NLNET**LABS**

ANNUAL REPORT 2019

Table of Contents

Welcome

In your hands you have the annual report of our activities in 2019. Officially established in December 1999, NLnet Labs will reach its 20th birthday this year. Twenty years open-source software development, applied research and contributions to open Internet standards. And although the world and the Internet have changed in the past years, not our goal and mission to work on the stability and security of an open Internet infrastructure and the privacy of end users.

In recent years we have, in addition to our DNS software development & research activities, created a strong group with talented software & research engineers to work on routing security. For our well-known DNS software NSD, Unbound and OpenDNSSEC we have made regular bug fixes and new functionality available, and with this the continued support of reliable software that is relevant to the industry. The routing security software, Krill and Routinator, which we have developed in the last two years, already receives serious traction and is used in different networks. These new software products complement our existing software nicely in supporting a stable and secure Internet infrastructure.

NLnet Labs is typically an R&D organisation, and the "R" of research is taken seriously. Our colleagues published a number of academic papers and collaborated with well-known researchers from universities and research organisations. We also presented our results at various venues, both in academic and network operations communities. We have also played an important role in the organisation of the Internet Measurements Conference 2019 (IMC 2019) and sponsored the event.

The new activities and ambitions can only be realised with talented professionals. In 2019 we were successful to grow modest with a software engineer to strengthen our DNS team and a researcher/software engineer on the topic of routing security.

The financial numbers show continuity and sustainability. NLnet Labs is a non-profit and the financing of our organisation consists of gifts, project grants, sponsored software features development and, via our wholly-owned subsidiary Open Netlabs, also support contracts.

In summary, when realising our mission and goals, NLnet Labs has made a difference to the global Internet in 2019. We developed open-source software, contributed to open Internet standards, collaborated in research projects and shared knowledge with the community. And all with passion and dedication!

Enjoy reading our report!

Benno Overeinder
Managing Director NLnet Labs

About NLnet Labs

NLnet Labs is a not-for-profit foundation, founded in 1999. Over the past 20 years our mission remains to develop open source software and open standards for the benefit of the Internet, and to perform applied research on Internet protocols. We focus our efforts particularly on the Domain Name System and inter-domain routing. NLnet Labs work supports the robustness, security and reliability of the Internet and safeguards the privacy of its users.

To accomplish our mission, we collaborate with key players in the Internet around the world. Organisations we work with include the Internet Engineering Task Force (IETF), the Regional Internet Registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN), leading Top Level Domain (TLD) operators, the International Standards Organisation (ISO), the Internet Society (ISOC), as well as a wide variety of others in the field, ranging from individual researchers to major industry actors.

NLnet Labs plays a leading role in promoting technologies that stimulate trust, security, privacy, scalability and the global nature of the Internet. Our peers see us as a major stakeholder in the creation and use of open standards and open software. We are leading experts on core Internet technologies, specifically the DNS and routing.

We are a lightweight organisation with a team of around fourteen people, consisting almost exclusively of developers and researchers, with minimal overhead. We attract talented people who want to make a difference in the well-being of the Internet, with a profound belief in open source and open standards.

We create powerful and professional tools that are used throughout the Internet industry, ranging from DNS root servers at the core of the Internet to small embedded devices running a secure recursive resolver. Our software is used for signing and validation operations in both routing and DNS security applications.

Our researchers pioneer new technologies, help craft future standards and build prototypes of technologies that promise to improve the Internet. We increase understanding of the Internet by studying its fundamental building blocks. By actively participating in both worlds, we bridge the gap between academia and industry.

Our expertise and advice is widely recognised by policy-making bodies, including regulators and governments. We advise on public policy decisions that affect the security and privacy of Internet users across the globe, as well as the stability of the Internet itself.

While users may not see it on the outside, we proudly say: **the Internet runs on NLnet Labs!**

Software Development

At a glance

Over the course of 2019, our software developers worked hard on new features for our existing DNS and RPKI projects, with seven releases for Unbound, six for NSD, three for OpenDNSSEC and a whopping twelve releases of Routinator, which is becoming a mature product very fast now. In addition to this, our developers created a brand new member of the NLnet Labs family that saw its first release in 2019: our Krill RPKI CA implementation.

Our DNS library, LDNS had a big bug fixing release in 2019, thanks to efforts both from our community and our developers. Other community project we contribute to also saw activity in 2019, with three releases of Net::DNS and two releases of getdns/Stubby.

The remainder of this section provides a more detailed overview of highlights for our various projects.

DNS(SEC) Software Projects

Unbound

In 2019, NLnet Labs participated in DNS Flag Day, a collaborative effort of the DNS implementers and operator community. As part of this, we released a version of Unbound in February that remove all EDNS0 workarounds. This marked a major change in behaviour and led to a bump in minor version number to 1.9.0.

A major milestone in 2019 was a security audit on the Unbound code bases performed by German security company X41 D-Sec funded by the Open Source Technology Improvement Fund (OSTIF). During the audit, the security researchers discovered a serious flaw in the IPSec command module that led to a CVE. All of the major and minor findings from the audit team were addressed in Unbound 1.9.4 - 1.9.6. We are very grateful to OSTIF for funding the audit and X41 D-Sec for their work and the professional manner in which they helped us address the issues that were discovered. Thanks to this audit, Unbound is now even more secure! [Further reading: OSTIF blogpost, X41 D-Sec blogpost]

Other major features added in 2019 include support for DNS transfer over TLS (AXFR-over-TLS, or XoT for short) and support for fully static building of Unbound.
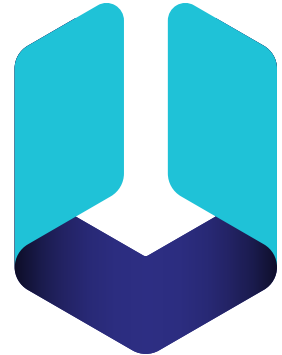
NSD

NSD's ability to limit the abusive impact of ANY queries was further extended in 2019 with the introduction of very minimal UDP responses to ANY queries. We also extended NSD with support for TCP Fast Open, to improve TCP performance and support for TLS on a user-defined port (with thanks to Sara Dickinson for both patches).

Over the course of the year there were also numerous minor bug fixes, many of which were contributed by community members.

For 2020 we have some exciting new developments in the pipeline that were started in 2019, which will further improve NSD's performance, keeping it at the forefront of high-performance DNS servers!

OpenDNSSEC

In 2019 we ended support for OpenDNSSEC 1.4 and announced that version 2.1 would be the de-facto supported version.

There were three releases of OpenDNSSEC 2.1 over the course of 2019, most of which focused on fixing minor issues discovered by our community after migrating to 2.1 from earlier versions of OpenDNSSEC.

Further reading: blogpost about the end-of-life of OpenDNSSEC 1.4

SoftHSM

The SoftHSM project, which NLnet Labs has made contributions to in the past, was incorporated as a project under the Commons Conservancy in 2019. The long-term goal of this move is to keep the project sustainable and to allow new partners to make significant contributions to the project. Exciting new features in the pipeline that are expected to become available from 2020 onward is support for "real" hardware features, such as secure enclaves based on Open Enclave.

DNS(SEC) Libraries

LDNS

Our general purpose C-language DNS library, LDNS, saw one release in 2019. This release contained a long list of bugfixes, most of which were contributed by our community. For 2020, we will continue maintenance of LDNS, without any plans for major changes in the foreseeable future.

getdns and Stubby

The getdns project brings a modern DNS API to applications with a number of language bindings, and Stubby, which is based on getdns, provides a local privacy-aware DNS resolver on UNIX-like systems. A binary port of Stubby for Windows is also distributed by the project. In 2019, getdns/Stubby had two releases. A major highlight is support for GnuTLS as cryptographic library, next to OpenSSL. Another major development that was started in 2019 is the switch to CMake as build system. At the end of the year, a first beta was released that uses this build system, and we expect a full release in 2020.

Net::DNS(::SEC)

NLnet Labs is a long time contributor and maintainer of the Net::DNS::(SEC) library that supports DNS functionality in the Perl scripting language. Over 2019, no major changes were made to the library. Over the course of the year, three versions of Net::DNS::(SEC) were released, fixing various bugs and bringing certain features (such as TSIG support) more in line with how other DNS implementations do this.

Domain Crate

Since 2018, NLnet Labs also has an experimental DNS(SEC) library for the Rust programming language: the domain crate. In 2019, this implementation gained experimental support for DNSSEC signing and was refactored to allow more flexible data management. We will continue gradual development of this library over the course of 2020.

Routing Software

In the summer of 2018 we announced our plans to develop a comprehensive toolset for Resource Public Key Infrastructure (RPKI), a technology aimed at making the Border Gateway Protocol (BGP) more secure.

RPKI is based on open standards and works by providing network operators a way to perform Route Origin Validation. Using the system, the legitimate holder of a block of IP addresses can make an authoritative statement, called a Route Origin Attestation (ROA), about which Autonomous System (AS) is authorised to originate their IP prefix in BGP. In turn, other network operators can download and validate these statements and make routing decisions based on them.

In 2019, the development of our routing software portfolio kicked in to high gear. RPKI Relying Party software Routinator 3000 had no less than 16 releases, and RPKI Certificate Authority software Krill had its production launch after three beta releases.

Project Funding

One of the reasons we could develop our RPKI toolset at full force is because several organisation in the industry decided to support us, either financially or with infrastructure. The National Internet Registry of Brazil, NIC.br, pledged to support the development of Krill and Routinator for two years, enabling us to work on the toolset with dedicated, full time staff. The RIPE NCC Community Projects Fund and the Mozilla Open Source Support Fund also contributed funding to the project.

Furthermore, DigitalOcean provided us with their cloud platform free of charge so we could set up an automated test platform for the software using virtual router software donated by Cisco, Juniper and Nokia.

All of these factors combined allowed us to full focus on what we do best: write awesome software.
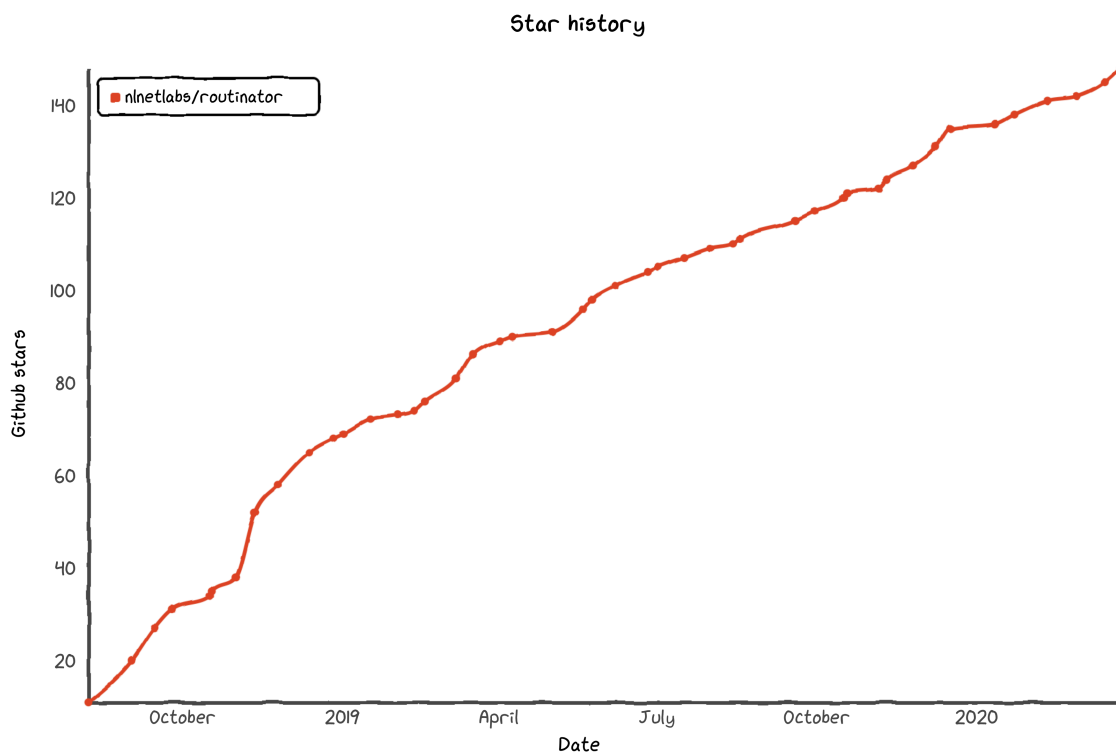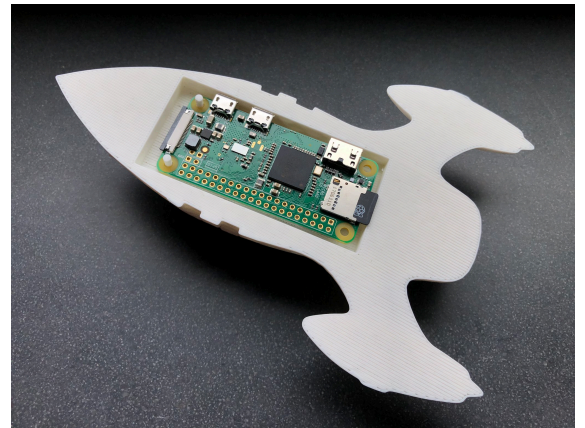
Routinator

Routinator is Relying Party software, also known as an RPKI Validator. Operators can use it to download and validate the global RPKI data set and feed the result into their routers, or use it elsewhere in the BGP decision making process.

Routinator connects to the Trust Anchors of the five Regional Internet Registries (RIRs) — APNIC, AFRINIC, ARIN, LACNIC and RIPE NCC — downloads all of the cryptographic material in their repositories and validates the signatures. It can feed the validated information to hardware routers supporting Route Origin Validation such as Juniper, Cisco and Nokia, as well as serving software solutions like BIRD and OpenBGPD. Alternatively, Routinator can output the validated data in a number of useful formats, such as CSV, JSON and RPSL.

After several beta releases allowing people to try out Routinator, the first version, named 0.1.0 'Godspeed!', was released at the in February. The software really did get off to a flying start, because in the same month AT&T announced at NANOG 78 that they were going to drop RPKI Invalid route announcements, using Routinator as one of the tools to achieve this.

Further traction was gained at the RIPE NCC RPKI Deployathon in March, where various network operators from around the globe got to try out Routinator and provide feedback on the initial version.

By May, Routinator 0.3.0 was out with RTR support, a Docker container, OpenBGPD support and an HTTP service with a Prometheus endpoint. By then, AMS-IX, DE-CIX, Wikimedia, XS4ALL, the BGPMon service and many more organisations announced the adoption of Routinator for their RPKI deployment.

NLnet Labs also released Gantry, a tool for deploying and testing network routers in the cloud. This enabled automated testing of Routinator releases possible with a wide variety of virtual routers from Nokia, Juniper and Cisco, as well as software solutions such as BIRD, VyOS and FRR.

Over the summer, a lot of effort was put into making Routinator feature complete. An API was added in version 0.5.0 and support for the RPKI Repository Delta Protocol (RRDP) was added in 0.6.0. The latter enables Routinator to fetch data using HTTPS instead of rsync, making the system faster and more robust. This release coincided with the milestone of 100,000 Validated

ROA Payloads being published in various RPKI repositories all over the world, making this addition all the more relevant.

Routinator was voted 'best validator' during the recent APNIC 48 meeting. Around the same time Telia, the world's largest Tier 1 carrier, announced their adoption of RPKI using Routinator as their weapon of choice.

Add Krill branding files

Alex Band authored 3 months ago

🖼 **Krill_Logo_Red.svg** 769 KB

Krill

With Krill, operators can generate and publish RPKI cryptographic material to authorise their BGP announcements. Up until now, operators were largely dependent on the hosted RPKI systems that each of the five Regional Internet Registries (RIRs) provide. Krill lets organisations run RPKI on their own systems as a child of one or more RIRs. It can also run under a different parent, such as a National Internet Registry (NIR), and, in turn, act as a parent for other organisations.

The implementation will support running the CA both upwards and downwards. Upwards means that operators can have multiple parents, such as ARIN, RIPE NCC, etc., simultaneously and transparently. Downwards means that the CA can delegate to child organisations or customers who, in turn, run their own CA. This makes Krill ideal for National Internet Registries and Enterprises.

A publication server is included in Krill, but can also be run as an independent component. This means organisations can host published certificates and ROAs themselves, or let a third party, such as a Content Delivery Network, do it on their behalf.

Krill is intended for:

- Organisations which do not want to rely on the web interface of the hosted systems that the RIRs offer, but require RPKI management that is integrated with their own systems

- Organisations that need to be able to delegate RPKI to their customers or different business units, so that that they can run their own CA and manage ROAs themselves

- Organisations that manage address space from multiple RIRs. Using Krill, they can manage all ROAs for all resources seamlessly within one system

- Organisations who want to be operationally independent from their parent RIR, such as NIRs or Enterprises

Major architecting and development of Krill was done throughout 2019, which resulted in the the first release, 0.1.0 'A View to a Krill' in September. This version was aimed at interoperability testing with the five Regional Internet Registries.

A new major release followed roughly every four weeks, adding and refining the functionality to bring Krill to a production grade solution. This culminated in release 0.4.0 'The Krill Factor' in December. At the GTER48 event in São Paulo, Brazil, NIC.br launched RPKI as a production

service to their members, powered by Krill. In the following days, more than 50 members set up RPKI using Krill, giving the software a flying start.

RPKI Analytics

To help the Internet community understand the uptake, effects and quality of RPKI deployment, we have written an analytics tool offering insight and assistance with troubleshooting.
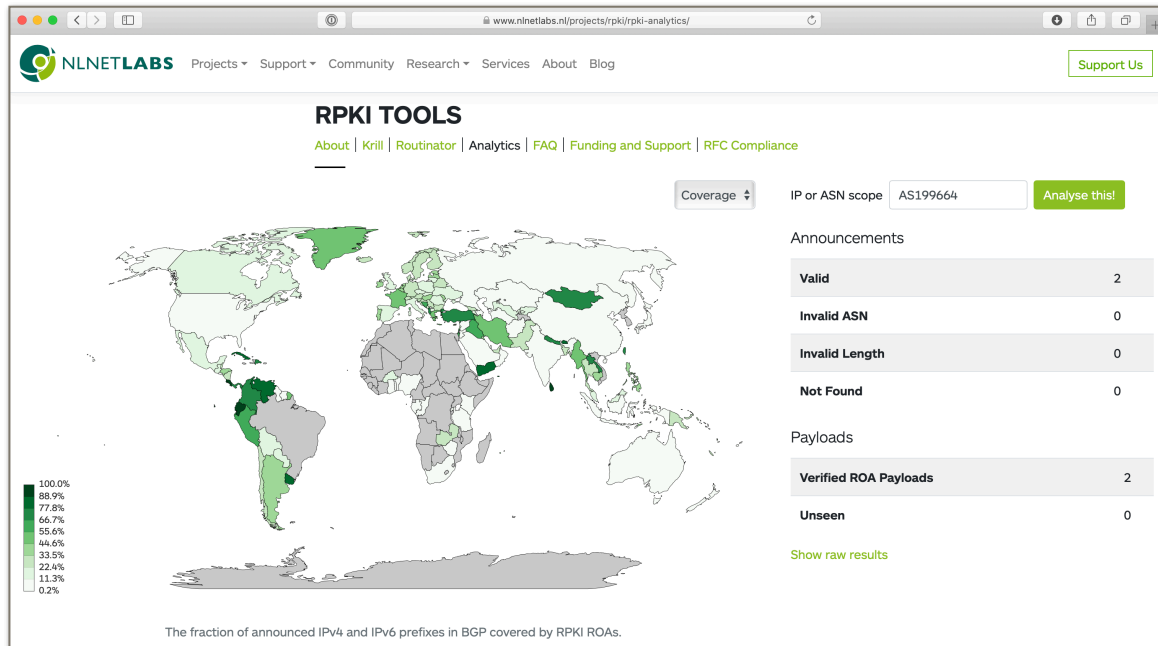
Research

Introduction

Research is a core part of NLnet Labs' mission (read our research vision for more information). In 2019, we continued building up our research efforts in collaboration with both the academic community and with industry. In this section, we will discuss our major research highlights of 2019, including detailed studies of DNS query name minimisation, the DNSSEC Root KSK rollover and a longitudinal study of the RPKI ecosystem. We also played a major role in organising the premier conference on Internet measurements (IMC 2019).

DNS and DNSSEC Research

Query Name Minimisation

Query Name Minimisation (or QNAME minimisation, for short), was introduced in 2016 as part of the IETF's efforts to reduce the privacy risks in the Domain Name System. The goal of QNAME minimisation is to limit what parts of a query name are visible to authoritative name servers when a DNS resolver is executing a DNS recursion.

We wanted to find out to what extent QNAME minimisation is already enabled by DNS resolvers on the Internet and how various DNS vendors implement QNAME minimisation. In order to do so, we performed a study together with researchers from the University of Twente, SIDN Labs and TU Munich. In this study, we used the RIPE Atlas probe network to test support for QNAME minimisation on resolvers in the wild, we studied data collected at the authoritative name servers for the .nl ccTLD and DNS K Root to look at adoption of QNAME minimisation from the perspective of authoritative name server operators, and we tested the impact of QNAME minimisation on query loads and query success in the major open source DNS implementations. Our results show a growing support for QNAME minimisation among resolvers in the wild. We also find a few worrying corner cases, where a combination of badly behaved or configured domains have resolving problems when QNAME minimisation is enabled. Overall, though, our conclusion is that QNAME minimisation provides tangible privacy benefits with a manageable impact on performance, and that resolver implementers are constantly improving their software to smooth out any remaining problems.
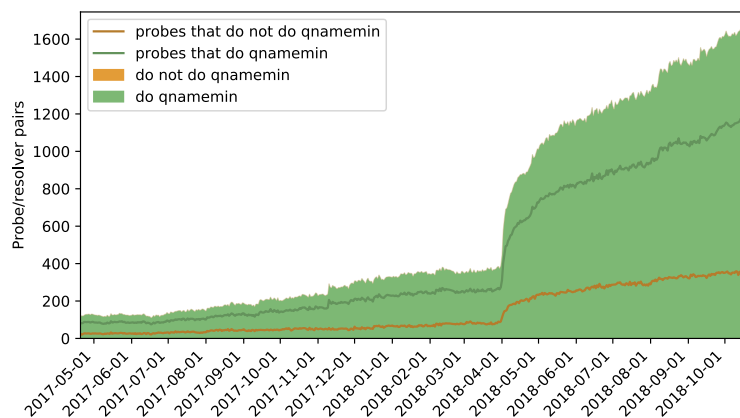
Read our paper, that was presented at the 2019 Passive and Active Measurements conference (PAM), and which won the Best Dataset Award!

NLnet Labs' Unbound DNS resolver supports QNAME minimisation, and in versions released after May 2018, this feature is enabled by default. Curious about the current level of support for QNAME minimisation among the RIPE Atlas probe population? Have a look at our experimental DNSThought platform.

DNSSEC Root KSK Rollover

In our Annual Report 2018, we already discussed that we were studying the DNSSEC Root KSK Rollover that took place in October 2018. Together with researchers from SIDN Labs, Verisign, USC/ISI, Rochester Institute of Technology and the University of Twente, we performed a comprehensive analysis of this event and its aftermath. We presented our results at the Internet Measurement Conference in Amsterdam (more on that conference further down) where our paper was awarded the Distinguished Paper Award. We are very proud our work received this recognition from the Internet research community and are confident that the work will play a major role informing policy for future changes to DNSSEC for the DNS root system.
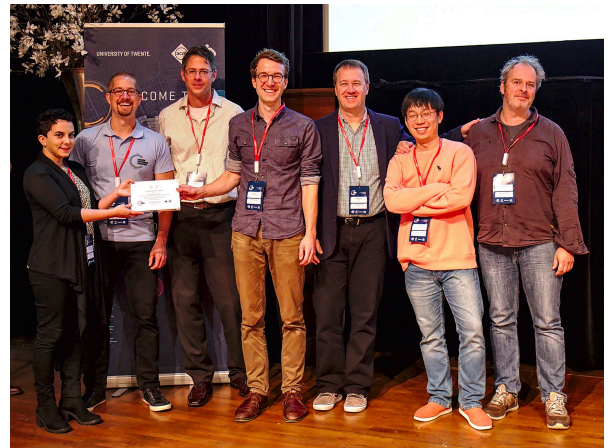

Award ceremony at IMC 2019 (people from left-to-right: Phillipa Gill (TPC chair), Roland van Rijswijk-Deij (NLnet Labs), Rob Beverly (TPC chair), Moritz Müller (SIDN Labs), Duane Wessels (SIDN), Taejoong Chung (RIT) and Willem Toorop (NLnet Labs)
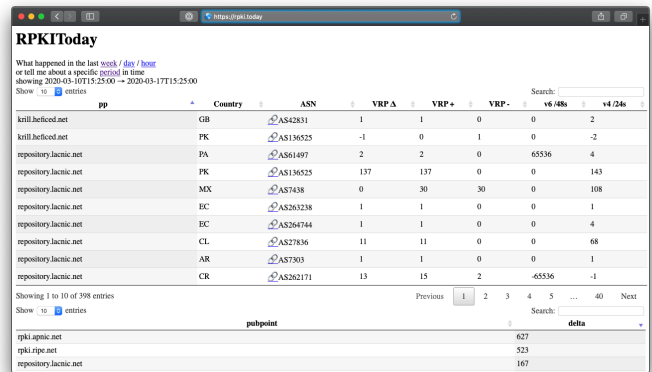
RPKI Research

Longitudinal RPKI Studies

Over the course of the year, we performed a number of longitudinal studies of the RPKI ecosystem. Much of this work was made possible by RIPE releasing a dataset with all RPKI repository data collected since 2011, for which we are extremely grateful. Our first analysis was presented at RIPE 78 in Reykjavik, Iceland in May. Further work was presented at IETF 105 in Montréal, Canada, where we presented an animation that shows the spectacular growth in RPKI adoption (video here) and RPKI data quality (video here). We also made our tool "Ziggy" available, that can be used to download RPKI data for a specified date from the RIPE archives, reconstructs trust anchor points and then runs Routinator to validate the data (read more about Ziggy in our blogpost). Finally, we worked with a team of researchers from RIT, RIPE, MPI, Northeastern University, the University of Maryland, Duke University, Akamai and Cloudflare to perform an in-depth longitudinal analysis about the first 8 years of RPKI. Our paper was presented at IMC 2019 in Amsterdam.
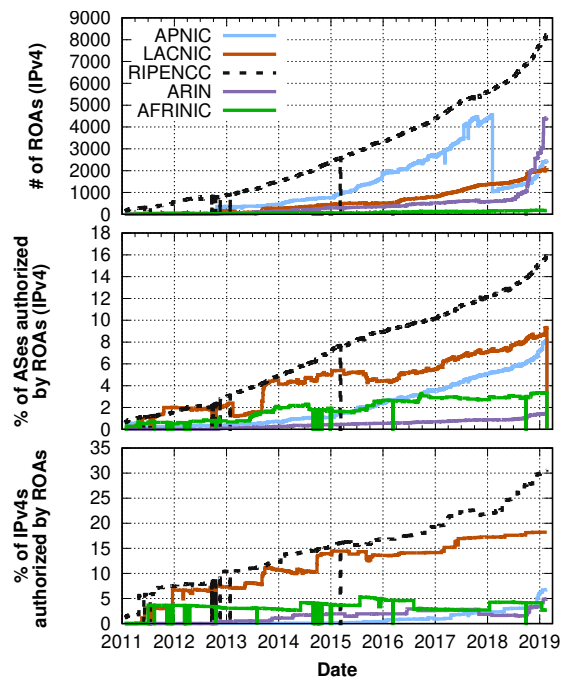
RPKIToday

In 2019, we started an effort to provide the community with insights about published information in the RPKI. Instead of showing total numbers, uptake and coverage, we focussed on the actual differences in published objects between two points in time. Our system, called RPKIToday, enables easy analysis of what happened in the last hour, the last day, or what happened a couple of weeks ago. For example, when a large increase of published ROAs under an RIR occurs, our system identifies which network operator(s) are responsible for these new publications. Or when setting up delegated RPKI, one can quickly see whether the ROAs indeed appear in the RPKI repository. Objects disappearing from RPKI are also presented in RPKIToday: a decrease in ROAs in November 2019 was quickly linked to Iranian networks, likely related to the Internet shutdown happening at the time. These examples show that RPKIToday is not only a valuable tool for operators to troubleshoot their networks, but could provide insights about geopolitical phenomena as well.

RPKIToday

What happened in the last week / day / hour
or tell me about a specific period in time
showing 2020-03-10T15:25:00 → 2020-03-17T15:25:00

Show 10 entries   Search:

pp	Country	ASN	VRP Δ	VRP+	VRP-	v6 /48s	v4 /24s
krill.heficed.net	GB	AS42831	1	1	0	0	2
krill.heficed.net	PK	AS136525	-1	0	1	0	-2
repository.lacnic.net	PA	AS61497	2	2	0	65536	4
repository.lacnic.net	PK	AS136525	137	137	0	0	143
repository.lacnic.net	MX	AS7438	0	30	30	0	108
repository.lacnic.net	EC	AS263238	1	1	0	0	1
repository.lacnic.net	EC	AS264744	1	1	0	0	4
repository.lacnic.net	CL	AS27836	11	11	0	0	68
repository.lacnic.net	AR	AS7303	1	1	0	0	1
repository.lacnic.net	CR	AS262171	13	15	2	-65536	-1

Showing 1 to 10 of 398 entries   Previous 1 2 3 4 5 … 40 Next

Show 10 entries   Search:

pubpoint	delta
rpki.apnic.net	627
rpki.ripe.net	523
repository.lacnic.net	167

As this limited feature set of RPKIToday already shows valuable additions to the existing tools available to the community, we plan to extend its functionality to include more information about valid published RPKI objects, invalid or erroneous RPKI objects, and statistics and diagnostics of the ecosystem as a whole. For this, we successfully applied for the RIPE NCC Community Fund in December 2019, securing further funding for our RPKI analytics tools.

Internet Measurement Conference 2019

One of the main highlights for research in 2019 was our contribution to the ACM Internet Measurement Conference 2019. Not only did we present two papers (one of which won an award), we also played a major role in the organisation of the conference and sponsored the event. Our principal scientist, Roland van Rijswijk-Deij, was one of the co-chairs, together with the chair of our board, Cristian Hesselman and Anna Sperotto from the University of Twente. IMC attracted a record number of 235 attendees from 28 countries and took place at the KIT Royal Tropical Institute in Amsterdam. All of the papers presented at the conference are available as open access through the conference website.

Other Research Highlights

LIGHTest

The year 2019 saw the conclusion of the EU-funded LIGHTest project. In the final year, NLnet Labs contributed to several deliverables, led the Critical ...onented and ...ponent. The final ...els in early 2020.

Open

...NTEL project. The project's goal is to serve as the "long-...mory" of the DNS and performs daily measurements of ...% of the global DNS name space. OpenINTEL is built on ...net Labs products (LDNS and Unbound). Other project ...are the University of Twente, SURFnet and SIDN.

...saw a further expansion of the country-code TLDs that it ...s started in 2019 to also support measurement of the ...o be able to start measuring the reverse DNS space for

OPENINTEL IS A JOINT PROJECT

...ects NLnet Labs participates in on our website.

| Document Identification			
Date	02.11.2016		
Status	Draft		
Version	Version 1.1		
Related WP	WP 12	**Related Deliverable(s)**	none
Lead Authors	Heiko Roßnagel	**Dissemination Level**	PU
Lead Participants	FHG	**Contributors**	Fabina Dietrich (USTUTT)
Reviewers	Don Thibeau (OIX), Charles Sederholm (GS)		

Community Outreach

Standardisation

NLnet Labs is an active participant in the Internet standardisation efforts of the IETF. In 2019, we contributed to multiple Internet drafts that improve DNS security and privacy, that provide guidance on implementing time in Internet protocols and that advance routing security. One of the NLnet Labs colleagues is co-author of RFC 8630 (RPKI TAL). Next to contributing to drafts, NLnet Labs is also an enthusiastic participant in IETF hackathons where the goal is to achieve the second half of the IETF's adagium of "rough consensus and running code".

Our further long-term commitment to open Internet standardisation is reflected in Benno Overeinder being appointed as one of the co-chairs of the IETF DNS Operations Working Group.

DNS Flag Day
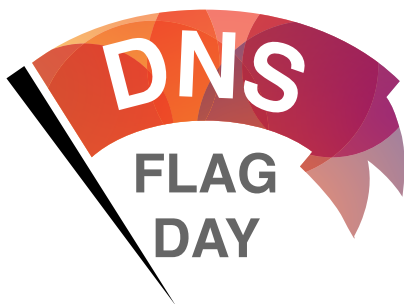
NLnet Labs is a supporter of DNS Flag Day. This initiative that brings together leading organisations in open source DNS development and DNS operations, aims to encourage deployment of a more robust implementation of the DNS protocol. In February 2019, on DNS Flag Day, all open source DNS implementers removed workarounds for broken EDNS implementations and large operators deployed software in production that does the same. For 2020, the focus is on operational and security problems in DNS caused by Internet Protocol packet fragmentation.

Internet.nl

NLnet Labs is a member of the Dutch Internet Standards Platform (Platform Internetstandaarden). Through this initiative various partners from the Internet community and the Dutch government collaborate to raise awareness about and increase the usage of modern Internet Standards, such as IPv6, DNSSEC, RPKI, TLS, SPF, DMARC and DKIM.

The website Internet.nl, launched in 2015, is used to educate and entice consumers and businesses to adopt modern Internet standards. NLnet Labs is responsible for the development and maintenance of Internet.nl. In 2019, the new TLS guidelines, drawn up by the Dutch NCSC, were implemented and an API for interactive email test for DMARC, DKIM SPF and DANE.

MANRS Observatory

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial guidelines to reduce the most common routing threats.

In 2019, NLnet Labs completed the second phase of the implementation of the MANRS Observatory. Our work focusses on data collection and analysis, and providing a RESTful API for a front-end (developed by another organisation). In the second half of 2019, we handed over the further development of MANRS Observatory to another software developer.

RPKI Documentation Project

At the end of 2018 and further into 2019, NLnet Labs took the initiative to create a comprehensive documentation project for the RPKI ecosystem. This project brings together in-depth information about how RPKI works as well as documentation for tools from different open source organisations. The project has already received community contributions, for example from the developers of the RTRlib toolchain, as well as documentation for operational guidance.
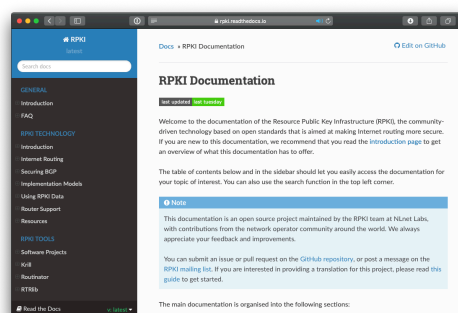
Presentations

NLnet Labs regularly presents in national and international conferences and meetings. Over 2019, we were present at all IETF, ICANN, RIPE and DNS OARC meetings, at NANOG, APRICOT, NLUUG, and various national events. A full overview and slide decks for our presentations can be found on our website.

Community Service

We fulfilled the following community positions in 2019:

Organisation	Role	Person
IETF DNSOP Working Group	Co-chair	Benno Overeinder
DNS-OARC	Board member	Benno Overeinder
RIPE	PC chair	Benno Overeinder
Forum Standaardisatie	Member	Benno Overeinder
ICANN	RSSAC Caucus member	Benno Overeinder
ICANN	SSAC member	Jaap Akkerhuis
ICANN	Various advisory roles	Jaap Akkerhuis
ISO	ISO 3166 MA member	Jaap Akkerhuis
DNS-OARC	PC member	Ralph Dolmans
DNS-OARC	PC member	Willem Toorop
TMA Conference	PhD School Chair	Roland van Rijswijk-Deij
ACM Internet Measurement Conference	General Chair	Roland van Rijswijk-Deij

Team

NLnet Labs strives to achieve its goals with minimal management overhead. The organisation values diversity, aiming to employ staff members from a wide range of nationalities, cultures and backgrounds. Our goal is to be as open and inclusive as possible, with the love for open source and open standards binding us together.

Almost all of the staff is comprised of software developers and research engineers. The foundation strives to maintain a compact team, with a healthy mix of experience ranging from junior to senior and people who focus on software development or research. Other responsibilities such as management, product development, finance and auditing, staffing and recruiting, as well as sales and marketing are shared by two people.

Developments in 2019

In 2019, three new staff members joined NLnet Labs:

- Ximon Eighteen joined in February 2019, bringing years of experience in cloud and container architecture at TomTom. Ximon works on containerising our RPKI solutions and in testing and improving OpenDNSSEC.

- Jeroen Koekkoek joined in June 2019. He has a background in C development for embedded and industrial applications. Jeroen works on our high-performance authoritative name server NSD.

- Luuk Hendriks joined also joined in June 2019. Luuk has Ph.D. in computer science from the University of Twente and will spend half of his time on development of our RPKI tools, and half of his time on research.

Outlook

For 2020, NLnet Labs is looking for a modest expansion, and is hoping to add one team member in a software development role. Looking further forward, our goal is to maintain a stable team size, in keeping with our philosophy of a lightweight team with minimal management overhead. We specifically keep one position open for a junior role, as we want to keep space for fresh ideas.

Funding

Income From Support and Development

Our strategy in recent years has been to increase revenue from support contracts and paid software development. As a non-profit foundation, NLnet Labs is required to adhere to strict tax regulations and is not allowed to offer taxable services. Therefore, support and development contracts are offered through Open Netlabs B.V. This company is a wholly owned, taxable subsidiary of the NLnet Labs Foundation serving the non-profit public benefit goals of its parent, as well as being guided and managed according its charter.

Open Netlabs B.V. offers support contracts with a service level for our production-grade software packages, such as NSD and Unbound. In addition to receiving support and early access to security patches, the financial contribution also supports our mission to provide free and open software for all. Lastly, Open Netlabs provides training and software development in the area of Internet security standards, as well as consulting services such as installation and integration support, optimisation and auditing.

In 2019, Open Netlabs generated income from both support contracts and contracted software development. We are thankful that this contributes to letting us build free, open source software in a sustainable way. We would like to specifically thank NIC.br, Stichting NLnet, Comcast Innovation Fund, the Mozilla Open Source Support programme, the RIPE NCC Community Projects Fund, the Dutch National Cyber Security Centre.

Grants and Subsidies

Since 2012 NLnet Labs has received a generous subsidy from SIDN. This pledge was renewed in 2017 for another five years. We are also grateful for the substantial, long term grants that Infoblox, Verisign and Internetstiftelsen have donated.

Last but not least, we have also received numerous donations from both organisations and individuals. Our gratitude goes out to Manu Bretelle, Jamison Guyton, Mohd Shahrul Azrin Shahrial and DirectOut GmbH, for their generosity. We couldn't fulfil our mission without your support!

Outlook

Looking toward 2020 and further, the financial outlook is excellent. We expect further funding support for the development of our RPKI toolset. In addition, we intend to expand grants-based funding from organisations that support open source development (e.g. the Mozilla Open Source Programme and the Comcast Innovation Fund) to other NLnet Labs products, such as Unbound and NSD. In terms of research projects, we intend to submit proposals to one or more of the new Next Generation Internet (NGI) calls from the European Commission. Looking to the long term future, our goal is to fully support the operational running cost of the organisation with support and development contracts, and to shift the use of grants and subsidies exclusively to fund research and risk-bearing innovation.

Financial Results NLnet Labs

Income			
	2018 Actual (k€)	**2019 Actual (k€)**	**2019 Budget (k€)**
SIDN Subsidy	225	200	200
Other donations	304	498	346
Consultancy and other income	135	132	137
Research and projects	125	140	175
Income from Interest	9	7	12
Total	**798**	**977**	**870**

Expenditure			
	2018 Actual (k€)	**2019 Actual (k€)**	**2019 Budget (k€)**
Staff	576	676	700
Housing	55	55	44
Travel	39	51	46
Depreciation	1	2	
Project Costs	49	126	35
Other Costs	44	55	60
Sub Total	764	965	885
Negative Result Open Netlabs B.V.	-44	-5	
Project Reservations	78	17	-15
Total	**798**	**977**	**870**

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	-	General Reserve	951
Open Netlabs B.V. Stock and Loans	269	Special Purpose Reserves	384
Receivables	412	Current Liabilities and Accruals	148
Bank and Cash	802		
Total	**1483**		**1483**

Governance

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its board consists of four to seven members with staggered terms. The board's composition and most recent rotation schedule is shown below.

NLnet Labs Board in 2019		
Name	**Role**	**End of Term**
Cristian Hesselman	Chair	June 30, 2021
Marieke Huisman	Secretary	August 30, 2021
Ted Lindgreen	Member	March 31, 2019
Sjoera Nas	Member	September 30, 2020
Andrei Robachevsky	Member	June 30, 2022
Jochem de Ruig	Treasurer	June 30, 2021

Four board meetings took place in the year 2019. Benno Overeinder participated in the board meetings in his role as director of NLnet Labs and as director of Open Netlabs BV.

Board members do not receive any compensation for their board work. Expenses may be reimbursed if necessary (€1.455 in 2019). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

Additional Functions Held By NLnet Lab Board Members and Directors in 2019	
Name	**Function(s)**
Cristian Hesselman	- Head of SIDN Labs - Member ICANN SSAC - Associate Professor University of Twente
Marieke Huisman	- Full Professor University of Twente
Sjoera Nas	- Senior Advisor at Privacy Company - Advisory Board SIDN Fonds
Benno Overeinder	- See the Community Service section for an overview
Andrei Robachevsky	- Technology Programma Manager Internet Society - Member EU MSP Standardisation
Jochem de Ruig	- Organic wine entrepreneur at Wilde Wijnen

Looking Ahead to 2020

The year 2020 will be a very special year for NLnet Labs, as it marks our 20 year anniversary! We will, of course, not let this anniversary pass without a celebration with the team.

At the time of writing in June 2020, we are in the midst of a global pandemic whose economic impact will be significant. As an organisation, with an office and daily interaction between colleagues, we have moved to a remote working environment. And with some adoptions, we are very successful in continuing to work on our projects and collaborations with external partners. Our sources of income also appear to be stable for 2020, with donations, grants and other income through support and development. The relevance of Internet technology companies seems to be more vital in a situation where remote working is the new standard.

For 2020, we will continue to support and extend our DNS(SEC) portfolio. Our work on Unbound will include the highly anticipated Response Policy Zone (RPZ), also known as DNS firewall, and further extend security and privacy functionality in Unbound. For NSD, we plan to integrate DNSSEC zone verification into our main development code branch (known as CreDNS). OpenDNSSEC remains a strategic project for many medium to large DNS operators. Finally, for our DNS library portfolio, LDNS2 is still in the pipeline and we continue to expand our DNS domain crate for Rust.

Our new inter-domain routing software portfolio is also expanding. In addition to the successful Routinator, we are thinking of an RPKI data proxy that will be essential in many RPKI setups by network operators. Krill will continue to evolve to be a unique solution for self-hosted or hybrid RPKI CA solutions.

Finally, a strong focus on research will continue to exist in 2020. We have a long-term data collection project like DNSThought and are thinking of starting similar projects for longitudinal studies of the RPKI ecosystem.

We look forward to working with all of you in the Internet community, especially during these times of limited travel!.

Colophon

Editors

NLnet Labs

Design

Richard de Ruijter, Graphic Design & Illustration

Photo Credits

Photo on page 6 by Adam Sherez on Unsplash
Photo on page 23 by Daniel Lerman on Unsplash

Contact

Stichting NLnet Labs
Science Park 400
1098 XH Amsterdam
labs@nlnetlabs.nl
www.nlnetlabs.nl

© NLnet Labs