Report of the

IETF 81

Québec, Canada

July, 25-29, 2011

Prepared for the CENTR Secretariat by Monika Ermert

Report contents

Highlights

IAB/IETF on the way to privacy by design?

The Privacy Program [1] of the Internet Architecture Board (IAB), the peer organisation of the Internet Engineering Task Force (IETF), is progressing with a dedicated Privacy Directorate of the IETF established recently. The Directorate on request of the security area directors of the IETF will review draft IETF documents and advise document authors, working groups and peer reviewers about potential privacy issues.

What is still lacking -according to Alissa Cooper, who has the lead of the Directorate for the IAB and organized a panel discussion on privacy at the Québec IAB technical plenary- was a more systematic view on the threat models for privacy and an agreement in the IETF about which threats should be addressed and which declared out of scope. Threats not addressed by the IETF could be documented in some form, Cooper said. The Privacy Directorate is preparing two basic documents to frame the discussion (here and here).

During the technical plenary several examples were presented of how standardization efforts neglected privacy in initial designs and faced problems to find more privacy-friendly workarounds later. An issue high on the agenda not only of engineers, but also of legislators currently, is the tracking of users on the web. “Today users are tracked as they browse around the Internet and it is done for a variety of reasons,“ said Andy Zeigler, Program Manager for the Internet Explorer at Microsoft.

“To me, as a user, my browsing history and what sites I go to is personal to me“, Zeigler said during the plenary and explained two different mechanisms now under development that could give back more control to users. One would allow users to flag their requests with a „do-not-track“-flag, the other was a mechanism called „tracking protection“. Tracking protection would enable users to integrate lists of tracking websites compiled by various providers. „So a privacy advocate or government regulator or whoever can author a tracking protection list that blocks tracking content and then users can get that list and browse the web and have that tracking content filtered out as they browse“, Zeigler said.

Microsoft's proposal has been tabled at the W3C (see here) and has announced “the inclusion of anti-tracking technology based on tracking protection lists in IE9” (Mozilla made a similar announcement, Google released a browser extension that “permits users to persist opt-out cookies”, according to the W3C).

The W3C, which is about to open a new Working Group on Tracking (see here), is cooperating with the IAB and IETF, still currently there seem to be “do-not-track-proposals” from both bodies. The IETF's draft document to standardize a “do-not-track-bit“ is currently under discussion in the IETF.

The value of mechanisms like the do-not-track-bit is heavily under discussion in the IETF because in order to be effective companies have to honour the users' self-expressed wishes (legislation, while under discussion for example in the US, has been rejected by some politicians as innovation-averse). Another concern expressed was that the RFC under discussion would only make baby-steps and still allow first party tracking and third party tracking agreed to by the user.

Another well-known example about how early intervention could have helped to avoid privacy issues, according to Cooper, was IPv6 (for all privacy reviews so far, see here). Fixed suffixes derived from MAC numbers are fatal from a privacy standpoint because they do allow easy tracking of users and have a considerable lifetime, normally the lifetime of the device they sit on. The MAC-address issue is exemplary with regard to persistence of privacy-averse code once it is in the wild. An additional vulnerability with IPv6 is that tracking becomes easier when the IPv4 NAT.

1 Other IAB programs are IANA Evolution, Internationalization, ITU-T Coordination, Liaison Oversight and RFC Editor (see below)

The examples, Cooper said, clearly showed that privacy issues better should be addressed pro-actively and not retroactively. This is what the new Privacy Directorate will do for future IETF standards. The 12 experts will review draft standards when requested by the Security Area Directors. Cooper said, she expected that concerned parties could point to potential problems and try to get documents reviewed, too. Another idea is to document privacy considerations in the RFCs in the future to, at least, give the problems more attention.

Privacy by Design certainly is what governments have been preaching for a long time, according to Fred Carter, Senior Policy and Technology Advisor at the Office of the Information and Privacy Commissioner of Ontario. Carter said during the panel discussion: „Privacy by design is gaining ground and now we are looking to take privacy by design to the next stage to have people such as yourself apply it in particular cases and teach us how, what the next best practices are."

Carter explained the focus of Canada's data protection authorities on privacy by design on the one hand and the huge interest of data protection officials around the world. Data officials from around the world in their annual conference in 2010 in Jerusalem had adopted privacy by design as an „essential component of fundamental privacy protection". The resolution, Carter said, invited the data protection officials to promote its seven basic principles, including the request to have privacy „embedded in the design".

Yet the data protection official also acknowledged that data protection authorities like his did not have „a mandate to pursue the international standardization. We can't go too far outside of our borders pursuing bad people. We don't have sufficient autonomy or resources to carry out detailed technical work to understand what it is you guys do." For example, while there are representatives from the Department of Defence, the National Telecommunications and Information (NTIA), the National Institute for Standards and Technology (NIST) and the Department of Homeland Security (DHS) at the IETF on a regular basis, data protection authorities participate only occasionally.

In the new Privacy Directorate, Tara Whalen, IT Research Analyst at Office of the Privacy Commissioner of Canada, and Rob van Eijk from the Dutch Data Protection Authority represent data protection agencies in the Directorate. Directorate member Kasey Chapelle is privacy officer at Vodafone. Besides there are six non-IAB members joining the group, like experts from companies, ISOC staff and academics.

IAB: IANA requirements to be set by materially affected parties

The Internet Architecture Board during the IETF week filed its comment to the "further notice of inquiry" of the US National Telecommunications and Information Administration (NTIA) and underlined it made the comment "as the body that approves the entity that serves as IANA for the IETF". The IAB in the statement asked the NTIA especially to give more weight to the "materially affected parties" with regard to the requirements written for the contractor.

"If the IANA is to effectively and efficiently carry out its key functions (which are primarily administrative and technical, and explicitly not policy-making), it is probably desirable that NTIA write requirements (and interpret requirements once written) in a way that focuses on "working relationships" with those who specify IANA actions or who are direct consumers of IANA decisions and registries rather than requiring close constructive working relations with anyone who merely claims to be interested and affected."

This requirement, according to the IAB, would not exclude any stakeholder from participation in the policy development processes that govern the maintenance of IANA tables and registries (these are ICANN supporting organizations for DNS, RIRs for IP addresses and AS numbers, and IETF for other protocol parameters).

The IAB clearly supports the split of policy work and operational work and therefore warns to oblige IANA to make judgement calls about the quality of the documentation that demonstrates consensus before adding new TLDs to the root (a provision added by the NTIA in the new SOW). Instead, the IAB pushes for a clear acknowledgement that the IANA contractor is accountable to the self-regulatory bodies. The idea to make the

IANA contractor liable to relevant national laws is viewed rather sceptical:

"It is not clear what is meant by 'the Contractor shall act in accordance with the relevant national laws of the jurisdiction which the TLD registry serves'. According to the governance model the Contractor shall act in accordance with the policies developed by the relevant PDB. It is the responsibility of the PDB to ensure that these policies are not in conflict with national laws where appropriate."

The IAB also reminds the NTIA of the preference of loosening the unilateral US control over IANA. "We don't consider the present situation in which a single governmental agency is seen as having close, management-level, oversight of IANA as ideal and hope that NTIA is working toward more autonomy for the IANA function."

With regard to the physical location the IAB notes that the US Government's requirement that all security and operational components should be within the US was contradictory to the robustness and off-continent replication principles of the Internet. Transparency in the operational management and reporting in the opinion of the IAB would strengthen the role of the policy making bodies. In fact, IANA should never be in a position where they are not able to point to publicly available data, reports or procedures. NTIA and VeriSign therefore also should participate in filling a dashboard to allow tracking ongoing operations.

IPv6 again - no, it's not over

All seemed to be said about World IPv6 day, but some interesting numbers and opinions were shared during a special section of the IAB technical plenary and the heavily loaded v6ops WG (which has currently 40 active documents on its table). Nobody wanted to question the success of the day, yet some of the content operators that participated clearly announced that "it was a lot of work for 0,229 percent of IPv6 users" (Yahoo). Figures of access over the new version of the IP protocol differed between 0,2 (Facebook, Yahoo), 0,3 Google, 0,5 (Microsoft) and 1,11 percent (Cisco). While for many sites like Yahoo, Facebook or Cisco it was a première, Google engineer Lorenzo Colitti spoke of "business as usual".

A positive development reported by many was an observed decline in brokenness. While 21 months ago Yahoo noted brokenness of about 0,078 percent, it's now, according to Igor Gashinsky, Principal Architect of Yahoo, down to 0,022 percent. Donn Lee, of Facebook's Network Engineering Team said brokenness changed from 0,03 before v6 day to 0,02 after the day. The Teredo-connections that have been said to be messy to debug did play a very little role (figures reported by Hurricane Electric) and according to Comcast statistics did not raise during v6 day while 6to4 doubled. According to the Facebook statistics 6to4 percentage was 0,04 of 0,20 percent of observed IPv6 usage.

De-preferencing 6to4 made sense, said Chris Palmer of Microsoft, as it was slower than IPv4. Palmer said that beside technical aspects the lack of geo-location data in IPv6 was a problem. When answering to a question he said that Microsoft was prepared to pay "big dollars" for such geo-location data – either getting it from a third party provider as they did in IPv4 or organizing them in-house.

Another interesting piece of detail is the difference in IPv6 traffic in various countries – France, according to several speakers, leads the way with a percentage of 3,4 percent, followed by Japan who, according to Colitti, made a big jump (to 1,4 percent since May) with a recent new IPv6 offer by KDDI.

The Japanese jump shows how fast access rates can go up with large carriers starting to offer IPv6. And it also shows that currently initiatives of one single provider are still very visible in global measurements. Another interesting peak was produced by German large hoster Strato who immediately after World v6 Day turned on v6 for the sites he hosted (around four million).

Practically all reports hammered in the message that no major issues happened and there were zero help desk calls. Only Colitti said there was no major change in brokenness and there had been issues, for example, with a South American Network that was responsible for nearly half of all brokenness on the net with 9 percent dual-stack failure.

Colitti also defended Google's fallback to serving v6-traffic toonly white-listed parties after v6 day for major sites (other large content providers like Yahoo or Facebook went back to IPv4) and pointed to IPv6 access to Youtube for everybody for now (similarly see also Microsoft's X-Box, zune.com and Facebook's developer site). A draft document to prevent further spreading of white-listing is currently still under discussion in the v6ops

WG. With respect to next steps in IPv6 deployment, Colitti said, user numbers had to grow.

Bob Hinden, engineer at Checkpoint, during the panel discussion challenged what he said was too much attention for the view of the large content providers only. Checkpoint also made its site available over IPv6 for the v6 Day and, as there were close to zero failure rates, kept it open. “It can be done and white-listing is not necessary,” he said.

At least with regard to IPv6-serving autonomous systems (AS) there was a very big jump over recent months, according to a Hurricane Electric statistic. The relevant date after which the rate rose considerably was the IANA announcement about allocation of the last v4 blocks earlier this year. In June 2010 4 percent of AS served IPv6, before the IANA run-out the rate was around 7 percent and had meanwhile gone up to 11,4 percent. More interesting news on IPv6 were presented during the v6ops group, for example a recent trial with IPv6 in China Mobile's network.

Internet as new incumbent on the road to decay

During the regular panel discussion of the Internet Society, APNIC Chief Scientist Geoff Huston warned against ossification of the Internet and the danger that pressure from the next innovative competitor would smash the Internet just like the latter had smashed the telephone system. Huston said there was no other incumbent right now than the Internet.

IAB Chair and Microsoft engineer Bernard Adoba confirmed that currently there were discussions about a deadline for the “POTS” system by the regulator in the US. The deadline under discussion was seven years from now – with a long list of issues to be dealt with including the question about what would happen to the Universal Service Fund. Adoba predicted that government was only starting to legislatively deal with the Internet.

With the old competitor on the verge of death and no new competitor around, the drive to innovate had been stalled, Huston warned in his panel speech. A good example for this was the slow adoption of IPv6. Even such a small change in the protocol, which IPv6 is according to him, seemed nearly impossible. Instead providers managed scarcity and some hurried to give Carrier Grade Network Address Translation (NAT) preference over introducing the new protocol control over data flows.

While he saw a clear market failure and with an urgent need for policy makers to step to balance the interests of incumbents with volume and small companies and newcomers, it were the large competitors who set the rules themselves. “We are recreating the system that was so disastrous,” Huston said. While the mega large content companies like Google or Apple would still be around in some time, even after retaliation of the carriers, newcomers would not be able to enter the market and pressure for revolution instead of evolution of the Internet would build up in the next decade. The Internet, that is Huston's prediction, will share the fate of the telecommunication system which it had driven to the verge of bankruptcy over the last decade.

While Huston looks for regulators to “get it right”, other participants blame protocol designs as nurturing anti-competitive trends. The IETF should not have gotten away with designing a new protocol version for IP without pressing for backward compatibility, Bob Briscoe of British Telecom said. Briscoe said, there were seven reasons for market failure listed in standard textbooks or Wikipedia – “and the Internet suffers from all of them.”

DNS related working groups drizzling out at the IETF?

With DNSSEC in deployment and the internationalization of domain names in the hands of implementers the DNS related working groups of the IETF seem to have lost some steam.

The DNSEXT WG did not meet in Québec at all, having mainly the still ongoing Aliases discussion on its agenda. During the DNSOP working group session (see below), which also ended early, the chairs asked for a round of discussion on potential new items that the WG wanted to address with only little reactions. Ondřej Surý's (from Czech ccTLD registry) said cz.nic would bring several new items to the WG from their labs. Overall people talking to this reporter said they saw a possibility that the DNS related working groups would be “drizzling out”.

This is in sharp contrast to several new working groups like the Real Time Communication Web (RTC Web) that met three times in Québec or like homenet (see below). The focus on port 80 has been noted by experts before.

There is on the other hand ongoing DNS-related work in the IETF, either in dedicated Working Groups like DANE (see below) or as drafts presented in other working groups, the latter being watched meticulously by the dnsop and dnsext chairs for potential harm to the DNS. One proposal under watch is for example the idea of a split-view DNS (to allow two views on the DNS by the ISP who could use this for "redirects"), that earlier failed to get support in the DNS WG and is now tabled in the Multiple Interface Group (MIF) wg. A split view DNS setup asks for maintenance of two DNSSEC trust-anchors.

One reaction to the ongoing debate about the relation between the DNS and new applications being standardized in the IETF (RAI and APPS areas) is a document currently shepherded by the Internet Architecture Board under its DNS Initiative. Version one of the document "Architectural Consideration on Application Features in the DNS", according to IAB member Jon Peterson, had been negative, criticizing the document had "misunderstood the history and purpose of the DNS". The documents' main target is summarized as follows:

Proposals to incorporate more sophisticated application behaviour into the DNS, however, have raised questions about the applicability and extensibility of the DNS. This document explores the architectural consequences of installing certain application features in the DNS, and provides guidance to future application designers.

The IAB during its most recent retreat had discussed how to proceed and if the document could "acknowledge split-horizon DNS without appearing to endorse it". According to the report from the retreat, there are "a number of DNS issues that may require more attention, and that they would benefit from more participation from outside the IAB". The IAB DNS initiative has also a decision about future work items related to the DNS on its agenda.

Working Groups and BOFs

DNSOP

The DNSOP WG discussed three documents more in depth. First, a special delegation of IPv6 reverse addresses to the AS112 project in order to sink IPv6 leaked local traffic. Also discussed were two documents of Matthijs Mekking on the nearly finalized DNSSEC key timing document and future work related to it, especially automatic key-rollover.

George Michaelson gave an update on various documents related to the AS112 project. The idea of the Michaelson/Huston document is to ask IANA to delegate a number of sub-domains to the AS112 project, to allow passing the increasing number of reverse DNS queries (resulting from the leakage of locally-scoped addresses, certain anycast addresses, and loopback addresses) into a "distributed sink".

There were still issues with the delegation list, Michaelson said. The proposal focussed on the delegation request to IANA by trying to keep it simple. Michaelson argued against a potential merger with another AS112-related draft currently under discussion. The draft by William Sotomayor, according to Michaelson, addressed interactions with locally served zones (RFC 6303) and discussed "operational issues with lame serve in AS112". Sotomayor's document requested delegation for several IPv4 reverse domains. The discussion in DNSOP focussed on a concern from Andrew Sullivan, co-chair of the DNSEXT WG, who said IPv6 was still early in its development, so there might be other possibilities to fix the problems. But Michaelson had underlined the majority of stupid DNS requests were IPv6 and that recommendations on local zone would not help. Discussion on the document, which is still not a WG document, will continue.

The second topic discussed was the timing of the DNSSEC key-timing considerations document. The first

document (expected to go to last call as version 03 soon) had been deliberately "incomplete" with algorithm roll-over, for example, not covered. Matthijs Mekking from NLnet Labs asked the WG how to proceed: either publishing the document and go forward with the update document right away or trying to include everything in one document? Having a bis-version of a document before the document itself was published was weird, participants felt. In conclusion the original document will be processed and the bis-document taken on next. Synchronization of parent-child zone for DS keys – covered by two draft documents (one proposing a new resource record and one describing the synchronization of existing trust anchors automatically between a child zone and its parent) - was discussed as a nice to have tool, which several registries said it could not be used by them because of their contractual relations with the registrars.

The DNSOP WG finally talked about the future direction of the WG in more general terms (see above). With not a lot of work left to be finished for the moment - four active documents, close or very close to IETF LC

draft-ietf-dnsop-rfc4641bis-07

draft-ietf-dnsop-dnsesec-dps-framework-04

draft-ietf-dnsop-dnssec-key-timing-02

draft-ietf-dnsop-respsize-12

there is a question if the WG should continue or not. For detailed minutes of the WG discussion, see here.

DANE

The DANE protocol document, according to WG chair Ondřej Surý, shall be finalized or be in IESG review before the next IETF meeting in Taipei, which would it make a rather speedy development of a new protocol. According to observers there are still two groups watching the marriage of TLS and DNSSEC closely: the opponents, who prefer selling TLS certificates for some more time, and the fans, who see it as the possible killer-application for DNSSEC. Still there are some tricky open issues, for example securing the last hop – this was discussed in Québec, but solutions still have to be tabled.

A new draft documenting the use cases of DANE that had been demanded during the DANE WG meeting in Prag is already in a second Working Group last call, according to Richard Barnes from BBN (author of the use case draft). The use case document makes the case that DANE could very well work together with existing Certification Services. DANE could, for example, be used to express information about "Certification Authority Restraints" to block mis-certification (unsolicited publication of certificates for a domain). CAs could also choose to issue a certificate for a given domain name and public key only when the holder of the domain name has provisioned DANE information with a certificate containing the public key. Also a domain name holder could advise a CA to use a third provider for validating the Certificates of a domain (instead of using a CA). The CA would then connect to the third party provider to obtain the trust anchor.

Despite the variety of use cases involving classical CAs in one form or another one major idea of DANE is to allow DNSSEC-secured self-certification or certification services by domain owners or their DNS providers. As the use case document describes:

"Alice would like to be able to generate and use certificates for her website on alice.example.com without involving an external CA at all. Alice can generate her own certificates today, making self-signed certificates and possibly certificates subordinate to those certificates. (….) Alice would thus like to publish information so that visitors to her site can know that the certificates presented by her application services are legitimately hers. When Bob connects to alice.example.com, he uses this information to verify that the certificate presented by the server has been issued by Alice. Since Bob can bind certificates to Alice in this way, he can use Alice's CA as a trust anchor for purposes of validating certificates for alice.example.com. Alice can additionally recommend that clients accept only her certificates using the CA constraints described above."

An issue not yet resolved is the last mile. On the last mile man-in-the-middle attacks between resolver and applications are possible. WG chair Surý pointed to wire security, trust in resolvers and API security. While he said that these were general problems, he asked for a decision from the WG on how to deal with them; They could either be addressed in the WG (if in scope), or shipped to another WG like DNSEXT, or the WG could look

at solutions elsewhere (like VPN, IPSEC or others for wire security).

Discussion on that question was inconclusive with some warnings against "dodging operational problems by creating hacks" (Lars Liman, Autonomica) and some recommendations to focus on show-stoppers for DANE exclusively, as there were still a huge numbers of issues with DNSSEC. DNSOP WG chair Peter Koch (DENIC) warned that the IETF should not react to slow implementation of things by "adding new knobs and transition mechanisms" that did not only increase complexity, but also would create "a moving target to implementers". Last mile and first mile provisioning both had to be looked at, he said. DANE-co-author Paul Hoffmann warned that the DANE protocol should perhaps not be pushed to the wire as long as secure operations was still in question. He said that this might result in a less of security, instead of better security.

Another issue discussed briefly after a presentation by Phillip Hallam-Baker (Comodo) was how wildcards, redirections and aliases could work with DANE/DNSSEC. The authors of the core protocol have added an annex to the last version of the DANE specification to elaborate on the effects of DANE for wildcards and aliases.

Another issue discussed heatedly during the Québec DANE session was serialization for fetching DNS (including DNSSEC) information, for example for browsers. The idea for which some code had already been developed (outside the IETF by Dan Kaminsky and Google engineer Adam Langley, see draft brought to IETF here) was to allow fetching all DNS/DNSSEC information "in one blob" and not necessarily over DNS. However, the document by Langley "did not say how to get the blob or use the blob, just about the shape of the blob", Hoffmann said. Potential problems by such a "blob" were staleness and time-out issues (with key roll-overs and TTL implemented all over the place), some participants warned. The Langley draft had also been presented in the TLS WG session and was said to be no WG item for DANE.

Issues like DANE for IPSEC/SMIME should be dealt with only after the DANE protocol was finished, participants agreed.

Apparea

One major discussion in the Apparea Open meeting touched a DNS issue, too. The draft on changes to the syntax for Top-Level Domain (TLD) labels in the Domain Name System (DNS) to allow encoding of Internationalized Domain Names has been around for quite some time (see discussion in Hiroshima, IETF 76, for example). While the authors (Lars-Johan Liman, Autonomica, and Joe Abley, ICANN) argue that it is a slight incremental change necessary to accommodate IDNs, DNS experts again warned that the IETF should not deal with policy issues – those would have to be solved by ICANN under its own processes. The draft by its proponents is declared as an incremental change to RFC 1123, which might need more systematic update. This declaration of an incremental change has not make it through the IETF process for several years now, while at the same time a more systematic update to RFC 1123 (that some say is necessary) has not been dealt with.

Two interesting BoFs were also announced during the Apparea meeting, namely a BoF on a reputation system (REPUTE) that would allow qualifying DKIM signatures further and a BoF on security measures for Java Script Object Notation (JSON).

Once more there is work on adapting/reforming the Whois with the idea to address the following requirements (according to Jay Daley from New Zealand Registry Services):

1. *Authentication (end user to provide credentials before accessing the system)*
2. *Access control (ability to provide different levels of access/restrictions)*
3. *Rate limiting (specialised case of 2)*
4. *Internationalisation (full support for internationalised registration data and domain names)*
5. *Standardized, machine readable queries, response and error messages*

A requirements document and several other documents for the "new Whois" exist. During the Apparea meeting the approach promoted by Andrew Sullivan was questioned because of the existence of the IRIS RFC

set. A major argument by those asking for Weirds to become a work item in the IETF is that IRIS has not been widely used, potentially because of complexity. A requirements document by Murray S. Kucherawy from Cloudmark can be found here.
Related documents according to Sullivan are documentation of "ARIN's RESTful Web Service for Whois Data" by Andrew Newton (from ARIN), documentation of "The RIPE Database REST API" by Benedetto Fiorelli from RIPE and a document by ICANN technical staff members Francisco Arias and Steve Sheng on "A RESTful Web Service for Domain Name Registration Data (RWS-DNRD)".

HOMENET – My home is my data centre, but how can I keep track?

With the advent of new Internet address numbers, IPv6 numbers and the growing number of devices and smart objects in the house, ordinary home networks will become literal data centers with subnets for communication, TV, smart grid management, health care applications and more. The declared target of the WG is to make these networks for John Doe easy to handle ("zero configuration", Fred Baker, Cisco).
The just seven day old WG was joined by around 250 engineers. The driving force behind the work is IPv6, which in the future will allow much more devices to be equipped with publicly routable addresses.
An example of how networks in "ordinary homes" might look in the future was given by Jari Arkko (Ericsson) during the session. Arkko's home network in Finland had already grown to 11 subnets, he said, including special networks running under IPv4 and IPv6, networks reserved for the members of the family, a special network for visiting friends and so on. Smart objects also sent data automatically to dedicated servers (like his weight scales from French technology company Withings).
One issue to be covered by the WG is to allow for separation of servers that can receive and send data, or send or receive only. For example, while he did not want to send anywhere the stats about his weight, his laundry should be able to send Facebook a message when it is dry. Similar issues arise with energy smart grid integration in the house. Also multi-homing had to be considered (for example for TV sets that could be connected to a Broadcasting provider for one, but also to the Internet).
Even for a geek the new data center at home was a challenge, with naming and addressing only being possible automatically, Arkko said. Chris Palmer of Microsoft said that one problem to solve was that there currently was "no definition of a local security boundary". Whether the scope of the WG, which includes some DNS work for the naming of devices internally, is too broad remains to be seen.

IRTF: virtualization/information centric networks/prices for routing papers

While work on the next generation IP Internet is ongoing, new ideas for networking are explored by the Internet Research Task Force (IRTF). IRTF started several new working groups including one on "virtualization of networks" and on the concept of "information centric networking".

Information centric networking starts from the idea that access to information is the most important activity. It wants to make most sought information available at core places and allow access to it above the existing network using new name and routing schemata, as Dirk Kutschner, Researcher at NEC Europe Laboratories explained during a meeting of the IRTF at the Québec IETF.

There is a lot of pressure from operators to use proprietary Content Delivery Networks (CDNs) for provisioning their content to users more efficiently and also in a more controlled way with regard to Intellectual Property Rights (differing rights for several regions). The CDNi WG now tries to fix the issue that proprietary CDNs cannot interwork.

While the current CDNs use existing naming and routing protocols, information centric networking would go for dedicated new mechanisms. Virtualization of networks would even go a step farther, Roland Bless from the Karlsruhe Institute of Technology said. "It could work on layer two and not use IP any more." Yet research might still take years on these new ideas and the problems with IP complexity and scarcity of old IP numbers have to be solved before, experts say.

The IRTF for the first time gave out prices for research papers – a new initiative together with ISOC. The two papers accepted and presented in Québec were both routing-related:
Mattia Rossi is looking to allow reducing BGP update announcement traffic by path exploration damping and Beichuan Chang proposes a mechanism to take out router line cards in order to save energy. For details on the price and the next application round see here.

IETF News

The IETF administrative plenary was marked by a controversial discussion on the quality of peer review by the IESG. One participant questioned the quality of the IESG peer review and requested to stop it because IESG members, in his opinion, were not able to review drafts that were often outside of their core technical competence. The comments were rejected not only by the IESG members, but also by the vast majority of IETF participants speaking at the microphone. The reform of the standardization process in the IETF from a three-layer to a two-layer process driven by the IETF Chair Russ Housley is still under way.
There was also a long discussion on cross-subsidization of meeting rooms by hotel rooms pre-arranged for by the IETF. The IETF so far had rejected to raise conference fees for those not booking hotel rooms through the IETF (contrary to other standardization bodies like the IEEE).
The detailed budget of the IETF for 2012 is still in the making, the rough figures for now are revenues of US$ 3.338.000 (2011 budget 3.317.000) and expenses of 4.919.000 plus an additional 415.000 for tools (2011 budget 5003.000 plus 429 for the tools). The 2012 contribution of the ISOC therefore shall be reduced to 1.751.000 from 2.115.000.
Contracts for the RFC production Center and RFC Publisher have been extended for two years. The RFC Editor currently is preparing to digitally sign RFC series documents.
The IAB set up a RFC Series Oversight Committee (RSOC) which has started the process to hire a new RFC Series Editor.

The next IETF meeting will take place in Taipei 13-18, November 2011.