When DNS Fails?
-- meeting the right expectations --

Peter Koch <koch@denic.de>

2010-10-26 – Internet Dagarna, Stockholm

The Domain Name System -- DNS

- Hierarchical Namespace
- Application use of the Namespace
- On the Wire Protocol
- Software
- Operational Interdependencies
- Provisioning
- Policy
- Research
- Education

The Domain Name System -- Namespace

- Hierarchical Namespace
  - Scalability? Addressability? (better: „Nameability“)
- Application use of that Namespace
  - Mapping function vs. Location vs. Discovery
  - What to query for and under which name?
  - RFC 1535 („*.EDU.COM“) style issues
  - Pointers vs. Data
  - Presentation and I18N
  - Under continued consideration within the IETF

The Domain Name System -- Protocol

- On the Wire Protocol
  - Lightweight, mostly UDP
  - Redundant, resilient, largely fault tolerant
  - Lack of data origin authentication, but DNSSEC is „available“
    - at the cost of reduced fault tolerance
  - IETF‘s responsibility
- Presentation issues (a.k.a. IDNs)
  - Protocol identifiers exposed to Humans
  - Largely context dependent
    - DNS hierarchy supports delegation of responsibility -- not inheritance
  - IETF work („sameness“) struggles with lack of clearly specified requirements

The Domain Name System -- SW + OPS

- Software
  - … has bugs, so does DNS software (sometimes)
  - … may initiate swarm effects
  - diversity is important!
  - … as is operator - vendor - research interaction
    - Which is what happens in the IETF, OARC and the various *NOGs
    - Please note that these fora provide a meta level of diversity!
- Operational reality
  - … also calls for diversity
  - DNS is only part of a puzzle (routing, general systems security, …)
  - Trusted (bottom up) communication between peers
    - cf OARC, *NOG, various peered lists

The Domain Name System -- Provisioning + Policy

- Provisioning
  - mostly standardized, but diverse in the details
  - key for security from the users‘ perspective
    - „loosing“ a domain name
  - R-R-R model provides for wide range of demands and requirements
- Policy
  - suggests what can be provisioned (registered)
  - needs to accept operational constraints and such in technology
  - can sometimes drive innovation
    - but only with deployment curve duly considered
    - as well as basic properties of underlying mechanics

The Domain Name System -- Research+Education

- Research
  - Pro-active to detect and explore risks
    - Root scaling, DURZ, …
  - Traffic and incident analysis
  - Increased level of attention from academia and operators
    - CAIDA, OARC, NDSS, measurement workshops …
- Education
  - … helps prevent human errors
  - Works by both
    - disseminating up-to-date technical knowledge
    - Establishing contacts between peers
  - Variety of channels and venues: IETF, ISOC, NSRC, TLD initiated prgs

The Domain Name System -- Summary

- Failure?
  - + Several examples of outages, glitches, mistakes and errors
  - - and how (sometimes concerted) efforts of a diverse set of organisations reacts, learns and prevents
- False assumptions
  - may lead to perceived failures:
    - policing content through DNS
    - presentation issues and user experience vs. protocol identifiers
    - names/identifiers vs. semantics

?

Thank You!

<koch@denic.de>