NLnet Labs

Annual Report 2011

For an Open Internet

Lectori Salutem,

I am happy to present the NLnet Labs Annual report 2011. It is intended to present an overview of Labs' various activities and accomplishments.

Our activities have lead to accomplishments: We are recognized for our seminal role in the deployment of DNSSEC through creation of high-quality DNS software and tools, training, 'engineering'. In 2011, we added new gems to the DNSSEC toolbox; we released dnssec-trigger, and started to develop dnssexy.

Routing is another field where we are making a difference; we have mentored talented students through their graduation and have been providing a neutral, expert view in the various debates on routing security and its stability.

More generally, we have brought and shared our insights and expertise in many discussions about Internet Governance and technical management of the Internet, thereby contributing to a better understanding of the Internet Model.

I proudly present our activities and accomplishments in much more detail in the first half of the report.

In the second half of this report you can read that we would not have been able to do all this work without financial support. In addition to a €447,000 subsidy from the NLnet Labs foundation we received generous donations from Afnic, Comcast, Cisco, and Verisign Inc. We hope to welcome you to these ranks[1]!

--Olaf Kolkman, Director NLnet Labs.

NLnet Labs, For an Open Internet

The Internet's strength is that it allows people to connect and communicate with each other on the Internet without any concern for the infrastructure between end-nodes. This allows people to publish, provide services, to purchase, read, and consume in a global and truly free manner. The availability of open source and open standards is one of the success factors for protocols being deployed on the Internet (RFC5218).

NLnet Labs is a research and development group that focuses on developments in Internet technology that turn a network of networks into one Internet. Our activities can best be described as contributions that bridge the gap between theoretical insights and practical deployments, that bridge between technology and policy, and that are rooted in engineering and standardization. All activities for which public interest is often more pressing than commercial interest. It is our goal to contribute to the public interest by playing an active and important role in the development of open source

1 Contact info@NLnetLabs.nl for more information, or see http://www.nlnetlabs.nl/labs/contributors/

software, participating in the development of open standards, and disseminating knowledge through training, consultancy, and *evangineering*. NLnet Labs is globally recognized for its expertise in Internet system technology and architecture, in particular in DNS and DNSSEC. NLnet Labs' software is an important component of the Internet infrastructure. NLnet Labs plays a significant role in standards development. Dissemination of knowledge is realized through education and collaboration.

Stichting NLnet Labs was founded in 1999 by Stichting NLnet. The budget of NLnet Labs, a non-profit organization, is mainly based on a subsidy from Stichting NLnet. Stichting NLnet has provided a long-term commitment in the form of a subsidy contract such that NLnet Labs can guarantee support for the software it develops.

Area of Interest: DNS and DNSSEC

DNSSEC Evangineering

NLnet Labs believes that deployment of DNSSEC, a security extension to one of the protocols that is essential to the operation of the Internet, is the area where NLnet Labs makes the most significant difference. We contribute to global deployment by providing tools and software such as NSD, Unbound, ldns, Net::DNS, and OpenDNSSEC. Additionally, we contribute technical information, teach courses, and popularize the technology. The combination of solid engineering combined with spreading the word on the necessity of the technology is what we have come to call *evangineering*.

In 2011, the deployment of DNSSEC in top-level domains (TLD) saw further uptake. By the end of 2011, about one third of all TLDs were DNSSEC signed and their number continues to grow. In 2011, .COM was signed and major ISPs like Comcast deployed DNSSEC validation. NLnet Labs' persistent efforts have played a continuing role in these developments and NLnet Labs' software is used in many deployments.

Tools and Libraries

The Unbound Recursive Name Server

Unbound is a reference implementation of a validating caching resolver implementation with full DNSSEC support targeted for ISP and Enterprise environments.

The first version, a C implementation based on a Java implementation (developed by Verisign, Nominet, and Kirei), was released in 2008. Since then, Unbound is present in many BSD port distributions and Linux package repositories.

NLnet Labs is currently not in the position to offer 1st and 2nd line support, but collaborates with parties such as Men and Mice whose employees were trained and who have a 3rd line support contract with NLnet Labs.

Unbound is available at the dedicated website http://unbound.net, hosted and maintained by NLnet Labs.

> In 2011, the Unbound versions 1.4.8 to 1.4.14 have been released. During 2011, three bugs were discovered that we marked as vulnerabilities[2]

2 CVE-2011-1922 / VU#531342 in May 2011 and CVE-2011-4528 / VU#209659 for two vulnerabilities in December 2011

DNSSEC-trigger: Validation for End Users

In August 2011 a new project was started: DNSSEC Trigger.

One of the major hurdles in DNSSEC deployment is 'the last mile problem'; how to make sure that validation information gets to the application. There are roughly two approaches: bring validations as close to the applications as possible, or set up a trust relation with a validating recursive nameserver and have that machine do validation for you.

This project aims to explore the first approach by using Unbound on end-users' machines combined with a smart probe and auto-configuration program, DNSSEC-trigger.

To enable DNSSEC for the applications on the user's machine, DNSSEC-trigger will first test the DNS servers that were provided by DHCP for DNSSEC compliance. It has a number of fail-over mechanisms with an eventual fall back to using semi-public recursive nameservers that are reachable over port 80 and 443, impersonating HTTPS traffic.

Our goal is to offer regular users seamless DNSSEC operation in all realistic operating environments e.g., in the presence of captive payment portals. We believe that the experience gained with this method crossing the last mile will be useful for other initiatives, such as the development of DNSSEC APIs.

DNSSEC-trigger is implemented in POSIX C and uses ldns, and Unbound code components.

Version 0.1 was implemented in August 2011, at the end of 2011 version 0.9 was released. Version 0.9 included OSX and Windows binary installs (with easy user-friendly GUI installers) and Linux packages.

OpenDNSSEC: A DNSSEC Turnkey Solution

OpenDNSSEC is a collaborative project, which NLnet Labs has joined in 2008. The goal is to create a product that will handle zone signing and key management, and can be easily integrated in existing DNS deployments. The software consists of two core modules, called the enforcer and the signer engine. The enforcer implements DNSSEC policies and handles key management. The signer takes care of continuous (re-)signing. Since the start of the project, the development of the OpenDNSSEC signer is in hands of NLnet Labs. The next generation enforcer (enforcer NG) is developed by Rene Post (XPT.nl, funded by SURFnet) in collaboration with NLnet Labs. NLnet Labs commits to maintaining the code for both components on the long term.

Known users of OpenDNSSEC are SURFnet, CAcert, ICANN, as well as some top-level domain registries including .NL, .SE, .UK, .DK, .FI, .FR, and .LU.

OpenDNSSEC is distributed under a BSD license. For more information, see the website at http://www.OpenDNSSEC.org.

Signer Engine

An often heard critique on OpenDNSSEC was the extensive list of software dependencies required. This motivated NLnet Labs to develop a C-based version of the OpenDNSSEC signer, dropping all the Python related dependencies. Also, the new signer is designed for incremental signing, making it possible to support IXFR and Dynamic Update in the future.

> These developments are part of version 1.2.0, which was released January 2011, followed by a patch version release 1.2.1 in March 2011.

The 1.2 version of OpenDNSSEC did not yet make full use of the hardware acceleration, available on the provided HSM. A part of the signer was redesigned in order to support multiple threads on a HSM. The new design was capable of performing the maximum number of RSA operations on the Sun SCA6000 HSM. This performance improvement is part of version 1.3, which is the current stable release of OpenDNSSEC.

> The 1.3 version was succeeded with five patch version releases, the current version is 1.3.5.

Enforcer NG

Due to changed requirements and new insights, the design of the enforcer is reaching its limits. The current enforcer does not provide much flexibility in signing schemes. Also, it does not support algorithm rollover. Together with SURFnet, NLnet Labs has been working on a new design and implementation of this component. The release for the Enforcer NG is scheduled for 2012 and will deprecate the current implementation.

NSD, NLnet Labs Authoritative Name Server

The NLnet Labs Name Server Daemon (NSD) is an authoritative RFC compliant DNS name server. It was first conceived to allow for more genetic diversity for DNS server implementations used in the root-server system. NSD has been developed for operations in environments where speed, reliability, stability, and security are of high importance. NSD is currently used on some root servers such as the L and K root-servers. It is also in use by several top-level domain registries such as .NL, .DE, .BR, .SE, and .UK.

NLnet Labs commits to long term support of NSD. Not only will it announce the termination of support two years in advance, it also offers support contracts in three varieties.

NSD3

NSD3 is the stable version and can be found in almost all software repositories.

Some notable maintenance was done on NSD3. We included an option that results in faster zone transfer management (at the cost of some performance degradation for negative answers), and we have taken steps to minimize responses in order to reduce the number of truncated responses, and thus fall back to expensive TCP transport.

> In 2011, NSD versions 3.2.7, 3.2.8 and 3.2.9 were released, mostly dealing with small improvements and minor bug fixes. Version 3.2.9 also introduces two more relevant features, to perform better in some existing environments.

NSD4

The NSD3 software lacks support for environments that require dynamic provisioning of zones, as well as support for a high number of zones. In 2011, work has been started to develop NSD4, which is aimed at resolving these issues. NSD4 will have the ability to add and remove zones without any service interruption. NSD4 will be scalable with respect of the number of zones: it will be efficient for a few large zones to many small zones. NSD4 had five milestone releases in 2011, and development will be continued in 2012.

DNSSEC proxy (dnssexy)

Some organizations that deployed DNSSEC encountered issues which caused them to serve badly signed zones. RIPE NCC asked NLnet Labs to develop a solution to fortify DNSSEC availability, by preventing badly signed zones from being published. The DNSSEC proxy (dnssexy) project was started to inventory the requirements not only for RIPE NCC, but also for other interested parties, and provide a solution that satisfies them.

The resulting design consist of a software-program that operates as a bump-in-the-wire between a hidden master and public slaves. It receives DNS transfers from the hidden master, but only notifies the public slaves when all records are properly assessed by a modular and extensible framework.

Version 1 of dnssexy is based on a fork of NSD3 and facilitate a hook in between zone reception (via AXFR or IXFR) and serving. NSD3 already has the functionality to transfer and serve zones, with ACL if necessary. The hook will be used to call a program or a script with arguments and environment variables that provide information on the calling NSD3 instance, which zone should be assessed, and what has changed. The program will operate as a framework that schedules what checks to run in what order. The adapted version of NSD3 should already serve the zone to be assessed to and only to those checks.

By the end of 2011significant progress was made and a 2012 release of version 1 was planned. NLnet Labs envisions a second version of dnssexy that incorporates the experiences gained with version 1, but which uses the OpenDNSSEC adapters instead of NSD as a much more versatile DNS substrate.

The development of dnssexy version 1 is partly financed by the RIPE NCC and is available under a BSD license.

The ldns Software Library

Ldns is a C library aimed to simplify DNS programming. It allows developers to easily create software conforming to current RFCs and Internet Drafts. Ldns is used by other programs, such as drill, Unbound, and OpenDNSSEC, but also in software not originating from NLnet Labs, such as Dan Kaminsky's Phreebird, and other 3rd party tools that are actively used in DNSSEC deployments.

Ldns is often used as reference implementation for new DNSSEC protocol extensions. For example, ldns implements Elliptic Curve DSA for DNSSEC (draft-hoffman-dnssec-ecdsa-04) and is used for a reference implementation of the experimental NSEC4 mechanism(draft-gieben-nsec4-00). In October 2011, an interoperability problem (an ldns signed zone not validating) triggered modification of the standards documents on canonicalization of DNS names in the RDATA section of RRSIG resource records. Ldns followed the standard more strictly than deployed name server software, and the standard was adapted to match the resolvers behavior.

Numerous feature requests and bug reports testify for the community interest in ldns. The more noticeable changes are the groundwork for alternative output formats, a fix to make serial time arithmetics work on 32-bit systems, a DENIC sponsored fix for properly identifying glue, a GNU and BSD compatible Makefile and the contribution of the ldns python module.

Ldns is distributed under a BSD license.

In 2011, ldns saw four releases 1.6.8 - 1.6.11.

The Perl Net::DNS and Net::DNS::SEC Libraries

The maintenance responsibility for the Perl libraries Net::DNS and Net::DNS::SEC is a task that NLnet Labs started in 2005.

In 2011, Net::DNS version 0.67 was released containing many bug fixes. By the end of 2011, the release of version 0.68, containing a contribution for Internationalized Domain Names, was pending.

DNS Communities and Community building

Integrating Testing And Learning of Interface Automata

NLnet Labs decided to become a user committee member in the research project ‘Integrating Testing And Learning of Interface Automata’ (ITALIA). This research, proposed by the Radboud University Nijmegen, deals with the design of algorithms that will allow computers to learn complex state diagrams by providing inputs and observing outputs. The research objective of the ITALIA project is to further develop this technique and to construct a tool set that will allow us to learn, routinely and fully automatically, state machine models with up to 40 state variables. The project is unique in bringing together research on automata learning with research on machine learning, model-based testing, game theory and computer-aided verification.

DNS (including the DNSSEC transition) is considered to be a system whose normal behavior is deterministic, but which may exhibit nondeterministic behavior due to exceptions, and is therefore to be considered an ideal system for this research. As a user committee member, we provide help with this specific case study.

Port Maintenance

We maintain the FreeBSD ports of software products we develop. This allows us to get a good handle on completeness of the installation instructions. Besides it provides insight on the availability of, and dependencies on a typical installation environment. We do not maintain ports and equivalent distribution mechanisms (such as RPM and DEB packages) for other operating systems.

Area of Interest: Routing and Addressing

The activities for 2011 in inter-domain routing can be dissected in BGP modeling and simulation, and in BGP routing security.

In the past years, Maciek Wojciechowksi developed the BGP simulator, while Shaza Hanif used this BGP simulator to study the influence of Internet topology (actually AS topology) on BGP performance. For 2011, two students from the VU University Amsterdam worked for six months on two modeling and simulation projects: Adriana Szekeres and Alex Stefanescu.

The project of Adriana Szekeres was an evaluation study of multi-path BGP routing protocols. With BGP, changes in prefix reachability and the involved path exploration to find a new best path to a prefix destination (route convergence), can set off a period of suboptimal reachability for this specific prefix, either by suboptimal paths or the prefix is temporarily unreachable. To alleviate this problem, and to make BGP respond faster to broken interconnections between networks, multi-path BGP protocols are devised. For the study, Adriana Szekeres selected three multi-path BGP protocols from literature: Resilient BGP (R-BGP), Selective Announcement Multi-Process protocol (STAMP), and Yet Another Multi-path Routing protocol (YAMR). All three approaches try to solve the fast path fail-over and increased stability, but achieve this goal with different approaches. The three different approaches are implemented and simulated using our BGP simulation framework. The study made clear that the different protocols widely vary in the number of fail-over paths and the induced number of extra BGP update messages to find these fail-over paths. Remarkably, R-BGP is the most effective solution, but also the protocol with the least number of extra BGP update messages and fail-over paths: the fail-over paths found are “high quality” paths that are maximal disjoint. The project resulted in the successful completion of a MSc. thesis by Adriana Szekeres.

Alex Stefanescu studied the effectiveness of route security protocols under development in the IETF Secure Inter-Domain Routing (SIDR) working group. With the development of RPKI and route origin validation, and BPG Security (BGPsec), various deployment questions arise as these new additions may not interfere with the stability and availability of the routing system. To evaluate the impact of routing security mechanisms in securing routes and availability of network prefixes, Alex Stefanescu modeled and implemented RPKI with route origin validation and BGPsec in our BGP simulation framework. With this model, different deployment scenarios can be studied, and their effectiveness evaluated. For example, first simulation runs showed that only a small percentage of tier 1 and large tier 2 networks have to deploy routing security to secure about 95% of the Internet, while a bottom-up approach would require a large deployment percentage to achieve any significant effect. Unfortunately, Alex Stefanescu did not finish his thesis before the end of 2011. All practical work has been accomplished, but writing the thesis is still on-going.

NLnet Labs and SURFnet started a collaborative pilot study to gain experience with RPKI in an operational environment. With SURFnet, an RPKI infrastructure was setup to secure route origin for prefixes of the (experimental) SURFnet network. Interoperability of different software parts were tested, i.e., the RPKI software from rpki.net, and the validator and certificate authority software from RIPE NCC. In 2011, we ran also two successful RPKI workshops during the RIPE meetings. This project was concluded with a report (see publication list), and a best current practice (BCP) document that will be submitted to the IETF SIDR working group.

Area of Interest: IPv6

IPv4 depletion and IPv6 transition are topics that are of constant interest. Software developed by NLnet Labs has always supported IPv6 from its first design. Specific contributions are made mainly in the form of evangineering. Examples of that in 2011 are participation in:

- the organization of the successful Dutch activities surrounding IPv6 World Day on June 8th, 2011 in Amsterdam. On this day, large networks switched-on IPv6 connectivity for one day for all users to test availability and interoperability issues. NLnet Labs participated in the organization of an event on this day to promote IPv6 availability and usage. About 300 participants attended a mix of practical IPv6 tutorials, practical dos and don'ts sessions, deployment experiences, and presentation reflecting on strategic scenarios in successful implementation and roll-out of IPv6 in networks. For 2012 another event is planned on June 6th, “IPv6 World Launch”, but this time IPv6 should stay switched on.
- the IPv4 depletion ceremony in Miami in February 2011; an event that caught significant media attention.

Area or Interest: Knowledge, Outreach, and Participation

NLnet Labs personnel actively participates on the tangent of technology, governance, and public interests. NLnet Labs volunteers its staff in various community supporting positions. This section provides an overview.

Kolkman stepped down as chair of the Internet Architecture Board in March 2011 and continues as a regular member for the remainder of his term. As the IAB chair, he was ex-officio member of the IESG, the IAOC, and is an IETF Trustee. As the IAB's IANA Evolution program-lead, Kolkman contributed to the stewardship over the IANA functions for the Internet in general and the IETF in particular. He is co-editor of RFC6220 and was primary editor for the correspondence between the IAB and NTIA on the renewal of the IANA contract[3]. While on the IAB, Kolkman acts as the IAB observer to SSAC.

Kolkman served as Acting RFC Series Editor from March to December 2011.

At the ISOC Internet New Years Event 2011, Overeinder gave a lightning talk on "Internet Routing Security: What's Next?": a non-technical presentation to spark off interest on a subject not well-known to a large audience. Mekking presented the new years resolution for OpenDNSSEC, while Kolkman chaired the chairperson's debate at the same event.

In January, Kolkman and Overeinder were invited to talk at a FI-ISAC meeting at the Nederlandse Bank. FI-ISAC meetings are organized for large Dutch financial institutes to discuss Internet security issues. NLnet Labs was invited to present recent developments in routing security and DNS security.

Overeinder participated remotely in the CAIDA Workshop on BPG and Traceroute Data (http://www.caida.org/workshops/bgp-traceroute/). We presented our work on RPKI and route origin validation deployment scenarios.

Overeinder co-organized two RPKI tutorials at the RIPE meetings RIPE 62 and RIPE 63. Kolkman moderated an RPKI debate at the RIPE63 plenary.

Overeinder presented the NLnet Labs/SURFnet RPKI pilot study at the SURFnet Research on Networks (RoN) meeting in March, and an overview of Future Internet approaches and proposals at the SURFnet RoN meeting in November.

Mekking was member of the program committee for the NLUUG Najaarsconferentie, Kolkman was invited to talk about current DNSSEC developments. Overeinder gave two presentations: Securing Your Network From Being Hijacked, and Ins and Outs of Inter-Domain Routing Security. The first was practical oriented, while the latter provided details on the fundamentals of routing security (and the origins of routing insecurity).

Kolkman and Overeinder were invited to attend the ISOC Routing Security Roundtable in December 2011. Overeinder presented the results of the ENISA routing security study from 2010, updated with some new information and insights. The goal of the meeting was to make an inventory of routing security threats and risks, current methods for to mitigate threats, and what would be needed to improve on current practice.

3 https://www.iab.org/activities/programs/iana-evolution-program/

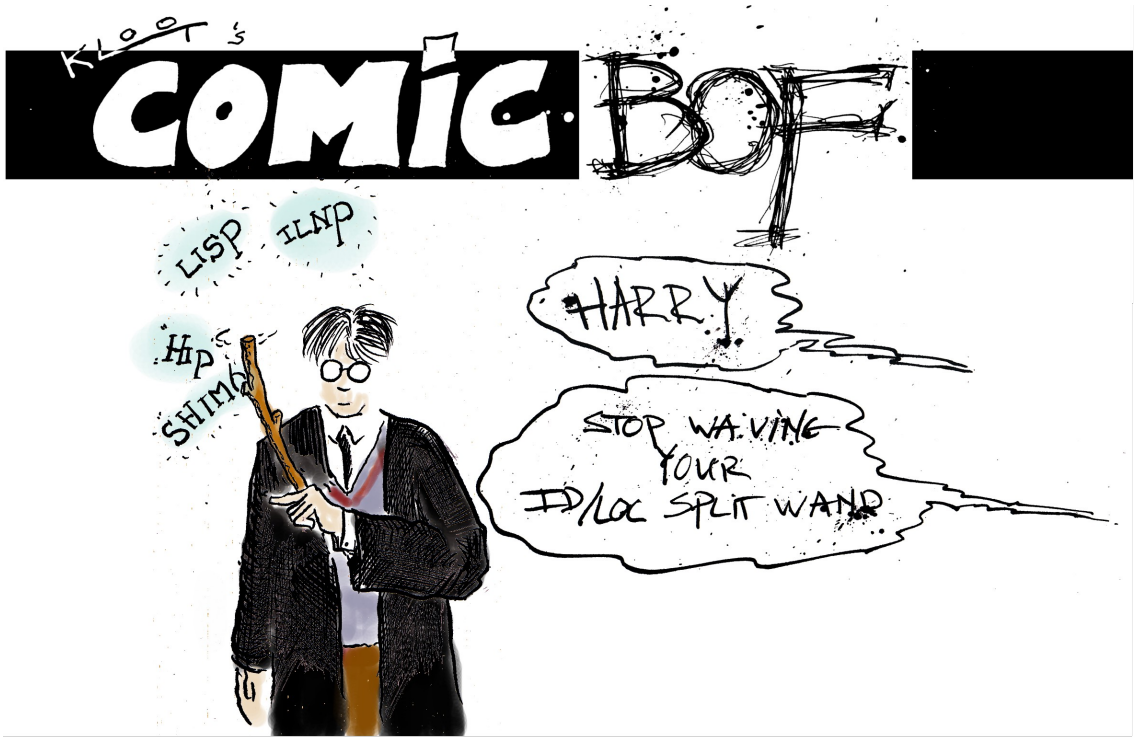
During 2011, Akkerhuis contributed as a paid consultant to ICANN for 1.5 days per month. As part of this role he is a member of the ISO 3166 Maintenance Agency, ISO's focal point for country codes and a candidate to become a Liaison type D for ICANN for the Working Group 2 of Technical committee 46 - Information and documentation[4]. Akkerhuis also participated in various activities of the ICANN ccNSO such as the ccNSO Study Group on Use of Names for Countries and Territories[5], the IDN PDP Working Group[6], and the Framework of Interpretation Working Group[7].

Akkerhuis en Kolkman are arbitrators for the RIPE NCC Conflict Arbitration procedure.

Akkerhuis is a member of ICANN's security and stability advisory committee SSAC and the Dutch IPv6 Task Force.

NLnet Labs has observer status in the Council of European Top Level Domain Registries (CENTR), is a member of OARC, the DNS Operations, Analysis, and Research Center (OARC), and a member of the DNSSEC Industry coalition. NLnet Labs continued to participate in the DNSSEC deployment group, that strives to coordinate global DNSSEC deployment efforts, is 'hosted' by Shinkuro, and funded by the US Department of Homeland Security

Furthermore, NLnet Labs staff has actively participated or tracked the work in the BEHAVE, DANE, DNSEXT, DNSOP, ENUM, SHIM6, IDR, SIDR, and GROW working groups, within the IETF, and the Routing Research Group, both in email discussions and during meetings. NLnet Labs staff is also participating in the RIPE meetings.



Work on LISP and other identifier locator split technologies did not get as much attention as previous years

4 http://www.iso.org/iso/iso_technical_committee?commid=48750
5 http://ccnso.icann.org/workinggroups/unctwg.htm
6 http://ccnso.icann.org/workinggroups/ipwg1.htm
7 http://ccnso.icann.org/workinggroups/foiwg.htm

The Future: Short and Medium Term

In this section we discuss the future areas of attention. In the section on Finances and Organization, we will be discussing the future of NLnet Lab's funding and possible organizational changes.

DNS

NLnet Labs will continue with a focus on DNS related activities.

DNS is one of the technologies on which virtually all applications on the Internet depend for their availability and —with initiatives like DANE[8] in combination with DNSSEC— on security. NLnet Labs develops software, tools, and expertise to improve the overall stability, security, and resiliency of the DNS.

We continue to extend our suite of software tools with comprehensive DNS management and control tools. Within that context, we are currently focusing on OpenDNSSEC and additional "Swiss army knife" tools that allow for troubleshooting and early warning, like dnssexy.

In 2011, we started developing NSD4 that is set out to support environments that have to support many zones in a dynamic fashion. In 2012, work on NSD4 will continue towards completion.

We continue to provide community support for NSD and Unbound, with a commitment to announce termination of such support at least two years in advance. This commitment provides users of our software business continuity, and thus contributing to the acceptance and dissemination of the technology.

Routing and Addressing

Stability and security of the routing system continues to be subject of interest.

We continue to use our routing simulation laboratory to test various hypothesis on why the background "noise" in the BGP control plane remains constant while the Internet has grown spectacularly in the past ten years and we intend to use the routing simulation laboratory in our collaboration with SIDN Labs. For instance, in assessing whether failure in anycast announcements lead to instabilities.

Routing security, based on the utility of a routing public key infrastructure (RPKI) that is currently being deployed by the regional Internet registries, continues to be another item of interest. While alternatives like ROVER[9] are being suggested, fundamental questions remain: The hierarchical structure of the RPKI (and ROVER) is at odds with the mesh-type infrastructure that characterizes BGP and Internet routing operations. We want to contribute to research and development through experimentation, deployment, and documentation of RPKI based methodologies for source and path validation, and their alternatives. For example, currently we are assessing whether there is sufficient interest for a generic tool base inspired on the obsolete IRR toolset[10].

And more

NLnet Labs' expertise on Internet System technology and architecture, focuses on the technologies in the 'waist of the hourglass': DNS, IP, and Routing. Technologies which benefit the users of the Internet at large, that provide security, stability, scalability, and reliance, and technologies that are crucial for further growth and maintaining openness of the Internet.

8 http://tools.ietf.org/wg/dane
9 http://tools.ietf.org/html/draft-gersch-grow-revdns-bgp-00
10 http://www.isc.org/software/irrtoolset

The IP protocol suite, in particular the openness of its addressing and routing technology, is key to the successful evolution of the Internet. However, there are several challenges in the near future to allow the network to scale for the next billions of users and their devices. Because scaling issues are a threat to the open nature of the Internet, NLnet Labs looks at the role scaling issues play in the Internet architecture. Both by investigating the need to create solutions and in investigating practical and deployable approaches that can solve mobility, scaling, and multihoming issues. As an independent expertise center on Internet architecture and technology with considerable experience in Internet Governance issues, NLnet Labs has acquired recognition in the field with a proven track record. This leads to corresponding responsibilities such as the involvement in several workshops about Internet Government issues, organized by the ministry of Economic affairs, Kolkman's role as IAB chair, and Akkerhuis' involvement in ICANN.

Long term outlook

NLnet Labs strives to be a technical expertise center that promotes the core values of an open, innovative, and collaborative set of networks: the Internet.

To that end NLnet Labs will continue to find pragmatic approaches to bridge between theory and practical deployment of Internet protocols. The specialism and expertise of the team determine which avenues are pursued. Exploration of new emerging areas relevant to the future of the Internet that fuel potential collaborations with other parties are inherent to the role NLnet Labs plays in the field. One of the main selection criteria for projects is whether our contribution makes a difference, whether our participation serves public interest and relates to an open and innovative Internet environment available to all.

NLnet Labs organization and finance

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.

Seven board meetings took place in the year 2011. Olaf Kolkman participated in the board meetings in his role of Director of NLnet Labs.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€551 for 2011). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2011	name	function	end of term
	Frances Brazier	secretary	December 28, 2014
	Frans Kollee	member	April 19, 2014
	Wytze van der Raay	treasurer	December 28, 2013
	Leo Willems	chair	February 1, 2013
	Ted Lindgreen	member	January 2012

Director and Board Member Additional Functions in 2011

Frances Brazier	Frans Kollee	Ted Lindgreen	Wytze van der Raay	Leo Willems	Olaf Kolkman
Professor Engineering Systems Foundations at the Technische Universiteit Delft (TU Delft)	Senior security consultant Madison Gurkha	none	Team leader CAcert critical system administrators	Owner TUNIX Digital Security. Member of the board of Stichting IT Projecten (StitPro).	Chair (until March 2011) and member of Internet Architecture Board
Vice-chair of the board of Landelijk Netwerk Vrouwelijke Hoog leraren (LNVH)					Until March 2011: Ex-officio member of the Internet Engineering Steering Group, the IETF Administrative Oversight Committee, and an IETF Trustee Arbiter for the RIPE NCC Conflict Arbitration Procedure

Staff

NLnet Labs employed seven people in 2011: Jaap Akkerhuis, Olaf Kolkman (director), Wouter Wijngaards, Benno Overeinder, Matthijs Mekking, Willem Toorop (per January 2011), and Yuri Schaeffer. 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.

Adriana Szekeres and Alex Stefanescu visited NLnet Labs for 6 month to perform research for their master-thesis study at the Vrije Universiteit Amsterdam.

Finances are administered by Patricia Otter of the Stichting NLnet.

Offices

NLnet Labs resided in Matrix 1 ever since its incubation in 1999. End 2010, the building was bought by SARA and in May 2011, NLnet Labs moved to another building on the Amsterdam Science Park, Matrix II.

Finances

Stichting NLnet Labs primarily finances its projects and activities from grants obtained from its parent organization Stichting NLnet. The long term financial commitment of NLnet towards NLnet labs has been codified since 2007 in a subsidy contract. In 2010 NLnet Labs was given notice that because of uncertainty of available funding, that contract is terminated as of Jan 1, 2016.

A second means of income are subsidies and donations by other parties. NLnet Labs has developed a sponsor agreement. For 2011, we would like to acknowledge AFNIC, Comcast, Cisco and Verisign for their generous support.

In addition, income may be obtained by providing Open Source Internet based consultancy and/or programming services to third parties. Unbound and NSD support contracts were sources of additional income in 2011 in the latter category.

NLnet Labs Acknowledges

See http://www.nlnetlabs.nl/labs/contributors/ for more information.

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.

Income in 2011

At the end of 2010, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2011, with a total of € 650,300. Based on this budget and the expected consultancy income, a grant was requested from Stichting NLnet for € 542,000 during 2011. Stichting NLnet allocated these funds for 2011, to be received by NLnet Labs on a quarterly basis, € 135,500 per quarter. By the end of 2011 it became obvious that the requested budget would be more than needed to cover 2011's costs. This was mainly due to unforeseen consultancy and subsidy income. At the end of the year, € 95,000 subsidy could thus be returned to NLnet. The net result is that during 2011, Stichting NLnet Labs received a total of €447,000 from Stichting NLnet and a total of € 92,306 in donations (from Verisign, Cisco, Comcast, and AFNIC).

The consultancy contract with ICANN from April 2005 was continued in 2011 (1.5 days per month). Besides, NLnet Labs offers support contracts for NSD and Unbound. Finally, NLnet Labs received a compensation for the bandwidth used by the secondary server for .PT. The total income for consultancy and support in 2011 came to € 87,957.The only other significant source of income during 2011 was interest derived from a savings account used to deposit funds temporarily. This amounted to € 2,480.

Expenditure in 2011

The major expenditure categories of NLnet Labs in 2011 are staff (total of 7 persons), travel and housing. Contributing to € 584,762 out of a total of € 629,398 of total costs.

Over 2011 NLnet Labs had a positive result of € 345. The financial reserve at the start of 2012 is € 67,535

The NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam on 29 May 2012.

Budget for 2012

The 2012 budget has been drawn up in October 2011. The expenditure is based on having 6 staff and 1 support engineer (totaling 6.7 FTE). We have budgeted a total expenditure of € 646,320.

NLnet Labs expects to receive about € 16.500 from consulting activities, € 27,000 though donations, and € 64,500 from support contracts.

On January 20, 2012 Stichting SIDN signed a five year contract committing to subsidizing 50% of the expenditure needed to execute our chartered activities. SIDN and NLnet will jointly cover € 536,520 in four quarterly grants of € 134,130.

6.3.5 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. Stichting NLnet has indicated it is willing and able to subsidize specific plans towards business development or other initiatives.

Stichting NLnet and Stichting SIDN are NLnet Labs' major benefactors.

Income 2011			
	2010 actual	**2011 actual**	**2011 budget**
NLnet Subsidy	402,000	447,000	542,000
Other Donations	31,017	92,306	33,000
Consultancy Income	86,650	19,250	16,500
NSD & Unbound Support	51,538	66,456	57,000
Interest Income	1,920	2,480	1,800
Other	0	2,250	0
Total	573,125	629,743	650,300

Expenditure 2011			
	2010 actual	**2011 actual**	**2011 budget**
Staff	450,105	506,490	515,400
Housing	39,598	36,225	43,300
Travel	43,453	42,047	48,000
Depreciation	3,515	2,899	4,800
Other costs	35,564	41,737	39,240
Total	572,235	629,398	650,740

2012 Budget		
	2011 actual	**2012 budget**
Staff	506,490	515,400
Housing	36,225	37.860
Travel	42,047	48,000
Depreciation	2899	4,200
Other costs	41,737	40,860
Total	629,398	646,320

Publications, Presentations, and Reports

- Adriana Szekeres, Multi-Path Inter-Domain Routing: The Impact on BGP's Scalability, Stability, and Resilience to Link Failures, Msc. thesis, Department of Computer Science, VU University Amsterdam, August 2011.
- Jac Kloots, François Kooman, and Benno Overeinder, Resource PKI (RPKI): Design and Operation of the Infrastructure, Technical Report, Gigaport3 deliverable FIP-11-02, SURFnet, Utrecht, The Netherlands, July 2011.
- Gieben, M., Mekking, W.M., "Authenticated Denial of Existence in the DNS", SIDN Labs document 2011/0x01-v1, November 2011. https://www.sidn.nl/fileadmin/docs/PDF-files_UK/wp-2011-0x01-v2.pdf

Work in progress

In this section we present Internet Drafts with NLnet Labs' authors or editors on which work has actively been done. The latest version published in 2011 is referenced.

- Architectural Considerations on Application Features in the DNS, Peterson, Kolkman, Tschofenig, and Aboba, http://tools.ietf.org/html/draft-iab-dns-applications-03
- RFC Editor Model (Version 2), Kolkman and Halpern, http://tools.ietf.org/html/draft-iab-rfc-editor-model-v2-02
- DNAME Redirection in the DNS, Rose and Wijngaards, http://tools.ietf.org/html/draft-ietf-dnsext-rfc2672bis-dname-25
- DNSSEC Operational Practices, Version 2, Kolkman and Mekking, http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis-08
- DNSSEC Key Timing Considerations Follow-Up, Mekking, http://tools.ietf.org/id/draft-mekking-dnsop-dnssec-key-timing-bis
- Elliptic Curve DSA for DNSSEC, Hoffman and Wijngaards, http://tools.ietf.org/html/draft-ietf-dnsext-ecdsa-07

Conferences and other contributions

ISOC Internet New Years Event 2011, Amsterdam, NL, January 2011.
- Overeinder, Internet Routing Security: What's Next?
- Mekking, "OpenDNSSEC New Years Resolutions" http://nlnetlabs.nl/downloads/presentations/opendnssec-20110113.pdf

FI-ISAC meeting, Amsterdam, The Netherlands, January 2011.
- Overeinder, Internet Routing Security: An overview of risks and mitigation

I* leadership meeting and the ICANN IPv4 exhaustion ceremony, Miami, FL, US, 3-4 February, 2011.

Combined US & EU Law Enforcement meeting, Brussel, BE, 23-25 February 2011
- Attended by Akkerhuis.

SURFnet Research on Networks meeting, Utrecht, NL, March 2011.
- Overeinder, Securing Inter-Domain Routing: Step by Step,

ICANN 61, San Francisco, CA, US 23-28 March 2011.
- Attended by Akkerhuis.

INEX member meeting, Dublin, IR, 24 March 2011.
- Kolkman, The current state of affairs with DNSSEC http://media.heanet.ie/page/5ea23bb7b67c424799c45fcdf603b072

IETF 80, Prague, CZ, 27 March – 1 April 2011
- Mekking presented OpenDNSSEC 1.3 at the IEPG meeting. http://iepg.org/2011-03-ietf80/iepg80-opendnssec.pdf
- Mekking proposed a follow-up on DNSSEC Key Timing Considerations in the DNSOP meeting. Mekking worked on RFC4641bis http://www.ietf.org/proceedings/80/slides/dnsop-2.pdf.
- Attended by Akkerhuis, Kolkman, Mekking, Overeinder.

Securing and Trusting Internet Names, SATIN 2011, Teddington UK, 4-5 April 2011.
- Attended by Kolkman.

Internet Freedom Conference - From Principles to Global Treaty Law?, Council of Europe, Brussels, BE, 18-19 April 2011.
- Kolkman participated in the panel on Internet Governance Principles.

IAB Retreat, Boston, Sterling, VA, US, 12-13 May, 2011
- Attended by Kolkman.

DNS Root Signing Ceremony EAST, Culpeper, VA, US, May 11, 2011.
- Attended by Kolkman as Trusted Community Representative.

RIPE 62, Amsterdam, NL, May 2011.
- Szekeres, Multi-/Fail-Over Path Routing, Routing Working Group.
- Stefanescu, Effect of RPKI Deployment Scenarios, Routing Working Group.
- Attended by Akkerhuis, Kolkman, Mekking, Stefanescu, and Szekeres.
- Overeinder co-organized an RPKI workshop.

ENOG, Moscow, RU, 8 June 2011
- Attended by Akkerhuis.

World IPv6 Day, Amsterdam, NL, 8 June 2011
- Overeinder participated in the organizing committee.
- Kolkman presented a keynote "IPv6 a world without it".
- Kolkman was member of the 'IPv6 application challenge' jury.

IETF 81, Quebec City, CA, 24-29 July 2011
- Mekking presented on DNSSEC Key Timing Considerations in the DNS OPS working group http://www.ietf.org/proceedings/81/slides/dnsop-2.pdf

BIND10 Open Day, Amsterdam, NL. 29 August 2011
- Attended by Mekking.

CAIDA Workshop on BGP and Traceroute Data, August 2011.
- Overeinder, Effects of RPKI Deployment on BGP Security,

ICANN SSAC Retreat, Washington D.C., US, 5-8 September 2011.
- Akkerhuis attended.

LACNIC XVI, Internet On, lacnog 2011, Buenos Aires, AR, 3-7 October.
- Kolkman gave a DNSSEC tutorial http://lacnic.net/en/eventos/lacnicxvi/agenda/tutoriales.html
- Kolkman "Keynote Presentation/Musings on Diginotar, Dane, and DNSSEC", http://youtu.be/Fr21e-WueYA
- Kolkman "NLnet Labs Software and OpenDNSSEC Update" http://lacnic.net/documentos/lacnicxvi/jueves/03-NLnet-Labs-Software.pdf
- Kolkman, "IPv4 as a Strategy, Meat and Greed Consultants" in Geoff Huston's "IPv4 Address Exhaustion: A Progress Report", http://lacnic.net/documentos/lacnicxvi/viernes/04-Huston-2011-10-06-exhaustion.pdf

NLUUG Najaarsconferentie 2011, 20 October 2011.
- Mekking was a member of the program committee.
- Kolkman, DNSSEC: Where do we stand?
- Overeinder and François Kooman, Securing Your Network From Being Hijacked.
- Overeinder, The Ins and Outs of Routing Security.

3rd Annual Global Symposium on DNS Security, Stability, and Resiliency, Rome, IT, 28-30 October, 2011, http://www.gcsec.org/sites/default/files/files/DNS_SSR3_REPORT_20120210.pdf
- Attended by Akkerhuis.

RIPE63, Vienna, Austria, 31 October-4 November 2011
- Overeinder co-organized a n RPKI workshop.
- Schaeffer presented Enforcer work to OpenDNSSEC Architecture Board.
- Attended by Akkerhuis, Kolkman, Overeinder, Schaeffer.

OpenDNSSEC developers meeting, Stockholm, Sweden 10-11 November 2011.
- Attended by Mekking, and Schaeffer.

IETF 82, Taipei, TW, 13 – 18 November, 2011.
- Attended by Kolkman, and Akkerhuis.

I* Leadership Retreat, Miami, FL, US, 29 November, 1 December, 2011.
- Attended by Kolkman.

ISO 3166 Maintenance Agency meeting, Geneva, CH, 1 December 2011.
- Attended by Akkerhuis.

ISOC Routing Security Roundtable, Amsterdam, The Netherlands, December 2011.
- Overeinder, Inter-domain Routing Security—Stocktaking, state-of-the-art, and future perspectives,
- Attended by Kolkman and Overeinder.

NLnet Labs

Science Park 400, 1098 XH Amsterdam

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