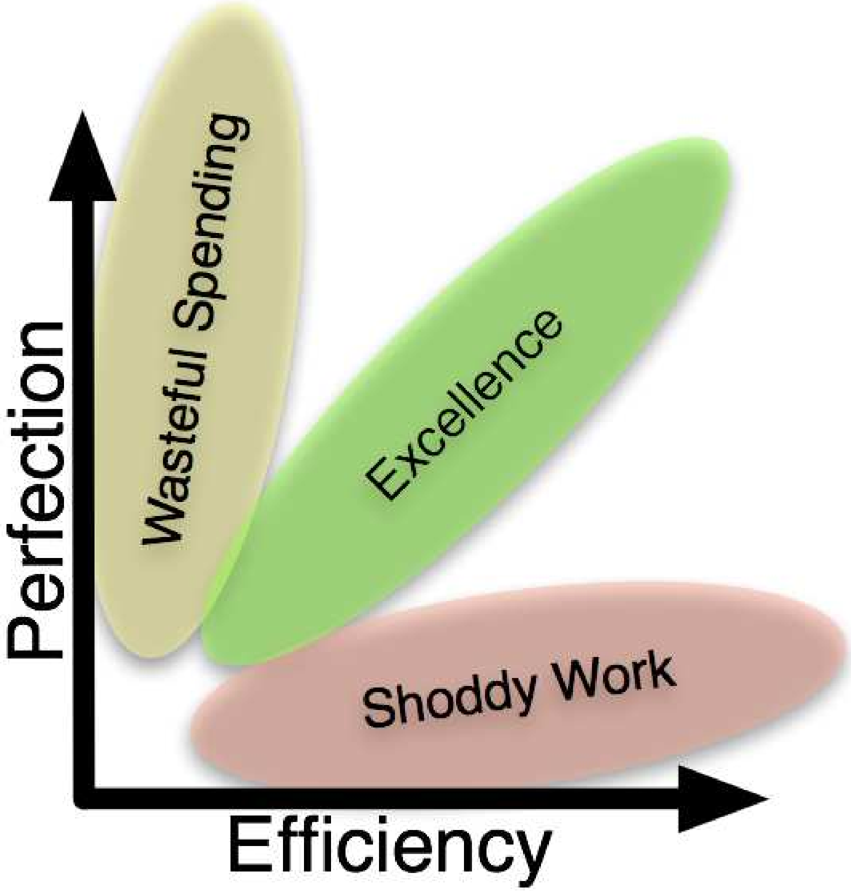
- Cache overwrite
  - At same credibility: ➔recommend against
  - Extend TTL's: ➔recommend against
- CNAME and DNAME chains:
  - ➔Recommend recursive resolvers perform the full chain processing, i.e. only accept first [CD]NAME from each answer.
- Fetch better data:
  - Some attacks rely on caches to overwrite existing data with newer data at same criticality, this can be prevented by explicitly asking authority for the data that is included in referrals.
  - Implications: more queries, may cause outages due to errors that are currently masked
    - ➔ Needs more study before recommendation

Topic: Query Fallback

- TCP
  - ➔ Should be avoided as much as possible
- Multiple UDP queries
  - Can increase entropy, when no other sources are available.
  - Increases load, and may get inconsistent answers in load balancer case.
  - ➔ Strongly preferred to TCP fallback, but more analysis needed of implications and policies (when to use, how to interpret answers, how many packets to send, where to send packets etc.).

Other options

- Do nothing, any work on this area will delay DNSSEC deployment.



Next steps: Open Microphone