Properties of an Ideal Naming System

draft-trammell-inip-pins

Brian Trammell, ETH Zürich Network Security Group

arcing BoF, Tuesday 5 April 2016, IETF 95, Buenos Aires, Argentina

Why am I here?

- Thought experiment: if we needed to design a system that did what DNS did, knowing what we know now, what would its properties be?

- Spoiler: You end up with a thing that looks a lot like DNS, with a few differences.

draft-trammell-inip-pins

(in a nutshell)

- List of properties of an idealized name system:
  - Federation, unity, transparency, revocability of authority (and uniqueness of names)
  - Authenticity of delegation and response (incl. negative)
  - Dynamic consistency, support for *explicit inconsistency* where necessary
  - Explicit support for tradeoffs among latency, efficiency, traceability, consistency.
- Musings about differences from DNS as deployed.

Insights

- Mandatory signatures make things (way) easier
  - Whole classes of problems simply disappear.
  - How long until we turn off the last non-SEC server and the last unsigned zone?
- The perfomance/privacy tradeoff space is richer than what one can implement with TTL.
- Every query and every assertion takes place within a context.
  - In the current DNS, these are always implicit.
  - And adding explicit contexts is *really hard*.

Application to ARCING

- Alternate resolution is a kind of context
    - currently (always?) implied by the name.
- Constraints on a solution for adding explicit support for it to DNS:
    - Given a name, determine resolution method unambiguously
        - Or determine it’s unresolvable with a diagnosable error
    - Add future resolution methods without breaking stuff