Council of European National Top Level Domain Registries

Report on IETF 89 London

3 - 7 March 2014

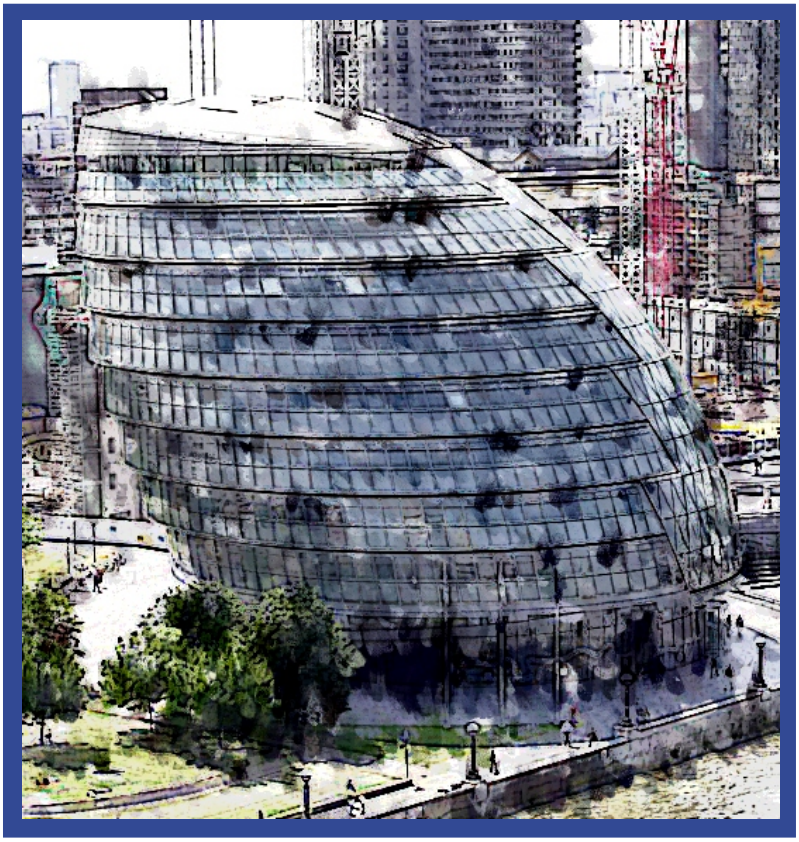

Table of Contents

More Hardening - STRINT workshop and more

For close to a year the technical community has had time to come to grips with the the ongoing stream of revelations about pervasive surveillance of Internet communication up to a point where security technology has been undermined or even manipulated. IETF Chair Jari Arkko in all public speeches given around the IETF meeting said that "security hardening" work had taken up a considerable amount of time of IETF work.

Following the commitment in the Vancouver technical plenary to start mitigating the "attack" of "pervasive monitoring" via protocol design and "make pervasive monitoring significantly more expensive or infeasible", the IETF community according to Arkko now has to deliver on its promise. Passing the Best Current Practice document on the commitment (sent to the RFC editor queue during the London meeting) certainly was only the first step, Arkko said during the administrative plenary in London. Coming up with and implementing protocol changes was more difficult, and possibly not as exciting.

Arkko himself pointed to the rise of secure connections as one more visible result for the efforts. A glance at the working group meetings in London also illustrates quite a lot of energy to work on the security/pervasive monitoring issue. Beside a burst of discussions over DNS privacy (see below), the ongoing work on the http renovation and considerations how to go forward in selecting crypto algorithms (see SAAG WG report below).

Using TLS in Applications

A brand new WG (that did not even have a preceding BoF) was dedicated to discuss "using TLS in applications" (UTA). There was a lack of interoperability and deployment of TLS with applications so far, Orit Levin, Microsoft Principal Program Manager and Standards Professional, said during the BoF when presenting the goals of a future UTA WG.

Deliverables discussed in the UTA meeting are documenting security breaches to application protocols, guidelines for using TLS, plus a set of documents describing existing and future practices for using TLS with applications protocols from SMTP, POP, IMAP, XMPP, HTTP 1.1. Also the BoF talked about a document on "opportunistic encryption", the latter being a hot topic in many discussions.

Workshop on "Strengthening the Internet Against Pervasive Monitoring (STRINT)"

Opportunistic encryption was also a topic discussed vividly during a dedicated workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT) organized by the IAB and W3C and partly funded by EU research funds, just before the IETF meeting. The meeting was attended by over 100 experts, and fed with close to 70 paper submissions of the participants on a variety of technical and policy topics related to pervasive monitoring.

The mechanism of opportunistic encryption should be explained in a "cookbook-like" RFC, IETF Security AD Stephen Farrell summarized rough consensus at the meeting. A guideline text recommending "on by default" security/encryption and a new edition (or addition) to BCP 72 on the security section of RFCs are also on the agreed upon to do lists.

During the strint meeting there were some prominent voices, including PGP developer Phil Zimmermann (Circle) and Steve Bellovin (Columbia University), who underlined the need to take

another step forward with regard to encryption. Due to a changed threat analysis and better computational powers it was the right choice.

Opportunistic encryption was defined at the workshop as encryption without prior authentication via certificates, DANE records or the likes. An exemplary implementation was presented for MPLS. One advantage of a light-weight opportunistic encryption that should be made the "on-by-default" standard, according to a clear majority at the meeting would be that users did not need to understand or even be asked.

There certainly are concerns that the measure, which leaves communication open to active attacks (while preventing the passive, pervasive monitoring type), would result in complacency and slowing down to make bigger steps towards real end-to-end security. One interesting project for example that is up and running is the Open Crypto Project that works currently on an open crypto chip design and prototype(s) and an assured Toolchain .

Another action items coming out of the STRINT workshop include a world day of bad certificates (with representatives from Chrome, Mozilla, Apple and Microsoft on the spot). A whole round of talks was dedicated to the problem of metadata and their possible minimization, here the XMPP community was pointed at as a potential guinea pig. Even for the DNS there have been ideas on how to make cautious steps, for example by not serving complete queries up the DNS chain.

Requests to not make the dissident-safe standard the common standard/"Legalize it!"

With a considerable interest in the hardening efforts there are on the other side concerns about undue burdening of infrastructure and devices (and or users). Steve Kent (BBN) for example warned during the STRINT workshop not to make the needs of "a few poor souls" the standard requirement (and thereby burden everybody with regard to complexity and latency). ISOC Chief Internet Technology Officer Leslie Daigle reacted by pointing out that one never was sure if one was one of those poor souls.

One problem discussed for some time was that of traffic monitoring (for a variety of academic or operational reasons). The "need to overcome the friend-foe-paradigm" was stressed in a STRINT paper by Jan Seedorf (NEC Labs) and others. There was a conflict between the protection against pervasive monitoring and user-friendly operations by services providers, such as proxying, fire-walling or performance monitoring. The paper mainly proposed to allow for specific operations on transmitted traffic using, potentially, homomorphic encryption. Seedorf said it might be possible to touch only parts of the secured traffic.

During an excellent IETF introduction session to privacy in protocols on Sunday several partici-pants called for a "legal way" to intercept traffic, in order to prevent parties to do it in "illegal" ways.

DNS WG needs an extra shift

A year ago it felt like there was not that much work left in DNS related Working Groups at the IETF. The specifications for DNSSEC were ready, adoption slow, DANE specs were finalized and the DNS Operation WG was chewing on some long living draft documents. DNS discovery and anew attempt to come up with a new structure and protocol for Whois came to live in other working groups. Post-Snowden everything seems changed, including the DNS. Not only were there two sessions discussing on privacy in the DNS. Requests for new special domain name zones – in one instance also a reaction to surveillance revelations – were discussed heavily in the DNS OP WG. The DNS WG now seems to have a busy year ahead with additional new Working Groups of interest to the DNS experts in Boundaries and ongoing work in Domain Service Discovery.

DNS Privacy: „Vanilla DNS susceptible to eavesdropping“

The revelations of Edward Snowden have pushed DNS experts to re-think privacy issues within the DNS. A flurry of drafts were presented in a Bird of Feathers session on DNS Encryption (DNSE) in London, that while said to be non-WG forming, had to be extended into a second session. Starting from two DNS specific problem statements by Stéphane Bortzmeyer (AfNIC) and Peter Koch (DENIC) the group spent a little time on possible solutions to enhance confidentiality and privacy in the DNS.

Problem Statements

In principle, problems are well-known (for current descriptions see Koch and Bortzmeyer). DNS queries are passed unencrypted and can easily be read and stored along the path and/or at the endpoints. DNSSEC has added authorization, but not confidentiality to DNS traffic – and moreover DNSSEC validation uptake has been very slow and only now, by raised interest in using the DNS as an anchor for all sorts of keying material or certificates might make another step forward (see also DANE report below).

The sites of political parties or alcoholics anonymous were public, for example. But users might not want to be observed accessing this time at a certain time. Moreover queries can happen without users even being aware of them, for example by local filtering software checking addresses to detect spam or other unwanted traffic or requests triggered by mail software when a user browses over spam ending up in his mailbox.

Finally, not only has the DNS been an easy target before. It also might become a more interesting point for eavesdroppers following a take-up of encryption, for example for web traffic (with https).

Solution Space

During the DNSE BoF and the additional DNS Privacy some ideas for solutions were explored, there are already several drafts out. Questions were mainly:

Can existing IETF protocols (TLS, DTLS, IPSEC) be reused to secure DNS traffic?
Or is there a need for new protocols?
Are changes to DNS operations possible to reduce the footprint/enhance privacy?
What are the side effects of DNS hardening measures?
What additional costs have to be considered?

Eric Rescorla in his presentation about the use of DTLS and IPSEC came to the conclusion that IPSEC probably would not work, while DTLS might be an option. Solutions had to be thought through for different parts of the chain: client machine to full resolver vs. resolver to authenticated name server. Designs like anycast for example would put themselves in the way of session-based encryption.

In general TLS for DNS, both authenticated or unauthenticated (opportunistic) were proposed in several drafts (including Bortzmeyer, Mankin, Wijngaards) as one viable path.

The proposal from VeriSign Labs and the University of Southern California (Mankin e. al.) is DNS-over-TLS-over-TCP (avoiding the UDP fragmentation problem). It wants clients and servers to set a bit in the flag fields of EDNS0 OPT meta-RR the TLS-OK (TO) bit would indicate support for a TLS session. Mankin's draft does touch on the certificate authentication briefly arguing that opportunistic encryption (connections without CA or DNSSEC based validation) might be of interest to DNS over TLS over TCP.

Support for DNS-over-TLS-over-TCP is already implemented in the Unbound resolver. Yet it was, according to Bortzmeyer, only safe when “pipelining multiple questions over the same channel”

and "name compression also (be) disabled". The DNS-over-TLS-over-TCP according to Koch could get traction not only because of the privacy agenda, but also because it could benefit protection against reflection amplification attacks.

The proposal by Wouter Wijngaards (NLnet Labs) and Glen Wiley (VeriSign) wants to introduce a new resource record. Arguing DNS over TLS (and also DTLS) would bring too high a toll for large authoritative servers, they present an "Encrypt RR" which would allow to fetch "a public key" for encrypting a session. Public keys for the various DNS servers could be cached.
Issues like middleboxes forcing a fall-back to unencrypted have to be thought through. The solutions as well as the DNS-over-TLS will not provide perfect forward secrecy.

In addition meta data of DNS requests still deliver much information about DNS users: data on timing, IP source and destination addresses, packet sizes, RR count, header flags and more. With more data stored in the DNS, for example private PGP keys additional information could leak, Bortzmeyer pointed out.

Side effects of all that "pixy dust"

Some ideas on how to minimize the DNS "footprint" might even add new privacy problems. More caching on one hand could help to obscure (create noise), on the other hand adds to storage of information. Also pushing encryption might fuel concentration of services, benefiting bigger services providers able to making the necessary investment. Instead, shifting caching and DNS resolution as close as possible to the end user might be beneficial against concentration in a few spots only, inviting eavesdroppers and/or big data interests of various kinds. "Sprinkling a little pixy dust" on everything perhaps would result in users being given a wrong impression that the problem had been solved by providers. Perfect or even close to perfect privacy looks like a rather hard problem for the DNS anyway, some of the proposals underline that their main goal is to make simple passive monitoring (on the wire) harder and more expensive.

Additional costs have to be borne not only by DNS eavesdroppers, but also by services providers and their users, given that encryption makes additional round trips necessary and result in higher traffic in general because of the keying material and keyed content flying around with the regular queries and answers. Companies engaged in either traffic management, sale or operation of middleboxes or big data business certainly are hesitant with applause.

Questions posed by various speakers were which enemies the efforts were directed against (Russ Mundy, government contractor Sparta) or about the cost-effect balance, given that protecting the wire only would give only incomplete protection (Ralf Weber, Nominum).

During the STRINT workshop (see further up) preceding the IETF meeting, Steve Kent (BBN, another US government contractor) in a session on opportunistic encryption in general questioned the thought that every user would be compelled to pay more for a level of protection only a minority really was interested in.

Next steps

The DNSE and additional DNS Privacy session were inconclusive with regard to next steps. Only after the session a decision was taken that the DNS Privacy work would be continued outside of the DNSOP WG with a non-WG mailing list ("dns-privacy") as a platform to discuss the issue and try to finalize a problem statement and possible requirements. Despite the high level of interest during the London meeting in the DNS privacy issue this does not look as if it will proceed very fast. Discussion about how broad or narrow the scope of the work should be, will continue.

Special Names - a little less expensive than 185,000 US$

The most sensitive discussion the DNS OP WG had during the London meeting was a potential reaction to requests to the IETF to delegation two sets of special TLDs according to the procedure laid out in RFC 6761, on Special-Use Domain Names. The relatively new standard track RFC by two authors from Apple elaborates on how the IESG/IETF should consider additions of special domains/TLDs, stating:

*"Similarly, **if a domain name has special properties that affect the way hardware and software implementations handle the name**, that apply universally regardless of what network the implementation may be connected to, **then that domain name may be a candidate for having the IETF declare it to be a Special-Use Domain Name** and specify what special treatment implementations should give to that name. On the other hand, if declaring a given name to be special would result in no change to any implementations, then that suggests that the name may not be special in any material way, and it may be more appropriate to use the existing DNS mechanisms [RFC1034] to provide the desired delegation, data, or lack-of-data, for the name in question. **Where the desired behaviour can be achieved via the existing domain name registration processes, that process should be used. Reservation of a Special-Use Domain Name is not a mechanism for circumventing normal domain name registration processes.** (Bold added by ME)*

With at least two recent requests to the IETF/IESG to provide registrations as special-use domains/TLDs the IETF has to consider answers to such requests.

Requests to IETF/IESG for delegation of special domains

One request is results from studies on name collisions with regard to the introduction of new gTLDs. ICANN itself has put several strings on hold that - according to the study of Interisle Consulting Agency – are widely used as pseudo-DNS names. .local receives 10.000 requests per second, studies showed, .home just a little less.

Interisle author Lyman Chapin and InterConnect Communications author Marc McFadden now wrote an Internet Draft requesting to have localdomain, domain, lan, home, host, corp, mail, and exchange put on the reserved domain list in conformance with 6761. Several of these have been applied for in the new gTLD application programm by one or several applicants, for .mail for example five of the original 7 applications still stand.

The second request to have an IETF TLD reservation has been tabled by a group of TOR and Gnunet developers seeking to enable what they call "fully-decentralized and censorship-resistant secure alternatives for DNS", yet on top of the DNS to allow for interoperability, "or, in the case of the ".exit" pTLD (pseudo TLD), to control overlay routing and to securely specify path selection choices [TOR-PATH]". The group which includes TOR campaigner Jacob Applebaum asks for the approval of ".gnu", ".zkey", ".onion", ".exit", and ".i2p" as special domains by the IESG in accordance with the RFC 6761.

One potential option for the IESG/IETF presented in London by Warren Kumari (Google) and Andrew Sullivan (Dyn) was to establish an .alt (for "alternative") special domain name subtree to give space to experiments outside of the DNS. Kumari mainly pointed out that there had been historic experiments with special-use domains motivated by the idea to allow for alternative usage of DNS-like strings namely .bitnet, .csnet, .uucp, .oz, .free. More might be coming. In order to record such usage a special .alt tree might allow to avoid problems, strings under .alt would not be looked up in the DNS. More features to allow for distinction of pseudo- and regular domains proposed by Kumari/Sullivan are:

1. *Stub resolvers MAY elect not to send queries to any upstream resolver for names in the ALT TLD.*

2. *Iterative resolvers SHOULD follow the advice in [RFC6303], Section 3.*
3. *The root zone nameservers should either return NXDOMAIN responses, or the ALT TLD should be delegated to "new style" AS112 nameservers. (TODO(WK): WK, JA, BD to revive AS112 /AS112-bis).*

Circumventing ICANN application procedures?

None of the recent application drafts for special-use TLDs were presented by their respective authors in London. The new Co-Chair of the DNS OP WG, Suzanne Woolf (ISC) who is as also a non-voting member of the ICANN Board and a member of the Root Server System Advisory Committee underlined the need for the WG to discuss operative (how can we help operators?) and interoperability issues. The WG was in no position to make formal decisions – that was up to the IESG.

Joel Jaeggli, one of the responsible Area Directors at the IESG, said there was a concern that delegations like that might "open the floodgates for special registrations". The IESG would still have a discussion and was "in no rush to make a decision" over the existing draft requests.

Next steps with regard to the requests are rather tricky for the technical community, with several issues deserving attention, according to the debate in London.

Even if special-use domains would be limited to not being resolved in the DNS, additional ones certainly would result in more leakage.
Applications might have issues with any sort of parallel systems.
With regard to the ICANN process one question was if blocking "squatted" domains (like .corp. .home, .mail) was ok. The other one, highly sensitive, was if a parallel IANA special use registration was not just a circumvention of the painful (and expensive) ICANN process and would invite to game the system, at least if the special use domains would be resolvable in the DNS.

Even with ICANN now possible developing into the final IANA-operator, this will be an interesting, highly sensitive debate.

Closing Ranks: Internet Governance@IETF

In the "Internet Governance Update"-session which seems to develop into a standard feature of the IETF meetings drawing considerable crowds of engineers one major topic took the center stage: the positioning of the IETF/IAB with regard to the future of IANA. Retrospectively the discussion certainly has to be looked as a step to rally consensus in the IETF community with regard to the then undisclosed joint statement of the I*-Organizations and other operator institutions (including CENTR) in reaction to the IANA announcement by the National Telecommunications and Information Administration (NTIA) on March, 14th.

During the update session Olaf Kolkman (NInet labs) presented core points for an IAB IANA statement that was very much in line with the core arguments of the later joint I*star statement:

- Internet Community able to handle protocol parameter function (one IANA task) well
- Function well served by ICANN (No Change of roles necessary)
- Operational Principles ("multi-stakeholder-modell"): open, transparent, accountable
- Internet Architecture needed registries working well
- Changes to function based on RFCs
- The IETF will continue its direction and stewardship of the protocol parameters function as an integral component of the IETF standards process and the use of resulting protocols. (IETF controls its destiny) resulting protocols. (IETF controls its destiny)

Despite broad consensus over the statement (a hum clearly in favour of the general position)

several points were made during discussion time with regard to **ownership/copyright of data** registered in the protocol parameter registry and the possibility for the IETF to **change the provider** down the road.

The respective principle in RFC 6220 is that the IAB "has the responsibility to define and manage the relationship with the Protocol Registry Operator" including "the selection and management of the Protocol Parameter Registry Operator" and so on. While some participants in the session were satisfied with ICANN Chairman of the Board, Steve Crocker, assuring the room that ICANN did not think of itself as copyright holder on anything it published, others recommended clarification along the lines of RFC 6220.

More critical comments (minutes of the complete debate see here) were made on the lack of differentiation between "Internet Technical Community" and "Internet Community" in the presented core points. Kolkman argued, the oversight by IAB and IETF over the protocol parameter function seemed like sufficient to ensure stability. At the same time governments could provide input into policy and standards more generally, which was a separate discussion.

Kolkman and Housley finally said the IAB would consider changes in the position, which shall be used not as "IETF position", but "guidance for the leadership" anyway.

There were some subtleties buried in the close to an hour long discussion, including a comment by Patrick Fältström, who recommended an interpretation of the discussed high-level points as consistent with the Tunis Agenda (passed by the World Summit of the Information Society) and therefore opposed to another edition of a full WSIS-follow-up meeting. Discussions about the WSIS follow-up 10 years after WSIS are ongoing on the diplomatic stage at this point.

ICANN Chair (and one of the early RFC authors) Steve Crocker explained the larger picture, of which globalization of IANA was one point, globalization of ICANN another, plus there was the ongoing discussion on Internet Governance exceeding ICANN and IANA. Crocker pondered that a mere vendor-like nature for the ICANN-IANA relation (similarly to IETF-RFC editor) might not be broadly accepted.

It is interesting that after the NTIA discussion ICANN President Fadi Chehadé said the ICANN/IANA globalization debate was led by the upcoming ICANN led consultation while the much referenced Brazil meeting would be devoted to the larger Internet Governance questions. No need to discuss ICANN's future there, he stated in the press conference following the NTIA announcement. It remains to be seen if some of the organizers will accept this or reject it as a re-framing.

DANE

If you want to "just quickly" implement DANE, don't do it – this was a recommendation of Victor Dukhovni when presenting drafts on "DANE TLSA implementation and operational guidance" and "SMTP security via opportunistic DANE TLS". The first-time IETF participant who has worked for a financial institution before and is in charge security at its new company has implemented DANE smtp and published drafts pointing to issues and potential safeguards to be taken into account, also in further editions of SMTP and DANE BIS.

The crossing of boundaries (provider of mailservices/mx-server and domain provider regularly are not the same) so far has prevented TLS use for securing SMTP traffic. The deployment of DNSSEC and DANE for the first time allowed authenticated TLS for SMTP to MX between parties that have not already established an identity convention out-of-band, Dukhovni's (jointly published with Wes Hardaker) draft RFC explains.

One of the major difficulties for implementers was the definition of as much as 24 different combinations of TLSA record parameters depending on what kind of certificate or key management was used for example. Additional complexity resulted from those use cases where the TLS transport endpoint was obtained indirectly via SRV, MX or CNAME.

When publishing the DANE specs, nobody seemed to have bothered with how SMTP would handle the notorious bad CA results, Dukhovni explained to this reporter. Using DANE TLSA with MTA to MTA SMTP therefore, according to his proposal, must be "cognizant of the lack of any realistic role for the existing public CA PKI" (see the draft for more details). According to Dukhovni, Postfix 2.11 was supporting DANE TLSA, work also was under way on general support of DANE TLSA in OpenSSL and, as a next step Exim support. Dukhovni said he personally knew about 20 domains supporting DANE SMTP, with 30 more being available already. By the end of the year, he thought, there might be 100. The possibility for incremental deployment with fall back possibilities was helping.

Other presentations at the DANE WG included very quick overviews over DANE/OPENPGP and DANE/IPSEC, for the latter there are different proposals (Eric Osterweil, VeriSign and others, see here, Valery Smyslov, Elvis Plus see here).
The OpenPGP DANE marriage would allow "securely publishing and locating OpenPGP public keys in the DNS using a new OPENPGPKEY DNS Resource Record. While the various proposals are still worked on (see also SMIME and DANE), with more DANE securing being eyed in XMPP (see IETF Berlin report) and now also a potential use of DANE TLSA for SIP. At this point it certainly looks as if DANE might take off a little more (and with it DNSSEC).

One cross-WG work item that is of interest to the DNS community is the work on DANE and DNS vocabulary by Olafur Gudmundson.

WEIRDs WG

The WEIRDS WG hopes to finalize its work even before the next meeting in Toronto in July, WEIRDS Co-Chair Olaf Kolkman said. All base documents have been sent to the IESG once, been back once and would be filed as a package again when the open questions in three remaining documents would be addressed, according to Co-Chair Murray Kucherawy. During the London meeting discussions focussed on the planned bootstrapping mechanism that shall help to locate RDAP servers.

The request to IANA to:

> *"Create a new registry of domain names, essentially TLDs, with the following columns: Domain and RDAP URL. The content should be initially populated by an extract of the Root zone database [domainreg]. The same registrants for these entries are entitled to provide the RDAP URL value for their respective space, using the same communication channels already established between the registrants and IANA." (three more IANA registries will cover IP addresses, ASN numbers)*

resulted in WG discussion and a private conversation between Kolkman and the Area Director Pete Resnick. Kolkman summarized the result during the session: "There is a concern around using IANA considerations to create registries that have name policy and name control. There are possible ways to weasel our ways out of it." Resnick said the WG could come up with a format for registries and entries, but should not touch how the registries would be populated.

There was no need to wait for the final publication of the Whois Experts Group at ICANN, Scott Hollenbeck, VeriSign, one of the authors of the WEIRDS specifications and a member of the ICANN expert group said. There would be support for RDAP. Later extensions if necessary (despite Whois fields now asked for by ICANN were covered) would be possible.

Interestingly the WEIRDS work did not address the ongoing DNS privacy discussions. The line of thought the authors and WG majority seems to be that registries will be able to chose which data they can provide to WEIRDS queries and which not. No connection was made to the already experienced problems by registries in jurisdictions with stricter privacy rules in their attempts to register exemptions from contractual obligations on Whois. Queries to list names associated with special IP-addresses, for example, might be privacy sensitive.

SAAG

There is much talk about the need to come up with alternative processes to select new ciphers, after NIST had to acknowledge its own process (on selecting a random number generator) had been influenced by one of its "stakeholders", the NSA.

During the London IETF the Crypto Forum Research Group (CFRG) of the Internet Research Group discussed the option for NIST-like competitions organized by the IETF. Kevin Igoe (NSA), Co-Chair of the Internet Research Task Force (IRTF), during the Security Area Group reported very briefly about the CRG-discussion, confirming the call to bring competitions into the IETF/IRTF.

Yet Igoe argued IETF/IRTF would have difficulty to fund a competitions, given that NIST had spent 25 man years of work, and spent around 2,5 Million US-Dollars for the recent algorithms contest. While NIST reps during the Vancouver meeting also pointed out that organizing the competitions needed a lot of expert work, during the London meeting one representative said to this reporter, using ciphers developed elsewhere would be an option for NIST given that process and quality of the ciphers would fit accepted standards.

The STRINT workshop in fact listed a consideration about IETF work on new algorithms as an action item. One expert said to this reporter: "Nist blew it and Nist is to slow". NIST only recently has asked for public comments on its crypto standardization work. While it has been mentioned repeatedly that the IETF has not enough crypto-knowledge during the CFRG meeting closer

cooperation of the IETF with the Crypto Community was addressed as a first step. More outreach would be done.

Co-Chair David McGrew said outreach to that community was necessary and future meetings of the CFRG could be co-located with conferences of the International Association for Cryptologic Research (IACR). Dan Gillmore said during the CFRG meeting that cipher competitions at the IETF/IRTF were commented on positively during the Real World Crypto Workshop in January. Such activities could bring more crypto experts to the IETF. Given the level of interest expressed by experts, there has not happened much open talk in London.

IAB Chair Russ Housley presented in London work on cryptographic algorithm ability. A new RFC shall address how the IETF allows for agility to change from weaker to stronger algorithms, preferably without changing base specifications. Algorithms shall be signalled via identifiers registered in a IANA registry.

Domain Bounderies BoF

A BoF session on "Domain Boundaries" explored potential alternatives to the Public Suffix List. The list currently managed by the Mozilla Foundation lists of suffixes (TLDs from ICANN or private area) with wildcards and exceptions.

The list is mainly used by browser vendors for various policy enforcement in cookie management, inter-webpage communication, transparency against phishing attacks and so on, according to a presentation by Gervase Markham, from Mozilla. It is also used from third parties, for example for the CAB Baseline Requirements (to avoid over-broad wildcards), DMARC (for anti-spam mechanisms), uses are documented on a special WIKI. The common denominator of the use cases was "which bits of the web are under common ownership", according to Markham.

Problems stated at the BoF (and the reasons for the BoF) included things like timeliness and completeness and also things like false positives and negatives. Just prior to the BoF for example three new gTLDs have been added to the root, but were not immediately showing in the Public Suffix List. There were also questions about how changes were processed, and what policies were in place for the processes.

Three drafts on potential alternatives were presented by Yngve N. Pettersen (Opera), Andrew Sullivan (Dyn) and John Levine (Taughannock Networks). All three are looking for some sort of DNS/ressource record oriented alternative. Yet also a mere step for more formalization of the existing public suffix list was considered.

With a lack of clarity about the scope of the problem a design group now has set up with the three authors, Olafur Gudmundson, Murray Kucherawy, Ed Lewis, Jothan Frakes and the Bof Chairs to discuss:

- Are we standardizing Public Suffix Lists functionality, and what use cases should be minimally supported?
- Who are the parties in the provisioning of the information, what are their respective roles, responsibility, and authority?
- Or according to questions from Joe Hildebrand where did data come from, how would it be transmitted, how would its authoritativeness established, and what was the relation to the web-security model?

A general discussion list for DBOUND is here.

The London meeting was also used by other I*-organizations to show up to close ranks (see for example Fadi Chehadé's shirt-sleeved speech underlined ICANN's) and to mark the handover of ISOC from Lynn St. Amour to Kathryn Brown, former Senior Vice President, Public Policy Development and Corporate Responsibility of Verizon.

New ISOC President/Internet@parliament

St. Amour received a lot of applause by former IETF and IAB Chairs and standing ovations from the plenary participants. She leaves a much grown ISOC to the hands of new President coming from the outside with some changes in mind. Brown said to this reporter cooperation with ISOC chapters was a topic on her list.

In her maiden speech at the IETF Brown promised the ISOC would be there in the upcoming Internet governance debates. Speaking in front of members of the British Parliament Brown mainly stressed the gathering of all stakeholders at the table where new legislation and rules would be prepared for the Internet.

The meeting organized by the British ISOC chapter and Afilias in Parliament during the IETF week also saw interesting statements by members of the British Parliament, including one member of the Joint Intelligence and Security Committee, George Howarth (Labour), a member of the Human Rights Committee, Julien Huppert (Liberals) and Tory politician David Davis. Davis and Huppert were highly critical of reactions by the Government to the Spy affair so far. Davis said Whitehall was "incompetent". Howarth acknowledged that more transparency of the work of intelligence services was needed. Pointing to the need to fight terrorism and child porn, Howarth said the debate about the balance between security and personal freedom has just yet started.

ICANN hosting IETF, Internet governance debate to be continued

ICANN was the host for IETF 89, so Chehadé gave the regular host presentation during the administrative plenary. He touched on ICANN's service to the IETF, the IANA function, under a service level agreement. The ICANN president applauded the IETF work and called it one reference point for the multi-stakeholder model, also pointing to upcoming discussions in Brazil and other conferences. The "Internet technical/operational community" is coming back two times to London this year, during the ICANN meeting in London in June a high-level government meeting is planned.

United Front of I*

Arkko in his speech beside the hardening issues (see above) also addressed the upcoming governance debates. He reiterated that the IETF had to do more outreach and said "governments have woken up to the fact that this internet thing does not go away". Events like the Internet@parliament meeting seem to become much more common even for the engineering community.

In conclusion, the I*organisations presented themselves as working very closely together with regard to the operational issues (IANA) but also at the politics and diplomacy front. Attendance of the IETF in London was high, with 1364 participants from 60 countries (up from Orlando 1115 from 51 countries).

Next meeting will take place in Toronto 20 - 25 July 2014