DNS Related Activities During IETF79

Johan Ihrén
Autonomica

November 12, 2010

DNS Related Activities During IETF79

- DNSEXT
  - The usual mix of Hard Problems(tm) and Bad Ideas(tm) ;-)
- KIDNS: Cryptographic Keys In DNS
  - We've talked about this for years, but now it is finally beginning to happen
- DNSOP
  - Main issues were DNSSEC Key Timing, NSCP (i.e. nameserver control protocols)

DNSEXT

DNSEXT: draft-faltstrom-uri-06

- URIs are a layer of indirection between domain names and point of service

```
$ORIGIN example.com.
_http._web IN URI 10 1 "http://www.example.com/"
$ORIGIN example.net.
_http._web IN URI 10 1 "http://www.example.com/"
```

- This proposal may be regarded as a superset of the functionality provided by `SRV` while "enhancing" the functionality of `NAPTR` (by allowing specification of what `NAPTR` records are of interest).
- A core issue is what to aim for with this proposal. For widest possible applicability it is needed to somehow support "unregistered services". On the other hand, for tightest possible binding something stronger than the "_" convention may be needed. Is the aim for something that plays well with other proposals?

DNSEXT: draft-yao-dnsext-identical-resolution-02

- Intended as "the problem statement" for the generic discussion of aliases and "variants" in DNS that has been going on for more than a year
- The real question with this draft is whether it is sufficiently close to "done" to actually close the "problem statement" phase. If not, this issue will be thrown over the wall with the hope that the IRTF picks it up
- Target for new revision in 4 weeks (early December). Hard Push for WG review of that version and WGLC in mid-January

DNSEXT:
draft-kitamura-ipv6-simple-dns-query-00

- Deals with the alternatives for issuing queries for A and AAAA respectively: in serial or in parallel.
- Percieved problems with issueing two queries: higher latency and twice the traffic. It may also cause difficult problems for "less clueful" end users
- The intent is to simplify this by sending just one query. Several alternatives are possible:
  - A send both A and AAAA query in same packet
  - B new combined type A+AAAA (a meta type)
  - C query for AAAA, return IPv4 mapped address in the v4 case
- Problem statement seems to be unclear. Strong message about the need to start with identifying a problem and clarifying the need to solve it.

DNSEXT: `draft-vixie-dnsext-resimprove-00`

- Main topics are
  - Delegation Revalidation Upon NS RRSet Expiry
  - Stopping Downward Cache Search on NXDOMAIN
    - "if there is an `NXDOMAIN` cached for `foo.bar.example.` then don't issue a query for `baz.foo.bar.example.` but instead just return the `NXDOMAIN`"
  - Upgrading NS RRset Credibility Upon Delegaton Events
    - new semantics for issuing extra "validation" queries to the child nameservers when detecting a zone cut
- In general, "optimizations" like these are hardly justified just because "it seemed like a good idea at the time"
- No clear enthusiasm in WG

KIDNS

KIDNS BOF: Crypto Keys In DNS

- Put a **key** or a **certificate** into DNS
- Sign the zone, including the new data
- Applications will trust the data based on being able to validate the DNSSEC signatures
  - Very similar to SSH+`SSHFP`

KIDNS BOF: Crypto Keys In DNS

- Put a **key** or a **certificate** into DNS
- Sign the zone, including the new data
- Applications will trust the data based on being able to validate the DNSSEC signatures
  - Very similar to SSH+`SSHFP`
- This is an old idea that has been talked about for years
- RFC 4398 (CERT RR)
- `draft-schlyter-pkix-dns` (very old and expired, was "too early")
- BOFs during IETF78 and IETF79, will become a WG before IETF80 next spring

KIDNS, cont'd

- DNSSEC is obviously needed for this to work out, however DNSSEC by itself is not really enough
  - For this to be viable there's a clear need for the client to **know** whether the answer was secured or not
  - . . . as well as the need for a **trusted** channel to the **trusted resolver**
  - Both of these are a bit problematic today

KIDNS, cont'd

The primary issue with KIDNS is:

- There is a major difference between using DNS as **transport** for keys and certificates that are otherwise secured and authenicated (i.e. a la the `CERT` record) and using DNS/DNSSEC as the **trust path** for the keys and certificates.
  - In the latter case documented process for verification of identity, etc, that a Certificate Authority does is replaced by processes managed by the chain of DNS/DNSSEC operators between the cert and the **`trust anchor`** that the validator chooses to use

KIDNS, cont'd

- But in spite of open issues with KIDNS it is clear that there is a lot of enthusiasm for the general concept and it seems likely that interesting things will happen in this area
- Mailing list: `keyassure@ietf.org`
- Proposed charter:

`http://trac.tools.ietf.org/area/sec/trac/wiki/Keyassure`

DNSOP

DNSOP: `draft-ietf-dnsop-dnssec-key-timing-02`

- This draft has been kicking around for more than two years, mainly due to the evolving nature of the subject matter
- The question was asked whether it would be best to publish now (with some known omissions)
  - in the spirit of "timeliness"

  or to continue work
  - in the spirit of "perfection"
- Consensus was for publication of current document with suitable caveats about open issues and also to initiate work on a `-bis` document to close the open issues

- The document is heading for `Informational`

DNSOP: draft-livingood-dns-whitelisting-implications

- The underlying idea with this proposal is that there is a certain fraction (larger than zero) of "customers" that will get in trouble if they receive a response to a **AAAA** query
  - Perhaps they don't have working v6 transport, but don't know that, etc. See Lorenzo's presentation earlier today
- . . . and if the customer is known, then it would be possible to define a policy of not giving out the **AAAA** response for customers that would be hurt by it
- There are issues with this. One is that this implies lying, potentially in an authoritative server (as opposed to the already widespread lying in recursive servers that exists). Another is that the lying will make it difficult to get this to work with DNSSEC

DNSOP: Nameserver Control Protocols

- This is a topic that has been kicked around for a number of years and to some the problem statement is “obvious”
  - Read: anycast operators and other large-scale DNS operators
- But to others it is not at all “clear”. For example, there are suggestions that one intended use is to control the “zone statement” for “my zone” in the slave server under someone elses control

DNSOP: Nameserver Control Protocols #1: `draft-kong-dns-conf-auto-sync-01.txt`

- This proposal is based on the idea that nameserver configuration "stuff" can be encoded in DNS zone data and transferred to a remote nameserver via standard DNS protocol
- The DNS message format for "configuration zones" is interpreted in completely new ways. There is also a need in here for a new DNS opcode (similar to `NOTIFY`)
- There are several examples of prior art to this, all, umm, kludges, as would be expected from this type of mix between "control plane" and "data plane"
- Question: doesn't the needed violence suggest that this is not the solution that would emerge from a design from scratch?

DNSOP: Nameserver Control Protocols #1: `draft-kong-dns-conf-auto-sync-01.txt`

- This proposal is based on the idea that nameserver configuration "stuff" can be encoded in DNS zone data and transferred to a remote nameserver via standard DNS protocol
- The DNS message format for "configuration zones" is interpreted in completely new ways. There is also a need in here for a new DNS opcode (similar to `NOTIFY`)
- There are several examples of prior art to this, all, umm, kludges, as would be expected from this type of mix between "control plane" and "data plane"
- Question: doesn't the needed violence suggest that this is not the solution that would emerge from a design from scratch? In other words, this seems to be the result of laziness à la

"if all you have is a hammer, every problem looks like a nail"

DNSOP: Nameserver Control Protocols #2: `draft-dickinson-dnsop-nameserver-control-01`

- This proposal is built on top of **`netconf`**, hence it hands off most of the transport and authentication infrastructure to **`netconf`** which allows more focus on the actual protocol functionality
- It is clearly mapped quite closely to the requirements document, which is good and makes evaluation easier
- It does suffer a bit from being more heavy-handed with the need for a **`netconf`** XML parser, etc (there are open source **`netconf`** implementations, but not many)
- But apart from that it is a rather clean solution

FYI: Multiple Interfaces WG (MIF)

- From the MIF Charter:
  "A host attached to multiple networks has to make decisions about default router selection, address selection, **DNS server selection**, choice of interface for packet transmission, and the treatment of configuration information received from the various networks. Some configuration objects are global to the node, some are local to the interface, and some are related to a particular prefix. Various **issues arise when contradictory configuration** objects that are global to the node are received on different interfaces. At best, decisions about these matters have an efficiency effect. **At worst, they have more significant effects such as security impacts**, or even lead to communication not being possible at all."
- Rephrase: "Guess what, split-DNS gets more painful when not only the firewall bridges namespace domains"

Other WGs with DNS Stuff In Them

- WEBSEC WG seems to be using/depending on DNSSEC, with potentially wrong intentions/assumptions/promises
- BEHAVE WG: DNS64 mapping ideas that are "not trivial"
- ALTE WG and GEOPRIV WG: weird ideas about using reverse DNS

- However, I haven't been able to follow any of these myself, so I lack enough details to really say anything more about them

Other WGs with DNS Stuff In Them

- WEBSEC WG seems to be using/depending on DNSSEC, with potentially wrong intentions/assumptions/promises
- BEHAVE WG: DNS64 mapping ideas that are "not trivial"
- ALTE WG and GEOPRIV WG: weird ideas about using reverse DNS

- However, I haven't been able to follow any of these myself, so I lack enough details to really say anything more about them
  - But it is clear that it seems to still be high season for using DNS for all sorts of strange and mysterious purposes. See earlier comment about "if all you have is a hammer"

DNSSEC History Wiki

- DNSSEC History Wiki, Steve Crocker
  - October, 2010: 53 TLDs signed, 42 in the root
  - November, 2010: 63 TLDs signed, 46 in the root
  - Goal to to try to capture as much history as possible before it is lost forever
  - Get involved at

    `https://wiki.tools.isoc.org/DNSSEC_History_Project`

DNSEXT

- The old mailing list **`namedroppers@ops.ietf.org`** is gone

DNSEXT

- The old mailing list **`namedroppers@ops.ietf.org`** is gone

- New name is **`dnsext@ietf.org`**
- We will just have to adapt