NLnet Labs

Annual Report 2013

Front page modeled and ray-traced using Blender.

I Highlights

Stable and reliable DNS and the opportunities to base a globally secured trust infrastructure on top of it using DNSSEC remains one of our key interests. The 2013 release of NSD4, a new major version spawning from 10 years of experience, is an important milestone in the continuous development and support of our authoritative name server software. We refined the rate limiting features in NSD and implemented the so-called client subnet option in Unbound. We continued contributing to the OpenDNSSEC project, the only open source comprehensive DNSSEC key-maintenance and signing product available, and allowed it to be used as 'bump in the wire' in more dynamic environments. In collaboration with Verisign we started work on implementing the so-called getdnsapi, intended to be the future de-facto manner by which applications will retrieve secured DNS information, an initiative with a high potential for others to innovate with. Further, we are proud of the publication of a DNSSEC Audit Framework as a tool to overcome common corporate deployment hurdles.

In the technical governance area we have actively participated in ICANN's new gTLD programme, through participation in the registry services evaluation panel, and collaboration in a study of name collision risks.

Our work in the European Multi Stakeholder Platform for ICT standardization has strongly contributed to the likely *identification* of IPv6 as the first set of IETF specifications that can be reference in public procurement. Finally we had staff join the *Panel on Global Internet Cooperation and Governance Mechanisms* chaired by President Ilves and Vint Cerf.

In the Routing Area we have bootstrapped a new project called the *Extendible Next Generation Routing Information Toolkit* (ENGRIT) and, together with SIDN Labs, defined a new project for Anycast routing research project called SAND. We secured funding for both projects.

We updated and published our mission, vision, and long-term plans in a Strategic Plan and incorporated the Open Netlabs BV, a wholly owned subsidiary that will be the entity under which we will develop support programs for NSD, Unbound and deploy other commercial activities.

We hosted a record number of 13 interns during 2013.

All our deliverables are targeted to enhance the open, secure, and innovative nature of the Internet for all.

2 Areas: DNS and DNSSEC

NLnet Labs' focus in this area is on the security and the stability of the DNS as a global system.

By developing and maintaining tools that facilitate the provisioning and use of DNSSEC we lower deployment barriers of a technology that will allow for further innovation of global Internet security mechanisms.

By developing alternative implementations of name-servers we also increase the stability of the DNS by offering diversity in code-base.

Through research we answer operational, technical, and theoretical questions about DNS security, architecture, operations, and deployment.

2.1 DNSSEC Zone and Key management: OpenDNSSEC

OpenDNSSEC is a turnkey solution for DNSSEC management. It is (to our knowledge) the only Open Source DNSSEC key-maintenance expert system that supports all documented key rollover scenarios and allows flexibility in operation varying from one key maintenance policy for all zones to per-zone configuration and maintenance.

Goals for *2013*

Maintaining stability of the version 1 branch and releasing and maturing version 2. Maturing of version 2 is mainly a matter of performance tuning, and creating additional adapters, for instance a dynamic update adapter, and making the product fully backwards compatible with version 1.

Activities

During the first half of the year NLnet Labs has mostly concentrated on finalizing the functionality in the adapters and general support. In the second half of the year NLnet Labs has mainly worked on general support and getting new OpenDNSSEC team members up to speed. While the version 2's functionality is developed and ready a large delay in delivery has been introduced by a late requirement for API compatibility with version 1.

Results

Publication of version 1.4 that supports AXFR and IXFR in April 2013 followed by three maintenance releases 1.4.1 (June 27), 1.4.2 (September 11) and 1.4.3 (December 4). In addition we saw maintenance release version 1.3.13 (February 20), 1.3.14 (May 16), 1.3.15 (September 19), and 1.3.16 (December 4).

Impact

OpenDNSSEC has lowered the barrier to deploy DNSSEC: its availability has been contributing to positive decisions with respect to the deployment of DNSSEC. OpenDNSSEC has a number of high-profile users as listed at http://www.opendnssec.org/about/known-users/.

2.2 DNS Name Servers

2.2.1 NSD

NSD is NLnet Labs authoritative-only name server. It is designed to be light weight, high performance, secure, and single purpose.

Goal

NSD3: continue to support NSD3 as a secure high-performance name server.

NSD4: make NSD appealing for a larger set of users. While it continues to use the proven DNS logic of NSD3, its internal data structures are being organized to allow for more flexible operations. In addition we have improved its performance.

NSD3 Activities

The use of authoritative name servers for reflection attacks has been an important part of our attention. We worked with researchers and the community in order to improve our implementation.

We have kept NSD3 up to date with bug fixes and newly specified RR types, such as NID, L32, L64, LP [RFC6742], EUI48 and EUI64 [RFC7043].

NSD4 Activities

After gaining experience with the beta code in some production environments and continuing our own testing efforts, we reduced the memory footprint and start-up performance prior to NSD 4's release. The first experiences with NSD4 provided us ideas and priorities for the 4.1 release that is expected in 2014.

Results

NSD 3.2.15 (February 4) introduced RRL and support for the ILNP resource record types. NSD 3.2.16 (July 22) saw enhancements in RRL support and introduced EUI48 and EUI64. This in addition to regular maintenance features.

A number of blog-post[1] explain some of the features, architecture, and resource usage to prospective users.

NSD 4.0.0 has been released 29 October 2013.

Impact

NSD clearly serves its design goals: to provide an alternative implementation of authoritative DNS servers in order to increase resiliency and stability of the global DNS infrastructure: NSD is used on root servers such as the L and K root- servers and many top-level domain registries, including .NL, .DE, .BR, .SE, and .UK. The main motivations for running NSD are high-performance, stability, and to have code diversity within the installed base.,

NSD4, together with the CzNIC's KNOT implementation, are currently the highest performance name server implementations available.

1-https://www.nlnetlabs.nl/blog/category/nsd/nsd4-nsd/

2.2.2 Unbound

Unbound is our secure recursive name server

Goals

Facilitate incorporation of Unbound in software stacks and platforms, and/or the deployment of Unbound as the default resolver in OS distributions. Maintain stability and high-performance. Review memory requirements.

Activities

We are supporting the role of Unbound in new and adapted setups for which new features are needed. We continue to be lenient towards feature requests, in part to foster the adoption of DNSSEC (-validators). Unbound itself is mature and requires an occasional bug fix.

In addition of maintenance of the product we made a start to remove the ldns dependency from the Unbound distribution as this facilitates the inclusion of Unbound in the base distributions of Red Hat and FreeBSD. This work will be finalized in 2014.

In parallel we have been working on an implementation of the 'client-subnet' functionality[2].

Results

Publication of versions 1.4.20 (March 21) and 1.4.21 (September 10). Full functioning beta release of the client-subnet branch.

Impact

Unbound is recognized as a leading implementation of secure and stable DNSSEC validator. As a mature and stable product, Unbound is in use in various high profile and high availability environments that are early deployers of DNSSEC validation. Unbound's availability continues to be a significant contribution in the deployment of DNSSEC and allows for redundancy and resiliency in critical infrastructures by offering a 'biologically' different code base.

The FreeBSD project uses Unbound as the default resolver starting with the version 10 release of the system.

2.3 DNSSEC Last Mile

The last mile (between central resolver and application) is an important hurdle in DNSSEC deployment. NLnet Labs contributes technology in order to bridge the gap and/or to understand the deployment issues.

Expected impact

These innovations allow applications to assert trust in DNS information and are expected to broaden the relevance of DNSSEC from a security mechanism for DNS only to a foundation for global trust infrastructure.

2.3.1 Secure libresolv (getdns.api)

Goal

A feasibility study to deliver a standardized API for DNSSEC resolution.

2-http://tools.ietf.org/search/draft-vandergaast-edns-client-subnet-01

Activity and Results

In June we agreed with Verisign Labs to step up collaborative efforts with respect to the development of an implementation of the 'getdns' api that is being developed by Paul Hoffman[3]. In the second half of 2013 a code-sprint and a *Hackaton* for Verisign's developers in December furthered the work.

Results

A working product based on libunbound that is expected to be released in 2014. Toorop will be coauthor on a forthcoming document describing the API.

Impact

Our involvement in the development improved the specification of the API. We expect this product to change DNSSEC acceptance and boost deployment on user-facing systems on the mid-long term.

2.3.2 DNSSEC trigger

Goal

Keep paying attention to the maintenance of DNSSEC-Trigger and allow ourselves to put the products development on the high priority queue if it is likely that it can move the needle on DNSSEC deployment.

Activity and Results

DNSSEC-trigger is actively being maintained in the Fedora and Debian Linux community where hooks to the network manager components of the OS have been developed. A new release incorporating feedback from this and other groups is expected for 2014.

Impact

Qualitative experience with last mile DNSSEC deployment and broadening operational experiences notably for, but not limited to, mobile applications.

2.3.3 CGA-TSIG.

TSIG can also be used to deliver authenticated DNS responses to the client. CGA-TSIG is a proposal for an extension of TSIG, taking away the scalability problems that shared keys introduce.

Activity and results

During 2013 two interns worked on proof of concept implementations of CGA-TSIG[4]. By the end of 2013 the work was finalized. A report will be published beginning 2014.

2.4 Supporting Software and Infrastructure

2.4.1 Ldns

Goal

Minimal: Memory reduction (mainly for OpenDNSSEC). Maximal: release of ldnsv2.

3-http://www.vpnc.org/getdns-api/ and http://www.vpnc.org/pipermail/getdns-api/
4-http://tools.ietf.org/html/draft-rafiee-intarea-cga-tsig-06

Activity

We reviewed the memory management of ldns and thereby optimized its performance. Additionally we resolved a number of bugs, added newly standardized features, and separated the functionality needed by Unbound as dependency. (So the dependency on ldns in the Unbound distribution is reduced, also see 2.2.2.)

Results

Results of these activities will be published as release 1.6.17, early 2014.

2.4.2 Net::DNS

Goal

Regular maintenance and continued clean-up of the architecture.

Activities

We continued to maintain Net::DNS. A notable feature introduced in Net::DNS is the support for TSIG validation. We continued to collaborate with Dick Franks, one of the most active community volunteers, on the low-level refactoring.

Results

Net::DNS 0.73 and Net::DNS::SEC 0.17 releases in December 2013.

2.5 Other Activities

2.5.1 DNSSEC Audit Framework

Description

A DNSSEC audit is the process of structural examination of a DNSSEC infrastructure. The purpose of such process is to evaluate the level of assurance of the system. A key document for performing an audit is a review checklist. The review checklist provides structure of the actual work and gives confidence that the audit scope is adequately covered. The DNSSEC Audit Framework-document is a generic checklist for a DNSSEC review and provides a framework that assists auditors to perform an actual DNSSEC audit[5].

Results

In collaboration with SWITCH, the TLD operator for .CH and .LI we developed a DNSSEC audit framework that has been made available under a Creative Commons License.

Impact

The availability of a framework will allow for lower costs audits of DNSSEC environments and is expected to lower barriers to deployment. Reviews of operational environments are expected to eradicate operational bugs, hence increasing the security of the Global Internet.

2.5.2 IETF DNS activity

Results

RFC 6912 “Principles for Unicode Code Point Inclusion in Labels in the DNS” by Sullivan, Thaler, Klensin and Kolkman was published in April http://www.rfc-editor.org/rfc/rfc6912.txt.

5-http://www.nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf

RFC 6950 “Architectural Considerations on Application Features in the DNS” by Peterson, Kolkman, Tschofenig, and Aboba was published in October http://www.rfc-editor.org/rfc/rfc6950.

An updated draft containing their musings on authentic denial of existence in the DNS[6] by Gieben (SIDN) and Mekking was approved for publication as RFC (to be published in 2014).

2.5.3 ICANN gTLD related activity

See section 5.1.

3 Area: IP and Routing

In order to increase the security and maintain the stability of the global routing system, NLnet Labs contributes to the understanding of its dynamics both in terms of technology as well as its operation. Besides, we try to develop tools and practices that lower the barriers to deployment of security features.

NLnet Labs role is unique in the sense that Labs is neither vendor, nor operator and takes an inter-operator global perspective.

3.1.1 BGPSimulation

Goal

Study stability, resiliency, and stability properties of the Routing System.

Activities

The bulk of the work in this area has been done by interns.

Jeffrey de Looff used our simulation lab to study the network complexity of our routing infrastructure, specifically looking at issues where more interconnections not necessarily result in a more robust network. In September Tim Blankers started to research what the cause is of the invariable signal of BGP background noise over the past decade

3.1.2 Inter-domain Routing Security and Stability

See section 4.1 where we describe our new ENGRIT project.

3.1.3 Network complexity research (IRTF NCRG)

See section 3.1.1 where we are looking at complexity issues in the context of routing.

3.1.4 National-Centric IP Critical Infrastructure

Goal

Utilize our expertise to contribute to the public debate on this topic.

Activities

In collaboration with SIDN we hosted two interns.

Result

Fahime Alizade and Razvan Oprea published a report on “Discovery and Mapping of Dutch National Critical IP Infrastructure”[7]

6-http://tools.ietf.org/html/draft-gieben-auth-denial-of-existence-dns-02
7-http://staff.science.uva.nl/~delaat/rp/2012-2013/p31/report.pdf

Impact

The work by Alizade and Oprea provides a unique perspective on the Dutch Critical Infrastructure[8]. We extend on this work in 2014 by hosting another intern that studies what (security sensitive) information can be gathered from critical infrastructure from open data (Open Data Initiative). Furthermore, in 2014 we will co-submit a proposal for an NWO grant to be used for a study on Critical Infrastructures.

3.1.5 Multipath Networking on layer 2 and layer 3

Goal

Bridge between research and practical use resulting in papers documenting deployment, road maps, and practices.

Activities

We have been collaborating with Roland van der Pol from Surfnet in the context of the RoN project *Multipath Networking* in which the use of Multipath TCP and OpenFlow was examined.

Results

Paper “Experiences with MPTCP in an intercontinental OpenFlow network" has been accepted for TNC 2013[9].

During the TNC 2013 conference Multipath TCP over one100 GE en two 10 GE transatlantic links was showcased[10].

4 New Projects

In 2013 we defined two major research projects that are expected to span multiple years of effort and an investment in additional temporary resources. For both projects we have secured the funding by means of a project reservation. The first project is well underway, the second project will be set in motion in 2014. We started the definition of a 3rd project at the end of 2013, that resulted in a letter of intent in the beginning of 2014. Execution of that project depends on acceptance of our proposal.

4.1 Extendible Next Generation Routing Information Toolkit (ENGRIT)

Goal

Design and development of a next generation Internet routing registry (IRR) toolset to decrease the costs of implementing and operating security practices.

Activities

After a definition phase we acquired Per Bilse as a consultant to work on the Extendible Next Generation Routing Information Toolset project (ENGRIT). This toolset is being developed in collaboration with a few industry partners who form a advisory board to provide feedback on the design and implementation.

8-At the time of writing a google search for “Dutch Critical Infrastructure” referred to this document in the first 5 hits.

9- https://tnc2013.terena.org/getfile/872

10-https://tnc2013.terena.org/core/event/30

Broadly, the design objectives for the new IRR toolset is to create a modular toolset, designed for extensibility. The guiding principle is this: if the job at hands is easy, tooling should also be easy and lightweight; but if the task is more complex, more effort can be demanded to realize this with the toolset. Such a gradual buy-in is currently not available with the tools. With an extensible toolset, small for simple tasks, more heavy for complex tasks, this can be realized. Also for maintenance, future developments, and inclusion of new technology, modularity and extensibility are important.

Explicit goals are:

- Trust in quality and longterm maintenance.
- Adaptable for commercial organizations (BSD license).
- Extendible by the community.
- Clean design and architecture.
- Well documented: Documentation of Architecture, Implementation, API, and User documentation.

Expectations

The project started in 2013 and is expected to deliver core functionality in 2014, and deliver a number extension modules during 2014 and 2015. A financial reservation to secure the continuity of this project has been made.

Expected Impact

The availability of a toolset will assist in providing easier automation of routing configuration tasks and the ability to incorporate cryptographically signed resource information thereby improving stability and security of the global Internet routing system. Besides, the availability of a good Open Source toolset may lower the entry to market for new ISPs in developing markets.

4.2 Self-managing Anycast Networks for the DNS (SAND)

Description

High availability can be achieved by distributing services, and for DNS this implies that the name server for the TLD is distributed, geographically and topologically (w.r.t. Internet). By distributing and strategically positioning DNS name servers for a TLD, one can also reduce the average latency for the clients resolving a name in the TLD zone.

Distributing DNS name servers can be achieved by different methods, but for TLDs one specific method has many advantages: DNS anycast addressing and routing. With anycast routing, one can take advantage of the robustness of the BGP routing infrastructure, where the same server IP address exists in multiple locations, possibly on different continents, to provide a decentralized service. While conceptually simple, namely the simultaneous announcement of an IP address (range) from different networks on the Internet, it is not trivial to implement. In particular if latency, robustness, and resilience are considered in the equation for selecting the locations of anycast nodes.

The decision where and how to place anycast nodes on the Internet is a complex one; For a dynamic system like the Internet with varying traffic and DNS query load, it is difficult to find an optimal point of operation that meets most operational requirements. Over-provisioning is standard practice, but in

case of incidents—accidental or with malicious intent—DNS traffic should adapt to new situation. The BGP routing infrastructure might provide connectivity over changes in the network, but for optimality of service, other parameters have to be taken into account as well.

This project proposal focuses on solutions for dynamic DNS anycast services to deal with changes in Internet connectivity, DNS query traffic, and other factors influencing their service in terms of availability, performance, and possibly security. And while optimizing for these quality of service terms, the operational costs have to be considered also. This complex system of anycast nodes must be managed automatically.

Self-management methodology can help to address the problem of automated management of a complex system like any-cast DNS. The practical deployment of the proposed methodology defines the impact of a solution. This has to be carefully studied, e.g, in incremental implementation, interoperability in the DNS/BGP ecosystem, return on investment, etc

The project sets out to use self-management methodology and apply that to anycast by developing measurement, adaptive mechanisms and controls so that the monitoring, analysis, plan and execute (MAPE) loop can be automated and the properties of anycast DNS will be better understood.

This project —its development and implementation— is a collaboration between NLnet Labs and SIDN Labs

Expected Impact

The focus of the SAND project on practical deployment of the results, defines the design space for solutions. The proposed research subject of DNS anycast with self-management components can be phased such that each milestone or deliverable in the project can be evaluated and validated on its integration and interoperability with current standard practices in DNS anycast.

Part of the research will be the evaluation of optimal (strategical) topological locations for anycast nodes. The availability of a set of locations to run anycast nodes must be known beforehand, either by available servers at that location, or guarantee of available IaaS services at certain networks covering a topological region. This work will be complementary to the self-management infrastructure and a relevant result in itself.

The final result of the project reduces the complexity of managing a DNS anycast infrastructure, and provides flexibility and adaptability to act upon changes in the network and DNS client behavior (flash crowd, DDoS, etc.). In its operation, the system can also reduce operational costs: it is not only adding or moving anycasts nodes, but if usage patterns indicate that certain nodes can be shutdown, this can reduce costs while performance metrics are still within specified bounds.

4.3 A Framework for Self-regulation for robustness of critical infrastructures

End 2013 we engaged in a collaboration with Brazier, Warnier, and van Eeten from TU Delft and Clark from NCSC that leads to request for a grant in the context of the NWO cyber security call in 2014.

Description

Infrastructures are very important for the national economy and all its facets that impact society. A number of infrastructures are critical to society: when such an infrastructures breaks down the economic and societal impact is enormous. Examples of such infrastructures are communication (Internet, telephone), power (electricity, gas), and drinking water networks.

Due to the high reliance on these critical infrastructures it is important that they are resilient: they need to continuously operate and if they fail, they should fail gracefully and be able to recover quickly from failures. Most of the work in resilience of critical infrastructures (especially infrastructures other than the Internet) has focused on safety properties (physical security properties like natural disaster, physical damage, etc.) and while safety implies some form of security, it does not address attacks that are specifically designed to cyber security attacks, by intelligent attackers, to bring the infrastructure down. This proposal focuses on these issues: security issues in the context of (Internet) networked critical infrastructures.

The main idea of this proposal is to design a framework that can be used to evaluate the robustness of critical infrastructures with respect to network security of remote and distributed attacks.

The framework will present a security assessment of the critical infrastructure. This assessment can be used as a basis for sector/industry partners to strengthen and self-regulate the security of critical infrastructures. Regulatory and other oversight authorities can use the same framework to check if the self-regulation works.

Approach

The project contributes to both theory building and empirical insight in the current state of critical infrastructures. The four main requirements for such a framework are:

1. good metrics, these will partly be developed in the project (theory building) based on existing literature;
2. measurements, that indicate the current state of an infrastructure;
3. good instruments/tooling to perform measurements and apply metrics (applied research) for a diverse range of infrastructures;
4. relevant data, the data is required to calibrate tools for individual infrastructures. Project partners will provide most of the data.

The framework should combine relevant metrics in a useful way and present relevant findings (visually) to the end user.

Scope

Two of the main critical infrastructures, electricity and the Internet, will be used as example critical infrastructures. A lot of data is required to make an accurate assessment of the vulnerability of these systems, therefore the project focuses on critical infrastructures in the Netherlands (where data can be acquired through the project partners). The developed framework should also be usable in other countries and for other infrastructures.

Expected Impact

This project will provide instruments with which stakeholders (operators of critical infrastructures, and regulatory authorities, etc) can assess the state of a network. Stakeholders can identify potential vulnerabilities, implement and deploy improvements, and make assess that identified problem is solved.

5 Area: Knowledge Dissemination, Outreach, and/or Community Participation

The Internet's governance depends on well informed stakeholders and decision makers. The various organizations and entities, which typically thrive on volunteer participation, are typically manned with quality personnel. NLnet Labs is an active participant in those areas where its expertise, and the expertise of its employees, will further the Open Internet.

NLnet Labs is active in various areas of Internet Governance.

5.1 ICANN New GTLD program

In this context Akkerhuis, as consultant, participated in ICANN's registry evaluation panel. Kolkman participated, as consultant, in a study of "Name Collision in the DNS" by Interisle resulting in a paper at http://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf

As volunteer Akkerhuis is involved in ICANN's Security Advisory Committee, which also takes an interest in the issues surrounding the new GTLD program. While Kolkman, also as volunteer, is engaged in the public debate. This resulted in the publication of a discussion paper "A Procedure for Cautious Delegation of a DNS Name"[11].

Finally Akkerhuis and Kolkman continue active participation in the ICANN preparation meetings hosted by EZ.

5.2 RIPE / Network Operations Community

NLnet Labs staff actively participates in the RIPE and broader operators community

Overeinder is also vice-chair of the RIPE Program Committee and co-chair of the RIPE BCPOP Task Force. Akkerhuis is a co-chair of the DNS-WG and and since December 2013 Akkerhuis is a member of the ENOG program committee.

During RIPE 66 Overeinder organized, in collaboration with Andrei Robachevsky a panel on "Seven Years of Anti Spoofing" trying to assess why BCP38 has so little deployment.

Also during RIPE66 and RIPE67 NLnet Labs' staff disseminated its knowledge and expertise with a number of high impact appearances.

5.3 IETF and Technical Community

Kolkman acts as chair of the WEIRDs WG and contributes to the timely specification of a Registration Data Access Protocol.

Kolkman is also active in IAB program that advises the IAB on the strategy with respect to the IANA function within that context he participated in I* leadership meetings and is the principal author of '*A Framework for the Evolution of the Internet Assigned Numbers Authority(IANA)*'[12]

In August 2013, Kolkman resigned as member of the RFC Series Oversight Committee.

11-http://tools.ietf.org/html/draft-kolkman-cautious-delegation
12-http://tools.ietf.org/html/draft-iab-iana-framework-00

5.3.1 MSP on Euro ICT Standardization.

Kolkman represents the IETF in the Multi Stakeholder Platform for European ICT standardization.

The Platform advises the Commission on all matters related to European ICT standardization policy and its effective implementation, including:

- the work programme for ICT standardization and its priorities;
- progress in ICT standardization and related activities in support of legislation and policies;
- recognition of technical specifications developed by global ICT Fora and Consortia where the requirements set out in annex II of the draft regulation are met.

Results

In particular, Kolkman has been actively involved in development of the positive advice for identification of IPv6[13], DKIM[14], LDAPv3[15], and DNSSEC[16]. Additionally we made a significant contribution to chapter 4 of the rolling plan on ICT standardization[17]. Experiences gained within the platform were at the basis of a discussion of quality control during the IETF87 plenary and the proposal to clarify the classification of proposed standards[18] which will be published as RFC in 2014.

5.4 Global Internet Governance

Kolkman joined the *Panel on Global Internet Cooperation and Governance Mechanisms* that formed in November 2013. The panel is a diverse group of global stakeholders from government, civil society, the private sector, the technical community and international organizations—all deeply devoted to the future evolution of the Internet.

The Panel seeks to engage in a collective dialogue on critical Internet cooperation and governance issues, and has expressed support for a multi stakeholder model. Building on the successes of the last two decades, its goal is to chart a roadmap for the future evolution of the global Internet cooperation, administration and governance ecosystem.

From December 2013 to May 2014, the panelists will meet three times in person. The first meeting was held in London December 12 – 13.

5.5 Other

Kolkman became member of the program committee for the Workshop and Prize on Root Causes and Mitigation of Name Collisions (WPNC14, http://namecollisions.net).

NLnet Labs is a knowledge partner of “Centrum Informatiebeveiliging en Privacybescherming” (http://http://www.cip-overheid.nl).

13-http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=8208
14-http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=8195
15-http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=8212
16-http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=8200
17-http://ec.europa.eu/DocsRoom/documents/116/attachments/1/translations/en/renditions/pdf
18-http://http://tools.ietf.org/html/draft-kolkman-proposed-standards-clarified

6 Area: NLnet Labs Continuity

6.1 Strategic plan

During 2013 we reviewed NLnet Labs mission, vision and strategy and, for the first time, published a Strategic Plan[19]. The document documents: our mission "*To provide globally recognized innovations and expertise for those technologies that turn a network of networks into an Open Internet for All.*"; how our mission relates to our statutes; the principles for setting direction; discusses the directions in which we plan to develop over the coming years; and our ideas to for financial continuity.

6.2 Open Netlabs BV

NLnet Labs will diversify its income by identifying and engaging with more parties to provide a continued commitment to fund its work and by cooperating with a wholly owned subsidiary: Open Netlabs BV.

Open Netlabs BV has been established and will be the commercial vehicle supporting the open source activities by generating sustainable income on the longer term. Positioning and promotion of the activities have started and the initiative has been launched with its own website http://www.opennetlabs.nl. The initial focus is on providing Unbound support and (limited) training and consultancy and contacts have been established for initial offerings. Adjusting and expanding strategy and portfolio will be a running process.

Han Brouwers is the director of Open Netlabs BV. Stichting NLnet Labs owns 100% of the Open Netlabs BV stock.

19-http://www.nlnetlabs.nl/labs/about/Strategic-Plan.pdf

7 NLnet Labs organization and finance

7.1 Board

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its board consists of three to five members with staggered terms. The board's composition and most recent rotation schedule is shown in the tables.

Six board meetings took place in the year 2013. Olaf Kolkman participated in the board meetings in his role of Director of NLnet Labs, Han Brouwers participated as the director of Open Netlabs B.V.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€177 for 2013). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2013

name	function	end of term
Frances Brazier	secretary	December 28, 2014
Roelof Meijer	member	May 31, 2015
Wytze van der Raay	treasurer	December 28, 2013
Leo Willems	chair	February 1, 2016
Ted Lindgreen	member	January 31, 2015

Director and Board Member Additional Functions in 2013					
Frances Brazier	**Ted Lindgreen**	**Roelof Meijer**	**Wytze van der Raay**	**Leo Willems**	**Olaf Kolkman**
- Professor Engineering Systems Foundations at *the Technische Universiteit Delft (TU Delft)* - Chair of the board of *Landelijk Netwerk Vrouwelijke Hoog leraren (LNVH)* - Member of the supervisory board of *Kennisnet*	none	- CEO of *SIDN* - Participant in *Platform Internet Veiligheid* - Participant in *Programmaraad Digivaardig & Digiveilig* - Chair *Digiveilig* - Member of the Council of the Board of *PI Lab* - Council member of *the ICANN ccNSO* - Participant in the *IGF* - Member of the advisory council of *Dutch ISOC Chapter*	- Team leader *CAcert critical system administrators* - Administrator, *Stichting Wereldwinkel Doorn*	- Owner TUNIX Digital Security. Member of the board of *Stichting IT Projecten (StitPro)*.	See page 24

7.2 Staff

NLnet Labs employed eight people in 2013: Jaap Akkerhuis, Olaf Kolkman (director), Wouter Wijngaards, Benno Overeinder, Matthijs Mekking, Willem Toorop, Yuri Schaeffer, and Ralph Dolmans (as of September 1, 2013). The director of Stichting NLnet Labs is responsible for the daily management of all activities of the laboratory, including development of strategies and plans for new activities.

Finances are administered by Patricia Otter of the Stichting NLnet.

7.3 Offices

NLnet Labs resided at the Amsterdam Science Park ever since its incubation in 1999. Its offices are located in the Matrix II building.

7.4 Finances

NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in May 2014, these are the unaudited numbers[20].

Stichting NLnet Labs primarily finances its projects and activities from grants obtained from two organizations:

1. Stichting NLnet: The long term financial commitment of NLnet towards NLnet labs has been codified in a subsidy contract since 2007. In 2010 NLnet Labs was given notice that because of uncertainty of available funding, that contract is terminated as of Jan 1, 2016.
2. SIDN, the Internet domain registry for the Netherlands: A subsidy contract between SIDN and NLnet Labs provides for structural financing for the period Jan 1, 2012 – December 31, 2016.

A second means of income are subsidies and donations by other parties. NLnet Labs has developed a sponsor agreement. For 2013, we would like to acknowledge AFNIC, Comcast, Verisign, and DK Hostmaster A/S for their generous support.

In addition, income may be obtained by providing consultancy or subsidized research on Internet architecture, governance, and technology issues and by providing Open Source programming services to third parties. Our activities in these areas are reported above.

Finally Unbound and NSD support contracts are sources of additional income in 2013.

20-Audited finances can be found in “Kengetallen jaarrekening 2013“ as published on http://www.nlnetlabs.nl/labs/about/

7.5 Fiscal Status

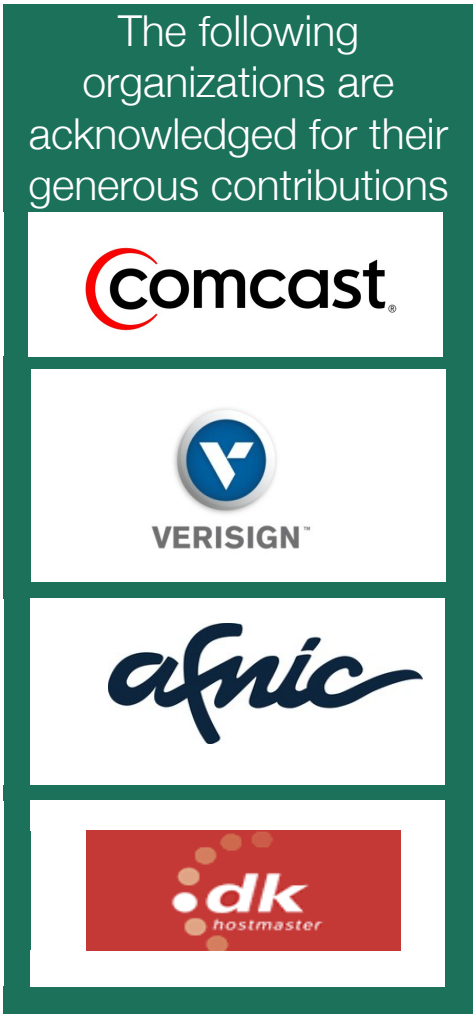
On 20 September 2007, NLnet Labs has been recognized as an institution with general benefit objectives, "Algemeen Nut Beogende Instelling (ANBI)". This status has become relevant under new regulations that are effective as of January 1, 2008.

7.5.1 Income in 2013

At the end of 2012, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2013, with a total of 692 k€. Based on this budget and the expected consultancy income, 286.6 k€ grants were requested from SIDN and Stichting NLnet. Both sponsors allocated these funds for 2013, to be received by NLnet Labs on a quarterly basis.

In addition to these regular subsidies Stichting NLnet awarded a subsidy of 132 k€ in order to perform business development within the context of the Open Netlabs BV. These funds were immediately allocated towards a special fund for business development, henceforth they appear on the balance sheet.

Regular sources of non-subsidy income are the NSD and Unbound support contracts and a consultancy contract with ICANN (mostly ISO3166 related work) and a compensation for the bandwidth used by the secondary server for .PT.



In addition we participated in funded research projects (Multipath TCP and the Interisle Study see sections 3.1.5 and 2.5.3 respectively) and received significant donations from Comcast, Verisign, Afnic and DK Hostmasters amounting to a total of 270 k€ income above budget.

Interest derived from a savings account used to deposit funds temporarily amounted to 3 k€

Finally NLnet Labs initially payed for the staff and other costs incurred for the Open Netlabs BV these costs (113 k€) were immediately recovered from Open Netlabs BV and are not shown in the tables.

7.5.2 Expenditure in 2013

The major expenditure categories of NLnet Labs in 2013 are staff, travel and housing. In september we expanded our 7 person staff (6.7 FTE) to 8 persons (7.7 FTE) the total expenditure on staffing of 564 k€. Housing and travel make up for another 89 k€ out of the total of 692 k€ expenditure.

In 2013 we made the following earmarked reservations: 132 k€ for Open Netlabs business development. 135 k€ for the ENGRIT project (see section 4.1) and 145 k€ for the SAND project (see section 4.2).

In 2013 Stichting NLnet Labs invested 1 k€ in stock of its wholly owned subsidiary Open Netlabs BV this investement is vallued for a net worth 1€ so that a negative result of 999€ has been accounted for.

After making these reservations and valuationsNLnet Labs had a negative result of € 338. The general financial reserve at the start of 2013 is 69k€.

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	1	**General Reserve**	69
Open Netlabs BV Stock	0		
Receivables	162	**Open Netlabs BV Bussiness Development Fund**	132
Bank & Cash	440	**Reservation Engrit**	135
		Reservation SAND	145
		Accounts Payable	4
		Tax and Social Premium Payable	48
		Other liabilities	70
Total	603		603

Income

	2012 actual (k€)	2013 actual (k€)	2013 budget (k€)	2014 budget (k€)
NLnet Subsidy	122	286	286	337
SIDN Subsidy	300	286	286	337
Other Donations	82	209	27	9
Consultancy and other Income	58	107	17	17
NSD & Unbound Support	74	80	74	79
Interest Income	4	3	2	2
Sub Total	630	972	692	780
Business Development Subsidy from NLnet	0	132	0	132
Total	640	1,104	692	912

Expenditure

	2012 actual (k€)	2013 actual (k€)	2013 budget (k€)	2014 Budget (k€)
Staff	517	564	547	615
Housing	38	44	40	55
Travel	55	45	52	64
Depreciation	2	2	4	5
Engrit Project Costs	0	3	0	0
Other costs	26	33	49	46
Sub Total	638	691	692	780
Result Open Netlabs	0	1	0	0
Project Reservation NLnet Business Development	0	132	0	132
Project Reservation ENGRIT	0	135	0	0
Project Reservation SMARD	0	145	0	0
Total	638	1,104	692	912

7.5.3 Budget for 2014

The 2013 budget has been drawn up on 9 October 2013. Based on having 7.6 FTE we have budgeted a total expenditure of 780k€

On January 20, 2012 Stichting SIDN signed a five year contractual commitment to subsidize 50% of the expenditure needed to execute our chartered activities. SIDN and NLnet will jointly cover 674k€ in four quarterly grants of 168k€.

Additionally, NLnet Labs expects to receive about 17k€ from consulting activities, 9k€ though donations, and 79k€ from support contracts.

7.5.4 Financial Outlook

In December 2010, Stichting NLnet has formally announced that it will terminate its subsidy contract by January 1, 2016, due to an expected lack of funds by that time. Director and board have started an effort to identify new sponsors and other sources of income with the goal of establishing a solid base for continued existence of NLnet Labs beyond the expiration of this subsidy contract.

In January 2013 Han Brouwers joined NLnet Labs as business developer. Stichting NLnet intends to subsidize this initiative, as of 2013, for 3 years. Accordingly, in 2014, just as in 2013, 132 k€ will immediately allocated towards a special fund for business development.

8 Publications, Presentations and reports

Publications

- RFC6912: "***Principles for Unicode Code Point Inclusion in Labels in the DNS***", Sullivan, Thaler, Klensin & Kolkman, April 2013, http://www.rfc-editor.org/rfc/rfc6912.txt
- "***Experiences with MPTCP in an intercontinental OpenFlow network***", van der Pol, Bredel, Barczyk, Overeinder, van Adrichem, and Kuipers, Terena Networking Conference 2013, June 2013, https://tnc2013.terena.org/getfile/872
- "***Measuring Spoofed Traffic***", Overeinder, ISOC Briefing Paper, July 2013, http://www.internetsociety.org/doc/benno-overeinder-measuring-spoofed-traffic
- "***Name Collision in the DNS***", Interisle Consulting group, study conducted by Chapin, Kolkman, Reid, Strutt, and Wade, August 2013, http://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf
- "***Study Group on Use of Names for Countries and Territories Final Report***", Akkerhuis (as member of the ccNSO Study Group on the use of Country and Territory Names), September 2013, http://ccnso.icann.org/workinggroups/unct-final-08sep12-en.pdf
- RFC6950: "***Architectural Considerations on Application Features in the DNS***", Peterson, Kolkman, Tschofenig & Aboba, October 2013, http://www.rfc-editor.org/rfc/rfc6950.txt
- SAC063 "***SSAC Advisory on DNSSEC Key Rollover in the Root Zone***", Akkerhuis as contributing SSAC member, November 2013, http://www.icann.org/en/groups/ssac/documents/sac-063-en.pdf
- "***DNSSEC Infrastructure Audit Framework***", Mekking and Kolkman, NLnet Labs Document 2013-02 version 1.0, December 2013, http://www.nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf

Presentations

- "***Innovation at the Waist***", Kolkman, Apricot 2013, february 2013, http://www.apricot.net/apricot2013/assets/innovation-at-waist_1361775779.pdf
- "***DNSSEC, DANE, and Diginotar***", Kolkman, Apricot 2013, february 2013, http://www.apricot.net/apricot2013/assets/dnssec-diginotar-dane_1361864377.pdf
- "***DNS Rate Limiting***", Mekking, FFG2013, February 2013, http://www.guug.de/veranstaltungen/ffg2013/abstracts.html#3_4_2
- "***Effects of RPKI Deployment on BGP Security***", Overeinder, Cisco SP Security Forum, Ferbuary 2013.
- "***Web Extensible Internet Registration Data Service (WEIRDS) Working Group Update***", Kolkman, ICANN46 (various constituency meetings), April 2013 http://beijing46.icann.org/meetings/beijing2013/presentation-weirds-update-07apr13-en.pdf
- "***Multipath Networking -- Multipath TCP and Multipath BGP***", Overeinder, guest lecture at System and Network Engineering (SNE), UvA, 10 April 2013, https://www.os3.nl/2012-2013/courses/an/start
- "***Response Rate Limiting***", Akkerhuis, ICANN46, April 2013, http://beijing46.icann.org/meetings/beijing2013/presentation-amplifications-akkerhuis-08apr13-en.pdf
- "***DNSSEC Key Rollover in the Root Zone***", Akkerhuis, ICANN46, April 2013 http://beijing46.icann.org/meetings/beijing2013/presentation-dnssec-root-zone-key-rollover-10apr13-en.pdf
- "***IETF Open Standards for an Open Internet***", Kolkman, ISOC.DE "Wer Macht das Internet", April 2013, https://www.isoc.de/wer-macht-das-internet/documents/Olaf.pdf
- "***DNSSEC: Diginotar and DANE***", Kolkman, SEE-2, April 2013, https://meetings.ripe.net/see2/presentation-upload/show.php?id=13
- ***DNSSEC Tutorial***, Kolkman, SEE-2 April 2013.
- "***Multipath Networking: MPTCP and OpenFlow -- Friend or Foe?***", Overeinder & v.d. Pol, SURFnet RoN, June 2013, http://www.nlnetlabs.nl/~benno/opendir/RoN%202013-06-28.pdf

- **“Innovation at the Waist”**, Kolkman, RIPE 66, may 2013, https://ripe66.ripe.net/presentations/111-RIPE66-Innovation_at_the_Waist.pdf
- “***WCIT takaways***”, Kolkman, RIPE 66, may 2013, https://ripe66.ripe.net/presentations/325-WCIT_2012-RIPE66.pdf
- "***The sky is falling: The sun is exploding Duck***”, Akkerhuis, RIPE66 may 2013, https://ripe66.ripe.net/presentations/331-Duck.pdf
- “***RRL is the best, For now***”, Mekking, CENTR R&D workshop, June 2013, http://www.centr.org/system/files/agenda/attachment/rd5-mekking-rrl_is_the_best._for_now-20130604.pdf
- “***Using Path MTU Discovery (PMTUD) for a higher DNS responsiveness***”, Toorop, CENTR R&D workshop, June 2013, https://www.centr.org/system/files/agenda/attachment/rd5-toorop_using_path_mtu_discovery-20130604.pdf
- “***AIT .TH DNSSEC workshop***”, Kolkman & Linden, June 2013, https://nsrc.org/workshops/2013/nsrc-ait-th-dnssec/
- “***RPKI Route Origin Validation Deployment Strategies***”, Servin, Martinez, Kloots, and Overeinder, Workshop on RPKI (http://rpkiws.realmv6.org), July 2013, http://www.nlnetlabs.nl/~benno/opendir/RPKI%20and%20ROV%20deployment%20strategies.pdf
- “***Some Available RPKI tools***”, Overeinder, Martinez, IETF87 SIDR WG, July 2013, http://www.ietf.org/proceedings/87/slides/slides-87-sidr-13.pdf
- “***Defending against amplification attacks***”, Akkerhuis, during the 6th International conference for ccTLD registries and registrars of CIS, Central and Eastern Europe, September 2013, http://meeting.cctld.ru/files/Akkerhuis.pdf
- “***RRL is the best, For now***”, Mekking, DENIC Technical Meeting, September 2013,
- “***De Internet Engineering TaskForce***”, Kolkman, during NLIGF Seminar “Geen cyber veiligheid zonder opgelegde regulering van de overheid” 1 october 2013.
- “***NSD4 Almost released***" Toorop, during RIPE 67 Open Source WG, October 2013, https://ripe67.ripe.net/presentations/232-nsd4.pdf
- **"*Using Path MTU Discovery (PMTUD) for better IPv6 DNS responsiveness*"**, Toorop during RIPE 67 DNS WG, October 2013, https://ripe67.ripe.net/presentations/230-pmtud4dns.pdf
- **"*Which habitat fits your name server’s nature best?*"**, Toorop during RIPE 67 DNS WG, October 2013, https://ripe67.ripe.net/presentations/250-habitat.pdf
- “***The Internet as the world's trading Platform: how and why is it so successful?***”, Reiter, Hickson, Aston-Hart, and Selli, panel discussion during the WTO Forum, 3 October 2013.
- “***Mapping Dutch Critical Infrastructure***”, Oprea and Overeinder, ENISA Workshop on Resilience of Network Interconnections, October 2013. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2013/resilience-of-network-interconnections
- “***The Multiple Stakes in DNS Security – Musings on DNS and Security***”, Akkerhuis, during Domain.Forum in Sofia, November 2013.
- "***Resolver Data Prefetch***", Wijngraards, during IEPG at IETF88, 2 November 2013, http://iepg.org/2013-11-ietf88/prefetch.pdf
- “***Weirds a Status Update***”, Olaf Kolkman, during ICANN48 (presented twice), November 2013, e.g. at http://buenosaires48.icann.org/en/schedule/sun-gnso-working/presentation-weirds-17nov13-en
- "***DNS Resolver Prefetch Data***”, Wijngaards, during DNSOP at IETF88, 5 November 2013, http://www.ietf.org/proceedings/88/slides/slides-88-dnsop-10.pdf
- “***Ensuring the continued evoloution and growth of the Internet for everyone***”, Esterhuysen, Kolkman, & Moisander, panel discussion during the internetdagarna, 26 November 2013.
- “***Congestion Control Algorithms: Open Questions”***, Overeinder during SURFnet Research on Networks Meeting, Utrecht, Netherlands, December 2013. http://www.nlnetlabs.nl/~benno/opendir/RoN%20Congestion%20Avoidance%202013-12-11.pdf

Work in Progress

- "***Authenticated Denial of Existence in the DNS***", Gieben & Mekking, November 2013, http://tools.ietf.org/html/draft-gieben-auth-denial-of-existence-dns
- "***A Procedure for Cautious Delegation of a DNS Name***", Kolkman, Sullivan, & Kumari, August 2013, http://tools.ietf.org/html/draft-kolkman-cautious-delegation
- "***Using Test Delegations from the Root Prior to Full Allocation and Delegation***", Huston, Kolkman, Sullivan, Kumari, Michaelson, October 19, 2013, http://tools.ietf.org/html/draft-kolkman-root-test-delegation
- "***Characterization of Proposed Standards***", Kolkman, Bradner & Turner, November 2013, http://tools.ietf.org/html/draftkolkman-proposed-standards-clarified
- "***Technical Considerations for Internet Service Blocking and Filtering***", Barnes, Cooper & Kolkman, December 2013, http://tools.ietf.org/html/draft-iab-filtering-considerations
- "***A Framework for the Evolution of IANA***", Kolkman, November 2013, http://tools.ietf.org/html/draft-kolkman-iana-framework-00
- "***Confidential DNS***", Wijngaards, November 28, http://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-00

Student Reports

In 2013 we had 13 interns. The following reports were published in 2013

- "***Defending against DNS reflection amplification attacks***", Rozekrans & de Koning, July 2013, http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdfhttps://www.os3.nl/_media/2012-2013/courses/rp2/p92_report.pdf
- "***Making do with what we've got: Using PMTUD for a higher DNS responsiveness***", Bagheri & Boteanu, February 2013, http://www.nlnetlabs.nl/downloads/publications/report-pmtud-bagheri-boteanu.pdf
- "***Identifying Patterns in DNS Traffic Using Visual Analytics to Discover DNS Abuse***", Lexis, July 2013, http://www.nlnetlabs.nl/downloads/publications/report-rp2-lexis.pdf
- "***Discovery and Mapping of the Dutch National Critical IP Infrastructure***", Alizadeh & Oprea, August 2013, http://www.nlnetlabs.nl/downloads/publications/RP2_report_Mapping_the_Dutch_Critical_Infrastructure.pdf

Student work in progress:

- Hosnieh Rafiee and Marc Buijsman both worked on CGA-TSIG. Buijsman will publish a report on "***Securing the last mile of DNS with CGA-TSIG***"
- Warwick Louw worked on "***Structural Measurement and Tracking of Path MTU and Fragmentation Porblems***"
- Jeffrey de Loof performed "***A Study into the Complexity of BGP Dynamics***"
- Stella Vouteva worked on "***BGP Route Leakage, Methods and Tools***"
- Tim Blankers worked on "***Analysis of Growth and Stability of the Internet Routing Infrastructure***"

Blog Posts

- Open Recursor Blocked, Wijngaards, April 2013, https://www.nlnetlabs.nl/blog/2013/04/
- Using PMTUD for a higher DNS responsiveness, Toorop, June 2013, https://www.nlnetlabs.nl/blog/2013/06/04/pmtud4dns/
- NSD4 Performance Measurements, Wijngaards, July 2013, https://www.nlnetlabs.nl/blog/2013/07/05/nsd4-performance-measurements/
- NSD4 High Memory Usage, Wijngaards, July 2013, https://www.nlnetlabs.nl/blog/2013/07/05/nsd-4-mem-use/
- NSD4 TCP Performance, Wijngaards, July 2013, https://www.nlnetlabs.nl/blog/2013/07/08/nsd4-tcp-performance/
- How 'National' is the Dutch Critical IP Infrastructure, Overeinder, September 2013, http://www.nlnetlabs.nl/blog/2013/09/24/dutch-national-critical-ip-infrastructure/
- RRL Slip and Response Spoofing, Wijngaards, September 2013, http://www.nlnetlabs.nl/blog/2013/09/16/rrl-slip-and-response-spoofing/

NLnet Labs staff responsibilities

- **Akkerhuis**:
  - ICANN representative in the ISO 3166 Maintenance Agency
  - Member of the ICANN Security and Stability Advisory Council (SSAC)
  - Co-chair of the RIPE DNS working group.
  - RIPE Arbiter
  - Member of the ccNSO study group on Use of Names for Countries
- **Kolkman**:
  - Chair of the IETF WEIRDS working group
  - Chair of the IAB IANA evolution program.
  - IAB/IETF representative in the EU Multi-Stakeholder Platform on ICT Standardization
  - RIPE Arbiter
  - Member of the Panel on Global Internet Cooperation and Governance Mechanisms
  - Member of the program committee for the Workshop and Prize on Root Causes and Mitigation of Name Collisions 2014 (WPNC14)
- **Overeinder**:
  - Member of the RIPE Program Committee

Stichting NLnet Labs

Science Park 400, 1098 XH Amsterdam

e-mail: labs@nlnetlabs.nl, *web*: http://www.nlnetlabs.nl/