Council of European National
Top Level Domain Registries

Report on

RIPE 67 Athens

14 - 18 Oct 2013

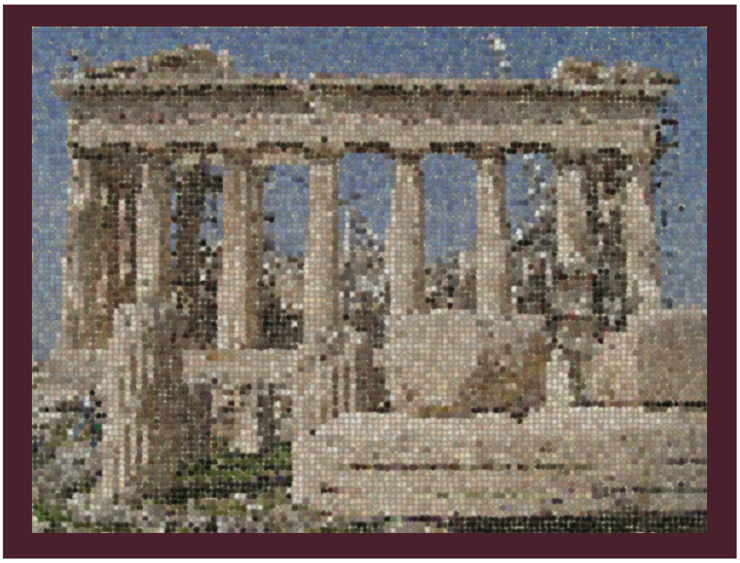


Table of Contents

Highlights 3

DNS Attacks - Using long domains, DNSSEC and response rate limiting against you 3

DNSSEC deployment and what is the French (or any other national) internet? 4

Surveillance - warming up the discussion 4

Intentionally compromised standards? 4

Actions underway at the IETF 5

New IP core network concept brought by you by an old incumbent operator 5

6

DNS WG 6

Cooperation WG 6

IP-Address Policy 7

.

Brokering and the new role of IP registries 8

Highlights

DNS Attacks - Using long domains, DNSSEC and rate response limiting against you

New possibilities to attack the DNS were described and demonstrated at the RIPE meeting and while DNSSEC – jointly with implementing BCP 38 filtering – would result in some better security, DNSSEC also can add to the new attack vector: IP fragmentation (and reassembling of packets). IP fragmentation attacks have been described in a paper by Amir Herzberg and Haya Shulman and have been tested and proved by cz.nic labs.

IP-fragmentation allows the attacker to offer his own version of the second part of a fragmented packet to the caching resolver, cz.nic Lab-researcher Tomas Hlavacek described at the RIPE meeting. Guesswork on the ID of the packet is eased by the short IP IDs (16 bit), and also by the fact that IP ID is generated by counter with no randomness. A forged second part of the packet is dropped off at the authoritative server. As soon as the authoritative server, following forged „ICMP destination unreachable fragmentation"-requests from the attacker, sends the first part of the packet the IP packages is reassembled. Wrong data (from the second part) has made its way into the caching revolver by then.

The fragmentation of the IP packets can be enforced by the ICMP-trick or by long DNS answers. DNSSEC signatures can there be one „enabling" factor. But more and more, according to Ralph Weber of Nominum, large requests are constructed by simply creating large domains, which are exchanged „fast-flux". „If you block one domain the next day you have another one", according to Weber. Domains could be made large by all sorts of resource records. Weber spoke at the DNS WG about „amplification attacks" targeting ISP DNS resolvers.

The Czech researchers presented their findings not only during the RIPE, but also earlier at the OARC meeting opening considerable discussion. The attack is not very sophisticated in what types of technology it uses. But it forces him to coordinate the different parts of the attack pretty well. The discussion during RIPE and the OARC meeting also was about the impact. Currently there is not much of a practical impact, said several experts, partly also because there are other, less arduous ways to make an attack (just plain cache poisoning for example).

More checks on the attack vector IP fragmentation, according to Hlavacek, is done at VeriSign by Brian Dickson. The next steps for the cz.nic-researchers are to check on the „vulnerability" for different server types. BIND had fallen for it in the tests, Unbound testing would be done soon and even Nominum was considering to test their systems.

What some see as much more dangerous is the possible exploitation of rate response limiting (RRL) observed by French Office for Network Security (ANSSI). RRL is used by a growing number of registry to prevent abuse of their highly redundant infrastructure as attack vector in amplification attacks. But the ANSSI-Researcher warn to not rely on the delaying or blocking (truncating) the answers completely from an authoritative server. The problem with rate limiting, which is instigated by the attackers, is that the attacker himself will use the time lapsed to send their own forged packets in and poison the cache of the recursive resolver.

The attack described by the French has been quietly notified to operators over the summer before going public, which might be some indication about the gravity. Ed Lewis from Neustar called this type of attack "more serious than the IP fragmentation only attack".

One fix to the fragmentation attacks would be the quick deployment of IPv6, said Stéphane Bortzmeyer from AFNIC (already during the OARC meeting). ANSSI recommends to answer all requests and stop none. Long-term solutions again were ubiquitous DNSSEC and BCP 38 filtering.

Putting RRL into BIND versions by default on the other hand, as Shane Kerr from ISC considered, was questionable, as it would feed this type of attack.

DNSSEC deployment and what is the French (or any other national) internet?

In theory all French domains could be signed by now, three years after the signing of .fr, Guillaume Valadon of the French Internet Resilience Observatory. Yet so far only 1,5 percent of .fr-domains are signed, according to the measurements the Observatory made together with AFNIC and ANSSI. The around 30000 signed TLDs only resulted from one single registrar who enabled DNSSEC by all his clients by default. The statistic is part of a larger report on the „French Internet" published this summer. Valadon was challenged about the definition of "French Internet", which he defended had been derived from entrances in the RIPE database.

Surveillance - warming up the discussion

Efforts for a "more national" Internet are just a little trendy, Jari Arkko, Chair of the Internet Engineering Task Force, who used the RIPE meeting obviously to prep for all the "the IETF and surveillance" talks to come. Arkko has since talked and reiterated his views at the Internet Governance Forum, and will bring back reactions and his views to his own community at the IETF meeting in Vancouver.

The IETF Chair at the RIPE meeting called a potential nationalization a "disaster for the global Internet and for the industry and for the people who basically depend on the global Internet to do all kinds of things and not just services in their country for the Internet." More interconnection, and diversity in the landscape would be welcome on the other hand.

Arkko's many talks show that currently it is not possible to have an Internet related event without a debate on the state surveillance revelations from former NSA employee and contractor Edward Snowden. Arkko's main points when speaking at the operators' community were the need to "understand what the real dangers in the Internet are for our packets", that the "crisis" was a reminder that there are some challenges in Internet security" and that finally the technical community could consider to take the opportunity and reversing the default: instead of allowing Internet traffic to be "insecure by default" one could "turn security on, like for web traffic".

Intentionally compromised standards?

Arkko said that communication about details were still sparse, but what had been news and "surprising" were the scale of the bulk intelligence collecting, information about obligations to email providers like Lavabit to hand over keys (not only traffic) and obligation to CA providers to cooperate with the services on certificates distributed to major Internet organisations. What was more nagging for the technical community were potential weak crypto with RC4 potentially a victim, back doors in firmware, software or random number generators which were not that random any more. NIST in fact has recommended recently against using its random number generator.

The single most worrying aspect of the affair for the IETF certainly is the allegation that there are vulnerable IETF standards. Arkko was cautious here, too, pointing to claims that standards might be manipulated during the standardization process, but Arkko was rather skeptic on that: "In many of these cases I have either talked to the people involved or been myself a little bit involved personally and at least our perception has to be that that is probably unlikely that don't believe everything that is said in the press about these kinds of things or claimed by someone."

Actions underway at the IETF

Snowden has opened a time window to turn on security. The reaction from the developer community might best be assessed during the IETF meeting in Vancouver where a technical plenary, a BoF (perpass) and several slots in existing WGs are dedicated to the subject. Ongoing work that might be influenced is Transport Layer Security (TLS 1.3) and Httpbis. Also protocols like IPSec had to be reevaluated. Much more difficult according to Arkko was to check out back doors.

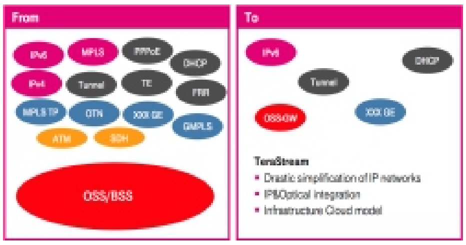
The IETF has invited Bruce Schneier, well-known and respected security and crypto-expert, to discuss his challenge published a few weeks ago that the engineering community had to "take back the Internet".

There is quite a bit disagreement about what the technical community should do. At the RIPE meeting several speakers warned against pushing up encryption and making it, in general, harder for law enforcement and services to "do their work". APNIC Chief Scientist Geoff Huston, who has been working in law enforcement earlier in his career, warned that cost for industry and every tax payer would go up. Huston said: "Thinking somehow that I secure one bit and I have got privacy is naive, and in fact, being a little bit more honest and open about the fact that this network is like the public space out there on the street and that almost everything you do is observable and start from that tenant, rather than trying to think that technology can invent me a cloak of invisibility is perhaps a little more honest."

European based RIPE operators who spoke up during the debate did not agree, warned that technology might not help to solve the issue as long as there is a lack of understanding and political will with governments. A Russian ISP reported that he had seen encryption in Russia going up steadily since the Snowden revelations.

New IP core network concept brought to you by an old incumbent operator

For years there has been research about an "Internet 2" with not much practical results so far. A concept on how to run a transparent IPv6-only based core network in 2020 drafted by well-known networking expert Peter Löthberg for German incumbent Deutsche Telekom attracted a lot of interest from operators gathered at RIPE. The major innovative step of "TeraStream", according to the experts: instead of adding new boxes and software, the number of necessary protocols and hardware devices is drastically reduced.



The network for which running code is in place at DTAG's subsidiary Telekom Croatia (500 customers according to Axel Clauberg at DTAG) is based on an IPv6-only network; IPv4 is a „service" realized via what Löthberg said were „keyed IPv6 tunnels" and what Telekom Labs described as a „special lightweight 4over6" tunneling procedure. IPv6 will be the language of the new network, and all non-IP-traffic is forwarded via Carrier Ethernet.

The other big diet Löthberg prescribed for TeraStream is to throw out optical filters and mirrors.

Working Groups

DNS WG

The RIPE community has to come up with a policy about who is eligible to have his secondaries run by the RIPE NCC. The organisation has run secondaries for many ccTLDs in the past, and currently provides pro bono services for 71 small registries (240 zones, including internationalized domains) of which 26 are in the RIPE service region. Anand Buddhdev who leads the DNS team at RIPE called to members to support the development of criteria about who will be eligible for this in the future. RIPE NCC wanted to have clear-cut rules now that many new TLDs were coming to the root. "We would like all our services to be provided in an open and transparent fashion and for this particular ccTLD secondary service we don't have very clear guidelines on who qualifies, who doesn't, whom do we say yes or no to, and with all the developments going on in the DNS world, we would like to have a clear and transparent policy about this, so that we can say to our community and users in general, operators, that this is the RIPE NCC's policy."

The DNSSEC validation rate keeps low, Geoff Huston, Chief Scientist at APNIC reported from a test using his often used flash-ad-gathered statistics.

ICANN has replaced the classical DNS Stats collector (DSC) with a new open source tool called hedgehog. The new development shall mainly address scaling problems DSC had, Dave Knight from ICANN said at the RIPE meeting. Knight, who said that the license of the tool was still in preparation, advertised the future potential to have additional ways to display data, for example "heat maps" or "word clouds". Data processing was moved from the presenter to the nodes and new data uploads were lighter than XML.

NRENum.net has a new policy document that shall enable easier VoIP and teleconferencing services for the NRENum members, Carsten Schiefner, chair of the dormant ENUM group reported at the RIPE Athens meeting. The Terena Executive Committee gave green light for the new document on 25 September and also for a new global Governance Committee (GNGC) for NRENum.net.

NRENum.net is "an end-user ENUM service run by TERENA and the participating NRENs (National Research and Education Networking organisations) primarily for academia". Members of the new committee are Tim Boundy (Janet), Erik Kikkenborg (NORDUnet) for Europe, Ben Fineman (Internet2), Alex Galhano Robertson (RNP) for the Americas and Bill Efthimiou (AARNet), Praveen Misra (ERNET) for Asia. Currently there are 32 countries in the ENUM (e164.arpa) tree.

The DNS WG heard talks on IP-fragmentation (see above) and amplification attacks (see above).

Cooperation WG

Nigel Hickson, ICANN Vice President, gave a brief report about ideas for ICANN's European engagement strategy. While Europe was well ahead in terms of infrastructure an exchange and engagement was envisaged, he said, to discuss upcoming EU legislation and also the new gTLD program. While Europe was second in applications there were still many companies who never had heard about the process. Also ICANN policy should be more informed by EU standpoints: „Would ICANN have ever really gone through with the new registry accreditation agreement, the RAA 13? I mean, that shouldn't have been adopted in the way it was." The RAA creates some difficulties for EU registrars with regard to data protection legislation. The European strategy of ICANN was still under development, Hickson said, and would be discussed during a Brussels briefing session on 5th or 6th of November. There would also be a public session on the European strategy at the ICANN next meeting.

The eID Regulation of the European Union has been discussed several times at RIPE meetings and concerns have not died down after a presentation from the EU Commission. RIPE Counsel Athina Fragkouli warned that the regulation included not only the authentication of electronic Ids, but also authentication of websites.

The regulation, which contrary to a EU directive will have immediate effect for all member states, could collide with the authentication process used for DNSSEC, as DNSSEC was based on the chain of trust rooted outside of the EU. The obligatory listing of trusted authentication providers which is part of the regulation also is a problem for DNSSEC services. The RIPE NCC has written to the Parliament and the Council of Ministers to address the potential collisions and ask for a set of amendments to take out the authentication of websites, for example. The lead committee in the EU recently passed its amended version, but did not limit the scope as narrow as proposed by RIPE NCC.

Elida Plexida from the Greek Ministry of Transport and Communication assured the participants at the RIPE meeting that many member states had concerns with regard to the regulation. The Lithuanian Presidency had just presented a new draft and the Council was going through this graph by graph. In the end it might be the Greek presidency who will have to finish the legislative process. The new digital agenda package presented by EU Commissioner DG Connect Neelie Kroes about which the RIPE also has a number of concerns, especially with regard to Internet security, might not make it before the end of this legislature which ends in April, next year.

The Cooperation WG is looking for a new Co-Chair to replace Patrik Fältström, Netnod.

IP-Address Policy

RIPE is moving forward with its clean-up policy for IPv4 address allocation and assignment despite a lot of discussion about it when it was first presented. Especially the “no need”-language which seemed to express that the needs-based principle for address allocation was not well received by the ARIN region. ARIN had signaled that they would not allow for inter-RIR transfers of IPv4 addresses if RIPE would relinquish the needs-based allocation.

At the RIPE meeting in Athens the Address Policy WG discussed a toning down of the proposal, while still staying on course with the intention to have less bureaucracy for address allocation. The policy's stated goal is to remove

- “conservation” as a stated goal from the policy
- obligations for documentation, evaluation of need, and validation of actual usage for both assignments and allocations
- the slow-start principle
- the assignment window mechanism
- limitations on size and frequency of sub-allocations.

Address policy WG Co-Chair Gert Döring said a more diplomatic text would now be co-authored by Tore Anderson (Redpil Linpro) and the more Internet Governance seasoned Malcolm Hutty (Linx).

Brokering and the new role of the IP registries

The address registries after IPv4 public address pool is gone (as is the case for APNIC and RIPE) quite obviously face the question about their future role. Geoff Huston who said he could not speak for APNIC in that discussion during a panel with three IPv4 brokers described the role conflict of the IP address registries. The running out of IPv4 addresses which in the end were allocated according to much discussed rules about fairness and procedure brought up the question: "What is our role as registries? Do we run a market? Do we facility a market? Are we the brokers?" The conflict, according to Huston, was between facilitating a market and being the title registry which everybody had to trust.

Several new issues resulting from the run-out of IPv4 addresses created more uncertainty about the role: what is the relation of brokers and RIRs? What is the relation of those who lease IP addresses from a RIR member? How are leased addresses reflected in the RPKI? Huston commented, the RIRs had to answer these questions about their future role.

RIPE has started to delve into a new role with regard to facilitating transfers. Not only is there a listing service, which currently lists around 400,000 IPv4 addresses for sale vs 16 million wanted. The RIPE also lists brokers that have signed the Recognized IP Transfers Broker Agreement, in which the Brokers commit to RIPE policies for address allocation. The list of brokers has grown considerably to 13.

The number of transfers has gone up since May last year, said Andrea Cima, Registration Service Manager at RIPE NCC, during the panel. Before, around 50.000 address monthly were transferred, now the median is 250.000 with peaks going up to 400.000 with 15 transfers per month being completed on average. Mergers and acquisitions observed in the RIPE region were around 30 per month.

The three brokers represented, Addrex, IPv4 market group and Kalorama, said they expected to stay in business for a decade, yet Louiz Sterchi said there were reservations of managers who witnessed high spending for frequencies to buy into the resource IPv4.

A comparison between 2012 and 2013 results for the regular EU IPv6 study show a slight increase of ISP intending to introduce IPv6 for their customers over the next two years. Still the number of users has to be found through a microscope, said Frank le Gall. It is still as low as one percent. An IPv6-only test during the RIPE meeting worked very well.

The next RIPE meeting will take place in Warsaw, Poland from 12 – 16 May, 2014