NLnet Labs

Annual Report 2015

For an Open Internet

1 Highlights

NLnet Labs promotes and contributes to a stable and reliable Internet infrastructure, where DNS and inter-domain routing are key components of the infrastructure. The authoritative name server NSD 4 was initially released late 2013, and after two years has shown to be a mature and stable upgrade for the proven NSD 3. Unbound 1.5 and newer releases have been made available with improvements to mitigate DDoS, options for undemanding algorithm rollover and features for enhanced privacy of end-users.

After the transfer of the OpenDNSSEC project to NLnet Labs, we continued with developments of the OpenDSSEC 1.4.x release branch. Simultaneously, we worked towards OpenDNSSEC 2.0 alpha and beta releases, and tested its functionality and stability with industry partners. In 2015, Open Netlabs BV took responsibility on the commercial aspects of the OpenDNSSEC project.

The routing (configuration) toolset project ENGRIT started in 2015, and the first prototype implementations and the interest of presentations of this work at workshops are promising. The SAND (self-managing anycast infrastructures for DNS) project is one year in full swing. Together with SIDN Labs and Universiteit Twente, we explore scalable and robust methods for managing and monitoring dynamic anycast networks, with the aim to increase stability and security of the service.

Education and research are important activities for NLnet Labs' signature. We contributed to colloquia and practicums (lab sessions), and hosted four interns during 2015.

All our efforts and deliverables are directed to strengthen the open and innovative nature of the Internet for all, and add to the security and stability of the core of the Internet infrastructure.

2 Areas: DNS and DNSSEC

The topics DNS and DNSSEC are strongly embedded in NLnet Labs' activities. Besides the well-known and widely adopted DNS name servers and DNS libraries developed by NLnet Labs, the OpenDNSSEC project and getdns API project are important initiatives for the Internet community. All our activities focus on the development and maintenance of tools that facilitate the provisioning and use of DNSSEC, and as such 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.

DNSSEC is one of the few enabling technologies that allows for the introduction of end-to-end authentication and confidentiality solutions. In this capacity, we see it to be a critical building block in designing trust in, and trust relations between components and services on the Internet. Development, deployment, and innovating on top of DNSSEC deployments take a long, multi-year, potentially multi-decade, breath.

Besides development of software, we continue to invest effort in research projects to answer operational, technical, and theoretical questions about DNS security, architecture, operations, and deployment.

2.1 Provisioning of DNS Server-Side

2.1.1 NSD

NSD is NLnet Labs' authoritative name server and designed to be light-weight, high-performance, secure, and single purpose. NSD 4 is one of our flagships and was released in October 2013. In the past two years, NSD 4 is mature and stable and has shown to be a feasible upgrade for NSD 3. In May 2015, we announced the end of support of NSD 3 by May 2016 to the community.

Goals

NSD 4: provide a stable and high-performance authoritative DNS server for a larger, more diverse set of users. Continued implementation and support of new IETF standards, improved performance and reduction of memory usage (memory footprint).

NSD 3: continue to support NSD 3 as a secure high-performance name server (end of support in May 2016).

NSD 4 Activities

NSD 4 is the primary development release of the NSD name server. For NSD 4, per zone statistics are introduced. A lot of crashes in the zone parser have been fixed after so-called fuzzing reports and integer overflow checks reports from community members.[1]

Additional TSIG hashes are available, and nsd-control features to add and remove long lists of zones more easily. The SO_REUSEPORT socket option is supported, for performance increases, mainly on Linux in multicore environments. The option is support for UDP only fornow, as the kernel support of this option for TCP seems to be troublesome.

1-John Van de Meulebrouck Brendgard and Loganaden Velvindron

NSD 3 Activities

We informed users about the approaching end of support of NSD 3 in May 2016. Support for NSD 3 was still available in 2015, but the bug reports we received were all related to NSD 4. So it seems that most users migrated to NSD 4 already. The NSD 3 releases followed the NSD 4 fixes, because the code is in large part shared between NSD 3 and 4, and thus bug fixes could be ported from one to the other.

Results

NSD 4 has seen a series of maintenance releases (v4.1.1 – v4.1.7) with bug fixes, performance improvements and new features in 2015. Per zone statistics was introduced in NSD 4.1.1 with flexible configuration options to specify how statistics are aggregated and presented. To improve the performance, so_reuseport support is implemented, but due to stability problems with some older Linux kernels, the option is not enabled by default. When enabled, it gives (sizable) speed improvements on multicore systems. Zone parsing by NSD 4 is improved and stable for various kinds of input (e.g., by fuzzing).

New features in NSD 3.2.19 and NSD 3.2.20 releases are support for types CDS and CDNSKEY, and the synthesizes of CNAMES with the same TTL as the DNAME.

Impact

NSD clearly serves its design goals: to provide an alternative implementation to 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.

Besides providing a reliable and high-performance name server, NSD 4 is also a reference implementation of relevant IETF RFC standards. By realizing reference implementations, we also contribute to the standardization process by communicating our experiences and sending feedback to the community.

2.1.2 DNSSEC Zone and Key management: OpenDNSSEC

OpenDNSSEC is a turnkey solution for DNSSEC management that hides the complexity of DNSSEC and enables an effortless deployment in operational environments. The DNSSEC zone management system takes unsigned zones, adds signatures and other records for DNSSEC and passes it on to the authoritative name server. Furthermore, the DNSSEC key-maintenance expert system 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.

In 2015, NLnet Labs both continued the support and maintenance of the OpenDNSSEC 1.4 branch and the development of the OpenDNSSEC 2.0 branch. All new features and structural performance improvements are implemented in the OpenDNSSEC 2.0 branch, for which a beta release was available at the end of 2015.

Goals

Continue the support and maintenance of OpenDNSSEC version 1.3 and 1.4 branches. Management of the release of OpenDNSSEC 2.0 by defining important (must have) features and optional features.

Activities

From 2015, all OpenDNSSEC activities, such as management, design, implementation and support, are taken care of by NLnet Labs.

OpenDNSSEC 1.3 is the Long Term Support (LTS) version of OpenDNSSEC. No new release for OpenDNSSEC 1.3 has been published in 2015.

OpenDNSSEC 1.4 has seen one release (v1.4.8.2) with new support for RFC5011-style KSK rollovers and some bug fixes. We advice to use OpenDNSSEC 1.4 in production for operational stability and supported features.

In 2015, we appointed new colleagues at NLnet Lab to join the OpenDNSSEC team. With the new team, we carefully looked at the design goals of OpenDNSSEC 2.0 and reviewed the road map mentioning functional and non-functional features. The minimal feature set for version 2.0 was determined on the inclusion of the new OpenDNSSEC enforcer module, and performance and scalability improvements. The other features that were part of the original 2.0 release plan (before 2015) are planned in subsequent minor and maintenance releases 2.1.x, 2.2.x, etc.

One new feature that was developed for operational security was the development of disconnected KSK deployment of OpenDNSSEC, allowing the signing of the key set in DNSSEC to be done in a secured environment that is not available to the operational environment in which a signer normally runs.

For the development and unit tests of OpenDNSSEC, all existing tests had to be adapted and improved for OpenDNSSEC 2.0. This implied a major overhaul of the test environment, but this is essential to bring out the public alpha/beta release. Having all tests running in OpenDNSSEC means that all known bugs have been tackled and testing can continue above the level of the previous 1.4 releases.

Results

OpenDNSSEC 1.4.8.2 maintenance release with RFC5011-style KSK rollover support. OpenDNSSEC 2.0 alpha/beta release for review by selected partners (early adopters). Enhanced test environment for unit testing of OpenDNSSEC 1.4 and 2.0.

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 https://www.opendnssec.org/about/known-users/.

2.2 Client-Side Availability of DNSSEC

2.2.1 Unbound

Unbound is one of the main implementations for DNSSEC-enabled DNS resolution and thereby an important contributor to the deployment and uptake of DNSSEC.

Goals

Create a versatile, high-performance DNS resolver that can be incorporated at various places in software stacks, embedded, as default resolver in OS distributions, and primary resolver for (large) ISPs. Maintain stability, implement new IETF Internet standards, and include relevant operational requirements.

Activities

For Unbound in 2015, the rate-limiting feature debuts (version 1.5.4), this can rate limit for resolution, stopping a large number of queries from going upstream, and also keeping them away from the resolver. Type ANY is also answered more succinctly.

Algorithm rollover is made easier by the new default for harden-algo-downgrade that is more lenient. This should allow algorithm rollovers as lenient as other software (e.g., BIND) supports. We were requested to stop Unbound from checking for algorithm rollover mistakes.

TLS support was already part of Unbound. For TLS-encapsulated DNS the temporary port assignment from IANA is used. Due to the DPRIVE IETF WG action the TLS service now has an official port number to run on, and the new default has been inserted.

In Unbound 1.5.7 Qname minimisation is introduced. This is an important privacy enhancement. Unfortunately, the deployment is hampered by non-conformance on the Internet of servers that do not support no-leaf nodes below NXDOMAIN or servers that do not respond to queries for the NS QTYPE. Unbound has a fall-back mechanism to stop QNAME minimisation when detecting a potentially broken server. And although the feature switch has been introduced, it has not been enabled by default because of that.

We continue the development of Unbound to have the recursive resolver fit in various setups and operational environments. We continue to be lenient towards feature requests, in part to foster the adoption of DNSSEC (-validators).

Results

Publication of versions 1.5.2–1.5.7 with some important new features such as rate limiting, lenient algorithm rollover and Qname minimisation.

Impact

Unbound is acknowledged as a leading implementation of a secure and stable DNSSEC validator. The software is used in various high-profile and high-available environments, amongst them various large ISPs, as a standard resolver in some OS distributions (e.g., FreeBSD and OpenBSD), and in several DNS appliances.

2.2.2 DNSSEC Trigger

DNSSEC Trigger is an effort to cope with the ‘DNSSEC last mile’ problem. In order to be able to rely on DNSSEC validation one wants to bring DNSSEC close to the application, preferably on the OS so that the benefits of DNSSEC are available for all.

Goal

Handle a number of corner cases that the software needs to deal with such as proper operation when the users bring up VPNs. Improve interaction with guest operating systems like Mac OS X, BSD, Linux, and Windows, and integration with NetworkManager and systemd.

Activity and Results

We continue to support DNSSEC Trigger, but no new releases have been published in 2015. Existing source and binary distributions did work with new releases of the guest operating systems (as mentioned above). Users do give positive feedback about the usability and relevance of the utility.

Impact

Further understanding about the impediments to get DNSSEC to the end users: a bridging tool that sets an example for other initiatives to follow.

2.3 DNS Development Frameworks

The development of applications and services that execute their own DNS resolving and are DNSSEC-enabled is an important step forward in the security awareness of applications and services. With DANE and TLSA (RFC 6698), not only security improves but takes also privacy to the next level by enabling encryption everywhere (see also Pervasive Monitoring Is an Attack, RFC 7258).

2.3.1 Secure getaddrinfo/getnameinfo (getdns API)

getdns is an asynchronous DNS API, which API specification is developed in collaboration with application developers. getdns API offers application developers a modernized and flexible way to access DNS security (DNSSEC) and alternative transport, like TCP pipelining, DNS over TLS, or STARTTLS for DNS (enhancing DNS privacy). A particular hope is to inspire application developers towards innovative security solutions in their applications.

Goal

Continued development of a modern asynchronous DNS API towards and realize a feature complete implementation of the getdns API library. Besides the development of the software, we generate some interest and traction of a new alternative for getaddrinfo/getnameinfo that includes DNSSEC functionality for application developers and provide a modern (asynchronous) DNSSEC-enabled system stub resolver.

Activities

In a collaboration between NLnet Labs and Verisign Labs, we worked towards a feature complete getdns API library (implementing almost 100% of the getdns API specification). In 2015, getdns had 11 releases from version 0.1.6 in January up to version 0.9.0 end of December. Our terms for a 1.0.0 release is a 100% specification complete implementation.

getdns API library has ldns version 2 functionality under the hood, and no dependency on libldns anymore. Some of the ldns version 2 functionality is exposed, such as conversions between wire, presentation and getdns format.

Native stub DNSSEC validation is implemented. This enables a very useful extension to the library, that is DNSSEC roadblock avoidance that probes available upstreams for DNSSEC support and only falls back to full recursive when all upstreams fail (on a per query basis), see Internet-Draft draft-ietf-dnsop-dnssec-roadblock-avoidance.

The implementation of native stub DNSSEC validation also triggered experimentation and the development of features to provision getdns as a system stub replacement (libnss_getdns).

The getdns API library supports DNS over TLS. The implementation goes intimately alongside the development of draft-ietf-dprive-dns-over-tls (DNS over TLS) and draft-ietf-dnsop-5966bis (DNS over TCP). Both drafts are targeted towards an IETF standard RFC.

Beside the development of the getdns API, a number of public presentations and events were organized to promote the adoption of the API.

Results

An almost 100% spec complete (feature complete) implementation released as getdns API 0.9.0. A new responsive website for the getdns API spec, implementations and language bindings. The Next Web 2015 Amsterdam and The Next Web 2015 New York, the IETF 92, 93 and 94 hackathons; presentations at DNS OARC Spring Workshop 2015, vBSDcon, RIPE 70, and RIPE 71.

Impact

The presentations of getdns API at various events showed that there exists serious interest by the industry. In particular, where DNSSEC and DANE are relevant, getdns API is considered to be a serious option.

2.3.2 Ldns

Goal

Work towards a major version release of ldns version 2. Important goals are consistent support for getdns API and memory reduction (mainly for OpenDNSSEC).

Activity

The activities for ldns v2 are closely related with getdns API developments. The results of these developments that are related to the ldns library will be moved to the ldns v2 development repository.

The memory management of ldns is optimized and the time complexity of some operations in ldns are reduced. Additionally we resolved a number of bugs and added newly standardized features.

Results

In 2015 no ldns release has been published. The development on ldns v2 is in the getdns API code base.

2.3.3 Net::DNS

Net::DNS is a DNS resolver implemented in Perl. It allows the programmer to perform nearly any type of DNS query from a Perl script. NLnet Labs will continue the maintenance and development of the Net::DNS suite.

Goal

Regular maintenance and continued clean-up of the architecture.

Activities

Net::DNS had six releases (mostly bugfixes) in 2015, including the 1.01 release in July. With the 1.01 release, the RRs that were previously in Net::DNS::SEC are now integrated in Net::DNS. The Net::DNS::SEC is now only shipped separately to do the cryptographic operations.

With the merge the licences for Net::DNS and Net::DNS::SEC have been aligned. All modules now have the BSD 3 clause license. For this effort we contacted all the original authors.

Results

Releases 0.82 through 1.04 of Net::DNS and releases 0.22 through 1.02 of Net::DNS::SEC.

2.4 Other Activities

2.4.1 Student Projects

Discovery Method for a DNSSEC Validating Stub Resolver

Xavier Torrent Gorjón (UvA SNE MSc. student) developed a discovery method to ensure DNSSEC information can be delivered to the end host. For this purpose, we used RIPE ATLAS to study the current state of DNSSEC aware and DNSSEC validating resolvers, and defined a course of action

from that information. Our proposed discovery method relies on using the default recursive resolvers and, in case of failure, proceed to use, in this order, the ISP recursive resolver, a public DNS resolver, or perform full resolving recursion from the host.

This study is presented at the DNS working group meeting at RIPE71 in Boekarest. Reference to the MSc. thesis reference can be found in Section 7.

Analysis of DNS Resolver Performance Measurements

Hamza Boulakhrif (UvA SNE MSc. student) devised a methodology to measure the performance of the Unbound, BIND, and PowerDNS resolvers. Measurements of these resolvers are required to be objective and not biased. Analysis is conducted on these performance measurements, where the implementations are compared to each other. Interesting insights are not just the response time performance, but the distribution of response times for the three resolvers. In particular Unbound is very persistent to find an answer no matter how long it takes, while the other resolver prefer failed responses over late responses. It appears that DNS resolvers do not only differ in performance but also in the response they give to certain queries. We found for some corner cases that certain resolvers behave either more lenient or strict when it comes to accepting and sending DNS data.

DNSSEC for Legacy Applications

Theogene H. Bucuti (University of North Texas MSc. student), supervision with Allison Mankin and Gowri Visweswaran, Verisign Labs.

The project looked for mechanisms to make applications to take advantage of a modern DNS stub resolver and library, without any changes to installed application binaries. By providing such mechanism, existing (legacy) applications can be given access to new DNS features that do not involve changes to the application interface, e.g., TCP pipelining, TCP fast open, DNS over TLS, and DNSSEC iteration as a stub (with roadblock avoidance).

Unix systems (Linux, FreeBSD, …) provide a default DNS resolver library with the getaddrinfo() and getnameinfo() application interface calls. The enhanced system-wide lookup based on the getdns API library makes use of the Unix resolution framework (nsswitch). An open source module libnss_getdns for nsswitch is developed that can replace dns with getdns.

The project is presented at the ICANN 54 DNSSEC Workshop (by Sara Dickinson, Sinodun) and at the RIPE 71 DNS-WG meeting (see also Section 7).

2.4.2 Hackathons

- getdns hackathons at The Next Web Amsterdam and New York.
- IETF 92 and IETF 93 hackathons with getdns development team.

2.4.3 IETF DNS activity

Results

A DANE Record and DNSSEC Authentication Chain Extension for TLS, draft-shore-tls-dnssec-chain-extension, M. Shore, R. Barnes, S. Huque, W. Toorop.

Confidential DNS, W. Wijngaards and G. Wiley, DPRIVE WG, IETF 92, Dallas, TX, March 2015.

Confidential DNS, draft-wijngaards-dnsop-confidentialdns, W. Wijngaards (NLnet Labs), G. Wiley (Verisign, Inc).

2.4.4 ICANN gTLD related activity

See section 4.1.

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. In addition, we put effort in the development of tools and practices that lower the barriers to the 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 Inter-domain Routing Security and Stability

3.1.1 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. A modular approach is the guiding principle in the design of the toolkit, enabling the extendibility and adaptability to simple, average and complex tasks. Performance and robustness are non-functional design goals to realize a dependable toolchain with transactional operations.

Activities

Stavros Konstantaras joined NLnet Labs in 2015 and was assigned to work on the ENGRIT project.

Before design and development of the ENGRIT toolchain, we tested and evaluated some related tools like BGPq3, RPSLtool and IRRToolSet. After this exploration phase, we initiated the development of the RPSL library, a Python-based client that retrieves BGP policies from IRR databases and exports the corresponding information in XML output. Related to the design and development of ENGRIT, an MSc project with two students was carried out at NLnet Labs on the topic of automated configuration of BGP on edge routers. The results of the this work could be integrated in the ENGRIT code-base. For reference to the thesis, see Section 7.

For testing and evaluation of the toolchain, we setup a small testbed to deploy Virtual Routers based on JunOS 12.1 in various topologies. We also did reach out the RIPE routing community, typically large network (ISP) operators and IXPs, to test our ideas and solicit for feedback.

Results

Prototype implementation of ENGRIT toolchain with contributions from MSc. projects hosted by NLnet Labs. As a first exercise, we worked toward a straightforward use-case for ENGRIT to retrieve AS policies from the IRR database and create filter set configurations for routers.

Konstantaras co-authored in the writing of the paper “Topology exchange and Path-finding in NSI environments”, an external project of SNE research group of UvA.

Expected Impact

There is clearly an interest from the industry in a toolset that can 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. In particular, small and medium-sized networks can profit from a good open source toolset, as these networks are typical in between manual configuration (very small networks) and proprietary, in-house developed tools (for large networks with sufficient NOC staffing).

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

Goal

This project 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. To achieve these operational performance and cost goals, we believe an automated management system potentially offers the best possible course of action.

SIDN Labs and NLnet Labs support this project with funding for an academic postdoc at the Universiteit Twente. Other industry partners are RIPE NCC, Netnod and SURFnet, whom support the project with in-kind contributions..

Activities

In the first full year of the SAND project, the main focus was on network and anycast service monitoring. Partly in collaboration with the FLAMINGO EU project, a set of anycast performance metrics were defined and evaluated on usability and relevance as performance indicator. With RIPE Atlas measurements different anycast networks were analysed and the ideal versus real roundtrip times compared.

The monitoring and analysis methodology are part of the MAPE cycle in our targeted self-management SAND system. (MAPE stands for Monitoring, Analysis, Planning and Execution.)

During 2105 we had planned project meetings with the main partners Twente University, NLnet Labs and SIDN Labs

Expected Impact

The 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 anycast nodes, but if usage patterns indicate that certain nodes can be shutdown, this can reduce costs while performance metrics are still within specified bounds.

3.1.3 BGP Route Leaks Analysis

Goal

Study and get insight in the occurrence of BGP route leaks. New routing security enhancements proposed in the IETF SIDR WG do not touch upon the problems of route leaks. For discussion and solutions, a better understanding in the frequency and extent of route leaks is necessary.

Activities

Benjamin Wijchers (MSc student) developed a framework to analyze BGP route leaks in the global Internet routing infrastructure. A route leak is a violation of the policies between the networks involved. Non-disclosure agreements about the nature of the relationships between networks make it hard to distinguish route leaks from regular announcements.

In this project, recent relation inferences from CAIDA have been used to detect possible route leaks in publicly available BGP data. These potential route leaks have been further investigated on their duration, the type of violation, and the type and origin of network that caused the leak-detection. Most detected possible route leaks had negligible durations. The ones with a longer life-time mostly

involved special relationships between networks not currently inferred by relationship datasets. Other possible route leaks detected require more information about the networks involved to properly analyse the situation.

Results

Implementation of a BGP routing analysis framework and an MSc thesis. Presentation at the RIPE 69 Routing WG.

Impact

Create better understanding of the problem, its frequency and extent—this can be important input for discussions on routing infrastructure security. Talents/students being trained in fundamental Internet architecture.

3.2 Inter-domain Routing Complexity

3.2.1 BGP Simulation

Goal

In the past years, we used our BGPSIM environment to study stability, resiliency, and stability properties of the Internet inter-domain routing system. Fundamental to this work is analysis of the complexity of the Internet routing infrastructure. We continue to work on this topic in collaboration with MSc students.

Activities

Bryan Eikema (UvA BSc student) worked on a project with the title "BGP Routing Security and Deployment strategies". In the project the effects of various strategies to deploy origin validation are studied and analysed. We use the BGPSIM simulator to simulate the effects on the security and performance of the network using several deployment strategies and security policies. We find that deploying origin validation to a smaller groups of large Autonomous Systems give the best results for securing the network. We see that some security policies have negative effects on the performance of the network, but have a positive effect on the security of the network. Finally, the study gives insights in the current status of BGP security.

Results

Publication of an BSc thesis, see Section 7.

Impact

Increased understanding of the stability of the routing system and talents/students being trained in fundamental Internet architecture.

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

NLnet Labs and its research engineers and software developers actively participate in areas where technology, governance, and public interest intersect with each other. NLnet Labs' staff volunteers in various community supporting positions.

4.1 ICANN

Akkerhuis is member of the Security and Stability Advisory Committee (SSAC) and the Root Server System Advisory Committee (RSSAC) Caucus[2].

Akkerhuis is appointed by the SSAC as a member of the Cross Community Working Group (CWG)[3]. ICANN proposed the creation of an IANA Stewardship Transition Coordination Group (ICG) "responsible for preparing a transition proposal reflecting the differing needs of the various affected parties of the IANA functions." The CWG was formed as an integral part of this transition process, and to develop a proposal for the elements of the IANA Stewardship Transition that directly affect the naming community. This work started in 2014 and continued in 2015.

Akkerhuis acts as a liaison for ICANN in the ISO Technical Committee 46, 3166/MA meeting. (ISO 3166 is the International Standard for country codes and codes for their subdivisions.)

Akkerhuis co-authored a number of SSAC and RSSAC report, see Section 7.

Akkerhuis en Overeinder attend the ICANN meetings and are actively involved in the ICANN TechDays and DNSSEC workshops.

4.2 RIPE / Network Operations Community

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

Overeinder is chair of the RIPE Program Committee and co-chair of the RIPE BCOP Task Force. Akkerhuis is a co-chair of the DNS-WG and member of the ENOG program committee.

During RIPE70 and RIPE71 NLnet Labs' staff disseminated its knowledge and expertise with a number of high impact appearances. See also Section 7.

4.3 IETF and Technical Community

NLnet Labs participates in the IETF and technical community by contributing to Internet-Drafts, discussions on the IETF mailing lists and with IETF WG meetings, and implement relevant RFCs in our software products. With these activities we initiate new ideas, give feedback on technical feasibility and realize proof-of-concept or reference implementations for Internet-Drafts and industry-grade implementations of RFCs.

Toorop and Overeinder participated in the IETF hackathon (IETF 93 and IETF 94) to develop and test new features for the getdns API project with the other project members and hackathon participants that joined our project.

For active contributions to Internet-Drafts see Section 7.

4.4 Other

Besides facilitating internships and research projects at NLnet Labs for BSc and MSc students, the staff gives colloquia and assists with practicums at the University of Amsterdam. The topics are Internet policy (ICANN and IETF-at-large), inter-domain routing, DNS, and multi-path routing (layer 2: TRILL and SPB, layer 4: Multipath TCP, and layer 7: Multipath BGP).

2-https://www.icann.org/resources/pages/rssac-caucus-2014-05-06-en

3-https://community.icann.org/display/gnsocwgdtstwrdshp/CWG+to+Develop+an+IANA+Stewardship+Transition+Proposal+on+Naming+Related+Functions

5 Area: NLnet Labs Continuity

5.1 Strategic plan

During 2015 we reviewed NLnet Labs mission, vision and strategy and published an updated Strategic Plan[4]. The document emphasizes our mission "*To provide globally recognized innovations and expertise for those technologies that turn a network of networks into an Open Internet for All.*" Further, it describes how our mission relates to our statutes and the principles for setting direction. The strategy plan also discusses the directions in which we plan to develop over the coming years, and our ideas to secure financial continuity.

In 1st half of 2017, we will update and extend our Strategic Plan for the next period of two to three years.

5.2 Open Netlabs BV

NLnet Labs is diversifying 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.

In the past years, Open Netlabs BV operated as the commercial vehicle supporting the open source activities by securing sustainable income on the longer term. The positioning and promotion of the activities are successfully made known and discussed during events like ICANN, IETF, RIPE and DNS OARC meetings. In 2015, support for the main software products of NLnet Labs, NSD, Unbound and OpenDNSSEC, were offered in different levels of SLAs. Adjusting and expanding strategy and portfolio will be a running process.

Stichting NLnet Labs owns 100% of the Open Netlabs BV stock.

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

6 NLnet Labs Organization and Finance

6.1 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.

Five board meetings took place in the year 2015. Benno Overeinder 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 (€414 for 2015). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2015

name	function	end of term
Frances Brazier	secretary	December 28, 2017
Cristian Hesselman	chair	June 30, 2018
Ted Lindgreen	Member	January 31, 2018
Roelof Meijer	member	May 31, 2015
Wytze van der Raay	treasurer	December 28, 2016
Jochem de Ruig	member	June 30, 2018
Leo Willems	chair	June 15, 2015

Director and Board Member Additional Functions in 2015					
Frances Brazier	**Cristian Hesselman**	**Ted Lindgreen**	**Wytze van der Raay**	**Jochem de Ruig**	**Benno Overeinder**
- 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*	- Manager SIDN Labs -	None	- Team leader *CAcert critical system administrators* - Administrator, *Stichting Wereldwinkel Doorn*	- CFO RIPE NCC -	See page 21

6.2 Staff

NLnet Labs employed nine people in 2015: Jaap Akkerhuis, Ralph Dolmans, Berry van Halderen, Stavros Konstantaras, Benno Overeinder (managing director), Hoda Rohani, Yuri Schaeffer, Willem Toorop and Wouter Wijngaards. 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.

6.3 Offices

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

6.4 Finances

NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in June 2016, these are the unaudited numbers[5].

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. In the past years, NLnet Labs has developed a sponsor agreement. For 2015, we would like to acknowledge Comcast, Verisign, IIS (The Internet Foundation In Sweden), Afnic, ICANN, CIRA and DK Hostmaster A/S for their continued generous support.

Open Netlabs B.V. is an additional source of income in 2015 by offering Unbound, NSD, and OpenDNSSEC support contracts to partners in the industry. 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. Relevant activities in these areas are reported above.

5-Audited finances can be found in “Kengetallen jaarrekening 2015” as published on http://www.nlnetlabs.nl/labs/about/

6.5 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.

6.5.1 Income in 2015

At the end of 2014, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2015, with a total of 772 k€. Based on this budget and the expected consultancy income, 358.8 k€ grants were requested from SIDN and Stichting NLnet. Both sponsors allocated these funds for 2015, to be received by NLnet Labs on a quarterly basis.

Stichting NLnet & Stichting SIDN

are NLnet Labs' major benefactors.

In the years 2013 and 2014 Stichting NLnet awarded a subsidy of 264 k€ in order to perform business development within the context of the Open Netlabs B.V. These funds were immediately allocated towards a special fund for business development, henceforth they appear on the balance sheet.

Previous regular sources of non-subsidy income via the NSD and Unbound support contracts are now with Open Netlabs B.V. The consultancy contract with ICANN (mostly ISO3166 related work) is still under NLnet Labs responsibility.

In addition NLnet Labs received significant donations from Comcast, Verisign, Afnic, DK Hostmaster A/S amounting to a total of 260 k€ income above budget.

IIS (the Internet Foundation in Sweden), ICANN and CIRA (.CA registry) generously donated funds for the continued development of OpenDNSSEC.

Interest received amounted to 17 k€

The following organizations are acknowledged for their generous contributions

6.5.2 Expenditure in 2015

The major expenditure categories of NLnet Labs in 2015 are staff, travel and housing. In January, we were at the budgeted staff of 8 persons (7.6 FTE). In February our team was strengthened by Stavros Konstantaras (0.5 FTE) on the ENGRIT project with its own project reservation (separate from the 2015 budget). The total expenditure on staffing in 2015 is 588 k€. Housing and travel make up for another 81 k€ out of the total of 731 k€ expenditure (not included project costs).

From the ENGRIT designated reservation of 114 k€ at the start of 2015, we withdraw 52 k€ for the 0.5 FTE at NLnet Labs. For the SAND project reservation, we transferred 40.5 k€ to Twente University for co-funding the SAND project (co-funding with SIDN Labs and matched funding from NWO).

After making these reservations and valuations NLnet Labs had a positive result of 504 k€. The general financial reserve at the end of 2015 is 568 k€.

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	8	**General Reserve**	568
Open Netlabs BV stock and loans	296		
Receivables	115	**Open Netlabs BV Business Development Fund**	330
Bank & Cash	745	**Reservation ENGRIT**	62
		Reservation SAND	104
		Accounts Payable	17
		Tax and Social Premium Payable	16
		Other liabilities	67
Total	1,164		1164

Income				
	2014 actual (k€)	2015 actual (k€)	2015 budget (k€)	2016 budget (k€)
NLnet Subsidy	337	337	359	0
SIDN Subsidy	337	359	359	366
Other Donations	130	155	36	215
Consultancy and other Income	17	87	16	196
NSD & Unbound Support	67	4	0	0
Interest Income	14	17	2	15
Sub Total	902	959	772	792
Business Development Subsidy from NLnet	132	66	66	0
Total	1,034	1,025	838	792

Expenditure				
	2014 actual (k€)	2015 actual (k€)	2015 Budget (k€)	2016 Budget (k€)
Staff	542	588	590	602
Housing	56	56	57	63
Travel	55	25	67	68
Depreciation	2	3	5	5
ENGRIT Project Costs	21	10	0	0
SAND Project Costs	0	40	0	0
Other costs	51	59	52	54
Sub Total	727	781	772	792
Negative Result Open Netlabs	201	-233	0	0
Project Reservation NLnet Business Development	132	66	66	0
Project Reservation ENGRIT	-21	-52	0	0
Project Reservation SAND	0	-41	0	0
Total	1,039	521	838	792

6.5.3 Budget for 2016

The 2016 budget has been drawn up on 25 October 2015. Based on having 7.6 FTE we have budgeted a total expenditure of 792k€

On January 20, 2012 Stichting SIDN signed a five year contractual commitment to subsidize 50% of the expenditure needed to execute our chartered activities. For 2016, SIDN will cover 366 k€ in four quarterly grants of almost 92 k€. Other donations and subsidies from industry will account for 350 k€, and Open Netlabs will contribute about 60 k€ to NLnet Labs..

6.5.4 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 intended to subsidize this initiative, as of 2013, for 3 years. In 2013 and 2014, 132 k€ was immediately allocated towards a special fund for business development. For 2015, the last installment of 66 k€ was allocated covering for the activities of the business developer for a half year.

The business activities within Open Netlabs have generated an increased turnover in 2015. With the expected growth in turnover and revenues in the coming years, Open Netlabs will help to secure the continuity of the NLnet Labs Foundation.

7 Publications, Presentations and Reports

Publications

- SAC070: "***SSAC Advisory on the Use of Static TLD / Suffix Lists***", Akkerhuis as contributing SSAC member, May 2015. https://www.icann.org/en/system/files/files/sac-070-en.pdf
- SAC071: "***SSAC Comments on Cross Community Working Group Proposal on ICANN Accountability Enhancements***", Akkerhuis as contributing SSAC member, June 2015. https://www.icann.org/en/system/files/files/sac-071-en.pdf
- SAC072: "***SSAC Comment on the Cross Community Working Group on Naming Related Functions Proposal***", Akkerhuis as contributing SSAC member, June 2015. https://www.icann.org/en/system/files/files/sac-072-en.pdf
- RSSAC 003: "***RSSAC Report on Root Zone TTLs***", Akkerhuis as contributing RSSAC member, August 2015. https://www.icann.org/en/system/files/files/rssac-003-root-zone-ttls-21aug15-en.pdf
- SAC073: "***SSAC Comments on Root Zone Key Signing Key Rollover Plan***", Akkerhuis as contributing SSAC member, October 2015. https://www.icann.org/en/system/files/files/sac-073-en.pdf

Presentations

- "***Confidential DNS***", Wiley and Wijngaards, DPRIVE WG, IETF 92, Dallas, TX, March 2015. https://www.ietf.org/proceedings/92/slides/slides-92-dprive-1.pdf
- "***internet.nl: Promoting Internet Standards***", van Halderen, Lightning Talk, RIPE 70, Amsterdam, The Netherlands, May 2015. https://ripe70.ripe.net/presentations/37-internetnl-ripe.pdf
- "***Building a More Trusted and Secure Internet***", Overeinder, panel, RIPE 70, Amsterdam, The Netherlands, May 2015. https://ripe70.ripe.net/presentations/45-Trusted-and-Secure-Internet-panel.pdf
- "***getdns API Implementation***", Toorop, Open-Source WG, RIPE 70, Amsterdam, The Netherlands, May 2015. https://ripe70.ripe.net/presentations/135-getdns-oswg-lt-ripe70.pdf
- "***One Year of DANE (Some) Lessons Learned***", Akkerhuis, DNSSEC Workshop, ICANN 53, Buenos Aires, Argentina, June 2015. https://buenosaires53.icann.org/en/schedule/wed-dnssec/presentation-dnssec-one-year-dane-24jun15-en
- "***getdns A new stub resolver***", Toorop, vBSDcon, Reston, VA. September 2015. https://www.verisign.com/en_US/internet-technology-news/verisign-events/archive/vbsdcon2015/index.xhtml
- "***Root Zone KSK Maintenance***", Akkerhuis, ENOG 10, Odessa, Ukraine, October 2015. https://www.enog.org/presentations/enog-10/95-KSKmaintenance.pdf
- "***Discovery Method for a Validating Stub Resolver***", Torrent Gorjón, DNS WG, RIPE 71, Bucharest, Romania, November 2015. https://ripe71.ripe.net/presentations/153-xaviertorrent.pdf
- "***DNSSEC for Legacy Applications***", Toorop, DNS WG, RIPE 71, Bucharest, Romania, November 2015. https://ripe71.ripe.net/presentations/180-DNSSEC-for-Legacy-Applications.pdf
- "***Root Zone KSK Rollover***", Akkerhuis, DNS WG RIPE 71, Bucharest, Romania, November 2015. https://ripe71.ripe.net/presentations/156-What-is-5011_5.pdf
- "***Using DNS for Fun and Profit***", Vixie, Hubert, Overeinder and Karrenberg (panel), Black Hat Europe 2015, Amsterdam, The Netherlands, November 2015. https://www.blackhat.com/eu-15/sponsored-sessions.html#using-dns-for-fun-and-profit

Work in Progress

- "***Confidential DNS***", Wijngaards and Wiley, March 2015. https://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-03
- "***A DANE Record and DNSSEC Authentication Chain Extension for TLS***", Shore, Barnes, Huque and Toorop, October 2015. https://tools.ietf.org/html/draft-shore-tls-dnssec-chain-extension-02
- "***Technical Considerations for Internet Service Blocking and Filtering***", Barnes, Cooper and Kolkman, November 2015. http://tools.ietf.org/html/draft-iab-filtering-considerations-09

Student Reports

In 2015 we had 7 interns (one of them remote). The following reports and thesis were published in 2015

- "***BGP Route Leaks Analysis***", Wijchers, MSc thesis, Vrije Universiteit Amsterdam, March 2015. http://www.nlnetlabs.nl/downloads/publications/msc-thesis-wijchers.pdf
- "***BGP Routing Security and Deployment Strategies***", Eikema, BSc thesis, University of Amsterdam, June 2015. http://www.nlnetlabs.nl/downloads/publications/bsc-thesis-eikema.pdf
- "***Discovery Method for a DNSSEC Validating Stub Resolver***", Torrent Gorjón, MSc thesis, University of Amsterdam, July 2015. http://www.nlnetlabs.nl/downloads/publications/os3-2015-rp2-xavier-torrent-gorjon.pdf
- "***Analysis of DNS Resolver Performance Measurements***" Boulakhrif, MSc thesis, University of Amsterdam, July 2015. http://www.nlnetlabs.nl/downloads/publications/os3-2015-rp2-hamza-boulakhrif.pdf
- "***DNSSEC for Legacy Applications***", Bucuti, Graduate Research Intern, University of North Texas, August 2015. https://ripe71.ripe.net/presentations/180-DNSSEC-for-Legacy-Applications.pdf
- "***Automated Configuration of BGP on Edge Routers***", Vouteva and Turgut, BSc thesis, University of Amsterdam, August 2015. http://www.nlnetlabs.nl/downloads/publications/os3-2015-rp2-vouteva-turgut.pdf

Student Work in Progress:

- "***Distributed Load Balancing of Network Flows using Multi-Path Routing***", Ouwehand, BSc student, University of Amsterdam.

Blog Posts

- "***Algorithm Rollover in OpenDNSSEC 1.3***", Schaeffer, October 2015. https://www.nlnetlabs.nl/blog/2015/10/29/algorithm-rollover-in-opendnssec-1-4/

NLnet Labs Staff Responsibilities

- **Akkerhuis**:
  - ICANN representative in the ISO 3166 Maintenance Agency
  - Member of the ICANN Security and Stability Advisory Council (SSAC)
  - Member of the ICANN Root Server System Advisory Committee (RSSAC) Caucus
  - Co-chair of the RIPE DNS working group
  - Member of the ENOG Program Committee
  - RIPE Arbiter
  - Member of the ccNSO study group on Use of Names for Countries
  - Member of the CWG on Stewardship Transition (SSAC member of the CWG)
  -
- **Overeinder**:
  - Chair of the RIPE Program Committee
  - Co-chair of the RIPE Best Current Operational Practices Task Force
  - Member of the ENISA Internet Infrastructure Security and Resilience Reverence Group

Stichting NLnet Labs

Science Park 400, 1098 XH Amsterdam

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