NLNETLABS

ANNUAL REPORT 2023

Table of Contents

About NLnet Labs

NLnet Labs is a not-for-profit foundation, founded in 1999. Over the past 25 years our mission has been 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 specifically 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 internet players 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 Organization for Standardization (ISO), the Internet Society (ISOC) and 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 DNS and routing.

We are a lean organisation with a team of around 16 people, consisting almost exclusively of developers and researchers, with minimal overhead. We attract talented people who want to make a difference to the well-being of the internet, with a profound belief in open source and open standards.

We develop open-source software that is used across the internet industry, ranging from the DNS root servers at the core of the internet to small embedded devices running a secure recursive resolver, and routing security software that helps protect the network of large operators.

Our researchers pioneer new technologies, help define 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 – development and research – we bridge the gap between academia and industry, and introduce solutions that are practical as well as innovative.

We also contribute to policy and governance by bridging technology and policy. Our technical expertise and advice is widely recognised by policy-making bodies. 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.

Software Development

At a glance

In 2023 we continued to develop and extend our existing DNS and RPKI software.

For the DNS products we have published several releases of Unbound and NSD. Alongside bug and security fixes, stability improvements and smaller features, we have implemented server-side DNS Cookies, NAT64 and DoC, and we have been working on improvements to the cache database, DNS64, EDNS and the Python interface in Unbound.

NSD now supports dnstap over TLS and the PROXYv2 protocol. We also have a first implementation of a new zone parser and a proof of concept for a more efficient core data structure. Next year we will implement the eXpress Data Path (XDP) framework.

The most notable new feature of Domain Crate is support for ZONEMD record types. This year the Sovereign Tech Fund (STF) awarded funding for the further development of Domain Crate, which allows us to have three developers working on the software until the end of 2024.

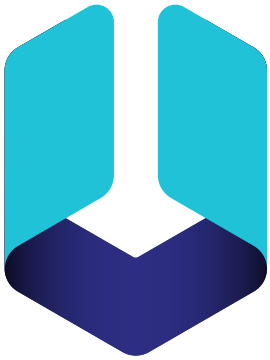
Our routing security software – Routinator, Krill, RTRTR and Rotonda – continued to mature and evolve. Routinator gained support for version 2 of the RTR protocol and for ASPA.

Krill now comes with a newly implemented user interface and support for the updated ASPA v1 profile. ASPA objects are supported through the command line interface by default. We hope to add support to the graphical user interface next year. Finally, Krill can now also be used as a full RPKI Trust Anchor, using a detached (possibly offline) signer for Trust Anchor key operations. NLnet Foundation will be partly sponsoring the implementation of high-availability features in Krill (in collaboration with LACNIC), which is planned for next year.

Rotonda has seen steady progress this year. All the main components have been completed and the software is ready for a 0.1 release early next year. Routecore, the Rust library with parsers for BMP and BGP packets, has seen additions for creating BGP messages as well as machinery to support BGP sessions with other BGP speakers. We also started work on a domain-specific language called Roto for filtering, querying and configuring BGP applications.

DNS(SEC) Software Projects

Unbound



After publishing maintenance release 1.17.1 of Unbound at the beginning of 2023, we published two significant versions this year. Version 1.18 included support for server-side DNS Cookies and NAT64. Version 1.19 brought several new functions for the cache database (the redis-logical-db and cachedb-no-store options), DNS64 (fallback to plain AAAA when no A record exists), EDNS (the disable-edns-do option), and the Python interface. Along the way, several bugs were fixed, and a few options added that contribute to Unbound's stability and robustness.

We have also completed the implementation of DNS-over-QUIC (DOQ). A thorough code review is the last remaining task before release, which is planned for next year.

Last year we started using GitHub milestones to manage new releases of Unbound. This provides insight into planned new features, their status and in what release they will become available to users. Version 1.17.1 was the first release published under this new regime.

DNS Cookies (defined in RFC 7873) are a lightweight authentication mechanism that mitigates DDoS and spoofing attacks. Both the client and the server send along cookies in an OPT record that have to be repeated back by the other side, thereby protecting the (UDP-based) connection between the two against off-path attackers.

QUIC, defined in RFC 9000 and adjacent RFCs, is a new protocol alongside TCP and UDP. It brings together the efficiency of UDP, the reliability of TCP and the security of TLS in a single internet transport protocol. In a similar way to HTTPS/3, DNS-over-QUIC (DoQ, defined in RFC 9250) provides a native mapping of DNS transport on QUIC.

About Unbound: Unbound is a DNSSEC-validating, recursive, caching DNS resolver. It is designed to be fast and lean, and incorporates modern features based on open standards. The software runs on FreeBSD, OpenBSD, NetBSD, MacOS, Linux and Microsoft Windows, with pre-built packages available for most platforms. It is included in the standard repositories of most Linux distributions. Installation and configuration are designed to be easy: just a few lines of configuration are enough to set up a resolver for your machine or network.

NSD

2023 saw two new releases of NSD. Version 4.7 added dnstap over TLS (in addition to TCP). Version 4.8 includes support for the PROXYv2 protocol and improvements to the performance of server stats collection, which previously was an issue for some customers.

Dnstap is a structured binary log format for wire-format DNS messages. It is supported in all popular DNS servers. Support for dnstap over TLS (e.g. encrypted monitoring) is a valuable addition to NSD now that DNS privacy and encryption of transport have become more important.

PROXYv2 allows propagation of the client's original IP address and other connection information through HAProxy's TCP proxy. This is typically used with server instances running behind a DNS load balancer. Last year we implemented PROXYv2 in Unbound, a project that was sponsored by SUNET. This year's PROXYv2 implementation in NSD has also been sponsored by SUNET (and already taken into production by them). Although this functionality was developed with industry sponsorship, it can be used more generally in DNS services and is available to all our users.

Last year we implemented zone verification, which allows zones to be checked for DNSSEC validity before publication. The development of this feature was partly sponsored by SIDN. Several parties, including Netnod and GoDaddy, are already using the new zone verification feature in their production systems, and others plan to do so. The feedback we have received so far has been positive.

We have also been working on several new technologies that will increase the performance and scalability of NSD. We already have a first implementation for a new zone parser that is more efficient than the current one for loading and starting zone files, and this will become available in NSD next year. We also have a proof of concept for an adaptive radix tree as the new core data structure of NSD, which will be more efficient in time and memory consumption. Together the new zone parser and the new database structure will allow loading and starting very large zones or a large number of small zones in parallel.

After some redesign, the implementation of catalog zones has now been made available to a few users for operational feedback. This feature is defined in RFC 9432 and provides a uniform way to specify how a DNS zone catalog is to be deployed.

Next year we will implement the eXpress Data Path (XDP) framework, a new network technology that can efficiently handle data over 10+ Gbps networks in applications.

About NSD: Name Server Daemon (NSD) is an authoritative DNS name server. It has been developed for operations in environments where speed, reliability, stability and security are essential. The software is designed with a pure philosophy that prioritises raw performance. This means that if you serve hundreds of thousands or even millions of queries per second, NSD is the world's leading name server. This makes it ideal for TLD implementations, DNS root servers and anyone in need of a fast and optimised authoritative name server. Currently, three DNS root servers and many TLD registries use NSD as part of their server implementation. NSD also strives to be a reference implementation for emerging IETF standards.

OpenDNSSEC

After ending support for version 1.4 of OpenDNSSEC in 2019, over recent years we saw continued upgrades and deployments of version 2.1 by large DNS operators – including TLD operators – who depend on a fully managed DNSSEC signing solution.

After putting considerable effort into outreach over the last four years, we are seeing intensive and smooth-running cooperation with the user community. Operators ask us for help with their upgrades and deployments, and provide feedback to further improve OpenDNSSEC. SIDN in particular has been an enthusiastic user and supporter of OpenDNSSEC.

The 2.1.11 and 2.1.12 minor releases we published at the end of 2022 improved support for RFC 9276 (with new recommendations for the salt and iteration values of NSEC3), and fixed several bugs. Version 2.1.13 published this year was also a small release to fix bugs and perform maintenance.

For 2024, our plans include implementing CDS/CDNSKEY and migrating the current (external) OpenDNSSEC website onto our own site and documentation system (in 2021 we migrated the documentation of Unbound and NSD to the Read the Docs platform).

ZONEMD was implemented last year. This year we completed the implementation of high-availability (failover) support, which is currently being tested. Both features will be released in 2024.

CDS and CDNSKEY are two relatively new record types (defined in RFC 8087) that allow operators of signed zones to have the DNSSEC parameters in the parent zone updated, based on the existing DNSSEC chain of trust. This allows for automated key rollovers and other updates without the need to upload DNSSEC data through EPP or a web interface.

ZONEMD is defined in RFC 8976 and allows for a new record type containing a cryptographic message digest over the full zone. The ZONEMD record itself is protected by a DNSSEC signature. Since the record is part of the zone file, the message digest can be used by a recipient to verify that the zone is correct and complete.

About OpenDNSSEC: OpenDNSSEC is a policy-based zone signer that automates DNSSEC key management and the signing of zones. The main goal of the project is to make the Domain Name System Security Extensions (DNSSEC) easy to deploy, thereby driving the adoption of DNSSEC and enhancing internet security.

SoftHSM

The SoftHSM project, to which NLnet Labs has contributed in the past, was incorporated as a project under the Commons Conservancy in 2019. The long-term goal of this step was to keep the project sustainable and allow new partners to make significant contributions. The last release of the software (version 2.6.1), however, was published back in 2020. We will keep managing the project, but we have not developed any new activities related to SoftHSM.

About SoftHSM: SoftHSM was developed to provide a software-based solution for people who wish to use OpenDNSSEC but are not willing or able to invest in a new cryptographic hardware device. It provides a software implementation of a generic HSM with a PKCS#11 interface. SoftHSM has been designed to connect directly to OpenDNSSEC, but thanks to its standard PKCS#11 interface it can also be used by other cryptographic products.

DNS(SEC) Libraries

LDNS

In 2023 we did not release any new versions of the ldns library.

We will continue to maintain ldns, with no plans for major changes in the near future.

About LDNS: ldns is a C library to simplify DNS programming. It supports all low-level DNS and DNSSEC operations. It also defines a higher-level API, which allows a programmer to quickly create or sign packets, for example. Developers can use ldns to easily create RFC-compliant software and build proofs of concept for various Internet Drafts.

We do not strive for ldns to be a comprehensive library that supports every (emerging) standard. The software includes a DNS lookup utility named drill (an alternative implementation to BIND's dig). As drill has nothing in common with either NSD or BIND, it allows for debugging and testing using an independent code base.

getdns and Stubby

In 2023 we did not release any new versions of the getdns library or the Stubby resolver.

About getdns: getdns is a modern asynchronous DNS API and library. It implements DNS entry points from an interface design developed and vetted by application developers, which was consolidated in an API specification. This implementation is developed and maintained through a collaboration between NLnet Labs, Sinodun and No Mountain Software. Although the code is written in C, bindings for several other programming languages are available. The software is published under the New BSD License.

About Stubby: Stubby is a local DNS Privacy stub resolver. It is built on the getdns library and is available for UNIX-like systems as well as Windows (the latter as a binary). Stubby uses DNS-over-TLS (DoT) to encrypt DNS traffic sent from a client machine (typically a desktop or laptop) to a DNS Privacy recursive resolver service, thereby improving end-user privacy.

Net::DNS(::SEC)

2023 saw quite a long series of minor releases of Net::DNS (versions 1.36-1.42) and Net::DNS::SEC (versions 1.21-1.23). The updates provide several improvements in functionality and implementation, plus a few bug fixes in the code and documentation.

About Net::DNS(::SEC): NLnet Labs is a longtime contributor to and maintainer of Net::DNS(::SEC), a DNS library written in the Perl scripting language. It consists of the Net::DNS resolver and the Net::DNS::SEC add-on. The latter adds DNSSEC support to Net::DNS. Net::DNS::SEC must be downloaded as a separate package from CPAN, because the two components may have mutually incompatible dependencies..

Domain Crate

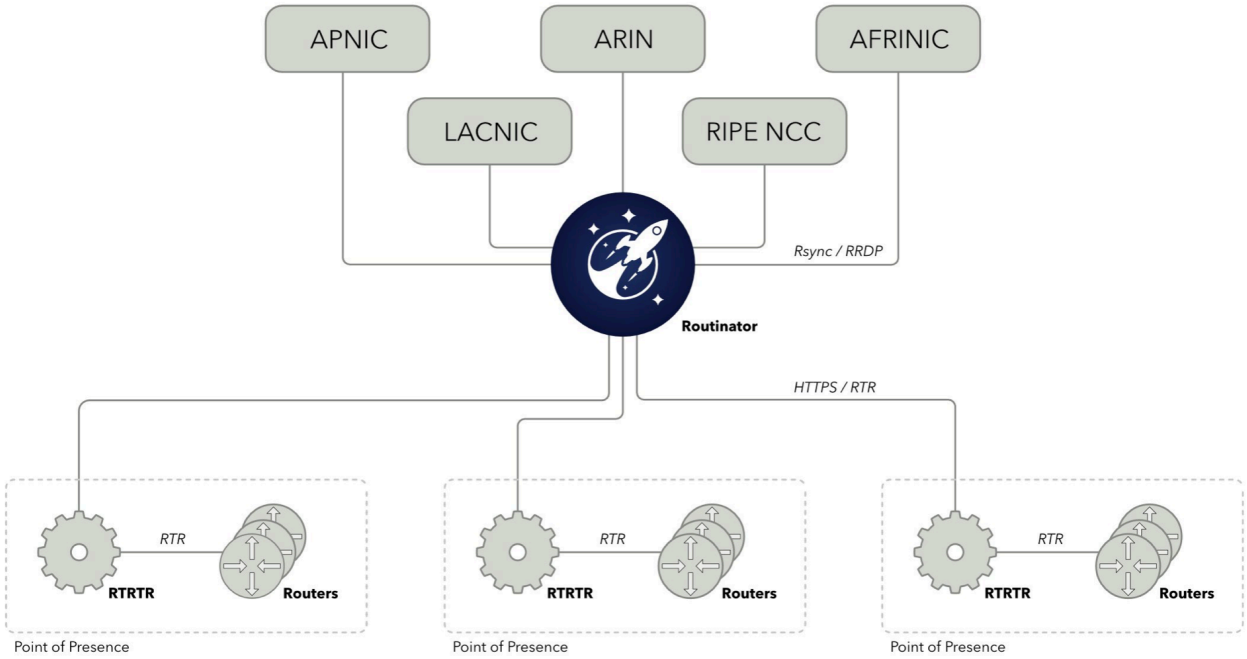
In 2023 we published two major and several minor releases of Domain Crate. Version 0.8 included many changes, improvements to the code, bug fixes, and new objects and methods. The most notable new feature of version 0.9 is support for the ZONEMD record (this function is described in the Unbound section above). Domain Crate is under active development, but the software is already being used in production.

This year the Sovereign Tech Fund (STF) awarded funding for the further development of Domain Crate. That allows us to have three developers working on the software until the end of 2024.

The work starts with the development of a basic stub resolver library, which will be extended next year to include response caching and DNSSEC validation. At the same time we will be working on the server side, which will support reading zone files, answering queries, zone transfers, and DNSSEC key management and signing. In the second half of 2024 we will be implementing proxy functionality and DNS query routing. In addition we will introduce Rust-based versions of DNS diagnostic tools, similar to the well-known tool 'dig'. These new tools will offer a different approach, focusing on enhanced usability and providing insightful information for a broad audience.

About Domain Crate: Domain Crate is a DNS library written in the Rust programming language. It contains an ever-growing set of building blocks for including DNS functionality in applications. These blocks currently include the basic data structures and functionality for creating and parsing DNS data and messages, support for signing and verifying messages using the TSIG mechanism, experimental support for reading data from DNS master files (also known as zone files), experimental and as yet incomplete support for DNSSEC signing and validation, and a simple Tokio-based stub resolver.

Domain Crate is already being used in production by a large company. The software library will serve as the basis under our memory-safe DNS software strategy.



Routing Software

Routinator

In 2023 we published two bugfix releases (versions 0.12.1 and 0.12.2) of Routinator and one feature release (0.13.0). Version 0.13 adds support for version 2 of the RTR protocol and for ASPA. We also made some additions and changes to the endpoints of the HTTP server, and support for filtering and adding router keys via local exception files was added.

At the end of 2023, around 2800 organisations were using Routinator, bringing its market share to almost 80 percent (and still growing fast). Independent statistics on the RPKI Validator market can be found at: https://rov-measurements.nlnetlabs.net/stats/.

About Routinator: Routinator is Relying Party software (written in the Rust programming language), also known as an RPKI Validator. This full-featured application is designed to be secure and highly portable. It is a lightweight implementation that can run effortlessly on almost any operating system using minimalist hardware.

The Routinator system periodically downloads and validates the global RPKI dataset. Routers can connect to Routinator to fetch validated data via the RPKI-to-Router (RTR) protocol. The built-in HTTP server offers a user interface and API endpoints for various file formats (e.g. CSV, JSON and RPSL), as well as logging, status and Prometheus metrics.

The user interface allows users to validate prefixes against Autonomous System Numbers (ASNs) found in BGP announcements. It also allows users to lookup related prefixes for the prefix they are searching for. These related prefixes can be more or less specific prefixes, prefixes routed in BGP, or prefixes that are allocated by one of the five Regional Internet Registries.

For larger networks we have developed RTRTR (discussed below) as a companion to Routinator. This makes it possible to centralise validation performed by Routinator and have RTRTR running in various locations around the world to which routers can connect.

RTRTR

In 2023 we did not release any new versions of RTRTR, as everything was working well and our users did not have any issues or feature requests. For next year we expect to release a new version with several additional features and options.

About RTRTR: RTRTR is an RPKI data proxy designed to collect Validated ROA Payloads from one or more sources in multiple formats and dispatch them onwards. It provides the means to implement multiple distribution architectures for RPKI, such as centralised RPKI Validators that dispatch data to local caching RTR servers.

For larger networks, RTRTR is an ideal companion to Routinator. For example, it is possible to centralise validation performed by Routinator and have RTRTR running in various locations around the world to which routers can connect.

RTRTR can read RPKI data from multiple RPKI Relying Party packages via RTR and JSON, and, in turn, provide an RTR service for routers to connect to. The HTTP server provides the validated dataset in JSON format, as well as a monitoring endpoint in plain text and Prometheus format.

Krill

In 2023 we published no fewer than ten releases of Krill, including two feature releases (0.13.0 and 0.14.0).

Version 0.13 came with a newly implemented user interface, resulting in a smaller browser footprint. The functionality of the user interface is mostly unchanged, but users now have the option to place a comment with each of their ROA configurations. These comments are not part of published the ROA objects; they are meant for local bookkeeping only. The new user interface was built by implementation partner Tweede Golf, who will remain responsible for the further development of this interface.

ASPA objects are now supported through the command line interface by default. We hope to add support to the graphical user interface next year.

Finally, Krill can now be used as a full RPKI Trust Anchor, using a detached (possibly offline) signer for Trust Anchor key operations. This is the RPKI function normally performed by the five RIRs.

Version 1.14 added support for the updated ASPA v1 profile. Any existing ASPA objects will be re-issued automatically.

This release also includes improvements to the datastore. This increases the robustness of the software today, but also paves the way for introducing support for clustering using a database back-end in a future release.

Other minor improvements, changes, and bug and security fixes were incorporated along the way.

NLnet Foundation will be partly sponsoring the implementation of high-availability features in Krill (in collaboration with LACNIC), planned for next year.

The implementation of the RPKI Trust Anchor functionality was sponsored by LACNIC. They also partly sponsored the High Availability implementation, and will be testing this new feature next year or in the first half of 2025.

After adding PKCS#11 support for HSMs and support for the Key Management Interoperability Protocol (KMIP) last year, ARIN, APNIC and RIPE NCC all introduced Hybrid RPKI services based on Krill's Publication Server. LACNIC plans to migrate its RPKI (CA) infrastructure to Krill next year. Deployment at LACNIC requires the implementation of Trust Anchor support, and the High Availability functionality to allow for redundant deployments. AFRINIC, which has smaller financial resources, hopes to share the benefits of this new functionality for its deployment of Krill.

Krill is now actively used by more than 1700 organisations in Brazil and over 1200 organisations in Indonesia.

About Krill: Krill is an RPKI Certificate Authority (CA) that lets you run Delegated RPKI under one or multiple Regional Internet Registries (RIRs). Through its built-in publication server, Krill can publish Route Origin Authorisations (ROAs) on your own servers or with a third party.

The software supports running the CA both upwards and downwards. Upwards means that an instance can have multiple parents, such as ARIN and RIPE NCC, 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 (NIRs) and enterprises.

The publication server that is included in Krill can also be run as an independent component. This allows organisations to host published certificates and ROAs themselves, or let a third party such as a Content Delivery Network (CDN) do it on their behalf.

Krill is intended for organisations who:

- 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; or
- need to be able to delegate RPKI to their customers or business units, so that that they can run their own CA and manage ROAs themselves; or
- manage address space from multiple RIRs; using Krill, they can manage all ROAs for all resources seamlessly within one system; or
- want to be operationally independent from their parent RIR, such as an NIR or an enterprise..

JDR: Explore, Inspect and Troubleshoot RPKI

JDR has not seen major changes in terms of functionality since 2022. With the increasing size and distribution of the RPKI

repositories, the deployment and parts of the codebase have been adapted to handle this increased load, and operate in a more resilient way.

About JDR: JDR is a tool to help explore, inspect and troubleshoot anything RPKI. Just like Relying Party software, JDR interprets certificates and signed objects in the RPKI, but instead of producing a set of Verified ROA Payloads (VRPs) to be fed to a router, it annotates everything that could somehow cause trouble. It will go out of its way to try to decode and parse objects; even if a file is clearly violating the standards and should be rejected by RP software, JDR will try to process it and give the end-user as much troubleshooting information as possible.

Rotonda

The Rotonda project, which was launched in 2021, has seen steady progress in 2023. All the main components have been completed and the software is ready for a 0.1 release early next year.

SURF started experimenting with Rotonda this year. Internet Initiative Japan (IIJ) and several Internet Exchanges have expressed an interest in this software, as have the CAIDA and RouteViews projects.

NLnet Foundation will be sponsoring further development of the Routecore and Roto software, which is planned for next year. Routecore is a low-level library written in Rust to parse and create BGP messages. It can be used as a library in any Rust application that needs BGP functionality. Roto is a domain-specific language that allows Rotonda users to create configurations for Rotonda, filters that fit into the pipeline, and queries for searching through the RIBs of Rotonda. Roto is a strongly typed, compiled scripting language..

About Rotonda: Rotonda is a modular, analytical BGP routing engine, made up of components that can be combined into a BGP application by the end user. As with all of our routing software, it is written in Rust, a fast, memory-safe programming language. Rotonda consists of several components: First is the rotonda store which handles the storage and retrieval of IP prefixes using a tree bitmap as the data structure. Routecore is a Rust library with fundamental building blocks for BGP routing – that is, types and traits for applications that need to deal with data related to BGP and routing. Other components are the Roto filter and querying language, and the Rotonda runtime, which handles the protocols, the runtime and the command-line interface.

Research

Introduction

Research is an essential part of NLnet Labs' mission (read our research vision here). As in previous years, we continued our research efforts in collaboration with both the academic community and industry. In this section we discuss our key research highlights of 2023.

Route Origin Validation of DNS resolvers

The Border Gateway Protocol (BGP) is responsible for routing on the internet. BGP lacks built-in trust and security measures, however, making it vulnerable to IP prefix hijacking and route leaks. To defend against these threats, the Resource Public Key Infrastructure (RPKI) standard has been developed in the IETF. RPKI/ROV secures the internet's routing infrastructure by signing and validating prefix origin data.

In the RPKI system, Route Origin Authorizations (ROAs) provide attestable statements specifying which prefix is authorised to originate from which Autonomous System Number (ASN) in BGP. Route Origin Validation (ROV) is the process of using the data from the ROAs in RPKI to determine whether a route announced in the BGP is valid, invalid, or unknown.

There are, however, still situations where an organisation may indirectly fall victim to prefix hijacks, even if its own AS is RPKI-protected. A good example of this is the Amazon Route 53 BGP exploit, in which the prefixes of Amazon's authoritative DNS servers were hijacked. In this case, any Autonomous System (AS) with a DNS resolver not protected by RPKI would receive a valid but malicious response from the hijacked authoritative DNS server, even if the AS from which the query originated was RPKI-protected. So, for end-users to be fully secure, in addition to the network in which they reside, their DNS resolvers must also be based in RPKI-protected networks.

In this research project, we will:

- Measure the uptake of Route Origin Validation by DNS resolvers. We will do that by scheduling long-running measurements targeting authoritative name servers hosted on an RPKI beacon.
- Measure the uptake of Route Origin Validation by authoritative name servers. This will be accomplished by sending queries to the authoritative name server operators originating from an RPKI beacon.

We have been measuring the uptake of ROV protection of DNS resolvers since January 2020 (see this thesis report).

To perform ongoing measurements to monitor the state of RPKI protection of DNS resources over the long term, we have set up an RPKI beacon under our own control, replacing the beacon kindly provided by Job Snijders until September 2021. Running our own beacon allows us to carry out these measurements for a longer period of time. Furthermore, our own beacon is set up in such a way that it can measure Route Origin Validation failures of hops on the path from a source to a destination. In 2023 we continued our work on building and extending this

infrastructure. Our measuring infrastructure and beacon is also being used by OARC's CheckMyDNS test platform to measure the Route Origin Validation status of resolvers.

This year, Keven Klercq, a security and network engineering student from the University of Amsterdam, carried out a research project under our supervision and using our RPKI beacon. He identified the most prevalent on-path BGP speakers that didn't do Route Origin Validation and redirected traffic to invalid announcements, even for paths for which the target resource is signed and the endpoint is validating route origins.[1] The aim of the project was to pinpoint which parties would have the biggest positive effect on routing security if they were to start doing Route Origin Validation. This research was presented on two occasions:

- At the SURF Internet Measurements and Analysis Workshop on 5 April 2023 in Utrecht, by Kevin Klercq (UvA SNE), Koen van Hove (NLnet Labs) and Willem Toorop (NLnet Labs)[2]
- At RIPE 86 on 26 May 2023 in Rotterdam, by Willem Toorop[3]

In 2024 we will be extending the beacon with additional prefixes to improve our insight into end-point ROV status..

Experimenting with DNS and XDP

In recent years, programmable network devices have received much attention from both academia and industry, and affordable hardware is becoming increasingly available. We think that network-programming technologies such as eBPF and P4 can also be used to improve the performance of DNS resolvers and name servers.

In 2020, we started a SURF-sponsored Research on Networks (RoN) project to assess eBPF's capabilities to improve the performance and stability of DNS resolvers and name servers. In that first phase we looked into the capabilities of the new technologies eBPF and eXpress Data Path (XDP). Using a proof-of-concept implementation, we wanted to find out how we can leverage the power of eBPF/XDP to improve name server performance, increase name server versatility, and perform low-level measurements on high-speed connections.

Since then we have produced a series of example programs illustrating how eBPF/XDP can be used to augment existing DNS setups with modules that deal with query rate limiting, DNS cookies and metrics in the most performant way at the earliest possible stage. These modules are DNS software agnostic and can be used with any DNS software running on Linux. The example programs were published as a series of blog posts and in APNIC PING podcast episodes.

---

[1] https://nlnetlabs.nl/downloads/publications/RP1_by_Kevin_Klercq.pdf

[2] https://wiki.surfnet.nl/display/SURFnetnetwerkWiki/Internet+Measurements+and+Analysis+Workshop+5+April+2023

[3] https://ripe86.ripe.net/archives/video/1124/

In 2023, Jannik Peters, a security and network engineering student from the University of Amsterdam, carried out research under our supervision, creating an XDP-based DNS hot cache, again augmenting existing DNS setups.[4]

For next year we are planning to extend NSD with XDP capabilities so it can respond to queries at the earliest possible moment, by-passing the Linux kernel.

Other Research Highlights

2STiC

2STiC, short for Security, Stability and Transparency in inter-network Communication, is a joint research programme in which ten Dutch internet organisations are collaborating. Its goal is to develop and evaluate new or improved mechanisms that increase the security, stability and transparency of internet communications, through both extensions of today's internet and emerging internet architectures. Its long-term objective is to establish a collaborative research centre for trusted and resilient internet infrastructures that will help to give the Dutch and European networking communities a leading position in the field.

Our participation in the 2STiC consortium focuses on two projects for which we contribute expertise on internet architecture and standards, and review results and papers:

- UPIN (User-driven Path Verification and Control for Inter-domain Networks):
  The goal of UPIN is to develop and evaluate a scalable distributed system that enables users to cryptographically verify and easily control the paths through which their data travels through an inter-domain network like the Internet, in terms of both router-to-router hops and router attributes (e.g. router location, operator, security level and manufacturer).
- CATRIN (Controllable, Accountable, Transparent: the Responsible Internet):
  The goal of CATRIN is to start up the Responsible Internet, a novel security-by-design concept and extension to the internet infrastructure that enhances the range of actions users have at their disposal to share information securely and confidentially. This will enable higher levels of trust and autonomy for users, organisations, and society.

RSSAC028

In 2017, ICANN's Root Server System Advisory Committee (RSSAC) presented various options for renaming the root servers. Adoption of a new naming scheme is under consideration because it would, for example, allow information about the root servers to be secured using DNSSEC, and allow root servers to become independent of the .net top-level domain (TLD) in some cases. The RSSAC put forward five alternative naming schemes.

In partnership with SIDN Labs, we have conducted a study to establish what implications these five alternative naming schemes would have for the root servers of the Domain Name System (DNS). We kicked off this project in the summer of 2022 with a short introduction and presentation to the Root Server Operators (RSOs). In September last year we started on the first

[4] https://nlnetlabs.nl/downloads/publications/report_xdp-based-dns-hot-cache_2024-02-14.pdf

work package, sending all RSOs a questionnaire. Last February Willem Toorop presented the project at DNS OARC 40.

This year we extended the existing simulation platform so that others now can independently run our experiments on their own (proprietary) infrastructures and share the results with us. This way collecting the measurements was fully automated.[5]

The project was successfully concluded by the end of this year with the publication of the final report.[6] The review of the draft report by ICANN was positive and the report was accepted without any major changes. A presentation of the outcomes for the root operators at IETF 117 also resulted in very positive responses.

RZERC002

After consulting with ICANN about further research into TLD zones and root servers, we submitted a proposal for a follow-up project to RSSAC028. RZERC002 (Recommendations Regarding Signing Root Zone Name Server Data, Recommendation 2) aims to further explore the cost/benefit tradeoffs and risks of signed root zone name server data. This project consists mainly of performing an analysis and producing a report. Presenting the results would be a separately funded task.

DNSThought

DNSThought is a DNS measurement and data analysis platform that provides longitudinal insight into resolvers and their capabilities. The project leverages the RIPE Atlas data collection measurement infrastructure, giving it a unique perspective from many vantage points on the Internet. Since its inauguration in April 2017, resolver capability measurements have been performed every hour, resulting in a valuable data set for the research and operations community. The continuous measurements allow researchers and operational engineers to study the status of standards and resolver functionality over time.

Further Reading

You can read more about all the research projects NLnet Labs participates in on our website at https://nlnetlabs.nl/research/projects/.

[5] https://indico.dns-oarc.net/event/46/contributions/1003/

[6] https://www.sidnlabs.nl/en/news-and-blogs/renaming-the-dns-root-opportunities-pitfalls-and-a-testbed

Community Outreach

Standardisation

NLnet Labs actively participates in the internet standardisation efforts of the IETF. In 2023, we contributed to several Internet Drafts in the DNS-related working groups and the SIDROPS working group. This year we worked with other open-source developers on the catalog zone standard to simplify the configuration and deployment of a large number of domains by a DNS service provider; this has been published as RFC 9432. We also contributed to the DNS Error Reporting IETF internet draft, which defines a lightweight reporting mechanism providing insights into resolving and validation failures.

We started work on specifying a method for DNS servers to signal programs outside of the server software – and which do not necessarily have anything to do with the DNS protocol – about conditions that can arise within the server. These signals can be used to invoke actions in areas that help to provide the DNS service, such as routing.

In SIDROPS we contributed to improve operational aspects, including operational recommendations for delivering resilient RPKI services. In GROW we discussed the standards relevant to BGP monitoring and data collection, which we use in the Rotonda project. As well as 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 motto of "rough consensus and running code".

Our long-term commitment to open internet standardisation is also reflected in Benno Overeinder's appointment as one of the co-chairs of the IETF DNS Operations Working Group and the IETF Hackathon.

Benno is also a member of Forum Standaardisatie, which promotes digital interoperability among Dutch government organisations and between government, businesses and citizens. The use of open standards to support interoperability, facilitate data (re)use and reduce dependency on specific suppliers is a key policy in the Netherlands.

Policy and governance

In 2023 we engaged with policymakers on two major EU policy initiatives that will shape the future of software development in Europe:

- The upcoming Cyber Resilience Act (CRA) sets market entry requirements for software. Our outreach positively affected the outcome of the negotiations between the parliament and council. The negotiated text introduced an obligation for all manufacturers that integrate software to upstream patches for security vulnerabilities to its (open source) maintainers. It

added nuance with respect to the scoping for developers of free and open-source software, and permits manufacturers of open-source software that is considered "important" to self-assess its compliance instead of requiring a third-party assessment.

- The updated Product Liability Directive (PLD) extends strict liability to software developers. Our outreach positively affected the outcome of the negotiations between the parliament and council by clarifying liability for the supply of free and open-source software by non-profit organisations.

To achieve these two results, we built working relationships with a number of free and open-source advocates active in Brussels, as well as the policymakers involved. To bring knowledge of these policy files to other open source developers, we co-organised presentations and a panel discussion at the FOSDEM conference in Brussels, inviting two of the authors of the CRA and PLD to discuss their work on the main stage.

In 2023 NLnet Labs remained an active participant in the Internet Standards Platform, a collaborative initiative in which public and private parties work together to promote the adoption of modern internet standards such as IPv6, DNSSEC, RPKI, TLS, STARTTLS/DANE, SPF, DKIM and DMARC. One of the key activities of the Platform is operating the internet.nl test and measurement platform, which monitors the adoption of modern and secure internet standards across both the public and private sectors.

In fall 2023 Maarten Aertsen joined ICANN's Security and Stability Advisory Committee (SSAC) as a member alongside Jaap Akkerhuis, who has served SSAC since its inception. SSAC advises the ICANN community and board on matters relating to the security and integrity of the internet's naming and address allocation systems. This includes operational, administrative and registration matters. SSAC engages in ongoing threat assessment and risk analysis of the internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.

Presentations

NLnet Labs regularly presents at national and international conferences and meetings. After the COVID restrictions of 2020 and 2021, 2022 was the first year that things were back to normal. This year we were physically present at the various IETF, ICANN, RIPE, DNS OARC, CENTR (online only), MORE-IP and SURF meetings. A full overview and the slide decks of our presentations can be found on our website at https://nlnetlabs.nl/community/presentations/.

Community Service

We fulfilled the following community positions in 2023:

Organisation	Role	Person
IETF	DNSOP co-chair	Benno Overeinder
IETF	Hackathon co-chair	Benno Overeinder
Forum Standaardisatie	Member	Benno Overeinder
Platform Internetstandaarden	internet.nl steering committee	Yorgos Thessalonikefs
ICANN	RSSAC Caucus member	Benno Overeinder Willem Toorop Jaap Akkerhuis

Organisation	Role	Person
ICANN	SSAC member	Jaap Akkerhuis Maarten Aertsen
ICANN	Various advisory roles	Jaap Akkerhuis
ISO	ISO 3166 MA member	Jaap Akkerhuis
Internet Society	Member advisory council	Jaap Akkerhuis
DNS-OARC	Board member	Benno Overeinder
DNS-OARC	PC member	Willem Toorop
RIPE	DNS WG co-chair	Willem Toorop
RIPE	BCOP TF co-chair	Benno Overeinder
NLUUG	PC member	Willem Toorop

Academia

As of March 2021, Ronald van Rijswijk-Deij has been appointed Professor of Network and Security in the chair of Design and Analysis of Communication Systems (DACS) at the University of Twente. He will also remain involved with NLnet Labs as a science advisor. In this capacity he works with Benno Overeinder in giving direction to NLnet Labs' R&D efforts on both strategic and tactical levels, collaborates with the people at NLnet Labs, and maintains contact with other parties.

Team

NLnet Labs strives to be a lean organisation, aiming to achieve its goals with minimal management overhead. We value 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, bound together by our love of open source and open standards (read our Code of Conduct: https://nlnetlabs.nl/conduct/).

Almost all our staff members are software developers or 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 and science. The team now also has two members focusing on bridging policy and government. Other responsibilities – e.g. management, product development, finance and auditing, staffing and recruiting, sales and marketing – are shared by two people.

Recruiting

Tom Carpay and Tim Bruijnzeels went for new opportunities and have left NLnet Labs. Tim's work on the RPKI tooling will be taken over by the other members of the BGP routing team for now.

Koen van Hove started on January 1st as a research and software engineer at Open Netlabs. His full-time assignment encompasses three days a week at our organisation as a software engineer, and two days at Twente University, where he will work on his PhD under Roland van Rijswijk-Deij.

Located at Amsterdam Science Park, NLnet Labs has strong local and international links with academia, research organisations and industry parties. Being part of that ecosystem makes us an appealing employer for developers and researchers with an interest in applied R&D and a love of impactful open-source software.

Funding

Income From Support and Development

As in previous years, a key objective for 2023 was to further increase the revenue from support contracts and sponsored feature development. To ensure the future sustainability of the NLnet Labs non-profit foundation, support and development contracts are offered through Open Netlabs B.V. This company is a wholly owned, taxable subsidiary of the NLnet Labs Foundation. As such, it serves the non-profit public-benefit objectives of its parent, and is governed and managed in accordance with the NLnet Labs charter.

Open Netlabs offers support contracts with a service level for our production-grade software packages such as NSD, Unbound, Krill and Routinator. Customers receive support and early access to security patches, and through their financial contributions also support our mission to provide free and open software for all.

Open Netlabs also 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.

Grants and Subsidies

Every year since 2012 NLnet Labs has received a generous subsidy from SIDN. This pledge was renewed in 2022 for another five years. We are also grateful for the substantial, long-term grants that Infoblox, Verisign, Meta, Comcast and SUNET have donated.

Last but not least, we have also received numerous ad-hoc donations from organisations as well as individuals, for which we are equally grateful.

One of the reasons we could develop our RPKI toolset with full force is because several organisations in the industry decided to support us, either financially or with infrastructure. The National Internet Registry of Brazil, NIC.br, supported the development of Krill during the period 2020–2022, which allowed us to dedicate full-time staff to work on the toolset.

APNIC (the Asia Pacific Network Information Centre), the regional internet address registry (RIR) for the Asia-Pacific region, also supported the continued development of our RPKI toolset, funding the development of Hardware Security Module (HSM) support for Krill. LACNIC funded features such as offline Trust Anchor and general improvements for Krill and the use of Routinator for pre-validation before publication.

Additional income came from several organisations, including internet service providers, internet exchanges, tier-1 carriers, CDNs and cloud providers purchasing support services.

Furthermore, DigitalOcean, Fastly and Amazon Web Services provided us with their services free of charge so we could set up an automated test platform for the software, host analysis tools, and make our production platform as resilient as possible.

Financial Results NLnet Labs

Income			
	2022 Actual (k€)	**2023 Actual (k€)**	**2023 Budget (k€)**
SIDN Subsidy	150	125	125
Other donations	217	162	210
Consultancy and other income	132	132	122
Research and projects	209	375	360
Income from Interest	2	3	1
Total	**710**	**797**	**818**

Expenditure			
	2022 Actual (k€)	**2023 Actual (k€)**	**2023 Budget (k€)**
Staff	674	693	700
Housing	68	73	69
Travel	31	31	30
Depreciation	3	5	0
Project Costs	1	75	0
Other Costs	41	45	35
Sub Total	818	922	834
Negative Result Open Netlabs B.V.	-3	144	0
Project Reservations	-105	-269	-16
Total	**710**	**797**	**818**

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	2	General Reserve	1096
Open Netlabs B.V. Stock and Loans	82	Special Purpose Reserves	11
Receivables	328	Current Liabilities and Accruals	189
Bank and Cash	884		
Total	**1296**		**1296**

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 2023		
Name	**Role**	**End of Term**
Cristian Hesselman	Chair	June 30, 2024
Marieke Huisman	Secretary	August 30, 2024
Sjoera Nas	Member	December 31, 2023
Andrei Robachevsky	Member	June 30, 2025
Jochem de Ruig	Treasurer	June 30, 2024

Four board meetings took place in 2023. Benno Overeinder participated in the board meetings in his role as director of NLnet Labs and Open Netlabs BV.

Board members do not receive any compensation for their board work. Expenses may be reimbursed if necessary (EUR 0 in 2023). The table below shows the additional functions held by board members and directors of Stichting NLnet Labs.

Additional Functions Held By NLnet Lab Board Members and Directors in 2023	
Name	**Function(s)**
Cristian Hesselman	- Director of SIDN Labs - Member of ICANN SSAC - Professor University of Twente - Member of the ACCSS Advisory Board - Member of the Supervisory Board of the Enschede Public Library - Member of the Cybers Security Council
Marieke Huisman	- Full Professor University of Twente
Sjoera Nas	- Senior Privacy Advisor, Privacy Company - Advisory Board SIDN Fonds - Board member of Stichting Appeltaart
Benno Overeinder	- See the Community Service section for an overview
Andrei Robachevsky	- Technology Programme Manager Internet Society - Member EU MSP Standardisation
Jochem de Ruig	- Organic wine entrepreneur at Wilde Wijnen

Looking Ahead to 2024

Over the next year, we expect our new projects to take shape and generate interest from users across academic institutions and industries, as well as individuals. Our DNS Rust library Domain has been funded by STF from October 2023 till the end of 2024. This funding allows us to establish new DNS functionalities for the future. Rotonda has generated significant interest in the routing community, both in industry and academia. In the coming year our focus will be on use cases based on Rotonda to demonstrate the framework's usability and enhance the project's financial sustainability. NSD, Unbound and Routinator remain strong products in demand for support contracts. Overall, these developments indicate positive growth and promising prospects for the future.

Our team has remained stable and largely unchanged over the past few years. For the coming years we anticipate a modest increase in full-time equivalents (FTE) to achieve our strategic goals, funded through sustainable revenue growth.

.

Colophon

Editors

NLnet Labs

Design

Richard de Ruijter, Graphic Design & Illustration

Photo Credits

Photo on page 6 by Brett Garwood on Unsplash

Contact

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

© NLnet Labs