Council of European National
Top Level Domain Registries

Brief report on IETF 85
4 - 9 Nov , Atlanta, USA

A glimpse from the IETF in Atlanta

Internationalization one reason for new Whois, but difficult to do protocol-wise

Discussions at the WEIRDS Working Group get interesting. Meeting in Atlanta, the group addressed the issues of „internationalization“ and security. Internationalization has been one of the major operational issues calling for another Whois reform, according to ICANN and the RIRs. Given the agreement in the WG that the IETF will not make requirements about what kind of languages (Chinese, English), character sets (Traditional or Simplified Chinese, ASCII or ASCII plus Umlaut) or even transliterations (Peter-Pedro-Pjotr) should be offered to incoming queries, the protocol presumably will allow to answer just with all that a registry got. Publication of no internationalized registration data will be one of the possible options for registries (besides publishing internationalized contact data only or with added translation or transliteration).

A status quo solution certainly will not address one major issue of law enforcement or the intellectual property community – the latter being the main users of the new Whois according to an ICANN Board member participating in Atlanta. Mentioning these user groups did not amuse the Working Group Chair, Olaf Kolkman, who said there were already many user groups. Certainly the ongoing debates about Whois and Whois data accuracy as an indispensable tool for law enforcement and the IP-community at ICANN – and the requests of the very same groups for „clean databases“ towards the RIRs explain the current push for a quick solution.

The Chair of the DNS WG, Peter Koch (DENIC), in a discussion about the attraction of the next Whois to the ccTLD community, warned that pointers to upcoming regulation making it mandatory were no good selling-point. Barbara Roseman from ICANN reminded the WG that only those TLDs under ICANN contract would be bound by a future Whois-policy. Certainly nothing would prevent any regulators to take up a finalized WEIRDS standards and make things mandatory, said former IAB member John Klensin, therefore the WG had to be careful when crafting the protocol.

With regard to internationalization issues, at least tags for character sets (based presumably on the tag list available from RFC5646) are expected to help to sort out some of the language issues. Simon Perreault (Viagenie) pointed to a vCard related draft by Peter St André that was addressing the internationalization issues.

How difficult it is to draw the fine line between policy and protocol – perhaps WEIRDS is one example making this difficulty very obvious – was illustrated by the discussion about the data model and a potential minimum answer to a WEIRDs query. Could a valid WEIRDS answer just be empty? Or should the protocol ask for a minimum set. The Working Group would have to carve that line very carefully to stay free from policy decisions, Area Director Pete Resnick said. The inclusion of a data model alone also is not yet on the list of the WG milestones. Should that data model be part of the standards package?

The model inventory document (drawn from an overview of Whois data sets in a variety of TLD registries) shall become final over the course of the next few weeks; during the Atlanta session there was no agreement on the completeness of data objects gathered in the inventory. Interestingly only 65 of 124 TLDs (106 ccTLDs, 18 gTLDs) surveyed delivered „registrant name“ to a Whois Query. The highest number of labels found for one data object was related to name server for which 63 variations were found (Name Server, Name Servers, nserver).

ICANN meanwhile has pushed the development forward by assigning CNNIC a pilot study on the new Whois – while the IETF protocol is still working. So far there are only implementations of the concept at the RIRs – that is, for numbers but not name registries. Scott Hollenbeck from VeriSign said during the session that VeriSign was also implementing already, yet as it was only a thin, and not a thick registry, additional implementations would be welcome alongside the CNNIC implementation.

A thick Whois Policy Development Working Group of the Generic Name Supporting Organization at ICANN has after some delay now been officially started (Charter is here), with Volker Greimann, Legal Counsel of the German Registrar Keysytems made the Chair. The ICANN Board also just announced that it has asked the new CEO to take a two-track approach. “In addition to a full examination of WHOIS, the Board wants to make certain that enforcement of existing Whois reporting requirements is strengthened (…)”, Crocker said according to an ICANN press release.

MDNSEXTBoF – Controversy about how Vendors use the IETF process

Driven by Apple, a BoF to extend DNS service discovery and multicast DNS was held in Atlanta. „Armed“ with a letter by the US academic community, Stuart Cheshire from Apple, presented a first requirements draft (co-authored with Kenny Lynn) to address issues of „service discovery beyond local links“ in a further extension to mDNS (RFC 6762) and DNS-SD (RFC 6763). Some observers warned that in fact Apple tried to get an IETF blessing for a „wider Bonjour-Services“. Bonjour is an Apple solution outside of the IETF process.

According to the Educause letter presented and quoted at lenght in the mDNSEXT requirements draft, the problem to be addressed is that Apple's Airplay often breaks when users (of Apple TV or Apple Print) are sitting in various subnets. Yet it was common practice in bigger academic, university or also enterprise networks, to use different IP subnets, the Educause letter further reads.
The lenghty quote of the Educause letter is rather unusual, and is potentially made in an effort to put pressure on hardware vendors.

The four scenarios addressed by the draft were enterprise scenarios, academic networks, multi-link home networks (envisaged in the IETF homenet group) and multi-link/single prefix (mesh) networks (envisaged in low-power lossy networks, RPL/6LoWPAN). The goal of a potential IETF working group would be a solution that „seamlessly integrates zeroconf (mDNS) and unicast (global DNS) name services“.

That very „marriage“ of the local name space with the global name space is what concerns some DNS experts as the question of boundaries would arise. During the BoF there were also hints to earlier solutions for the issue, especially the „service location protocol“ that allowed registering services and requesting for these in large, yet local networks.
An additional document based on the use of a „.site“ gTLD coupled with an obligation to send all queries for names ending with sites to “the xmDNS multicast address (FF05::FB) and its IPv4 equivalent to 239.255.255.239“ is currently discussed on the mailing list.

An IETF for BoFs

None of the major DNS-related Working groups – DNSOP, DNSEXT or DANE – were meeting in Atlanta. Instead there was a considerable number of BoF sessions, three in the security area alone and yet another web security related in the Operations Area. There are several more recent working groups that tackle Web security, with Websec and Oauth, already.
The current rush to addressing authentication, authorization and TLS certificate issues, while certainly resulting from leak events (DigiNotar, etc), also could be read as an answer to the competition to the certification business as a whole from DANE. Both the the CERTRANS and WPKOPS BoF consider certificate issues specifically.

CERTRANS on „certificate transparency“ is considering an obligation for all certification issuers to publish certificates. This would allow to get alert messages on certificates issued for their domains (comparable to Google alert messages on selected news topics, as described by Adam Langley from Google). The proponents argue that that would help, for example, to prevent that certificates are wrongly issued (without the permission or knowledge of the resource owner). Certainly it is unclear if certification companies would agree to move to such a „register“ over a proposed period of 5 or 10 years.

The draft proposal („sunlight proposal") written by Langley and two Google colleagues presented during the CERTRANS session speaks of publicly auditable „certificate logs“. The logs shall contain a server certificate that would enable querying a PKI path to a root.

The question of how self-signed certificates based on Dane would fit into that system was immediately discussed. Contrary to the publicly searchable „logs“, according to DNSOP Chair Peter Koch, Dane was still allowing non-public certificates. Sunlight co-author Ben Laurie has just announced that the authors wanted to get an experimental RFC first before considering a WG. The experimental RFC would „cover the operation of the log, the log protocol and TLS client verification of CT.“ The authors wanted to „specifically target the use of CT with PKI and HTTPS, and not other applications such as DNSSEC, self-signed certs, device certs or TLS secured protocols.“

WKPOPS - The major goal of WKOPS described during the session was to document existing practices in web PKI which had grown a lot over the last 15 years and were messy and often broken. A problem list was presented by Jeff Hodges from Paypal (including different profiles of X509, various uncertainties regarding to user agent behaviour and inconsistency of browser behaviour). A survey study to document current practices that would lead – potentially – to guiding principles for better harmonization was talked about, but was at the time of the Atlanta BoF not part of the draft charter. It is expected that a WG could start in the Apps area.

The BoFs seemed to push for some reform in the certification business, yet some call these efforts a „swan song“.

HTTPAuth – During the HTTPAuth session there was a heated discussion about the scope of a potential WG. HTTP authentication while already available was not much in use, therefore the WG wanted to offer additional HTTP authentication schemes for experiments. Basic idea of most is to create alternatives for password-based HTTP authentication.

Due to the fact that web authentication is well developed with OpenID, OAuth or the older SAML, the BoF resulted in a rewrite of the potential WG charter, underlining that web authentication was out of scope, as well as websec, which has a special WG (that excluded HTTP authentication). A potential WG would closely cooperate with httpbis. A big re-write of HTTP authentication, many said, was not possible. How big the interest is in the topic is illustrated by the number of drafts tabled: there are five from different author teams.

draft-williams-http-rest-auth
draft-oiwa-http-mutualauth and draft-oiwa-http-auth-extension
draft-farrell-httpbis-hoba
draft-montenegro-httpbis-multilegged-auth
draft-melnikov-httpbis-scram-auth

VideoCodec - One of the BoFs was related to the ongoing RealTimeWeb. After standardizing an audio codec for realtime web applications, the IETF is now about to tackle the video codec. Audio Codec WG Chair Cullen Jennings presented caveats to the BoF, pointing not the least to the IPR discussions around what was intended to be a really royalty-free codec. While Mozilla's external counsel has said the IETF Opus audio codec did not need a licence, Qualcom's lawyers disagree. The Trust has accordingly assigned licenses allowing derivative works from the Audio Codec which is rather unusual.

Cullen Jennings recommended to have a clear strategy for how royalty free would be realized, also if the WG wanted to choose from existing technology or was creating new technology. For the video codec, again, there was a group bringing a practically ready protocol, while another was proposing building blocks.

Proposals for the video codec have been tabled by Mozilla and Google (VP8). Stephan Wenger, former Nokia IPR employee, rejected the idea that a royalty-free codec was close to impossible. Wenger also went on about the IETF again rubberstamping a codec where the IETF had no video codec experts.

Interestingly the IETF gets into troubled waters with the video codec, with different other standardization organisations developing codecs, like the ITU, who is rather proud about its Emmy-award-winning H264-codec (which finally was developed by ITU and MPEG-Visual in what is called the Joint Video Team.)

SAAG: Catastrophic failure to happen soon due to SSH problems
Tatu Ylonen, from SSH Communication Security, warned against vulnerabilities from sloppy SSH key management.

A survey according to Ylonen showed that many companies and organizations, for example some of the top ten banks in the world, had so many SSH keys they completely lost track of it. There was no limitation about who could set SSH keys, and there was no documentation about the existing keys. In one large of the top 10 banking institutes there were 1,7 million keys, for 10000 servers, making the average number of keys sitting on one single server 170.
The main problem was that with an attacker once successfully broken into one tightly knit mesh, he got access to all that keys lying around and, as no passphrases were necessary but automatic access to services was the norm, this was the perfect back door.

In principle this was no technical problem of the protocol, rather it was sloppy administration. Most companies for example did never remove keys, but still added new ones to the pile. In the end when employees left the companies their keys were still sitting there and finally nobody dared to delete them out of fear the key might be important for one of the services in the network.

Access to keys sometimes also was made very easy by the decommissioning of old machines. Ylonen reported about an instance in which the Airforce had decommissioned a server and asked the new owner to please wipe the data. Again, the lack of rules, monitoring and documentation was the problem.

A worst case scenario according to Ylonen would be the quick propagation of a virus over a compromised system using the keys found and the automatic access opened to a variety of servers, perhaps hosted machines and services outside of the originally infected networks. The spread to one million servers in 20 seconds was realistic, Ylonen thinks. Especially when core infrastructure systems were targeted, the consequences could be catastrophic. If combined with destruction code, he is concerned, banks, logistics, telecommunications, refineries or government agencies could be affected and down by a large scale attack.

The idea presented by Ylonen at the Security Area Advisory Group (SAAG) was to write a best practices document on the SSH key management to avoid issues as mentioned.

IETF News

IETF IAOC Chair Bob Hindon presented the the budget for the coming year, with no big changes, especially no changes in registration fees. Major contracts would be extended.

The 2013 expected revenues are 3.3 million US dollar (combination of revenues and sponsorship) expected expenses are 5.3 million, with ISOC paying for the deficit (including some capital IT investment in 300.000 US Dollar for IETF and the RFC editor) of around 2.2 million. The 2012 year figures presented by Hinden showed that it was possible to cut the ISOC contribution to for 2012 by 573.00 US $.

Hinden also announced that it was still looking for hosts for IETF 88 (Vancouver) and 89 (London); hosts for IETF 86 were Comcast and NBC Universal, while DENIC and EURID were sponsors for the IETF 87 in Berlin. Additional sponsors for IETF 87 were welcome.

Trust Chair Marshall Eubanks had stopped participating in the work and communication of the Trust and as he did not get back to calls and other communication the IETF Trust did remove him as a chair. While a call for a new trust chair is out, Ole Jacobsen has taken up the function until March 2013 on an interim basis.

Chair Russ Housley in Atlanta reported back to the Community about the over 20.000 US $ donations made so far for the Open Internet Endowment.