NLnet Labs

Annual Report 2016

For an Open Internet

1 Highlights

NLnet Labs promotes and contributes to a stable and reliable Internet infrastructure, where key technologies make up a network of networks into the Internet. Much of our work is focussed on Internet infrastructure and DNS security and stability, involving activities in different areas like software development, protocol standardization, and policy and governance. NLnet Labs also carries out research projects to deepen our knowledge and increase our understanding of the fundamental behavior and operational impact of new and innovative protocols and technologies.

Software Development

The authoritative name server NSD 4 sees continued development and maintenance for performance and memory usage optimization. Unbound 1.6 was released with functionality for policy filtering and views, two important new features for client-based filtering. The development on the asynchronous and flexible getdns library continued, with special attention to DNS privacy extensions (see IETF DPRIVE WG) and the getdns stub resolver with all privacy options enabled, named Stubby.

The milestone release of OpenDNSSEC 2.0 was published in July 2016. We are very proud on this major release which is well-tested and stable. Most important change in the 2.0 release is the new (policy) enforcer that allows flexible and robust key roll-over scenarios. All new features will be introduced in OpenDNSSEC 2.0 and subsequent releases, and OpenDNSSEC 1.4 is the long-term support release.

Internet Protocol Standards

NLnet Labs is actively involved in the standardization of Internet protocols by participating in IETF meetings. We contribute to the IETF TLS WG with the draft on DNSSEC authentication chain with the intent to allow TLS clients to perform DANE Authentication of a TLS server without performing additional DNS record lookups and incurring the associated latency penalty. Drafts and RFCs in the DNS WG are implemented and feedback is provided as part of the standardization process.

Internet.nl is a “measurement” platform to test standards compliance of ISPs, websites and email services that generates a lot of interest and positive attention. The initiative is an effort by a number of partners, and NLnet Labs is responsible for the technical realization.

Policy and Governance

NLnet Labs participated with TNO and SIDN in the CDAR project: an ICANN commissioned project that studied the impact of the New gTLD Program on the stability of the root server system. A draft report for public comments has been published in October 2016, and the project will finish early 2017.

Akkerhuis was member of the KSK roll-over design team that published a report with a roll-over plan. The report presents a number of recommendations for the implementation of the Root Zone KSK roll-over.

Research

With a consortium of ten partners, NLnet Labs was granted funding of the EU H2020 project proposal called LIGHTest. The objective of LIGHTest is to create a global cross-domain trust infrastructure, build on top of the DNS infrastructure (relying on DNSSEC and DANE). In September 2016 the kick-off meeting was organized and the project will run for three years.

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 robust, light-weight, high-performance, secure, and single purpose. From its first release in 2002 up to the latest major release of NSD 4 in late 2013, the software has shown to be a mature and dependable authoritative name server that is used in many places like root servers, TLDs, CDNs, ISPs, up to enterprises and SMEs. With NSD 4 being in production for more than one year, we announced in 2015 the end of support of NSD 3 by May 2016. NSD 4 sees active developments to improve performance, to reduce memory usage, and implementing new open standards and features to meet operational requirements. The design philosophy remains with the principles of robust, light-weight, high-performance and secure.

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). Additional features to meet operational requirements are also considered to comply with current and future practices.

NSD 4 Activities

NSD 4 is the primary development release of the NSD name server. In 2016, we continued with the development and maintenance of the source code to support new open standards and to accommodate to new operational requirements.

Changes in prioritizing AAAA records in priming queries and for referrals when a query is received over IPv6 are important improvements to make IPv6 an "equal"-class citizen to IPv4. Further, the code has been modified to have more extensible EDNS option handling.

A number of improvements on the zone transfer (AXFR/IXFR) mechanism have been implemented to improve the robustness of the server and reduce potential zone transfer attempts to lower the load on the system.

To further reduce the memory consumption of NSD 4, we implemented a more memory efficient data structure for zone data. The red-black tree data structure reduces the memory usage for about 15%, at the cost of some speed performance.

NSD 3 Activities

We informed users about the approaching end of support of NSD 3 in May 2016. In June 2016, after the end of support date, we published NSD 3.2.22 with two small bug fixes as a courtesy to our users.

Results

NSD 4 has seen a series of maintenance releases (v4.1.8 – v4.1.14) with bug fixes, performance improvements and new features in 2016.

In the NSD 4.1.10 release we introduced a change in the wire output for the DNS protocol: it has transport preference for glue. This means that for priming queries over IPv6 it will prioritize AAAA records in the additional section, but for priming queries over IPv4 it will prioritize A records in the additional section. This preference is also used for normal referrals, so that delegations that are too large to fit in one response are more likely to return usable addresses to the downstream resolver.

The NSD 4.1.11 release contains a patch for the unlimited AXFR vulnerability; with a config option to limit AXFR sizes. This vulnerability is from Toshifumi Sakaguchi, and this release fixes CVE-2016-6173 JVN#63359718 JPCERT#91251865. The flaw involves sending unlimited data in a zone transfer that causes a denial of service in the server. With NSD 4.1.14 the number of zone transfer attempts is lowered, and hence reducing load on the server.

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 I, 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.

Goals

Continue the support and maintenance of OpenDNSSEC version 1.4 branch. Release of major version OpenDNSSEC 2.0 and focus for all developments of new features will be for the 2.0 release and its successors.

Activities

OpenDNSSEC 1.4 has been the de-facto long-term support (LTS) release, and this has been made explicit by publicly declaring 1.3 to be end-of-life in July 2017, one year after making the statement. We have not given a minimal lifetime for the 1.4 LTS, but we foresee that we will keep 1.4 alive until at least 1.3 has passed its end-of-life and we have seen at least one major user of 1.4 make a move to a version 2 release. After this we will have at least one year of additional 1.4 support but by providing the version 2 of OpenDNSSEC we hope to phase out 1.4 as well.

Since a release for version 2.0 of OpenDNSSEC was really imminent, we could make it clear that the 1.4 releases are maintenance releases only. No new features will be added to 1.4 and we will target no more structural improvements.

Results

Notwithstanding our focus on the 2.0 and subsequent minor releases, we have seen some real major fixes in 1.4, of issues that have been outstanding for a long time and could finally be fixed by our commitment to OpenDNSSEC. This resulted into three releases: 1.4.9 in January, 1.4.10 in May, 1.4.12 in October, the public release of 1.4.11 was skipped. These greatly improve the stability, the handling of concurrent transfers and prevent the leaking of resources (memory).

In July 2016, the overdue 2.0 release was made a reality after a couple of public release candidates earlier in 2016. In the past years, improvements and even new features were forced into 1.4 by the overdue 2.0 release. By taking over the management of the OpenDNSSEC project we were able to push out the 2.0 release.

OpenDNSSEC 2.0 got an entire re-write of the enforcer. This part of OpenDNSSEC controls changing signing keys in the right way to perform a roll-over. Before, the enforcer would perform a roll-over according to a strict paradigm. One scenario in which deviations would not be possible. The new enforcer is more aware of the zone changes being propagated in the Internet. It can therefore decide when it is safe to make changes, rather than to rely upon a given scenario. The new capabilities to keep a zone valid even in situations where changing parameters could trap you into a bogus situation. OpenDNSSEC chooses the fastest safe steps to keep (or even heal) your zone.

After the 2.0 release, we had two public updates, version 2.0.1 (July) and version 2.0.3 (October) mostly targeting migration issues, and fixes that were also made in version 1.4 of OpenDNSSEC. Version 2.0.2 was not published to incorporate late fixes.

Impact

OpenDNSSEC has lowered the barrier to deploy DNSSEC: its availability has been contributing to positive decisions with respect to the deployment of DNSSEC. Alternative solutions are available but the policy-based zone signing and key management are unique features of OpenDNSSEC and valued by its users.

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. Unbound is a flexible and versatile resolver that performs well in both small setups and large, complex cluster architectures, and of sizes in between. Unbound deployments can be found at large ISPs, CDNs, cloud services, and small home routers.

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

New features were added to Unbound to depend DNS answers on the address of the client. Unbound 1.5.10 introduced the tag functionality. This feature makes it possible to divide client source addresses in categories (tags), and use local-zone and local-data information for these specific tags. Unbound 1.6.0 introduced views. A view in Unbound is a named list of configuration options. The currently supported view configuration options are local-zone and local-data. A blog post describing the usages of the new tag and view functionality has been published at the NLnet Labs website.[1]

Other noteworthy activities are the new generic EDNS options processing framework in Unbound, and the implementation of support for DNS over TLS (as standardized in the IETF DPRIVE working group).

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

In 2016 a series of 1.5.8–1.5.10 releases have been published, and in December a new 1.6.0 release. Versions 1.5.8–1.5.10 saw some code maintenance and fixes. Unbound 1.5.10 also incorporated the tag functionality and in Unbound 1.6.0 the views feature was introduced.

A new EDNS processing framework was introduced in Unbound 1.6.0. The framework allows for native handling of EDNS options and exposes the functionality to all modules including the Python module. This was also the first step in merging the EDNS Client Subnet branch into the master branch of Unbound that will come at the first quarter of 2017.

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 and CDNs, as a standard resolver in some OS distributions (e.g., FreeBSD and OpenBSD), and in several DNS appliances and home routers (e.g. as a package in OpenWRT).

1-https://www.nlnetlabs.nl/blog/2016/12/22/client-based-filtering-in-unbound/

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. The principle of DNSSEC validation at the end-point and bringing it close to the application is also a design goal of the getdns library, see Section 2.3.1.

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/macOS, BSD, Linux, and Windows, and integration with NetworkManager and systemd.

Activity and Results

DNSSEC Trigger had one release version 0.13 in 2016. It contained a large number of patches for the Fedora Python bindings to NetworkManager. The release was necessary because of changes on the Apple OSX (macOS) platform for the installation script, that tries to create a separate user account to run the daemon under. This installation script no longer works on new versions of the platform.

In its current design, DNSSEC Trigger is a set of scripts and code that relies on Unbound that either uses the forwarders obtained from DHCP, or falls back to do its own recursive queries. In 2017 we will study how getdns stub resolver fits in, and whether it can be an alternative setup of DNSSEC Trigger.

Impact

The initial impact was to advance the understanding about the impediments to get DNSSEC to the end users. Secondly, the tool has set an example for other initiatives to follow, most prominently is the adoption of the ideas, design and code into the Fedora Linux distribution.[2]

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, whose 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). The library incorporates a number of methods to successfully receive a DNSSEC validated answer, for example DNSSEC roadblock avoidance or DNS64 at the end-point for validation of IPv4 answers by IPv6-only clients.

A particular hope is to inspire application developers towards innovative security solutions in their applications.

The getdns project is a collaboration between a number of partners: NLnet Labs, Sinodun, No Mountain Software, and Salesforce.

2-https://fedoraproject.org/wiki/Networking/NameResolution/DNSSEC#dnssec-trigger

Goal

Continued development and maintenance of the modern asynchronous DNS API library. Besides the development of the software, we generate 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 that is versatile in many situations and setups, e.g. DNSSEC roadblock avoidance or DNS64 in IPv6-only networks.

Activities

getdns saw two lines of development in 2016. One was in preparation of the 1.0.0 release and saw two beta releases 1.0.0b1 and 1.0.0b2. Development on the 1.0.0 release was primarily focused on maturing and stabilizing the code base and gaining confidence for a production quality release. Simultaneously, development on a 1.1.0 new features release was started, which saw two alpha releases 1.1.0a1 and 1.1.0a2.

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

Results

In the 1.0.0 development line, the modular and pluggable event loop system, which empowers the application with control over all asynchronous I/O, has been extended to libunbound. Libunbound is used by getdns to do full recursion DNS lookups. Before, libunbound managed its own private event loop and signaled the application of ready events over a file descriptor. This was not a portable method and did not work on Windows. To resolve, libunbound has been equipped with a pluggable event API too, modeled after the one in getdns, which was released in version 1.5.9. getdns detects and uses the API, resulting in consistent asynchronous control for the application with both stub and full recursion resolution, and also the availability of full recursion with getdns on Windows.

Further development on 1.0.0 was mainly targeted at measuring its behavior and assessing all possible ways to use the library and, in doing so, increasing code coverage. To this end, development on 1.0.0 also included enhanced and detailed reporting of internal operations and performance, such as the used transports, timings, authentication success and method, etc. The getdns_query test-tool which is used during development to try out and test the libraries functionality was significantly improved and extended. Two notable added features to getdns_query are the ability to read and process configuration files, and to act as a small DNS daemon listening for requests and returning the replies as processed by getdns internally.

The two 1.1.0 alpha releases exposed the functionality added to getdns_query as new function prototypes for the public API. getdns_query's ability to read and process configuration files resulted in functions to convert strings into getdns data structures and to configure a getdns context from a getdns dictionary data structure. Also new prototypes were introduced to enable applications to build DNS server programs with getdns.

The second 1.1.0 alpha release introduced Stubby. Stubby is a version of getdns_query, that is preconfigured to listen on the loopback interface, and acts as a local stub resolver daemon. Stubby is a follow-up on our "DNSSEC for Legacy Applications" study in 2016. Stubby unlocks the versatile stub resolver capabilities of the getdns library to legacy applications. Research into signaling, sharing and re-using information from the getdns system component (Stubby) and the getdns library (for example to share stateful connections, and signal of the level of privacy) is on the roadmap for 2017.

getdns development has been intimately alongside the development of DNS over TLS (RFC7858). Stubby is presented as a DNS Privacy stub resolver delivering all the privacy DNS features getdns has to offer to legacy applications.

Impact

The proposition of the getdns API library and stub resolver is received with enthusiasm and an increasing group of potential users in the industry showed interest to deploy the software in their organization. We presented getdns and DNS privacy at various meetings (IETF, RIPE, OARC, ICANN).

2.3.2 Ldns

The ldns library is like a Swiss army knife multitool for building DNS applications, e.g., servers, DNSSEC signer, applications for experiments, tests, and analysis.

Goal

Work towards a major version release of ldns version 2 that incorporates many ideas from getdns API. Note well, ldns targets DNS engineers, while getdns targets application developers.

Activities

Maintenance of ldns1 code-base and incorporating DANE support via OpenSSL 1.1.0 library. Design and development of ldns2.

Results

ldns1

Support for DANE has been in ldns shortly after the RFC was published since version 1.6.14. However, in 2015 we were notified that there was an issue with a specific set of parameters, for which DANE validation with ldns could potentially be false (the DANE-TA usage type). This specific usage type could not be managed with the underlying crypto library (OpenSSL) in a straight-forward manner. Luckily, direct support for DANE in OpenSSL itself was in the making and was released in 2016 with OpenSSL 1.1.0. This resulted in version 1.7.0 release of ldns, which uses OpenSSL 1.1.0's DANE support directly from its DANE API. This release also contained a long list of small bugfixes and updates that were accumulated in the period waiting for the OpenSSL 1.1.0 release.

ldns2

The core for ldns2 is in getdns (and partly also in Unbound) and is stable. For a ldns2 release we want to keep providing the former API alongside the new functions, but have it use the newer functions underneath. This has not been done in 2016 and is still on the roadmap for 2017.

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

Three version updates of Net::DNS have been released in 2016, mostly concerned with minor bugfixes, and updates. Most notable effort and was the co-operation with John Levine in the context of a Perl implementation of draft-levine-dnsextlang, to create a suitable interface for extending the Net::DNS's resource records with ones provisioned by an external module.

Results

Releases 1.05 through 1.07 of Net::DNS and release 1.0 3 of Net::DNS::SEC.

2.4 Other Activities

2.4.1 IETF DNS activity

I-Ds and RFCs

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

This internet draft, which is a joined effort of NLnet Labs with researchers from No Mountain Software, Mozilla and Verisign Labs, describes a TLS extension for transport of a DNS record set serialized with the DNSSEC signatures needed to authenticate that record set. The intent of this proposal is to allow TLS clients to perform DANE authentication of a TLS server without needing to perform additional DNS record lookups and incurring the associated latency penalty. It also provides the ability to avoid potential problems with TLS clients being unable to look up DANE records because of an interfering or broken middlebox on the path between the client and a DNS server. And lastly, it allows a TLS client to validate DANE records itself without necessarily needing access to a validating DNS resolver to which it has a secure connection.

The draft was presented at the TLS working group at the IETF95 in Buenos Aires, Argentina. The TLS working group has subsequently adopted the draft as a working group document. A working prototype of a TLS proxy offering the TLS extension and a TLS client that can authenticate with this extension was developed during the hackathon of the IETF95. Feedback from the TLS working group mailing-list has let to one revision of the document in 2016.

Hacakthons

- IETF 95 Hackathon, DNS/DNSSEC/DANE/DNS-over-(D)TLS:[3]
  - (partial) implementation of draft-ietf-dnsop-edns- chain-query
  - (partial) implementation of draft-ietf-tls-dnssec-chain-extension
- IETF 96 Hackathon, DNS/DNSSEC/DPRIVE/DANE:[4]
  - DNS64 in getdns API library
- IETF 97 Hackathon, DNS/DPRIVE/DNSSEC/DANE:[5]
  - Stubby test and interop
  - out of order processing (OOOP) in Unbound and `delaydns` reliability test for OOOP

2.4.2 ICANN gTLD related activity

For the ICANN New gTLD scalability study see Section 3.2.1. For activities with the ICANN meetings and in the community, see Section 4.1.

3-https://www.ietf.org/proceedings/95/slides/slides-95-hackathon-13.pdf
4-https://www.ietf.org/proceedings/96/slides/slides-96-hackathon-13.pdf
5-https://www.ietf.org/proceedings/97/slides/slides-97-hackathon-sessb-dns-00.pdf

3 Area: IP and Infrastructure Security and Stability

In order to increase the security and maintain the stability of the Internet infrastructure, 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, applications 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

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 have developed an RPSL library, a Python-based client that retrieves BGP policies from IRR databases and exports the corresponding information in XML and YAML output. The prototype implementation has been presented at the RIPE 72 Routing WG meeting.

Results

The prototype implementation does not implement all RPSL attributes and operators, but is compatible with more than 95% of the routing objects published by tier 1 and tier 2 (including small tier 2) operators. For tier 3 operators we measured about 90% compatibility. The performance of the Python-based clients greatly improves on existing tools, also the IRRToolSet.

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).

Parallel to the interest, we do hear that operators want to move away from RPSL: “it’s showing its age”. The formalism does fit well with the current operational reality, and an alternative specification language like RDL (routing documentation language) could fill this need. The design and implementation of such a new specification language would require a substantial investment in effort and time.

3.1.2 A Hybrid System for Automatic Exchange of Routing Information.

MSc. student Stamatis Maritsas, supervised by Stavros Konstantaras and George Thessalonikefs, finished his internship on designing and evaluating a hybrid system for automatic exchange of routing information.

Goal

Design and evaluate a hybrid system that will automatically exchange routing policies between autonomous systems. By using a hybrid approach, control of the policy information is transferred to authorities themselves and they are in charge of what policy information they share with whom. In this way, network operators will have more incentive to keep their policy information properly updated.

Activities

Stamatios Maritsas (Msc student intern) designed a hybrid system for automatic exchange of routing information. The system facilitates distribution of routing policies using a central point that points to an autonomous system's routing policy. Each autonomous system is in charge of hosting its own routing policy and shares it with interested parties. One innovation during the design was the use of 'policy views' which give an autonomous system the ability to choose the amount of routing policy information it shares based on the requester.

Results

Publication of a MSc thesis, see Section 7.

Impact

Talents/students being trained in fundamental Internet architecture. The internship was a stepping stone for his first job at a networking company.

3.1.3 Self-managing Anycast Networks for the DNS (SAND) and DNS Anycast Security (DAS)

Goal

The SAND 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.

The goal of the DAS project (matched funding by NWO) is to investigate the large-scale development and deployment of DNS anycast services, in particular the virtualisation, security and (self-)management of such services. Our approach is to collect unique measurement data from the large-scale DNS infrastructures operated by our industrial partners and analyze this data to validate our scientific results.

SIDN Labs and NLnet Labs support both projects with funding for an academic postdoc at the Universiteit Twente. A PhD position in the DAS project is funded by NWO. Other industry partners are RIPE NCC, Netnod and SURFnet, whom support the project with in-kind contributions. Some of the parts of the project are a collaboration with the Information Sciences Institute (ISI), USC.

Activities

To measure, evaluate and assess anycast networks, an anycast testbed has been created.[6] The anycast testbed consists of 9 locations and is supported by a number of organisations. For measurements of the "performance" (given a set of parameters) the RIPE Atlas measurement infrastructure is used. Results of the experiments and measurements are presented at operational meeting (RIPE and IEPG) and at academic conferences.

Results

The research activities resulted in a number of presentations, i.e. RIPE 73 and IEPG at the IETF 97, and academic publications (received PAM 2017 best paper award), see Section 7.

Impact

Insight in the important parameters that define the performance of anycast networks, e.g. RTT/delay to service, robustness under DDoS attacks, etc. The presented results of the research helps operational community to monitor and analyze their anycast network and plan and execute improvements to meet predefined performance indices. Other contributions are proposals for novel approaches to virtualize, secure and manage large scale DNS anycast services.

3.2 Security and Stability of Critical Infrastructures

3.2.1 CDAR: ICANN Commissioned New gTLD Stability Study

CDAR (Continuous Data-driven Analysis of Root Stability) is a joint research project by a consortium formed by NLnet Labs, SIDN Labs, and TNO. This consortium was selected by ICANN to investigate the technical impact of the New gTLD Program on the Root Server System.[7]

Goal

Measurement-based study into the effects of the recent introduction of TLDs under the New gTLD Programme on the stability of the global DNS root server system.

Activities

The CDAR study relied on empirical data obtained from longitudinal measurements, both passive and active.

For the passive measurements, the project relied upon the DITL (Day in the Live of DNS) data which is available to DNS-OARC members. The data of the root letters in the root server system is systematically analyzed for the past five years (period 2012–2016). Also data from individual root servers have been used for other time slots where new gTLDs were introduced, and the effects at the root server of this introduction could be studied.

The passive measurements are measuring the effects of the introduction of new gTLDs for the end-users. Data collected by RIPE Atlas measurements of the past years are used to analyze the effects of this. The RIPE Atlas probes run frequent measurements (RTTs) to the various root servers. This is a build-in measurement running for the past years (from its inception).

In 2015 and 2016 we presented the project at various meetings, like ICANN, DNS-OARC, IEPG (with the IETF meetings) and RIPE. To create community acceptance and support, we shared our approach of the study and asked for feedback. In a later phase, we presented results (first observations, and analyzed and refined results).

6-http://www.anycast-testbed.com/
7-http://cdar.nl/

Results

The result of the study and the presentations at the various events, is a draft report published to the community for feedback.[8] The final report after incorporating feedback is published in 2017.[9]

Impact

The report that finalizes the CDAR study is used by the different stakeholders in the ICANN community, e.g. for policy development and for the series of reviews of the New gTLD Program.

3.3 Adoption of Open Standards: IP and Security

3.3.1 Platform Internet Standaarden and Internet.nl

Platform Internet Standaarden is a national initiative in the Netherlands to promote open standards for a secure and stable Internet.[10] New Internet standards for IPv6, DNSSEC, TLS and email (SPF, DMARC and DKIM) are important but find slow uptake by ISPs. The platform informs and promotes new standards by reaching out to the different stakeholders and make insightful what they can do to speedup adoption and deployment of these standards.

The website Internet.nl is instrumental to the approach of Platform Internet Standaarden.

Goal

NLnet Labs is one of the members of Platform Internet Standaarden and contributes to the Internet.nl initiative. The website is an important tool to reach out to stakeholders of the Internet community: e.g., ISPs, network and service operators, Internet hosting companies, end-users, and government.

Activities

Continued development on the Internet.nl website and made the third revision of the website available. At different meetings we reach out to the community members, either in context of Platform Internet Standaarden/Internet.nl at conferences and workshops, or individually/ad-hoc at operational meetings.

In a collaboration with the Kosciuszko Institute, the Internet.nl website has been translated in the Polish language. Automatic language selection based on the browser language has been added to the website.

NLnet Labs' staff participated in the STARTTLS and DANE expert meeting. The goal of this meeting was to give an advice whether the combination of STARTTLS and DANE should be added to the "comply or explain" (Dutch: "Pas toe of leg uit") list for Dutch governmental organisations, departments, offices, etc. This meeting resulted in the advice to adopt these standards.[11] This advice resulted in the adoption.[12]

Results

In 2016 we made the third incarnation of the Internet.nl web-site. It had been placed live in July 2016, with four later updates containing some changes and improvements.

8-https://www.icann.org/public-comments/cdar-draft-2016-10-27-en
9-https://www.icann.org/news/announcement-2017-03-08-en
10-https://ecp.nl/activiteiten/platform-internetstandaarden/
11-https://www.forumstandaardisatie.nl/sites/bfs/files/20160215 Expertadvies STARTTLS en DANE 1 0.pdf
12-https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

For the Internet.nl we:

- Made tests more stringent to test HTTPS configurations over IPv4 comparing with IPv6 and content similarity checks;
- Multilingual support without multiple deployments;
- Incorporated the testing and scoring of the forced HTTPS redirection and usage of HSTS policies. The usage of HTTPS and HSTS are generally deemed a requirement now for websites;
- We facilitated the translation into Polish, at least for a major part of the site, some parts were left in English to target redesign work;
- Several updates to messages, time-out settings/rate limit avoiding.

As well as many other changes, fixes and improvements.

The Internet.nl website has been nominated for the ISOC-NL innovation award 2016.

Impact

Both the Platform and the website do increase the awareness of open standards and the importance of deployment of these standards to increase stability and security of the Internet infrastructure in the Netherlands. We do see repeated measurements where the results improve towards the 100% score on the website. The individual measurement tools are also used by organizations to monitor their standards readiness on a regular basis.

Individual countries are interested in similar initiatives. To support this, one instance of internet.nl containing multiple languages is hosted at NLnet Labs.

NLnet Labs' staff participated the STARTTLS and DANE expert meeting organized by the Dutch government. The goal of this meeting was to give an advice whether the combination of STARTTLS and DANE should be added to the "comply or explain" (Dutch: "Pas toe of leg uit") list. This meeting resulted in the advice to adopt these standards.[13,14]

3.4 DNSSEC-Based Security and Trust

Trustworthy and dependable DNS can be used as a building block of a security and trust infrastructure. With a minimal set of assumptions and dependencies, security can be bootstrapped from the ground-up using DNSSEC, DANE, and X.509 certificates (for TLS, s/MIME, …).

In this section, two projects are presented that build upon DNSSEC-based security to provide trusted and dependable services.

3.4.1 EU H2020 LIGHTest Project

The objective of LIGHTest is to create a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions. The name LIGHTest is derived from the one-line project description "Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes".

13-https://www.forumstandaardisatie.nl/sites/bfs/files/20160215 Expertadvies STARTTLS en DANE 1 0.pdf
14-https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

LIGHTest is funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. Partners in the project are: NLnet Labs, Fraunhofer Institute (Stuttgart), DTU – Technical University of Denmark, time.lex, OIX Open Identity Exchange, ATOS Spain, Correos, GlobalSign (Finland), IBM (Denmark), University of Stuttgart, EEMA, Giesecke & Devrient, TU Graz, and TÜBITAK

Goal

Design and implement a cross-domain trust infrastructure by reusing existing governance, organization, infrastructure, standards, software, community, and know-how of the existing Domain Name System (DNS), combined with new innovative building blocks. This approach allows an efficient global rollout of a solution that assists decision makers in their trust decisions. By integrating mobile identities into the scheme, LIGHTest also enables domain-specific assessments on Levels of Assurance for these identities.

Activities

The LIGHTest project started September 2016 with a kick-off meeting in Stuttgart, hosted by the Fraunhofer Institute.

NLnet Labs is involved in different work packages, in specific tasks in the work packages, to contribute DNS, DNSSEC and DANE expertise, and related to the integration of LIGHTest with the DNS infrastructure. Major activities of NLnet Labs for this year are the DNS building block inventory report for the consortium and the critical infrastructure analysis.

Results

Contributions to the various tasks and reviews of documents. NLnet Labs is task leader in two tasks related with DNSSEC expertise and building blocks, and critical infrastructure analysis. We started with the analysis and writing of the documents. The deliverables for both tasks are planned in 2017.

Impact

Trust is a prerequisite for a wide range of offerings on the digital single market. By providing a component to "trust list enable" arbitrary applications, LIGHTest enables the creation of a variety of innovative new trust-sensitive applications and services.

The design of LIGHTest with DNSSEC and DANE to build/bootstrap trust is an excellent showcase of the potential of these technologies in security and trust.

3.4.2 DNSSEC-Based Secure Email

Goal

Present a proof of concept security platform that demonstrates trustworthy email exchanges across organizational boundaries and includes authentication of mail servers, signing and encryption of email, and binding cryptographic key certificates to the servers.

The goal of this project is to help organizations:

- Encrypt emails between mail servers
- Allow individual email users to digitally sign and/or encrypt email messages
- Allow email users to identify valid email senders as well as send digitally signed messages and validate signatures of received messages

The test and evaluation platform uses the Domain Name System Security Extension (DNSSEC) protocol to authenticate server addresses and certificates used for Transport Layer Security (TLS) to DNS names.

Activities

NLnet Labs collaborated, together with Microsoft, ISC, Secure64 and Fraunhofer, in a NIST/NCCoE project titled "Domain Name Systems-Based Electronic Mail Security". The goal of the project was to demonstrate how the security of e-mail communication can be improved using available technologies. Unbound, NSD and OpenDNSSEC were tested, together with products from the project partners.

Results

This project resulted in the NIST special publication 1800-6.[15]

Impact

The NIST special publication gives an insightful view on the value of DNSSEC-based secure email services and assesses the interoperability between the different (open-source) software vendors. The publication shows that employees are able to exchange personal and enterprise information via email with significantly reduced risk of disclosure or compromise; enables the use of existing security protocols more efficiently and with minimal impact to email service performance; it integrates capabilities into various server and client IT infrastructure environments.

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.[16]

Akkerhuis continued to be the SSAC appointed-member of the Cross Community Working Group (CWG).[17] 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 until 2016, when the IANA Stewardship Transition was approved and submitted to the NTIA.

Akkerhuis acts as a liaison for ICANN in WG 2 of the ISO Technical Committee 46, and represents ICANN in the 3166 Maintenance Agency. (ISO 3166 is the International Standard for country codes and codes for their subdivisions.)

Akkerhuis was member of the KSK roll-over design team that published a report with a roll-over plan.

15-https://nccoe.nist.gov/projects/building-blocks/secured-email
16-https://www.icann.org/resources/pages/rssac-caucus-2014-05-06-en
17-https://community.icann.org/display/gnsocwgdtstwrdshp/CWG+to+Develop+an+IANA+Stewardship+Transition+Proposal+on+Naming+Related+Functions

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

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

Akkerhuis and Overeinder where part of the consortium which conducted a study about the technical impact of the New gTLD Program on the Root Server System.

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 RIPE 72 and RIPE 73 NLnet Labs' staff disseminated its knowledge and expertise with a number of high impact appearances. See also Section 7.

Van Halderen participated in the LACNIC 26 meeting. With Ihrén (Netnod), he organized a one-day course on DNSSEC and OpenDNSSEC. Van Halderen was also invited to attend the LACTLD meeting at the end of LACNIC 26.

Toorop attended the NANOG 68 meeting in Dallas, TX. At the NANOG meeting, Toorop presented there Stubby, the getdns stub resolver.

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.

Dolmans, Toorop and Overeinder participated in the IETF hackathon (IETF 95, IETF 96 and IETF 97) to develop and test new features for the getdns API project with the other project members and hackathon participants that joined our project (see Section 2.4.1).

For implementations of I-Ds and RFCs, see the relevant software projects described in Section 2. For active contributions to Internet-Drafts see Section 7.

Dolmans, Toorop and Overeinder attended OARC meetings in 2016. References to OARC presentations can be found in Section 7.

Colleagues from NLnet Labs also attended Dutch technical community meetings like Holland Strikes Back, NLnog Dag, and SURFnet RoN++ meeting (Research on Networks). We also attended the NCSC One Conference in The Hague to listen and discuss Internet infrastructure security and stability.

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).

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.[18] 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 the first 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' strategy for sustainability and continuity of the organization is based on three principles: multi-year subsidy contracts, sponsoring by industry partners, and provide additional services via a wholly owned subsidiary: Open Netlabs BV. With this approach, we diversify NLnet Labs' income by identifying and engaging with more parties to provide a continued commitment to fund its work and by cooperating with Open Netlabs BV.

Open Netlabs BV operates 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 2016, support for the main software products of NLnet Labs, NSD, Unbound and OpenDNSSEC, were offered in different levels of SLAs. Besides SLA support, Open Netlabs also provided consultancy to users and collaborated in a funded research project with partners.

Besides SLAs, advice and funded research projects, Open Netlabs will develop additional services to create value to (end-) users. The new business development will be partly aligned with NLnet Labs, but for all, the values and the mission of both entities will be shared and strengthened by each other.

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

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.

Four board meetings took place in the year 2016. Benno Overeinder participated in the board meetings in his role of Director of NLnet Labs. Han Brouwers participated as the director of Open Netlabs BV.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€231 for 2016). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2016

name	function	end of term
Frances Brazier	secretary	December 28, 2017
Cristian Hesselman	chair	June 30, 2018
Ted Lindgreen	member	January 31, 2018
Wytze van der Raay	member	December 28, 2016
Jochem de Ruig	treasurer	June 30, 2018
Andrei Robachevsky	member	June 30, 2019

Director and Board Member Additional Functions in 2016

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)*	- Manager SIDN Labs	None	- Team leader *CAcert critical system administrators* - Administrator, *Stichting Wereldwinkel Doorn*	- CFO RIPE NCC	See page 26

6.2 Staff

NLnet Labs employed nine people in 2016: 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 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 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 Finances

NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in May 2017, these are the unaudited numbers.[19]

Stichting NLnet Labs primarily finances its projects and activities from grants and donations. Until last year (2015), the budget of NLnet Labs was largely covered by grants from two organizations: Stichting NLnet and SIDN. The subsidy contract with Stichting NLnet was terminated as of January 1, 2016.

In 2016, about half of our budget was covered by the subsidy contract with SIDN (the Internet domain registry for the Netherlands). This subsidy contract provides for a structural financing for the period Jan 1, 2012 – December 31, 2016. End of 2016, a next term of five year (until 2021) funding by SIDN was codified.

A second means of income are donations and sponsoring by other parties. In the past years, NLnet Labs has developed a sponsor program with a number of partners from the Internet industry. For 2016, we would like to acknowledge Comcast, Verisign, Infoblox, IIS (The Internet Foundation In Sweden), Afnic, ICANN, CIRA, NZRS, and DK Hostmaster A/S for their continued generous support.

Open Netlabs BV is an additional source of income in 2016 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.

For the financial sustainability and continuity of NLnet Labs, 2016 was an important year. This was the first year without the subsidy of Stichting NLnet. With the sponsoring by industrial partners, an EU H2020 project and income generated by Open Netlabs, the financial position of NLnet Labs is healthy.

19-Audited finances can be found in "Kengetallen Jaarrekening 2016" as published on http://www.nlnetlabs.nl/labs/about/

6.5.1 Income in 2016

At the end of 2015, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2016, with a total of 792 k€. Based on this budget and the expected income from donations and consultancy, 366.4 k€ grant was requested from SIDN. The sponsor allocated these funds for 2016, to be received by NLnet Labs on a quarterly basis.

Stichting SIDN
is NLnet Labs' major benefactor.

Previous regular sources of non-subsidy income via the NSD and Unbound support contracts are now with Open Netlabs BV. 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, Infoblox, Afnic, DK Hostmaster A/S amounting to a total of 145 k€ income above budget.

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

Interest received amounted to 14 k€.

The following organizations are acknowledged for their generous contributions

6.5.2 Expenditure in 2016

The major expenditure categories of NLnet Labs in 2016 are staff, travel and housing. In January, we were at the budgeted staff of 9 persons (8.1 FTE). The total expenditure on staffing in 2016 is 629 k€. Housing and travel make up for another 95 k€ out of the total of 773 k€ expenditure (not included project costs).

From the ENGRIT designated reservation of 114 k€ at the start of 2015, we withdraw 60 k€ for the 0.5 FTE at NLnet Labs for the past two years (thus up to and including 2016). For the SAND project reservation, we transferred 35.5 k€ to Twente University for co-funding the SAND and DAS projects (co-funding with SIDN Labs and matched funding from NWO).

The H2020 LIGHTest project is partly pre-financed. The payment for the next reporting period has been assigned to a reservation in our balance sheet.

After making these reservations and valuations NLnet Labs had a positive result of 135 k€; 1 k€ is added to the general financial reserve (total of 569 k€ at the end of 2016) and 134 k€ to special-purpose reserves (total 300 k€ at the end of 2016).

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	3	**General Reserve**	569
Open Netlabs BV stock and loans	291	**Open Netlabs BV Business Development Fund**	330
Receivables	230	**Special purpose reserves**	300
Bank & Cash	772	**Current liabilities and accruals**	97
Total	1,296		1,296

Income				
	2015 actual (k€)	2016 actual (k€)	2016 budget (k€)	
NLnet Subsidy	337	0	0	
SIDN Subsidy	359	366	366	
Other Donations	155	381	215	
Consultancy and other Income	87	170	196	
NSD & Unbound Support	4	7	0	
Interest Income	17	14	15	
Sub Total	959	938	792	
Business Development Subsidy from NLnet	66	0	0	
Total	1,025	938	792	

Expenditure				
	2015 actual (k€)	2016 actual (k€)	2016 Budget (k€)	
Staff	588	621	603	
Housing	56	56	63	
Travel	25	47	68	
Depreciation	3	5	5	
Project Costs	50	51	0	
Other costs	59	44	53	
Sub Total	781	824	792	
Negative Result Open Netlabs	-233	-22	0	
Reservation Fund NLnet Business Development	66	0	0	
Project Reservations	-93	134	0	
Total	521	936	792	0

6.5.3 Budget for 2017

The 2017 is based on having 7.6 FTE we have budgeted a total expenditure of 832k€

In June, 2017 Stichting SIDN signed a five year contractual commitment to subsidize a substantial part of the expenditure needed to execute our chartered activities. For 2017, SIDN will cover 250 k€ in four quarterly grants of almost 62.5 k€. Additionally, SIDN committed 75 k€ on special projects subsidy for 2017. Other donations and subsidies from industry will account for 180 k€, funded projects (ICANN, NLnet, EU H2020) will account for 200 k€, and Open Netlabs will contribute about 50 k€ to NLnet Labs.

6.5.4 Financial Outlook

The year 2016 was different from all previous years in the way NLnet Labs was financed to achieve its mission and goals. The strategy for financial sustainability aims to work towards a situation where one part of the budget is secured via a longterm commitment via a grant of SIDN, one part from industrial partners, and one part via income generated by our fully-owned subsidiary Open Netlabs BV.

The business activities within Open Netlabs BV have generated an increased turnover in 2016. Current growth in income is primarily based on SLA support contracts and consultancy. For future growth in turnover and revenues, we will expand the activities of Open Netlabs into the development of new business and creating additional value. With the expected growth in revenues in the coming years, Open Netlabs will help to secure the continuity of the NLnet Labs Foundation.

7 Publications, Presentations and Reports

Publications

- RSSAC002v2: "***Advisory on Measurements of the Root Server System***", Akkerhuis as contributing ICANN RSSAC Caucus member, January 2016. https://www.icann.org/en/system/files/files/rssac-002-measurements-root-07jan16-en.pdf
- "***Root Zone KSK Rollover Plan***", Akkerhuis as contributing Design Team member, March 2016. https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf
- "***Technical Considerations for Internet Service Blocking and Filtering***", Barnes, Cooper, Kolkman, Thaler and Nordmark, March 2016. https://tools.ietf.org/html/rfc7754#page-33
- RSSAC002v3: "***Advisory on Measurements of the Root Server System***", Akkerhuis as contributing ICANN RSSAC Caucus member, June 2016. https://www.icann.org/en/system/files/files/rssac-002-measurements-root-06jun16-en.pdf
- SAC084: "***SSAC Comments on Guidelines for the Extended Process Similarity Review Panel for the IDN ccTLD Fast Track Process***", Akkerhuis as contributing ICANN SSAC member, August 2016. https://www.icann.org/en/system/files/files/sac-086-en.pdf
- SAC090: "***SSAC Advisory on the Stability of the Domain Namespace***", Akkerhuis as contributing ICANN SSAC member, December 2016. https://www.icann.org/en/system/files/files/sac-090-en.pdf

Invited Presentations

- "***From the Ground Up Security: DNS-based Security of the Internet Infrastructure***", Overeinder, JCSA16 – Journée du Conseil Scientifique de l'Afnic 2016, Paris, France, July 2016. https://www.afnic.fr/fr/l-afnic-en-bref/agenda/182/show/jcsa16-journee-du-conseil-scientifique-de-l-afnic-2016.html
- "***OpenDNSSEC 2.0 and Beyond***", Overeinder, Netnod autumn meeting 2016, Stockholm, Sweden, October 2016. http://www.netnod.se/sites/default/files/2016-12/Benno_Overeinder_Open_DNSSEC2_Beyond.pdf

Presentations

- "***Continuous Data-driven Analysis of Root Stability***", Overeinder and Hesselman, Root Stability Study Workshop, ICANN 55, Marrakech, Morocco, March 2016. https://meetings.icann.org/en/marrakech55/schedule/tue-root-stability-study/presentation-cdar-08mar16-en.pdf
- "***New gTLD Program Reviews and Related Activities***", Overeinder and others, panel discussion, ICANN 55, Marrakech, Morocco, March 2016. https://meetings.icann.org/en/marrakech55/schedule/mon-new-gtld-reviews
- "***Unbound QNAME Minimisation***", Dolmans, OARC 24, Buenos Aires, Argentina, March 2016. https://indico.dns-oarc.net/event/22/session/2/contribution/16/material/slides/0.pdf
- "***How we are developing a next generation DNS API for applications***", Toorop and Dickinson, OARC 24, Buenos Aires, Argentina, March 2016. https://indico.dns-oarc.net/event/22/session/8/contribution/19/material/slides/0.pdf
- "***DNSSEC Authentication Chain TLS extension***", Toorop, Hackathon at the IETF 95, Buenos Aires, Argentina, April 2016. https://www.ietf.org/proceedings/95/slides/slides-95-hackathon-13.pdf
- "***DNSSEC Authentication Chain TLS extension***", Toorop, TLS WG, IETF 95, Buenos Aires, Argentina, April 2016. https://www.ietf.org/proceedings/95/slides/slides-95-tls-3.pdf
- "***DNSSEC Authentication Chain TLS extension***", Toorop and Huque, Bits-n-Bites at the IETF95, Buenos Aires, Argentina, April 2016.
- "***ENGRIT: Extensible Next Generation Routing Information Toolset***", Konstantaras, Routing WG, RIPE 72, Copenhagen, Denmark, May 2016. https://ripe72.ripe.net/presentations/143-RIPE72_ENGRIT_SK.pdf

- "New gTLDs and the Stability of Root Service System", Akkerhuis, ENOG 11, Moscow, Russia, June 2016. https://www.enog.org/presentations/enog-11/167-cdar-enog.pdf
- "***QNAME Minimization in Unbound***", Dolmans, DNS WG, RIPE 72, Copenhagen, Denmark, May 2016. https://ripe72.ripe.net/wp-content/uploads/presentations/120-unbound_qnamemin_ripe72.pdf
- "***Stubby***", Toorop, Dickinson and Mankin, Lightning Talk, NANOG68, Dallas, TX, October 2016. https://www.nanog.org/sites/default/files/3_stubby-nanog68.pdf
- "***Impact of New gTLD on the Root System – Preliminary Results***", Akkerhuis, DNS WG, RIPE 73, October 2016. https://ripe73.ripe.net/presentations/147-cdar-ripe-73.pptx
- "***Unbound KSK Rollover***", Akkerhuis, DNSSEC Workshop, ICANN 57, Hyderabad, India, November 2016. http://schd.ws/hosted_files/icann572016/49/Jaap-Akkerhuis-Unbound-KSK-rollover.pdf
- "***From the Ground Up Security: DNS-based Security of the Internet***", Overeinder, SURFnet RoN+ + Meeting, Utrecht, The Netherlands, December 2016. https://surfdrive.surf.nl/files/index.php/s/og8zJW5aUdbbzpx/download?path=%2F&files=RoN2016_NLnetLabs_From_the_Ground_Up_Security_BennoOvereinder.pdf
-

Work in Progress

- "***A DANE Record and DNSSEC Authentication Chain Extension for TLS***", Shore, Barnes, Huque and Toorop, June 2016. https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension-01
- "***Root Stability Study Draft Report***", TNO, NLnet Labs and SIDN, October 2016. https://www.icann.org/en/system/files/files/cdar-deliverable-d1-root-stability-report-draft-27oct16-en.pdf

Student Reports

In 2016 we had one intern. The following thesis is published in 2016.

- "***A Hybrid System for Automatic Exchanges of Routing Information***", Maritsas, MSc thesis, University of Amsterdam, December 2016. https://www.nlnetlabs.nl/downloads/publications/rp2-stamatios-maritsas.pdf

Blog Posts

- "***I Can't Believe It's Not DNS!***", Schaeffer, August 2016. https://www.nlnetlabs.nl/blog/2016/08/16/i-cant-believe-its-not-dns/
- "***Client based filtering in Unbound***", Dolmans, December 2016. https://www.nlnetlabs.nl/blog/2016/12/22/client-based-filtering-in-unbound/

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/