A Technical Overview of `.tel`

Jim Reid
`jim@telnic.org`

Introduction

- Why **`.tel`** is different
- Architectural overview
  - Technical/business considerations
- DNS characteristics/challenges

Why `.tel` is different

- Not just yet another (boring) registry-registrar type new TLD
  - Conventional delegation-only model though
- No user defined address records in `.tel`
  - ICANN made us do it...
- `.tel` delegations will primarily contain NAPTR records
  - It's about **contact** data, not content

Architectural Overview

- Sponsoring Organisation System
  - Member database & guests
  - Developer web site
- Name Service Provider System
- Applications

NAPTR Records - 1

- Identify arbitrary communication end-points:
  - Phone numbers, email/SIP addresses, IM handles, URLs, SMS/MMS, etc., etc.
- Amazingly powerful and flexible
  - Order and preferences
  - Regexp matching and substitution
  - Can build data structures in DNS
- Essentially mini-programs

NAPTR Records - 2

- Horribly, horribly ugly:

-
  ```
  jim.tel. IN NAPTR 10 54 "U" "E2U+voice:sip"   \
  "!^.*$!sip:jim@rfc1035.com!" .
  ```
  - A SIP address for yours truly
- Even experts get these wrong
- Can’t ever put these in front of the public
  - Try explaining this to your mother...
  - Conventional zone file managers just won’t do

DNS Challenges in `.tel` - 1

- Very different zone characteristics
- Conventional zone files are small and static
  - Handful of “usual” RRs that rarely change
- `.tel` zones should be big and frequently changing
  - Many tens (hundreds?) of NAPTRs
  - Potentially updated several times a day
    - Changes have to propagate FAST
    - Low TTLs to avoid stale data getting cached

DNS Challenges in `.tel` - 2

- Usual server/zone provisioning models won’t do
  - Typical push 1-2 times a day
  - **`.tel`** will need far more rapid propagation than that
    - Effectively updating in real-time
- Lots of zones to manage too
  - => Database-driven back ends
- Can’t really do this with text-based zone and config files

DNS Challenges in `.tel` - 3

- Lookups in `.tel` have to be fast and reliable
  - If not, "`.tel` is bad..."
- All name servers in `.tel` will be accredited
  - Must meet Telnic requirements
    - No lame delegations or misconfigured servers
  - All name servers live under **`dns.nic.tel`**
    - Should mean no more than two lookups to resolve anything

DNS Features

- Privacy
  - Users must be able to protect their private contact details, but DNS is public
- Profiles
  - Switch published contact data:
    - “I’m on a plane/asleep/in a meeting/at home”
    - New RR in the pipeline to indicate this
- Keywords
  - Useful for search/directory services

DNS Provisioning

- NSP system (Tel-hosting)
  - Published specs and SOAP API
  - Free open-source software implementation
  - Initially free hosting service from Telnic
- Registrars will probably run NSP systems (one day)
- Tel-hosting providers will be accredited too...
  - Support SOAP APIs, privacy & profile features, import/export, keyword insertion, undo, etc.

NSP Overview

- Written in Java (J2EE)
  - Tomcat & Apache
  - Postgres as default back-end database
    - Would work with any reasonable RDBMS
- Partitions: multiple virtual instantiations
  - Could be one per registrar
  - Or one per reseller on a registrar's NSP
- Supports most sane DNS implementations
  - BIND (text or DLZ), PowerDNS, NSD, etc.

The Privacy Issue

- How can an email address or phone number go into the DNS and be unreadable by spammers and marketing scumbags but still be available to friends and family?
  - Encrypt them!
  - Use **`x-crypto`** NAPTR service type
  - See I-D **`draft-timms-encrypt-naptr-01`**
- Friending system analogous to social networking web sites

How Friending Works - 1

- Bob wants to get private contact data from Alice
  - SO system generates RSA key pair for Bob
    - Public key component stored in the DNS as KEY (NKEY) RR
    - Private key stored in PKCS#8 at SO system
      - SO system doesn’t know Bob’s private key
- Bob sends a “can I be your friend?” message to Alice saying where this public key lives

How Friending Works - 2

- Alice accepts the request at her leisure
  - Alice's NSP gets Bob's public key from DNS
  - Alice's NSP encrypts contact data for Bob with his public key
  - Private contact data for Bob stored under ***`uniquestring`*****`.alice.tel`**
- Friending acknowledgement from Alice tells Bob which domain name to use to retrieve the encrypted content she's just set up
  - Bob remembers this :-)

What this means for **`alice.tel`**

- Alice may have tens of contacts
  - Phone/fax/mobile/work numbers, email & SIP addresses, IM handles, etc., etc.
- If she has tens of friends, she can publish different encrypted contacts for each of them
  - => Some hundreds of NAPTRs in **`alice.tel`**
- NSP can store encrypted NAPTRs in its database
  - No need to encrypt on the fly when Alice switches her profile

What this means for NSP

- Users will want to publish same contact data to a group of individuals
- Granularity of NSP is one-to-one
- NSP has the concept of groups
    - Group can have arbitrary number of members
    - Same content published to entire group
    - Each group member has a discrete RSA public key and subdomain of **`alice.tel`**

Applications

- Need to provide tools to promote usage:
  - Publish and lookup stuff in `.tel`
- Unhappy experiences with web browsers
  - Telnic-operated web proxy
- Free open-source software:
  - Plug-ins to do address book integration for Outlook, Windows Mobile & Blackberry
  - Proof of concept iPhone client

Parked Applications

- MacOSX AddressBook plug-in
- Java client for Symbian mobile phones
- NTN wizard
- Likely to be thrown over the wall to developer web site: **`dev.telnic.org`**

`vip.tel`

- Free test of the **`.tel`** system
  - Get real-world experience of user behaviour and what functionality is liked/hated
  - Staged introduction of feature set
    - Applications, privacy, profiles
- Will go away when **`.tel`** launches
- Sign up by email: **`vip@telnic.org`**

Launch Timetable

- **`vip.tel`** to be announced at ICANN meeting next week
    - Stops at Landrush but may re-emerge later
- Sunrise starts 15:00 GMT Dec 3rd 2008
- Landrush starts 15:00 GMT Feb 3rd 2009
- GA begins 15:00 GMT March 24th 2009