Council of European National Top Level Domain Registries

Report on

RIPE 66

Dublin

13-17 May 2013

Table of Contents

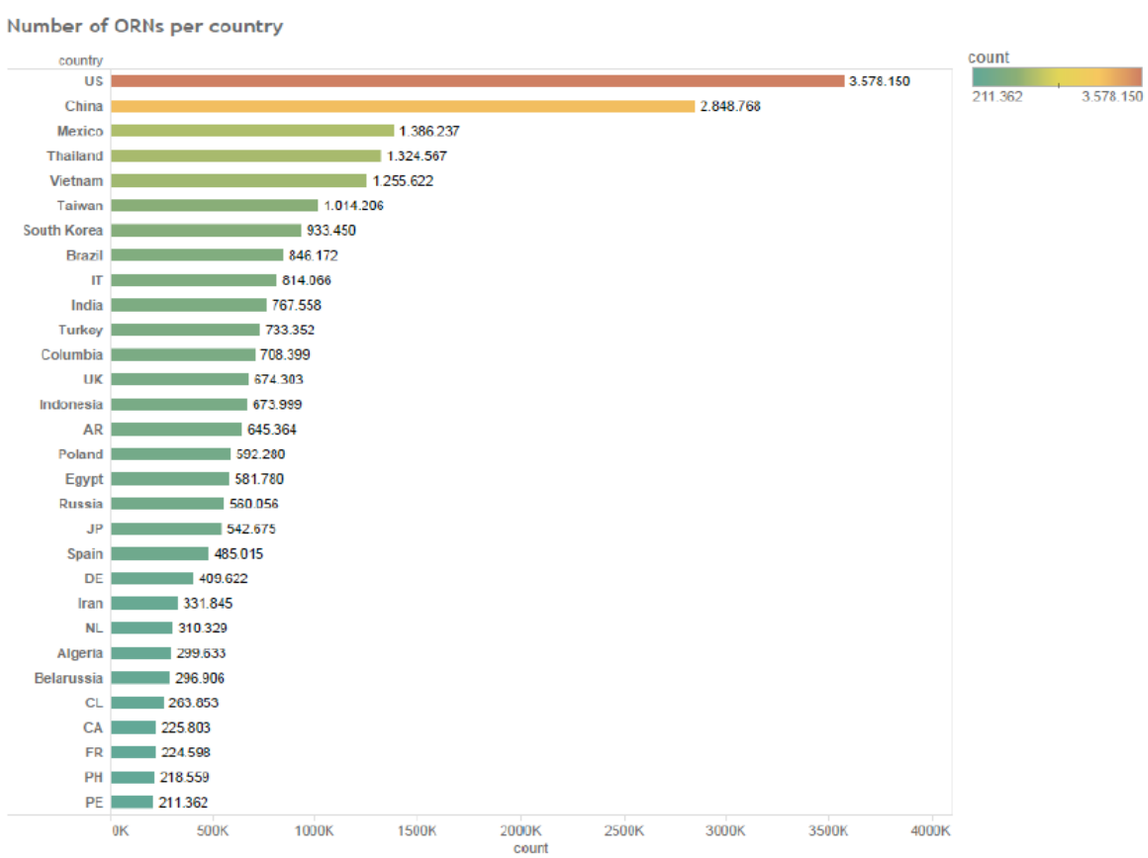
Can self-regulation still save the DNS?

The growing number of large-scale attacks on the Domain Name System (DNS) and the trend to abuse overprovisioned authoritative systems in so called amplification reflection attacks were made the topic of a full plenary session and additional talks in the DNS WG at RIPE 66. The issue had also been discussed during the OARC meeting that preceded RIPE 66. Operators seem to be at a loss for how to turn the tide in the DNS, some even said regulation might be needed in order to close off some of the open doors in the DNS (including address spoofing, open resolvers). Meanwhile the DNS community dives into a debate about rate limiting on authoritative servers, which is seen as religious change.

80 percent white, 20 percent black sheep

Seven years ago an anti-spoofing task force at RIPE passed RIPE 431, a how-to document for address filtering, and also tried to make the case for network hygiene in RIPE 432. RIPE 432 addressed the alleged problem that address source filtering, as proposed by BCP 38 of the IETF, "would be expensive and would only help the 'other guy' who is being attacked".

According to regularly cited statistics, the number of spoofable systems has gone down to around 20 percent (see latest figures for example at the MIT spoofer project), which is still enough to support attacks. Also the number of open recursive resolvers, according to Merike Kaeo, is currently as high as 30 million with an urgent need to close those that were not intended to be open (for figures presented at the OARC meeting see Jauch below and also Gudmundson)



After the well-publicized attacks on Spamhaus earlier this year the question of securing the DNS has not only resulted in a restart about how to attack the "20 percent" in the operator and technical community. State bodies like the European Network and Information Security Agency (ENISA), but also other national agencies (including for example the German Federal Office of Network Security) have started to look into lack of compliance with BCP 38, BCP 140 (open recursive resolvers), made recommendations on DNSSEC and even secure routing tools.

DNS used against itself

Some security measures, including for example DNSSEC, have on the other hand been fired back with answers to forged DNS requests getting even more amplified with DNSEC keys sent back to the victim of the attack.

According to Paul Ebersman (Infoblox), DNSSEC is "not securing data because, realistically speaking, DNSSEC is not truly useful until the end client on that machine does its own validation and actually does something useful with different validation states and possibly fails to connect. So instead what we have done was, we have increased the fragility of our DNS and the overhead on our machines for very little positive security impact, at least currently." NSEC3, too, was used to amplify attacks.

Unintended positive effects on the other hand were originated by anycast deployment of authoritative servers, as it naturally spreads out attack traffic more between the anycast servers.

No „magical stick" out there for regulators or self-regulators

The heightened attention by state actors nurtures fears in the technical community against onerous (and not or only locally effective) regulatory acts. Some statements on the other hand showed a certain level of resignation on the site of the technical community. David Freedman from Full Service Provider Claranet said, after waiting for people to implement easy measures like BCP 38 for 13 years, "I am not sure the self-regulation thing is working as well as it should." Penalties for noncompliance could be the "magic stick" of regulators.

Potential industry self-regulatory steps beyond the mere appeal and education effort toward the "black sheep" proposed during the panel discussion were:

- Name and shame
- Depeer with non-compliant networks
- Vendors delivering products with „secure configuration" set as default (prevention of unintentional mistakes in re-configuring secure default)
- Industry funding a „can and a couple of of people to go around and look at everybody's network and make sure they clean it, sometimes it's the hand holding that is absolutely necessary" (Merike Keao); Andrei Robachevsky (ISOC) said, with only 40.000 AS „it's doable, I guess"
- A BoF at the RIPE meeting also talked about an initiative from the ISOC 360 degree program to develop a new series of best practice documents better suited to the operators' practical needs (Best Current Operator Practices, BCOP, see below).

Technical measures proposed by Ebersman were to protect:

cache servers:	randomness in Ids and source ports, better checks on glue, DNSSEC;
authoritative servers:	perimeter ACLs, higher capacity servers, clustering or load balancing, fatter pipes, more servers, anycast, high availability
protect users via DNS:	anti-virus, block at perimeter (NGFW, IDS), block at client, Response Policy Zones (RPZ)

Rate Response limiting

Rate Response Limiting (RRL) having been discussed during the DNS OARC meeting before RIPE 66 got spotlighted during the DNS session briefly with a presentation from Stephan Rütten, SIDN. After observing amplification attacks using ANY traffic, SIDN started to use u32, a script written by Stéphane Bortzmeyer from Afnic to "generate firewalling rules in IP tables". Afnic is also using rate limiting.

To implement u32 SIDN had to change from FreeBSD or OpenBSD to Linux, as it did not work with the former. SIDN in a second step also started to implement RRL for BIND and NSD users to mitigate amplification attacks.

SIDN has communicated the change from answering all DNS queries to checking the validity of the requests first, since attackers have moved elsewhere, according to a release. No announcements have been made by ICANN, who uses rate limiting for its L root server, Afnic and other DNS operators, possibly. DENIC answered questions on rate limiting by underlining that tools and measures were being analyzed and that the registry would decide on implementing them on a case by case basis. More data and background had to be gathered, a DENIC spokesperson wrote.

One issue to be further discussed are amounts and effects of false positives (questions dropped by accident). Antoin Verschuren said at the RIPE Dublin meeting that SIDN was seeing false positives, "but they don't affect the regular traffic that much, so we are still tweaking with the slip rate to see if we can bring that down". What is also of concern to some operators is that the various DNS Server versions (NSD, BIND and KnotDNS) behave differently.

All that bad stuff that happens: Certificates for non-existing domains

157 Certificate Authorities have delegated considerable numbers of certificates for non existing TLDs, for example-like names that are only used internally (like .site, .corp). A problem arises when certificates are given out for soon-to-be delegated TLDs. According to the SSAC report 057 presented by SSAC-Chair Patrik Fältström during RIPE 66, in fact a large number of certificates have already been given out for applied TLDs.

SSAC 057 describes the ease of not only getting a certificate, but also of setting up a fake root in which a non-existing TLD was delegated. Tests allowed them to use these certificates in all browsers. With the first new TLDs getting live possibly later this year, SSAC is highly concerned about man in the middle or other kind of attacks using the certificates for the respective TLDs (or names in that TLD) before.

Meanwhile the CA Browser Forum has reacted to ICANN's call and passed a policy that 30 days after an ICANN contract is signed for a new TLD no more certificates will be provided for the respective name for internal use. 100 day after the contract was signed pre-existing certificates need to be revoked, according to the document.

Fältström said the problem was not solved after that move because not all Certification authorities were members of the CA Browser Forum and one single CA that would not follow the policy could make the PKI system fall apart. Also it is unclear how good revocation lists are processed by browsers. More work was needed, according to Fältström. The ICANN Board in its meeting on May, 18th set aside additional funding for a study to be commissioned by the ICANN CEO to further research the problem. SSAC is expected, based on the study, to make additional recommendations.

Do away with „needs based“ allocation for Ipv4 (and other address policy news)

Most address policy work seems to be done after IPv4 (and the need for last-mile- and running-out-fairly-policies) have more or less served their cause and are over. In fact one of the more controversial policy proposals in Dublin tried to make the case that policies on IPv4 allocation should be very much facilitated. Tore Anderson, from a Norwegian provider, promoted to get rid of the obligation to provide documentation to the RIPE NCC address handling staff allowing a check on the "need" of an operator for another IPv4 allocation.

With a core aim of the needs-check - "extending the lifetime of IPv4 address pool" - gone and allocations for specific timeframes (originally 3 years, but with the emptying pool much shorter) bureaucratic overhead should be reduced. The concrete proposal, according to Anderson, would lead to 50% less paperwork for members (mainly forms to be filled out for the address consumption of each customers of the members).

The proposal interestingly led to a major controversy between RIPE members, who clearly welcomed the initiative, and members from various US organisations. Bill Woodcock from Packet Clearinghouse, warned against potential speculation with IPv4 addresses. "The purpose of conservation is to conserve the resource for the use of the community", he said. Now there was no longer a pool "getting rid of needs-based allocation would mean that speculators would have an immediate effect on the market."

Gaming the system was possible already now, said Address Policy WG Chair Gert Döring. A black market of IPv4 so far also had not developed, argued Anderson. There was much more talk about IPv4 transfers than actual transfers were happening, he said.

Transatlantic differences

Abandoning a needs-based allocation would put the RIPE at odds with its North American colleagues at ARIN. ARIN still has some addresses to distribute and, moreover, might have some more in the future as it is the region with the biggest potential to recover IPv4 addresses that were handed out generously to large US cooperations before the regional IP address registries came into being.

ARIN has declared earlier to its RIR colleagues that is is not willing to share these so called legacy address resources with anybody who would not be conservative and follow a needs-based allocation policy. ARIN's rather conservative position towards transfers of addresses has been the topic of discussion and research over recent years. Cutting oneself from a potential stream of IPv4 addresses when ARIN has the largest bite left would perhaps not be wise, said Rüdiger Volk (Deutsche Telekom). APNIC has in fact reacted to ARIN's calls by changing its own allocation of recovered or transferred IPv4 addresses to „needs-based" again. RIPE members in the Middle East also might be very interested in receiving recovered addresses, despite some progress in deploying more IPv6 in that region, observed by Paul Rendek, who represents RIPE NCC in Dubai.

But many RIPE members pointed to the fact that the RIR community so far had not been able to agree on a common Inter-RIR transfers policy. Attempts to get there are stuck in various stages of the policy-making process of the different RIRs and the lack of such an Inter-RIR policy has been mentioned in the report by ITU Secretary General, Hamadoun Touré for the WCIT report (see below). In some respect this RIPE debate also can be politicized.

Address Policy WG Chair Gert Döring regretted after the session that the discussion had been somehow misleading due to the "no-needs" title.

Doing away with burdensome paper forms and documentation by now means would lead to overly generous IPv4 allocations. RIPE NCC address handlers even check need for allocations from the plentiful IPv6 address space. The German Government that came back to ask for additional IPv6 space – after already receiving a /26 block in 2009 – would have to demonstrate its need, confirmed RIPE CEO Axel Pawlik. Pawlik in his status update also appealed to members to not only get IPv6 numbers assigned – as more than 50 percent of the 9200 RIPE members have done by now – but also put them to use. Data of the Atlas measurement network organized by RIPE labs shows that IPv6 is growing at more than 100 percent per year, but still is at only 0,2 percent of overall IPv4 traffic.

WCIT and WTPF as seen from Dublin

The failed 2012 World Conference on International Telecommunications and the World Telecommunication Policy Conference (WTPF), which was just underway during the RIPE 66 week, did get quite a lot of attention at RIPE 66. Three talks were devoted to the the ITU organized conferences, including some reporting back from the Geneva.

"A non-event", the WTPF was called by one RIR staff and while certainly an effort to get over the split during the WCIT. With only six "opinions" to be passed by the ITU member states ITU Secretary General Hamadoun Touré spoke of a "low-pressure environment". Still, Brazil with a proposal of a new seventh opinion that focused on pushing governments' role in internet governance venues with support from ITU ("operationalize the role of government in the multi-stakeholder framework of internet governance") allowed for some WCIT-like negotiations (as did the much more radical Russian proposal to some extent).

With no compromise possible and process and time constraints being cited by US and EU countries, debate in the end came down to where further discuss Brazil's proposal, either in the ITU Council Working Group on Internet related public policy issues (Russia) or more open fora like the Internet Governance Forum (EU, US). Touré's announcement to promote openness in the CWG, was welcomed by civil society of which some warned against closed government procedures for the follow-up process to WSIS plus 10. (*WTPF documents can be found online, Civil Society Statement is* here*, ITU post WCIT press releases is* here).

RIR dilemma

Interestingly, the participation of RIRs in said conferences resulted in a lot of RIPE-proposed text ending up in official documents, according to Paul Rendek, head of external relation for RIPE NCC. Not only was promotion of IPv6 the topic of two of the opinions adopted, the report of ITU Secretary General Touré included problem statements, for example, on the lack of an Inter-RIR transfer policy, or the debate on secure routing, RPKI, including the controversy of a single trust anchor.

Is this a success? Olaf Kolkman (NLnet Labs) reviewing WCIT said the participation of the technical community in the events made a difference for them. Engagement with the international organisations was "incredibly important", he said, "trying to keep friendly with your regulator and trying to be constructive in the dialogue". The technical community, supported by ISOC and the RIR administrations has in fact flocked to the Intergovernmental and international fora in recent years. Chris Buckridge pointed to the Internet Technical Advisory Committee (ITAC) and to the OECD, which just commissioned their first study to be deliberated by OECD governments (about cables, backbone and IXP) and was finalizing a study on the state of IPv6 deployment (written by Geoff Huston, with support from CZ.NIC and the Czech government for follow-up work)

The dilemma to face on the other hand was openly addressed by Tahar Schaa, IPv6 consultant, who had prepared an analysis of the ITU Secretary General's report to the German Ministry of the

Interior. Schaa said ITU did try to make the issues addressed on the basis of RIPE input its own. Schaa's recommendation was a less defensive positioning of the RIR and technical community.

Constanze Bürger, regularly representing the German Ministry of the Interior at RIPE meetings made an appeal to government colleagues to discuss the developments and, in her view, protect the status quo with regard to resource allocation. With nobody from the European Commission participating in the RIPE meeting, there was a gap. Governments regularly do come to the closed RIPE roundtable meetings, but shy away from the open Cooperation WG.

Nurturing IGF as a positive alternative to intergovernmental processes

Acting NRO Chair Paul Wilson commenting on Kolkman recommended to support the IGF as a positive alternative to the more traditional intergovernmental fora. The NRO, he reported, was funding the not well-funded IGF with 100.000 US Dollars this year.

WG, BoFs and Plenary Talks

eID – regulating authentication in the EU? (Cooperation WG)

A controversial debate took place with regard to a draft new EU regulation on mutual acknowledgment of e-Identification in the European Union. The regulation is a follow-up to an earlier (and obviously failed) directive and at this time is still under discussion in Council and European Parliament.

According to Andrea Servida, European Commission, Cabinett of Neelie Kroes, the eID regulation if adopted, would oblige public authorities in the Union to mutually acknowledge systems of electronic identification notified with the Commission as official eID systems. States will also be obliged to provide free online authentication facility for its notified eIDs and, according to Servida, they also would be "liable for unambiguous identification of persons an for authentication".

The private sector could be allowed to use the notified eID. Member states would be completely free in their choice of the eID services (it could very well be privately provided eID services in use for access to public services).

During the RIPE meeting there were critical questions relating to possible technical mandate through supporting secondary legislation that would step up to set minimal security standards (for example for revocation of compromised keys). Another stern warning came from Patrik Fältström, who underlined the regulation would go against what was developed in multi-stakeholder fora with regard to authentication schemes (like DNSSEC and RPKI) in that it would oblige member states to trust a listed provider/scheme, potentially even contrary to what their own „trust anchors" (in the wider sense) said.

Implementation of the potential eID very much also depends on acceptance from member states, who may or may not be notifying a lot of eID services.

At the same time one can wonder if the final aim of the Commission is not much more harmonization (creation of an EU eID standards), which could become releave when considering that a long list of national eID schemes would somehow have to be trusted. Servida said an European eID scheme was definitely not the aim of the current regulation, but other projects

were working toward more harmonization and interoperability, see the Stork-project.

The long list of amendments to the regulation from Members of the EP is on Amelia Andersdotter's site which provides also her concerns with regard to the detailedness of technical requirements (also privacy issues).

New: RIPE Open Source WG/ENUM closed

The ENUM WG will go into hiatus after a series of meetings that did not see a lot of progress. The only projects currently advancing according to Niall O'Reilly was internal ENUM use by NREN members and a small Brussels firm that provided ENUM service to the UN. The WG could be revived if necessary.

After a well-received BoF (the third edition of an Open Source Software BoF at RIPE) the RIPE closing plenary voted in favor to open a full-fledged Open Source Software WG (for a charter proposal see here). Ondrej Filip, BoF Co-Chair and CEO of CZ.NIC, said an open source WG would bring operators and developers together and could attract new people to RIPE meetings.

Research labs of ccTLDs over recent years have produced such new additions as KnotDNS and Yadifa, name server alternatives to BIND and NSD. Both initiatives did present updates during the DNS WG. Overlap of the new Open Source WG with other WGs could be managed by WG Chairs, participants agreed.

RIPE NCC with its Labs tries to offer a platform for developers and announced its open source database whois code repository.

A very interesting issue the new WG took on its to-do-list once established as a WG is production of a document promoting OS software in order to lend support to developers in companies. The WG in that process might discuss different licensing models for that effort.

At RIPE 66 open source software presentations delivered were "Bird Internet Routing Daemon" (Ondrej Zajicek) and Kea - DHCP servers in BIND10 (Tomek Mrugalski).

Best Current operator practices

Another attempt to close the gap between developers and operators was discussed during a BoF organized by Jan Zorz from the Internet Society 360 Degree Programm. Zorz presented two main problems regarding the relation between RIPE (i.e. operators) and IETF (i.e. developers). One, more feedback from the operational community to the developing community to get "better standards", he said. Operators lacked time and funding to travel and get involved in the sometimes year-long discussions. The problem was acknowledged by regular IETF participants, including IESG member Richard Barnes (BBN) or DNS WG Co-Chair Peter Koch (DENIC).

Caution on the other hand was asked for with regard to the second issue (and main action item) from Zorz, the establishment of a new document series of Best Current Operator Practices (BCOP) that would complement IETF BCP documents or comparable RIPE best practice documents. Especially the idea to create a Board for selection/peer review and publication of such documents was said to be premature, even if it was very much acknowledged that localized and more down to operators' earth documents might indeed be helpful. Zorz declared after the BoF discussion that he had somehow changed its mind with regard of how to proceed. He wanted to look for local "nodes" for the activity now in the first place.

News from Abuse WG

With the abuse contact record now done and even in the middle of being implemented, the Abuse WG is looking for next steps – an idea presented already briefly during the Database WG by Co-Chair Brian Nisbett is to look into validation of the abuse contact record, then followed potentially by validation for other records – tech C, admin C and so on. Validation and verification of such records been high on the wish lists of law enforcement during the controversy over the new contracts between ICANN and its accredited registrars (the Registrar Accreditation Agreement, RAA).

RIPE in fact could learn from what had been done at ICANN, Richard Leaning, an officer from the newly established European Cybercrime Center (E3C) said during the session. Leaning said law enforcement had been "naive" about what the RIRs could do so far, "but we have been educated". Cultural differences between Leas and the technical community he noted: "we do not like to share information". His office intended to take part in RIPE meetings at a regular basis. Marco Hogewonig, RIPE NCC, reported about the RIPE NCC outreach to LEAs, three courses so far had been provided to LEAs in the UK, UAE and to Europol.

Michele Neylon, well-known Irish registrar and active in ICANN promoted ASOP EU, an initiative supported by large pharmaceutical companies, industry associations, patient organisations and some intermediaries (Google). According to Neylon, 97% of websites offering to sell medicine were "illegitimate" (no data given on what illegitimate meant: counterfeit, dangerous with regard to health, fraudulent with regard to other aspects). There was no intention to ask for website take-downs, said Neylon when questioned about the target of the appeal to operators.

The next RIPE meeting will take place in Athens between 14 – 18 October 2013