NLnet Labs

Annual Report 2017

For an Open Internet

1 Highlights

Welcome to the Annual Report of the NLnet Labs Foundation for the year 2017. This is where we report on our activities over the last year. It aims to provide transparency on our efforts to help make the Internet more stable and secure for everyone.

NLnet Labs has a long heritage in research and development, Internet architecture and governance, as well as stability and security in the area of DNS and inter-domain routing. This was acknowledged by Jaap Akkerhuis being admitted into the Internet Hall of Fame, as recognition for the tireless work in the development of the Internet in the Netherlands and Europe since the early 1980s.

The focus on Internet security and stability is also reflected in the work that the foundation does as member of the Dutch Platform for Internet Standards. As an extension of these efforts, we are also responsible for the development of internet.nl, which is widely recognised for the quality of the tests and informative information that help organisations adopt modern standards. This culminated in NLnet Labs presenting at the yearly congress of ECP, where we demonstrated how to impersonate emailing in the name of a minister and explain how to effectively protect against such spoofing.

2017 was also the year that saw a major focus on DNS privacy. Internet users became much more aware of the fact that private information can be leaked through the DNS, and looked for ways to minimise this. The launch of the Quad9 DNS service fuelled this interest even more, with several blog posts mentioning that this solution was powered in part by Unbound. As Quad9 offers secure connections using DNS-over-TLS, there was also a massive spike in the interest in the getDNS library, in particular the stub resolver implementation it offers called Stubby. Several blog posts were written on how to use Stubby to securely communicate with Quad9 and various other DNS services that support security features, further strengthening the DNS privacy community efforts that are spearheaded by NLnet Labs, Sinodun and No Mountain Software.

Another highlight is our active involvement in the preparation for the KSK key roll-over, planned for October 2017. Jaap Akkerhuis has been an active participant in the KSK Rollover Design Committee several years ago, Benno Overeinder participated in panels at ICANN meetings and contributed to blog posts and outreach activities by ICANN. This, together with the Root Canary project together with SURFnet and the fact that Unbound was full ready for the KSK 2017 rollover, ensured that everything was in place to make the process a success.

Meanwhile, considerable effort was put in our core software lineup, which includes the authoritative name server NSD, the validating recursive resolver Unbound, the policy-based zone signer OpenDNSSEC, as well as getDNS, the modern, asynchronous DNS API that is specifically aimed at application developers and operating system distributors. This year saw a large number of releases with new functionality, keeping up with the demands of DNS operators around the world. This active development led to the developers at NLnet Labs discovering a flaw that made it possible to downgrade secure connections, which affected Unbound, Google public DNS, PowerDNS and Dnsmasq. We managed to work with all DNS resolver implementers to reliably document and fix this issue, earning respect and praise from the DNS community.

2 Areas: DNS and DNSSEC

The topics DNS and DNSSEC are strongly embedded in NLnet Labs' activities. Besides the well-known and widely adopted DNS name servers and DNS libraries developed by NLnet Labs, the OpenDNSSEC project and getdns API project are important initiatives for the Internet community. All our activities focus on the development and maintenance of tools that facilitate the provisioning and use of DNSSEC, and as such we lower deployment barriers of a technology that will allow for further innovation of global Internet security mechanisms.

By developing alternative implementations of name servers we also increase the stability of the DNS by offering diversity in code-base.

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

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

2.1 Provisioning of DNS Server-Side

2.1.1 NSD

NSD is NLnet Labs' authoritative name server and designed to be robust, light-weight, high-performance, secure, and single purpose. From its first release in 2002 up to the latest major release of NSD 4 in late 2013, the software has shown to be a mature and dependable authoritative name server that is used in many places like root servers, TLDs, CDNs, ISPs, up to enterprises and SMEs. NSD can be found at different parts in authoritative name server infrastructures, for example, as a reliable and performant secondary name server serving queries for a hidden primary, or as an instance of an Anycast DNS service.

NSD 4 is actively maintained and there are new developments to improve performance, to reduce memory usage, and to implement new open standards and features to meet changing operational requirements. The design philosophy remains with the principles of robust, light-weight, high-performance and secure.

Goals

NSD 4: To provide a stable and high-performance authoritative DNS server for a larger, more diverse set of users. Continued implementation and support of new IETF standards, improved performance and reduction of memory usage (memory footprint). Additional features to meet operational requirements are also considered to comply with current and future practices.

NSD 4 Activities

In 2017, we continued with the development and maintenance of the source code to support new open standards and to accommodate to new operational requirements.

In discussions with authoritative DNS nameserver operators we made a number of specific improvements on NSD. For faster notification of secondary nameservers, we have implemented parallel notification with faster timeouts. For the zone transfers more sockets are used. This speeds-up communication with a larger set of servers. The memory usage is further reduced by using a more memory efficient data structure resulting in about 16% memory reduction. A second improvement is a compile option to use packed data structures at the expense of unaligned memory reads. This gives another 17% memory usage reduction.

Results

NSD 4 has seen a series of maintenance releases (v4.1.15 – v4.1.19) with bug fixes, performance improvements and new features in 2017.

The NSD 4.1.16 release introduces the option in nsd.conf to enable minimal responses, e.g., responses without the NS record in the authority section and glue for that in the additional section, when such an NS record is not necessary. The NS record is of course still present for prime responses and referral responses. The zone parser can parse the ED25519 and ED448 acronyms.

The release of NSD 4.1.18 incorporates the two important improvements mentioned above in the previous section, namely features for saving memory and faster notification.

Impact

NSD clearly serves its design goals: to provide an alternative implementation to authoritative DNS servers in order to increase resiliency and stability of the global DNS infrastructure: NSD is used on root servers such as the I, L, and K root servers and many top-level domain registries, including .NL, .DE, .BR, .SE, and .UK. The main motivations for running NSD are high-performance, stability, and to have code diversity within the installed base. The new features and improvements to meet operational requirements makes NSD a well-established option for an authoritative name server.

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

2.1.2 DNSSEC Zone and Key management: OpenDNSSEC

OpenDNSSEC targets to be a complete solution to DNSSEC management that has been designed to be integrated seamlessly in existing DNS set-ups. It will take unsigned zones from file or an existing DNS server adding signatures before passing the zone to the public authoritative name serves. It will do incremental zone signing for large zones and handle the complex key management and roll-over for any kind of scenario. It allows for flexibility in operation varying from one key maintenance policy to per-zone configuration and integrate with any authoritative name server (vendor independent).

Goals

Continued development and support of OpenDNSSEC. The 1.4 branch will serve as the LTS version and will not be used to develop new features, whilst the newer version 2 will see focus for new features and code improvement.

The main focus in 2017 was the continued development and maintenance of OpenDNSSEC version 2 for stability in production environment. Next the we started implementing new features for so-called fast-updates (for incremental zone updates via IXFR, Dynamic DNS or a RESTful API) and high-availability. The goal for fast-updates was set of the end of the year, however this objective was adjusted to first half of 2018.

Activities

In 2016 we already announced that version 1.3 to be going end-of-life in 2017. There are no 1.3 installations yet in existence to our knowledge and were told some installations have been upgraded (even to version 2). We have not set a lifetime on 1.4 and will not do so for the next year to allow for proven in-production stability of the development branch of version 2. At that time we will give a one-year notice of end-of-life of the 1.4.

Major development for OpenDNSSEC 2.2 has been fully underway in 2017. Whilst version 2.0 and 2.1 mainly focussed on the enforcer, structural improvement for the signer were postponed. Fast updates, where a change to the input zone is visible in the signed output zone in at most minutes, requires a much higher level of concurrency that the signer currently can deliver.

For the enforcer we do however also have some improvements in 2.2 that allow the enforcer to lay out the scenario of a roll-over in advance.

We have updated and improved the course on DNSSEC and OpenDNSSEC. The two different courses for OpenDNSSEC that were developed earlier with external partners have been largely merged and practical problems experienced with previous trainings have been addressed.

Results

We have released an update on OpenDNSSEC 2.0 branch. Version 2.0.4 contained only a small urgent fix and support for OpenSSL 1.1. The first release of 2.1 could follow shortly thereafter. Since 2.1 is a gradual improvement of OpenDNSSEC, we were comfortable to immediately cease support for version 2.0 and to declare 2.1.0 the direct successor of 2.0.4 that requires no upgrade procedure.

OpenDNSSEC 1.4 is still the LTS version and received two releases to fix some issues. One important fix was to handle a case where, with an incorrect input zone, the produced signatures could be bogus. This fix still however requires some manual intervention once the incorrect input zone file has been repaired. OpenDNSSEC versions up to 2.2 will require some interventions but will keep the zone correctly signed.

In 2017 we released the gradual improvement of OpenDNSSEC version 2.1. No migration was necessary and version 2.1 contained several smaller improvements. Most notably is that the enforcer will be better to schedule changes per zone individually. There is now support for ECDSA and GOST, we actively discourage the use of SHA1 for DS records, memory leaks have been addressed, and the signer will have a faster start-up time in case the underlying HSM is slow to iterate over many keys. New zones will short cut the roll procedure and be used fully signed faster.

Impact

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

OpenDNSSEC has a number of high-profile users as listed at https://www.opendnssec.org/about/-known-users/.

2.2 Client-Side Availability of DNSSEC

2.2.1 Unbound

Unbound is one of the main implementations for DNSSEC-enabled DNS resolution and thereby an important contributor to the deployment and uptake of DNSSEC. Unbound is a flexible and versatile resolver that performs well in both small setups and large, complex cluster architectures, and different sizes in between. Unbound deployments can be found at large ISPs, CDNs, cloud services, and small home routers.

Goals

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

Activities

Unbound has seen a number of noteworthy new features and improvements in 2017. Two important activities were preparations for the KSK-2010 to KSK-2017 roll-over planned in October 2017, and merging the EDNS client subnet implementation into the main development branch.

In preparation of the KSK-2017 roll-over planned for October 2017, we have included the new root trust anchor ID 20326 (the new KSK-2017 key) in Unbound. For version 1.6.5 we fixed RFC5011 trust anchor tracking for users that install Unbound (a fresh install) between September 11 and October 11, 2017. For Unbound resolver clients, we implemented a trustanchor.unbound CH TXT query that responds with the trust anchors and their key tags. RFC8145 support is also made available to signal trust anchor to authoritative name servers. Eventually the KSK-2017 roll-over is postponed to 2018, as the various measurements by ICANN indicated that a certain group of resolvers did not yet accepted the new KSK-2017 as a trust anchor (for reasons still indeterminate, but likely legacy code or misconfiguration).

Two contributions by external software developers are response actions based on IP address (for client-based filtering) and dnscrypt support in Unbound. On special request, we implemented an Unbound module ipsecmod for opportunistic IPsec.

Ralph Dolmans and Karst Koymans (University of Amsterdam) discovered a DNSSEC downgrade attack, published as CVE-2017-15105. Coordination with other DNS software vendors and responsible disclosure resulted in a public announcement in January 2018. Dolmans published a blog post detailing on the vulnerability and its solution.[1]

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

Results

In 2017 a series of 1.6.1–1.6.7 releases have been published. The releases include some regular code maintenance and bug fixes. For the planned KSK 2017 key roll-over, almost all versions included new functionality or improvements.

1-https://medium.com/nlnetlabs/the-peculiar-case-of-nsec-processing-using-expanded-wildcard-records-ae8285f236be

IP address based response actions are released with Unbound 1.61, and version 1.6.2 incorporated EDNS client subnet and dnscrypt. Version 1.6.4. introduced support for ED25519 algorithm, fastrpz patch in contrib, and the new ipsecmod module.

Impact

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

2.2.2 DNSSEC Trigger

DNSSEC Trigger is an effort to cope with the 'DNSSEC last mile' problem. In order to be able to rely on DNSSEC validation one wants to bring DNSSEC close to the application, preferably on the OS so that the benefits of DNSSEC are available for all. The principle of DNSSEC validation at the end-point and bringing it close to the application is also a design goal of the getdns library, see Section 2.3.1.

Goal

Develop a concept and prototype implementation of a tool to deploy DNSSEC validation at the end-point, i.e., the user application. Important is the interaction with guest operating systems like macOS, BSD, Linux, and Windows. DNSSEC Trigger plays also a part in the incorporation of DNSSEC support in GNOME NetworkManager, which is primarily developed by Red Hat software engineers.

Activity and Results

DNSSEC Trigger releases are not frequent. In general new versions are necessary to deal with install and integration with new OS releases. DNSSEC Trigger 0.14 was released in October 2017 to fix install problems on macOS Sierra and High Sierra. The binary packages for macOS and Windows bundled the just-released unbound 1.6.7 that sends telemetry data about the root trust anchor. Version 0.15 was release in December 2017 to fixe failure to start on macOS and Windows.

For the Linux/GNOME NetworkManager we receive patches from the Red Hat software engineers, which we merge with our code base.

In its current design, DNSSEC Trigger is a set of scripts and code that relies on Unbound that either uses the forwarders obtained from DHCP, or falls back to do its own recursive queries. In 2018 we will study how getdns stub resolver fits in, and whether it can be an alternative setup of DNSSEC Trigger.

Impact

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

2.3 DNS Development Frameworks

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

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

by enabling encryption everywhere (see also Pervasive Monitoring Is an Attack, RFC 7258). The use of DNS-over-TLS (as part of DNS Privacy activities) is getting some traction with the introduction of Quad9, an anycast DNS platform that provides end users robust security protections and privacy.

2.3.1 Secure getaddrinfo/getnameinfo (getdns API)

getdns API is an asynchronous DNS API, whose API specification is developed in collaboration with application developers. getdns offers application developers a modernized and flexible way to access DNS security (DNSSEC) and alternative transport, like TCP pipelining, DNS-over-TLS, or STARTTLS for DNS (enhancing DNS privacy). The library incorporates a number of methods to successfully receive a DNSSEC validated answer, for example DNSSEC roadblock avoidance or DNS64 at the end-point for validation of IPv4 answers by IPv6-only clients.

With all its flexibility, expressiveness and by making primitives for security and privacy easily available, the getdns library can stimulate application developers to design innovative security solutions in their applications.

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

Goal

Continued development and maintenance of the modern asynchronous DNS API library. Besides the development of the software, we generate interest and traction of a new alternative for getaddrinfo/-getnameinfo that includes DNSSEC functionality for application developers and provide a modern (asynchronous) DNSSEC-enabled system stub resolver that is versatile in many situations and setups, e.g. DNSSEC roadblock avoidance or DNS64 in IPv6-only networks.

Part of our outreach activities are meetings with network engineers and software developers to introduce DNSSEC and DANE functionality in other API libraries. For example, a conceptual high-level and easy to use ConnectByName library to setup connections with options for happy eyeballs, DNSSEC, DANE and authenticated TLS would greatly increase modern standards and improve security and privacy of the end-users.

Activities

getdns started out with the 1.0.0 release in January 2017, the first complete, stable, robust and production ready implementation of the getdns API spec. Since then, getdns saw 7 more releases in 2017. One of the most prominent features was introduced with the 1.2.0 release (September 2017), and inspired by the DNSSEC root Key Signing Key rollover, namely Zero-configuration DNSSEC.

In November 2017, the first DNS-over-TLS public DNS service started: Quad9. Because of this, and because of the blog posts by Alex Band[3] and Stephane Bortzmeyer[4] describing how to use this service with Stubby, Stubby gained much popularity.

Results

The first stable and complete implementation of getdns library version 1.0.0 was released in January 2017. The 1.1.0 release (April) introduced the DNS Privacy stub resolver Stubby. Stubby encrypts DNS queries sent from a client machine (desktop or laptop) to a DNS Privacy resolver increasing end user privacy.

3-https://medium.com/@alexander_band/privacy-using-dns-over-tls-with-the-new-quad9-dns-service-1ff2d2b687c5

4-https://labs.ripe.net/Members/stephane_bortzmeyer/quad9-a-public-dns-resolver-with-security

New features with 1.1.0 release were all related to Stubby:

- Hooks for asynchronous DNS serving capability
- Conversion from string to getdns data types and configuring from a getdns dictionary, which formed the basis for configuration files in use with stubby.

Zero-configuration DNSSEC introduced in getdns 1.2.0 allows tracking and automatically acquiring the root DNSSEC trust anchor securely on the fly when needed, in a way completely transparent to the applications making use of getdns. It takes into account that those applications might run sporadically (rendering RFC5011 tracking unusable), and run with user privileges which puts higher security requirements on persistent storage.

To deal with packaging difficulties, Stubby was moved to it's own repository in September too.

The start of Quad9 DNS-over-TLS public resolver generated some publicity for getdns and Stubby. As a result, we received much feedback about many different installation platforms, resulting in many fixed bugs and a few new desirable configuration parameters, which led to version 1.3.0 the final stable getdns/Stubby release in December.

Impact

The ideas that are at the basis of the getdns API library and stub resolver are adopted with interest by the industry. The Quad9 public open resolver and the publicity that came with it, is a good indicator that security and privacy become more and more relevant, also for DNS.

We presented getdns and DNS privacy at various meetings in 2017, amongst other the IETF and RIPE meetings, OARC workshops, or at the ICANN meeting.

2.3.2 ldns

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

Goal

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

Activities

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

Results

ldns1

ldns1 has not seen releases in 2017, but there has been a steady stream of contributions and bug fixes which have been addressed in the git repository. A 1.7.1 release with these is expected in 2018.

ldns2

The core for ldns2 is in getdns (and partly also in Unbound) and is stable. For a ldns2 release we want to keep offering the former API alongside the new functions, but have it use the newer functions underneath. This has not been done in 2017 and is still on the roadmap for 2018.

Impact

The ldns library is popular with DNS sofware developers and research engineers. ldns is used in tools, servers and by researchers to implement experiments, for example for DNS measurements and analysis.

2.3.3 Net::DNS

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

Goal

Regular maintenance and continued clean-up of the architecture.

Activities

In February we celebrated Net::DNS's 20th birthday with a 1.08 release. At that time, Net::DNS had seen 85 releases since the 0.02 release in 1997. In 2017 seven more releases followed mostly dealing with user requests and bug reports.

No new version of Net::DNS::SEC were released in 2017.

Results

Releases 1.08 through 1.14 of Net::DNS.

Impact

Net::DNS and Net::DNS::SEC are used in many Perl applications. One of the most well-know application (or tool) is SpamAssassin.

2.4 Other Activities

2.4.1 IETF DNS activity

I-Ds and RFCs

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

This internet draft, which is a joined effort of NLnet Labs with researchers from Fastly, Mozilla and Salesforce, describes a TLS extension for transport of a DNS record set serialized with the DNSSEC signatures needed to authenticate that record set. The intent of this proposal is to allow TLS clients to perform DANE authentication of a TLS server without needing to perform additional DNS record lookups and incurring the associated latency penalty.

The draft has seen four revisions in 2017 and makes good progress towards finalization. IETF TLS Working Group Last is expected to be issued in first half of 2018.

Hacakthons

- IETF 98 Hackathon, DNS/DNSSEC/DANE/DNS-over-(D)TLS:[5]

5-https://datatracker.ietf.org/meeting/98/materials/slides-98-hackathon-dns-00

- Zero configuration DNSSEC in getdns

- IETF 99 Hackathon, DNS/DNSSEC/DPRIVE/DANE:[6]
  - Deckard root KSK rollover testing of Unbound
  - DNSSEC chain TLS extension in getdns and Unbound, draft-ietf-tls-dnssec-chain-extension]
- IETF 100 Hackathon, DNS/DPRIVE/DNSSEC/DANE:[7]
  - DANE Authentication of TLS Upstreams in Stubby, draft-ietf-dprive-dtls-and-tls-profiles
  - best overall winner of hackathon

2.4.2 Root Canary

In May 2017 NLnet Labs joined the Root Canary Project, together with SURFnet, the University of Twente, Northeastern University, SIDN Labs, the RIPE NCC and ICANN. The goal of this project is to monitor and measure the rollover of the DNSSEC root Key Signing Key (KSK), that is due to take place in 2017/2018.

In early June, we have setup a matrix of 86 Signed zones with all different delegation hash algorithms and all different signing algorithms, including expired ones, and the until then never in the before used ED448. Each zone is resigned every week. Since early July, the zones are transfered from the master servers at NLnet Labs to the secondaries of the RcodeZero anycast network which was kindly offered for this purpose by nic.at. RIPE provided measurements that query for a secure and a BOGUS record for each zone, every hour from every probe on RIPE Atlas.

The root KSK rollover was initially scheduled for October 11 2017, but was hen postponed. Although the initial measurement purpose of the Root Canary was not met, the initiative had valuable spin-off results and has amongst other things led to fixes in PowerDNS and Knot Resolver.

3 Area: IP and Infrastructure Security and Stability

In order to increase the security and maintain the stability of the Internet infrastructure, NLnet Labs contributes to the understanding of its dynamics both in terms of technology as well as its operation. In addition, we put effort in the development of tools, applications and practices that lower the barriers to the deployment of security features.

NLnet Labs role is unique in the sense that Labs is neither vendor, nor operator and takes an inter-operator global perspective.

6-https://getdnsapi.net/presentations/ietf99-hackathon/
7-https://datatracker.ietf.org/meeting/100/materials/slides-100-hackathon-sessa-dns-team-00

3.1 Inter-domain Routing Security and Stability

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

Goal

The SAND project[8] focuses on solutions for dynamic DNS anycast services to deal with changes in Internet connectivity, DNS query traffic, and other factors influencing their service in terms of availability, performance, and possibly security. And while optimizing for these quality of service terms, the operational costs have to be considered also. To achieve these operational performance and cost goals, we believe an automated management system potentially offers the best possible course of action.

The goal of the DAS project (matched funding by NWO) is to investigate the large-scale development and deployment of DNS anycast services, in particular the virtualisation, security and (self-)management of such services. Our approach is to collect unique measurement data from the large-scale DNS infrastructures operated by our industrial partners and analyze this data to validate our scientific results. The DAS project concluded in Spring 2017.

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

Activities

To measure, evaluate and assess anycast networks, an anycast testbed has been created.[9] The anycast testbed consists of 9 locations and is supported by a number of organisations. For measurements of the "performance" (given a set of parameters) the RIPE Atlas measurement infrastructure is used. Results of the experiments and measurements are presented at operational meeting (RIPE and IEPG) and at academic conferences. In the second half of 2017, the partners prepared a second phase of the SAND project, called SAND-3[10], with a kick-off date in Spring 2018.

Results

The research activities resulted in a number of presentations, i.e.and IEPG at the IETF 98, IETF 99, IETF 100, and academic publications (PAM 2017 best paper award and IMC), see Section 7.

Impact

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

Phase two of the SAND project will focus both on research, measurements and analysis, *and* on the design and implementation of tools to support anycast operators in running their infrastructure.

8-https://www.sand-project.nl
9-http://www.anycast-testbed.com/
10-There is no SAND-2 project for similar reasons there is no IPv5.

3.2 Security and Stability of Critical Infrastructures

3.2.1 NTP Security Weaknesses

Goal

The aim of the study is to strengthen and secure the current-state-of-art of the Network Time Protocol (NTP) and Domain Name System (DNS) ecosystem in the Netherlands by understanding how weaknesses in NTP protocol can be leveraged to exploit DNS and undermine the security provided by DNS Security Extensions (DNSSEC).

Activities

During the project, we collaborated with Aanchal Malhotra, a PhD student from Boston University, and Sharon Goldberg, a professor at Boston University. In July, August and September, Aanchal Malhotra was visiting NLnet Labs for the project.

In the project we studied the integrity of the NTP pool in Netherlands that operates important stratum 1 and 2 NTP servers that serve timing information to most of the Internet in the Netherlands. The goal of this measurement is to identify vulnerabilities in these NTP servers that can be exploited for off- and on-path Denial of Service and Timeshifting attacks as described by Malhotra and Goldberg in earlier work on NTP security. In a lab-based experimental study we evaluate how these time-related attacks on NTP can be used to launch attacks on DNS and DNSSEC. With the network measurements and the lab-based experiments we can provide insights into the potential impact of these kind attacks on the Netherland's DNS ecosystem.

Results

The most prominent result from the research project is the observation that current Internet software (including the DNS server software from NLnet Labs), translate time spans to wall clock time stamps, which are vulnerable for NTP attacks.

This work has led to several presentation and to a recommendation Internet draft: draft-aanchal-time-implementation-guidance, which was presented at the NTP working group at the IETF100 in Singapore. The topic of the Internet Draft was received with enthusiasm and the draft became a candidate for working group adoption.

Impact

Despite the importance of NTP, the community still lacks visibility into the robustness of the NTP ecosystem itself, as well as the integrity of the timing information transmitted by NTP. In this study we exemplified the impact of attacks on time protocols (NTP) on DNS and DNSSEC. To the best of our knowledge no previous work has explored this issue before.

3.2.2 Risk Categories in the Impairment of the Internet

NLnet Labs collaborated in a study led by TNO to explore risk categories in the impairment of the Internet. The study focusses on the critical parts of the internet infrastructure (what makes a network of networks into an internet) and which risks are known to exist. The resulting report gives an overview of the risks with a categorisation for further analysis. This document is intended to be input for follow-up discussions, studies, and plan-of-actions *how* to mitigate the risks to the impairment of the internet.

Goal

With the National Security Strategy, the government is investigating which threats may endanger national security and what we can do about it. The first step of the National Security Strategy is to identify and analyze different types of disasters, crises and threats: “What is threatening us and how bad is it?”.

Activities

The exploration was carried out through a combination of desktop study, interviews with various experts, and an expert session in which the results were discussed and tested. During the research, the interim results were always discussed with a peer group with representatives from the Ministry of Justice and Security (specifically NCTV and NCSC), the Ministry of Economic Affairs and Climate and the National Security Analysts Network.

Results

The interviews with national (Dutch) and international experts resulted in a multifaceted display of threats and risks, which were presented to our peer group mentioned above. In January 2018 a final workshop is planned with the peering group and all experts that were interviewed in second half of 2017.

The final report of the project will be ready in the first quarter of 2018.

Impact

The results of the exploration will be described in a report that form a framework with which in a next National Safety Profile (which is expected to appear in mid 2020) the risk of damage to the functioning of the internet can be assessed.

3.3 Adoption of Open Standards: IP and Security

3.3.1 Platform Internet Standaarden and Internet.nl

Platform Internet Standaarden is a national initiative in the Netherlands to promote open standards for a secure and stable Internet.[11] New Internet standards for IPv6, DNSSEC, TLS and email (SPF, DMARC and DKIM) are important but find slow uptake by ISPs. The platform informs and promotes new standards by reaching out to the different stakeholders and make insightful what they can do to speedup adoption and deployment of these standards.

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

Goal

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

Activities

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

11-https://ecp.nl/activiteiten/platform-internetstandaarden/

NLnet Labs' staff participated in several expert meetings, and presented with other partners of the platform at the ECP.nl conference on safe email.[12] Some of the platform members had a meeting with dmarcian[13] (a full service provider of DMARC) at NLnet Labs. Besides discussions on safe email (DMARC, DKIM and SPF), there were also specific software discussions, in particular on features for libunbound that can be used in context of these technologies.

Results

In July 2017 a redesign (of the user interface) of internet.nl was launched. The comprehensive explanations on the improved test website provide more guidance to users to get modern Internet Standards. The redesign makes the website better accessible on mobile devices and for users with disabilities.

Besides the new design, there has been many other changes, fixes and improvements made to the website. We continuously maintain and improve the internet.nl website.

Impact

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

Individual countries are interested in similar initiatives. With project partners funded by GFCE[14] we are planning for 2018 to provide internet.nl in other languages, such as Russian, Spanish, or Portuguese.

3.4 DNSSEC-Based Security and Trust

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

3.4.1 EU H2020 LIGHTest Project

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

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

12-Plenary opening Jaarcongres ECP, https://ecp.nl/jaarcongres-2017/programma/
13-https://dmarcian.com
14-https://www.thegfce.com

Goal

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

Activities

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

NLnet Labs organised with OIX Open Identity Exchange a small workshop during the IETF in Chicago to talk with experts from this community. At another IETF meeting in Singapore, we had an informal followup meeting discussing design decisions and alternatives, and received useful feedback. At the IRTF (IETF Prague), we presented the LIGHTest project at the Decentralized Internet Infrastructure Research Group (dinrg).

Results

Contributions to the various tasks and reviews of documents. NLnet Labs is task leader in two tasks related with DNSSEC expertise and building blocks, and critical infrastructure analysis.

As the task leader, we delivered a report on DNS and DNSSEC building blocks in August 2017. We contributed to the various other tasks, either writing reports, giving advice or setting up infrastructure for use-case validation by other partners.

The critical infrastructure analysis report is due for August 2018.

Besides the different meetings we have attended, NLnet Labs presented the LIGHTest project at different meetings and workshops. See also Section 7.

Impact

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

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

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

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

4.1 ICANN

Akkerhuis is member of the Security and Stability Advisory Committee (SSAC) and the Root Server System Advisory Committee (RSSAC) Caucus.[15] Akkerhuis co-authored a number of SSAC and RSSAC reports.[16]

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

Akkerhuis and Overeinder attend the ICANN meetings and are actively involved in the ICANN TechDays and DNSSEC workshops. They also participated in the CDAR root stability study commissioned by ICANN. In February 2017 the final report wast published, see Section 7.

4.2 RIPE / Network Operations Community

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

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

During RIPE 74 and RIPE 75 NLnet Labs' staff disseminated its knowledge and expertise with a number of presentations at the RIPE working group sessions. See also Section 7.

Van Halderen and Akkerhuis participated in the APTL 72 meeting in Tbilisi. Van Halderen organized a two-day course on DNSSEC and OpenDNSSEC, which was well-reiceved.[17]

4.3 IETF and Technical Community

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

Dolmans, Toorop and Overeinder participated in the IETF hackathon (IETF 98, IETF 99 and IETF 100) to develop and test new features for the getdns API project, with RFC compliance testing of Unbound with Deckard (RFC5011 compliancy), or evaluate new proposed protocols like DNS-over-HTTPS.

15-https://www.icann.org/resources/pages/rssac-caucus-2014-05-06-en
16-https://www.icann.org/groups/ssac/documents and https://www.icann.org/resources/pages/rssac-caucus-work-parties-2017-06-20-en
17-https://www.nlnetlabs.nl/news/2017/Sep/11/dnssec-training-at-aptld-72/

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

Dolmans and Toorop attended OARC meetings in 2017. References to OARC presentations can be found in Section 7. Ralph Dolmans is appointed as DNS-OARC PC member for 2017-2018.

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

4.4 Other

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

5 Area: NLnet Labs Continuity

5.1 Strategic plan

During 2017 we reviewed NLnet Labs mission, vision and strategy and published an updated Strategic Plan.[18] The document emphasizes our mission "*To provide globally recognized innovations and expertise for those technologies that turn a network of networks into an Open Internet for All.*" Further, it describes how our mission relates to our statutes and the principles for setting direction. The strategy plan also discusses the directions in which we plan to develop over the coming years, and our ideas to secure financial continuity.

In the first half of 2018, we will update and extend our Strategic Plan for the next period of two to three years.

5.2 Open Netlabs BV

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

Open Netlabs BV operates as the commercial vehicle supporting the open source activities by securing sustainable income on the longer term. The positioning and promotion of the activities are successfully made known and discussed during events like ICANN, IETF, RIPE and DNS OARC meetings.

In 2017, support for the main software products of NLnet Labs, NSD, Unbound and OpenDNSSEC, were offered in different levels of SLAs. Besides SLA support, Open Netlabs also provided consultancy to users and collaborated in a funded research project with partners.

18-https://www.nlnetlabs.nl/downloads/foundation/Strategic-Plan.pdf

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

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

6 NLnet Labs Organization and Finance

6.1 Board

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its board consists of three to five members with staggered terms. The board's composition and most recent rotation schedule is shown in the tables.

Four board meetings took place in the year 2017. Benno Overeinder participated in the board meetings in his role of director of NLnet Labs and as the director of Open Netlabs BV.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€617 for 2017). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2017

name	function	end of term
Frances Brazier	secretary	September 30, 2018
Cristian Hesselman	chair	June 30, 2018
Ted Lindgreen	member	March 31, 2019
Sjoera Nas	member	September 30, 2020
Andrei Robachevsky	member	June 30, 2019
Jochem de Ruig	treasurer	June 30, 2018

Director and Board Member Additional Functions in 2017	
Frances Brazier	• Professor Engineering Systems Foundations at the Technische Universiteit Delft (TU Delft)
Cristian Hesselman	• Manager SIDN Labs
Ted Lindgreen	None
Sjoera Nas	• Autoriteit Persoonsgegevens • Advisory board member SIDN Fonds
Andrei Robachevsky	• Technology programme manager Internet Society • Member EU MSP Standardisation
Jochem de Ruig	• CFO RIPE NCC
Benno Overeinder	See page 26

6.2 Staff

NLnet Labs employed eight people in 2017: Jaap Akkerhuis, Ralph Dolmans, Berry van Halderen, Benno Overeinder (managing director), Hoda Rohani, Yuri Schaeffer, Willem Toorop and Wouter Wijngaards. The director of Stichting NLnet Labs is responsible for the daily management of all activities of the laboratory, including development of strategies and plans for new activities.

Finances are administered by Patricia Otter of Stichting NLnet.

6.3 Offices

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

6.4 Fiscal Status

On 20 September 2007, NLnet Labs has been recognized as an institution with general benefit objectives, "Algemeen Nut Beogende Instelling (ANBI)". This status has become relevant under new regulations that are effective as of January 1, 2008.

6.5 Finances

NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in June 2018, these are the unaudited numbers.[19]

Stichting NLnet Labs primarily finances its projects and activities from grants and donations. In 2017, about 40 percent of our budget was covered by the subsidy contract with SIDN (the Internet domain registry for the Netherlands). This subsidy contract provides for a structural financing for the period Jan 1, 2017 – December 31, 2021. For 2017, the contract provides a subsidy of €325.000, split in a €250.000 gift and a €75.000 sponsorship on projects. In the budget for 2017 the gift and subsidy were added together (see table Income), but in the actual income column in the table we have split the two properly. (Hence the difference in budgeted SIDN subsidy and actual SIDN subsidy.)

A second means of income are donations and sponsoring by other parties. In the past years, NLnet Labs has developed a sponsor program with a number of partners from the Internet industry. For 2017, we would like to acknowledge Verisign, Infoblox, IIS (The Internet Foundation In Sweden), Afnic, ICANN, CIRA, NZRS, and DK Hostmaster A/S for their continued generous support.

Open Netlabs BV is an additional source of income in 2017 by offering Unbound, NSD, and OpenDNSSEC support contracts to partners in the industry. In addition, income may be obtained by providing consultancy or subsidized research on Internet architecture, governance, and technology issues and by providing Open Source programming services to third parties. Relevant activities in these areas are reported in Section 5.2.

For the financial sustainability and continuity of NLnet Labs, 2017 showed a positive perspective. With smaller portion guaranteed financed budget, the organisation showed that with sponsoring by industrial partners, an EU H2020 project and income generated by Open Netlabs, the financial position of NLnet Labs is healthy.

19-Audited finances can be found in "Kengetallen Jaarrekening 2017" as published on https://www.nlnetlabs.nl/annualreports/.

6.5.1 Income in 2017

At the end of 2016, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2017, with a total of 759 k€. Based on this budget, a 250 k€ gift and a 75 k€ projects sponsorship was granted by SIDN.

Stichting Internet Domeinregistratie Nederland

is NLnet Labs' major benefactor.

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

In addition NLnet Labs received significant donations from Infoblox, Verisign, Afnic, DK Hostmaster A/S amounting to a total of 61 k€ income above budget.

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

Interest received amounted to 11 k€.

The following organizations are acknowledged for their generous contributions

VERISIGN

Infoblox

IIS

afnic

ICANN

.ca | Canadians Connected

NZRS

dk hostmaster

6.5.2 Expenditure in 2017

The major expenditure categories of NLnet Labs in 2017 are staff, travel and housing. In January, we were at the budgeted staff of 8 persons (7.6 FTE). The total expenditure on staffing in 2017 is 631 k€. Housing and travel make up for another 93 k€ out of the total of 766 k€ expenditure (not included project costs).

To finance our routing security plans in 2018, we increased the ENGRIT designated reservation to 65 k€. In 2015 and 2016, we co-funded a postdoc researcher at the University of Twente. In 2018, we start another two year project with the University of Twente (and co-funding with SIDN Labs). For this collaboration we set the SAND reservation to 81 k€ for payments in 2018 and 2019.

The H2020 LIGHTest project is partly pre-financed in 2016 and has been assigned to a reservation in our balance sheet. In 2017 we have withdrawn 70 k€ from this reservation to cover our direct project costs.

After making these reservations and valuations NLnet Labs had a positive result of 41 k€; 88 k€ is added to the general financial reserve (total of 657 k€ at the end of 2017) and 47 k€ is withdrawn from the special-purpose reserves (total 253 k€ at the end of 2017).

6.5.3 Budget for 2018

The 2018 is based on having 7.6 FTE we have budgeted a total expenditure of 855k€.

In June, 2017 Stichting Internet Domeinregistratie Nederland (SIDN) signed a five year contractual commitment to subsidize a substantial part of the expenditure needed to execute our chartered activities. For 2018, SIDN will cover 225 k€ in four quarterly grants of about 56 k€. Additionally, SIDN committed 75 k€ on special projects subsidy for 2018. Other donations and subsidies from industry will account for 180 k€, funded projects (ICANN, EU H2020, community funds) will account for 300 k€, and Open Netlabs will contribute about 50 k€ to NLnet Labs.

6.5.4 Financial Outlook

The year of 2017 was the second year with a different financing structure for NLnet Labs. The strategy for financial sustainability aims to work towards a situation where one part of the budget is secured via a longterm commitment via a grant of SIDN, one part from industrial partners, and one part via income generated by our wholly-owned subsidiary Open Netlabs BV.

The business activities within Open Netlabs BV have generated an increased turnover in 2017. Current growth in income is based on SLA support contracts and consultancy. For future growth in turnover and revenues, we will expand the activities of Open Netlabs into the development of new business and creating additional value. With the expected growth in revenues in the coming years, Open Netlabs will help to secure the continuity of the NLnet Labs Foundation.

Balance Sheet (k€)			
Assets		**Liabilities**	
Inventory	2	**General Reserve**	657
Open Netlabs BV stock and loans	310	**Open Netlabs BV Business Development Fund**	330
Receivables	225	**Special purpose reserves**	253
Bank & Cash	786	**Current liabilities and accruals**	83
Total	1,323		1,323

Income				
	2016 actual (k€)	2017 actual (k€)	2017 budget (k€)	
SIDN Subsidy	366	250	325	
Other Donations	381	206	258	
Consultancy and other Income	117	243	143	
Research and projects	60	109	18	
Interest Income	14	11	15	
Sub Total	938	819	759	
Business Development Subsidy from NLnet	0	0	0	
Total	938	819	759	

Expenditure				
	2016 actual (k€)	2017 actual (k€)	2017 Budget (k€)	
Staff	629	631	646	
Housing	56	55	63	
Travel	39	38	45	
Depreciation	5	3	5	
Project Costs	51	59	15	
Other costs	44	39	57	
Sub Total	824	825	831	
Negative Result Open Netlabs	-21	-46	0	
Reservation Fund NLnet Business Development	0	0	0	
Project Reservations	135	40	-72	
Total	938	819	759	

7 Publications, Presentations and Reports

Publications

- "***The Root Canary: Monitoring and Measuring the DNSSEC Root Key Rollover***", van Rijswijk-Deij, Chung, Choffnes, Mislove and Toorop, SIGCOMM2017, August 2017. https://wwwhome.ewi.utwente.nl/~rijswijkrm/pub/sigcomm2017-rootcanary.pdf
- "***Continuous Data-driven Analysis of Root Stability (CDAR)***", TNO, NLnet Labs and SIDN, March 2017. ICANN commissioned root stability study, https://www.icann.org/en/system/files/files/cdar-root-stability-final-08mar17-en.pdf

Invited Presentations

- "***Hands on getdns***", Dickinson and Toorop, JCSA17 – Journée du Conseil Scientifique de l'Afnic 2017, Paris, France, July 2017. https://www.afnic.fr/en/about-afnic/news/general-news/10659/show/back-to-the-2017-edition-of-the-afnic-scientific-council-day.html

Presentations

- "***How to get a trustworthy DNS Privacy enabling recursive resolver***", Toorop, DNS Privacy Workshop @ NDSS2017, San Diego, USA, February 2017. https://www.nlnetlabs.nl/downloads/presentations/trustworthy-privacy-enabling-resolver.pdf
- "***Everything you ever wanted to know about caching resolvers but were afraid to ask -- DnsThought***", Lundström and Toorop, RIPE DNS Hackathon, Amsterdam, Netherlands, April 2017. https://www.nlnetlabs.nl/downloads/presentations/RipeDnsHack17DnsThought.pdf
- "***DNS-based email security***", Platform Internetstandaarden, April 2017. https://www.nlnetlabs.nl/downloads/presentations/platform_internet_20apr2017.pdf
- "***The importance of being an earnest stub***", Toorop, DNS-OARC26, Madrid, Spain, May 2017. https://www.nlnetlabs.nl/downloads/presentations/an-earnest-stub.pdf
- "***ECS support detection and birthday attack hardening***", Dolmans, DNS-OARC26, Madrid, May 2017. https://www.nlnetlabs.nl/downloads/presentations/unbound_ecs_oarc26.pdf
- "***DNS Privacy Enhanced Services***", Overeinder, RIPE 74, May 2017. https://ripe74.ripe.net/presentations/149-RIPE-74-DNS-Privacy.pdf
- "***De impact van NTP security tekortkomingen op DNS(SEC)***", Toorop, SIDNfonds Startbijeenkomst call 1, Utrecht, Netherlands, June 2017. https://www.nlnetlabs.nl/downloads/presentations/impact-NTP-tekortkomingen-op-DNSSEC.pdf
- "***The Root Canary -- measuring and monitoring the impact of the KSK rollover***", Toorop, IEPG @ IETF99, Prague, Czech Republic, July 2017. https://iepg.org/2017-07-16-ietf99/root-canary-iepg-prague.pdf
- "***Measuring IXP Interconnectivity - A Study on Canadian Network Interconnection***", Toorop, RIPE NCC::Educa, Amsterdam, Netherlands, October 2017. https://www.nlnetlabs.nl/downloads/presentations/measuring-ixp-interconnect-RIPE-EDUCA.pdf
- "***Living on the Edge: (Re)focus DNS Efforts on the End-Points***", Overeinder, RIPE 75, October 2017. https://ripe75.ripe.net/presentations/111-RIPE-75-DNS-on-the-End-Points.pdf
- "***Mailen namens een minister? (E-mail spoof demo)***", Dolmans, Jaarcongres ECP, November 2017. https://www.nlnetlabs.nl/downloads/presentations/20171114a_slides_maildemo_ECP-1.pdf
- "***Impact of security vulnerabilities in timing protocols on Domain Name System (DNS)***", Malhotra (Boston University and visiting researcher NLnet Labs), IEPG @ IETF100, Singapore, November 2017. https://iepg.org/2017-11-12-ietf100/DNS-IEPG-Aanchal.pdf
- "***The impact of NTP security weaknesses on DNSS(SEC)***", Toorop, SURFnet RoN++, Utrecht, Netherlands, December 2017. https://www.nlnetlabs.nl/downloads/presentations/The-impact-of-NTP-security-weaknesses-on-DNSSEC.pdf

Work in Progress

- "***A DANE Record and DNSSEC Authentication Chain Extension for TLS***", Shore, Barnes, Huque and Toorop, October 2017. https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension-05
- "***On Implementing Time***", Malhotra, Hoffmann and Toorop, October 2017. https://datatracker.ietf.org/doc/draft-aanchal-time-implementation-guidance/

Blog Posts

- "***Testdriving the CrypTech Alpha Board***", Schaeffer, March 2017. https://medium.com/nlnetlabs/testdriving-the-cryptech-alpha-board-57a1e163d8f
- "***Privacy: Using DNS-over-TLS with the Quad9 DNS Service***", Band, November 2017. https://medium.com/nlnetlabs/privacy-using-dns-over-tls-with-the-new-quad9-dns-service-1ff2d2b687c5

NLnet Labs Staff Responsibilities

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

Stichting NLnet Labs

Science Park 400, 1098 XH Amsterdam

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