Annual // Report 2018

Since 1997 NLnet foundation (after its historical contribution to the early internet inside and outside of Europe) has been financially supporting organizations and people that contribute to an open information society. It funds those with ideas to fix the safety, robustness and privacy of the internet.

The articles of association for the NLnet foundation state: *"to promote the exchange of electronic information and all that is related or beneficial to that purpose"*. Stichting NLnet is a recognised philantropic non-profit foundation according to the Netherlands Tax Authority (Belastingdienst)

The internet has no borders, and neither does NLnet. It operates internationally, and is driven by donations from individuals and from private and public organisations. NLnet is independent, and all projects are based on open standards, open source software, hardware and content.

Introduction

Dear reader,

thank you for your interest in NLnet Foundation. You have before you the annual report of 2018, a year that may turn out to be a pivotal year for NLnet. A key indicator for that was FOSDEM in Brussels, where during a jam-packed keynote we presented the study "Next Generation Internet 2025" to MEP Marietje Schaake and Georgios Tselentis from the European Commission. A very strategic policy document based on a study which we had performed together with a team from Gartner Europe, involving countless contributors from the trenches of the open internet: from the technical and operational community of the internet, the digital rights community, the free software community, the hacker community and from internet users. The study delivered a vision and strategy for the European Commision's Next Generation Internet (NGI) initiative. That may not sound extremely exciting, but if you have not already done so we urge you to read it - there are few documents like it.

The NGI initiative is of course not a paper exercise. As the name indicates, the goal is to literally create a next generation internet to fix the many fundamental issues of the first generation internet. NLnet intends to take up its responsibility in actually making that happen. And so far, we are on track. In June 2018 our foundation was selected to lead NGI Zero, a coalition of partners that will coordinate two of the four first Research & Innovation Actions within the Next Generation Internet initiative. The topics of these two actions are *privacy and trust enhancing technologies* on the one hand, and *search, discovery and discoverability* on the other. Between 2018 and 2021 we are able to grant a total of 11.2 million euro to independent researchers and open source developers working on these topics. And there is additional budget to support them with important issues like security, accessibility, standardisation, internationalisation, packaging, building healthy and diverse communities, software license compliance, documentation, software quality assurance and more. We have a number of amazing partners within NGI Zero to jointly deliver this support, and we are excited to have the opportunity to be one of the quartermasters of the NGI initiative. We got to work straightaway, and the first round of calls for NGI Zero was announced in november 2018. The calls from NGI Zero are held together with our regular open calls. In order to support this exciting work, Joost Agterhoek joined NLnet as a policy and technology advisor.

The funding from NLnet is unique because of its technical depth and strategic focus, as well as well as the flexibility and simplicity for applicants. We go out of our way to enable talented individuals and organisations of any type to work on important ideas that contribute to a better internet for everyone. As a public benefit organisation, we are able to direct money to worthwhile efforts because of incoming donations of normal citizens, as well through support from a number of public and private organisations. That support is vital to the continuity of our work.

In 2018 we continued our fruitful cooperation with The Commons Conservancy and with the European association of research networks GÉANT and its members. Again this year this fruitful collaboration helped NLnet provide support to a number of highly relevant projects with meaningful financial support from in particular various international research networks as well as the Netherlands Cyber Security Center. In 2018 we received grants and donations from a other organisations like the Netherlands national standardisation forum, and from other foundations like Vietsch Foundation. Work also continued within the Internet Hardening Fund, set up with a sizable donation from the Netherlands Ministry of Economic Affairs in 2016.

Our subsidiary The Commons Caretakers B.V. supported a number of relevant initiatives as well and received help from many volunteers, in particular related to the collaboration with The Commons Conservancy and its various Programme Boards. And we were delighted to see continued growth at Radically Open Security, the not-for-profit security company set up by dr. Melanie Rieback, John Sinteur and others in 2014. ROS is a poster child for the post-growth economy. It is a 'fiscal fundraising entity', which means that the company has committed to donate at least 90% of all its profits to NLnet. This is just amazing. We are thankful to all the organisations and people we work with, for their energy and commitment to our mission. Today we make the internet of tomorrow, and we stand by our motto.

On behalf of the NLnet team,

Bob Goudriaan
Chair Governing Board

Michiel Leenaars
Director of Strategy

Table of Contents

1 NLnet organisation

History

NLnet's history started in April 1982 with the announcement of a major initiative to develop and provide network services in Europe. The Netherlands Local Unix User Group (NLUUG) played a major role in raising the so-called pan-European "UNIX" Network, EUnet; to support these activities the NLUUG members founded NLnet. NLnet was formally established by the NLUUG as a "stichting" (Dutch for foundation) on February 27, 1989.

Funding source

In November 1994, NLnet Holding BV was formed by the foundation in order to create a commercial base for its internet activities. NLnet Holding BV was the very first commercial Internet access provider in the Netherlands. The sale of NLnet's Internet Service Provider (ISP) activities to UUnet (now part of Verizon) in 1997 provided Stichting NLnet with the means to actively stimulate the development of network technology and to make this freely available to the community in its broadest sense.

More and more funding for NLnet activities comes from external sources. Other commercial and non-for-profit organisations donate to NLnet when they see that the technology being fostered by NLnet is in line with their mission and market development expectations. Stichting NLnet is a recognized public benefit organisation (Algemeen Nut Beogende Instelling or ANBI) according to Netherlands legislation.

Domicile

NLnet Foundation holds offices at Science Park Amsterdam, a technology hotspot with a long history of pioneering in network technology R&D in The Netherlands. It is opposite the road of the location where the first regular connection to the public internet outside of the United States of America was made in 1988 (CWI), where the NLnet activities were located at the time.

Supervisory Board

In 2018, the Supervisory Board (Raad van Toezicht) of Stichting NLnet consists of:

- Maarten Botterman
- Frank van Rijn
- Hanneke Slager

These positions are non-remunerated positions in accordance with the NLnet Statutes, except for a financial compensation for time spent ('vacatiegeld'). In 2018 the Supervisory Board in its entirety has received a total compensation of € 7650,-.

Governing Board

The Governing Board of Stichting NLnet in 2018 consisted of:

- Bob Goudriaan, chair
- Harm Rietmeijer, treasurer

- Simon Hania, secretary

These positions are non-remunerated positions in accordance with the NLnet Statutes, except for financial compensation for time spent ('vacatiegeld'). In 2018, the Governing Board, with the exception of the chair, received a total compensation of € 10.000,- .

Operations

For daily operations the NLnet Bureau was staffed in 2018 with the following people, totaling the staff to 2,6 fte (Full Time Equivalent), all are remunerate positions:

- Bob Goudriaan, general director (0,8 FTE);
- Patricia Otter, administrator for NLnet, NLnet Labs and OpenNetLabs, (0,6 FTE);
- Michiel Leenaars, strategy director (1,0 FTE);
- Joost Agterhoek, policy & technology advisor as of December 1st 2018 (0,6 FTE).

Total actual FTE costs in 2018 for 2,5 fte: € 291.488,-

Total budgeted FTE costs in 2018 for 2,4 fte: € 250.335,-

Operations support

For external (financial and legal) advice and consultancy, Stichting NLnet is supported by:

- Koningsbos Accountants (accountancy)
- Bourquin Business Lawyer (legal advice)

The NLnet website https://nlnet.nl is maintained by Mark Overmeer (MARKOV Solutions).

Independent Review Committee Internet Hardening Fund

An independent review committee consisting of three experts from the technical and academic internet community review the outcomes of the selection procedure of the Internet Hardening Fund based on criteria of eligibility and efficacy. The review committee may set additional conditions for granting. Members of the committee, their employers, colleagues and family members are disallowed for submitting projects to the *Internet Hardening Fund*. The members of the committee are not linked to NLnet in a role as employee, member of the board of directors or supervisory board.

In 2018 the independent review committee consisted of:

- Leon P. Kuunders, CISA CISM CISSP
- Niels Sijm
- Bert Wijnen

2 Overview

Statutory goal and Mission

NLnet financially supports open development of information society technologies. NLnet strives to facilitate shock waves of innovation.

The articles of association for the NLnet foundation state: *"to promote the exchange of electronic information and all that is related or beneficial to that purpose"*.

This is done through stimulating strategic technology research and development in the area of computer networking and the internet. NLnet looks at impact, so while projects may revolve around new technologies they can also focus on improving existing technology, encouraging new applications of existing technology or dissemination of relevant knowledge.

The current focus is twofold: on strenghtening the position of the individual user on the internet and on improving the overal security of the internet.

NLnet actively stimulates the development of open network-related technology and making this technology freely available to the community in the broadest sense of the word. The technology should support and contribute to a better exchange of information.

Free Software, Open Source, Open Content, Open Hardware

Throughout the years, NLnet has supported a wide range of Internet and technology related projects. A precondition for all funding is suitable 'open' licensing conditions - such as GNU GPL, BSD license, Open Hardware License, Creative Commons and such. NLnet wants the projects it supports to reach as far and wide as possible, and to have a broad future that is open to continued development well beyond its originators or originating context.

Not-for-profit

NLnet Foundation does not derive any financial benefits from projects or their results.

Any future possible benefits will be used to meet the statutory goals of NLnet.

Co-operation

NLnet maintains a warm relationship with other institutes and foundations:

- Accessibility Foundation
- AMS-IX
- Association for Progressive Communications
- Bits of Freedom
- Center for the Cultivation of Technology
- CWI
- DDA
- Digital Infrastructure NL
- DHPA
- EDRi
- Free Software Foundation
- Free Software Foundation Europe
- GEANT
- ICANN
- iFROSS
- Internet Society Netherlands
- Internet Society
- ISPConnect
- LOT Network
- NixOS Foundation
- NLnet Labs
- NLUUG
- Open Invention Network (OIN)
- OpenDoc Society
- OpenForum Europe
- Petites Singularités
- RIPE/RIPE NCC
- SIDN/SIDN Fonds
- SURFnet
- Software Heritage
- The Commons Conservancy
- The Hague Security Delta
- Translate House
- USENIX
- Vietsch Foundation
- W3C

Their regular activities, technical conferences, programs and occasional actions are being seen by NLnet as major forums to make its plans public, to encourage cooperation between information technology professionals and to obtain feedback from them. In addition, NLnet regularly interacts with several academic and public institutions, such as the European Commission (in particular DG CNECT), Forum Standaardisatie, Netherlands Cyber Security Center and various Netherlands ministries (Ministry of Economic Affairs, Ministry of Justice and Security, Ministry of the Interior and Kingdom Relations, Ministry of Education, Culture and Research and Ministry of Foreign Affairs) and similar organisations inside and outside of Europe.

Finance

In 2018 NLnet sponsored projects, programs and other activities to the sum of € 1.065.593, compared to € 615.149 in budget 2018, excluding loans. The total expenditure was € 1.424.930, compared to € 925.561 in budget 2018, excluding loans. The total profit equals € 207.853, compared to - € 159.111 in budget 2018, excluding loans.

The 2018 profit still includes amounts (to the sum of € 321.167) for future funding obligations. After adding these amounts to the reservation for future expenditures, the total decrease in equity in 2018 is - € 113.314.

For 2019 NLnet has allocated € 4.338.333 (excluding loans) for financing of projects, programs and other sponsoring. The total budgeted expenditure in 2019 is forecast to be € 4.809.099 excluding loans. The total budgeted decrease in capital in 2019 is forecast to be - € 151.766 excluding loans.

3 Strategy and working methods

Strategic Themes

NLnet maintained and expanded focus in 2018 on the following areas of attention through thematic funds:

- Cryptocurrency Fund
- DNSSEC
- Data Delivery Fund
- Honeypot Technology Fund
- Infrastructure & Hosting Fund
- Internet Hardening
- Internet Measurement and System Stability Fund
- Open Document Format
- Real-time communication
- Research & Education Fund
- Software Quality Fund
- Technology Awareness Fund
- VPN Fund

See for more information: https://nlnet.nl/themes

Third parties willing to donate to NLnet may choose to dedicate their donations to one of these themes, or to a new theme, or to NLnet in general.

Donations and Loans

NLnet offers three types of support:

- Project donations – projects requiring not more than € 50.000 with a duration typically of eighteen months or less. If successful, follow-up projects can be submitted.
- Standalone donations – one-time sponsoring of conferences, workshops, hackathons, seminars, contests and financial compensation of travel costs for participants of these events.
- Loans – for efforts with a significant likelihood that funds spent can be returned to NLnet.

Project donations

NLnet sees a major role for itself (and has a strong preference for) supporting strategic projects in the earlier phases of (re)development. Project budgets typically range between € 1000 and € 50.000, and have a duration of eighteen months or less - but that is decided on a case by case basis. This class of project is suitable in particular for establishing new technologies, as well as for proving the need to sunset legacy technologies. NLnet's funding allows projects to deliver break-throughs in their fields, as well as do technology reconnaissance and critical investigation.

For more details on projects sponsored in 2018 see Annex 1.

Standalone donations

NLnet may choose to provide standalone donations to organisations and individuals, in order to support and stimulate their activities - assuming these are in line with the NLnet mission and philosophy. Standalone donations also encompass incidental support for community building in the form of workshops, hackathons, conferences, setup of legal entities, and other efforts. Note that the volume of standalone donations continued to decrease in 2018 within the NLnet portfolio, in favour of project donations. This is not by choice or lack of relevance - we believe these activities can both be strategic and very cost effective - but due to the limited availability of suitable funding resources.

More details on standalone donations sponsored by NLnet in 2018 are provided in Annex 1.

Loans

Projects funded by NLnet result in free software, open content, free hardware designs and other intangible assets which are given away *gratis*, which in many cases makes it unlikely they will make enough money to return the funds allocated and make them sustainable/revolving. In some cases, however, this is different. For instance when there is a cash flow issue as other sources of income (like a grant from another funding agency or public institition) operate too slow, putting an organisation at risk. Or when there is a suitable business model. When project proposals fit with NLnet's mission and the applicants can be reasonably confident that the funds requested are likely to be returned, they can ask NLnet for a loan. Loans have the advantage that the same money can be re-used over and over again for other relevant projects within NLnet's mission.

Distinctive investment

NLnet derives its yearly budgets from the available capital, the interest gained from banking of (a part of) this capital, from donations and subsidies, and some revolving activities. The challenge is or course to make sure that in the long run sufficient funding strength remains to continue its beneficial work.

Therefore NLnet decided to experiment with investing a part of our assets in technologies we understand, in people we trust and in concepts we believe will change the world to the better. And to gain money with this which can be used to accomplish the mission of NLnet.

For this purpose a few investments were made since 2012:

- Appcache Ltd ('5apps') in 2012 (currently 37,5 % equity)
- Rockstart in 2014-2016 (currently convertible loans in GAYR4 BV, GAYR5 BV, and GAYR6 BV)

4 Finances

Fiscal Status

Stichting NLnet finances its projects and activities from donations by individuals and organisations, inheritances and subsidies, as well as the annual return and interest as received on its invested capital and other assets. NLnet actively solicits donations from third parties to finance project activities, and co-sponsors projects with other organisations. A non-negotiable condition is that the independence of NLnet in choosing and financing projects is assured, and that its mission is respected.

Stichting NLnet does not derive any financial benefits from the supported projects or their results.

Since 1999, Stichting NLnet has had a non-profit tax status (so-called Article 24 status, "Algemeen Nut Beogende Instelling").

In accordance with ever changing legislation NLnet in 2007 obtained and in 2009 was confirmed its non-profit tax status (ANBI-regeling) with the Netherlands Tax Authority.

Administration

Salary administration was contracted to Cent Lonen in Haarlem.

Koningsbos Accountants in Amsterdam has been charged with compiling and auditing Stichting NLnet's Annual Accounts 2018 and have given an unqualified opinion. The accountancy report is a separate document. The figures are incorporated in this annual report.

Cost of activities in 2018

The Actual costs and Revenues of activities in 2018 is summarized below, and compared with Budget 2018, and compared with Actual 2017 and Budget 2019 (excluding loans):

	Budget 2019	Actual 2018	Budget 2018	Actual 2017
Cost of programs and projects	4.338.333	1.065.593	586.875	447.905
Cost of staff	365.500	291.448	250.335	309.255
Cost Rental Office	14.850	12.948	12.632	12.840
Office costs	8.500	5.588	3.987	4.292
Advisory costs	5.000	0	10.000	0
Remuneration Mgt & Supervisory Board	17.650	17.650	17.650	17.650
Miscellaneous costs	59.266	31.602	43.923	35.865
Depreciation of inventory & equipment	0	101	159	120
Total	4.809.099	1.424.930	925.561	827.927

Revenue of activities

	Budget 2019	Actual 2018	Budget 2018	Actual 2017
Income and returns	4.657.333	1.540.452	766.450	425.756

Balance Sheet 2018 (2017)

	2018		2017	
	debit	*credit*	*debit*	*credit*
Assets				
Equipment	0		101	
Financial Fixed assets	436.250		465.551	
Total fixed assets	**436.250**		**465.652**	
Current assets	31.943		29.382	
Liquid assets	9.796.140		2.790.635	
Total Assets	**10.264.333**		**3.285.669**	
Liabilities				
Capital		2.503.839		2.617.153
Appropriated reserves		948.070		626.903
Total Reserves		**3.451.909**		**3.244.056**
Current and accrued liabilities		6.812.424		41.613
Total Liabilities		**10.264.333**		**3.285.669**
Total Balance	**10.264.333**	**10.264.333**	**3.285.669**	**3.285.669**

In June 2018 our foundation was selected to lead NGI Zero, a coalition of partners that will coordinate two of the four first Research & Innovation Actions within the Next Generation Internet initiative. The topics of these two actions are privacy and trust enhancing technologies on the one hand, and search, discovery and discoverability on the other. Between 2018 and 2021 we are able to grant a total of 11.2 million euro to independent researchers and open source developers working on these topics.

In 2018 we received an advance payment from the EC these projects. This explains the substantial increase in the balance sheet totals.

Spread of liquidity

	2018	2017
Bank 1	7.483.202	611.320
Bank 2	2.048.605	2.028.322
Bank 3	201.668	140.314
Bank 4	61.588	10.483
Bank 5	1.077	196
Total	9.796.140	2.790.635

Budget for 2019

The budget for 2018 (excluding loans) as approved by the board, is as follows:

	Budget 2019
Cost of programs and projects	4.338.333
Cost of organisation including staff	470.766
Depreciation of inventory & equipment	0
Total	4.809.099

Annex 1: Programs, projects and activities in 2018

Programs in 2018

NLnet Labs

NLnet Labs is the Research, Development, and Expertise center for those technologies that turn a network of networks into one Internet. Established by the NLnet Foundation in 1999, NLnet Labs contributes innovative ideas to open source software and open standards. NLnet Labs is recognized for its work on DNSSEC and BGP security, as well as being the home of high-quality DNS software and tools, training and engineering efforts. NLnet Labs is led by Dr. Benno Overeinder.

Anno 2018, NLnet Labs Foundation is a fully independent and sustainable organisation that can stand firmly on its own feet. NLnet Labs has been officially recognised as a not-for-profit (ANBI, Algemeen Nut Beogende Instelling), with its own independent governance which has no overlap with that of NLnet Foundation. It collaborates with other organisations such as Verisign Labs, ICANN, SIDN and USC/ISI. NLnet Labs' work is funded by contributions from users who support its mission and want to see the maintenance and development of its software continued for everyone. An addditional source of income are software support contracts through its subsidiary Open Netlabs B.V. which also provides software development, training courses, audits and consultancy.

NLnet Foundation sponsors NLnet Labs by providing free administrative services.

The Commons Conservancy

NLnet actively contributes to The Commons Conservancy through a joint Memorandum of Understanding with NLnet and Géant. The Commons Conservancy provides a lightweight organisational structure for open projects. Its mission is to strive towards a stable democratic and open global information society in which individuals can collectively scrutinise, reconfigure and improve upon any technology they depend on - unleashing and empowering human innovation at the widest possible scale, with the express intention to empower any individual to participate in all facets of social, cultural, economic and private life under conditions of his or her own choosing and with secure and reliable technology they can have full control over themselves. The Commons Conservancy is an independent foundation.

NLnet supports The Commons Conservancy with logistics, insurance for its board members and recurring costs such as domain name registration for the foundation and its programmes.

Received proposals

In 2018 NLnet has received in total 141 project proposals (compared to 112 in 2017), whereof 26 requests were (partially) granted (against 29 in 2017).

Projects supported in 2018

ARPA2

ARPA2 is the ambitious effort by InternetWide.org to develop tools to repopulate a decentralised global internet that offers security and privacy by design. It aims to make the internet live up to its full potential. With TLS Pool (part of the SecureHub project) it aims to increase control over TLS security, shielding nomadic users and unpredictable services against even the most common external attacks. With TLS-KDH the project is trying to standardise the use of Kerberos combined with Diffie-Hellman, for use over TLS. SteamWorks is aimed at providing live configuration across unreliable networks. Earlier the project was co-funded together with the programme "veilig door innovatie" from NCTV , currently also by the Internet Hardening Fund. See all Arpa2 projects at projectwebsite.

Build graphs

Finding out if files contain known vulnerability and if files with known vulnerabilities have been deployed on systems is not trivial. By using build tracing (example: strace) it becomes possible to create build graphs that capture which files were used to build a binary. These graphs can be loaded into a graph database. By decorating the build graph with information (checksums, build identifiers) and combining with different databases (license compliance, security, etc.) it becomes possible to search the build graphs and answer questions such as "Did we build a program that contains a certain vulnerable file and if so, in which builds did these files occur?".

Implement Cake in CeroWRT

Cake is a mechanism to better queue networking traffic inside networked devices, and offers a built in shaper. The project implements Cake into CeroWrt, the experimental firmware aiming to push forward the state of the art of edge networks and routers. Without advanced queue management, traffic handling can get unpredictable. Cake is the intended successor of the Fq_codel module currently in the Linux mainline kernel. The project is led by Dave Taht and Johathan Morton from Bufferbloat.net, and should help make Cake reach feature-complete status and stabilise its API & ABI. See progress at project website.

Declarative web service security

Creating secure webservices is non-trivial. Every application has its own security configuration mechanism, which means there is lots of room to make mistakes, neglect flaws and end up with vulnerable systems. NixOS is a Linux distribution with a unique approach to package and configuration management. Built on top of the Nix package manager, it is completely declarative, makes upgrading systems reliable, and has many other advantages. It is used increasingly in complex environments where reproducible behaviour and configurability matter, from desktop systems and embedded devices to top 500 supercomputers and complex datacenter setups. The Nixcloud project will allow to combine the power of declarative packaging with cutting edge security characteristics to create a unique delivery channel for decentralised internet applications. These improvements will greatly simplify the creation and delivery of robust and secure services. The project will demonstrate the new capabilities in the project by providing a number of examples of different types of web services, such as classic LAMP applications, NodeJS and Java application containers.

Reverse dynamic linking

The topic of dynamic linking of executables is not as well researched as it ought to be. In particular, currently there is no "search" capability, which would allow for answering questions like "which programs use this particular library" or "which symbols from a particular library are actually used by programs". This is very relevant in a software engineering context, to discover if it is safe to remove libraries, or replace them with equivalent librarie. It can also give insight into whether it makes sense to lift parts of a library into separate libraries to decrease bloat. ELF linking has legal implications, and the tool built in this project can help there too. The project will create tooling for creating ELF linking graphs.

Democratic Sendcomm

Democratic Sendcomm aims to provide an easy to use (like Micro:Bit or Raspberry Pi) connected telemetry appliance with just enough configurability to teach decentralised communication while keeping the learning curve flat. It aims to provide an open source (CERN HW license) design of cheap yet high performance LoRaWAN devices. Requirements include or resemble functions of Tor's Atlas project while design resembles that of typical Physical Web beacons. The communication technology is subgigaherz LoRa and IP networked. The project is funded through the Research and Education Fund, in collaboration with Vietsch Foundation.

Dowse

Dowse is a smart digital network appliance for home based local area networks (LAN), but also small and medium business offices, that makes it possible to connect objects and people in a friendly, conscious and responsible manner. Dowse provides a central point of soft control for all local traffic: from ARP traffic (layer 2) to TCP/IP (layers 3 and 4) as well as application space, by chaining a firewall setup to a transparent proxy setup. A core feature for Dowse is that of hiding all the complexity of such a setup. Its motto is: "to perceive and affect all devices in the local sphere". See progress at the project website.

DIME

DIME is a serious attempt to provide end-to-end encrypted email. Starting from a very strict threat model, it brings some novel ideas on how to improve the concept of email and bring it into the 'age of distrust'. It was setup by the people behind Lavabit, the ISP that resolved itself after refusing to hand information about a well-known whistleblower that used its platform.

eduPVN

We live in a society that wants to be online whenever possible, and WiFi is a common technology for achieving connectivity. Unlike the "home" network (which could be described as a 'trusted' environment because you connect from a known device to an access provider you selected yourself), we also make heavy use of public offerings of WiFi that offer far less guarantees. When being a guest on third party networks, we should take precautions against a numer of risk (such as the risk of rogue attacks on our connections and systems). eduVPN is an effort to make VPN technology commonly available, by building better and more user-friendly tools to connect to trusted parts of the internet.

The eduVPN programme produces a family of open source tools that can be used to set up a VPN server, federate with other servers, connect various types of client devices, and more. eduVPN is part of The Commons Conservancy. The project has received a contribution from Vietsch Foundation, through the Research and Education Fund.

Explain.Direct

Online Open Courseware and MOOCs promised to herald a new age of education, open for all. Many reputable universities provide high-quality materials for free on different platforms, like for example lecture videos or whole courses. However, in most cases, this material is still intended to be consumed in a traditional course-based manner (e.g., learners partaking in a course over 8 weeks), and targeted access to content is hard, unnecessarily complicating many use cases like re-use of material in higher education, or tailored access for life-long learning scenarios. In this collaborative project between the Web Information Systems group of TU Delft and FeedbackFruits, the aim is to provide effective and efficient access paradigms for open educational material based on state-of-the-art content analysis and recommendation techniques. This will allow for easier and more direct access to valuable educational material. The core contributions of this projects are twofold: open source technical solutions for analyzing, recommending, and querying open educational materials within the context of higher education. And intensive user and case studies for further improving the quality of the project, and increasing the utility for the target audiences in higher education. The project is funded through the Research and Education Fund, in collaboration with Vietsch Foundation.

Faster and configurable datapath Linux xfrm

The project entails rewriting nftables (which is a subsystem of the Linux kernel responsible for packet filtering and classification) to make it easier to combine with xfrm (which is the common framework to work with IPSec in Linux). IPsec was originally developed in conjunction with IPv6 but is just as often used with IPv4 as well. IPSEC encrypts traffic, providing key features absent in the regular IP layer - like data integrity, data origin authentication and confidentiality. The project is expected to make an important contribution to improving the IPSEC capabilities, usability, speed and robustness in many systems.

FileSender

The purpose of the FileSender software is secure transient storage and sharing of very large files (of unlimited size, in fact). The problem the software aims to solve is the need to send bulk data to someone via the internet. The software is not intended as a permanent file publishing platform: a file should be available for download for a certain number of downloads and/or a certain amount of time, and after that should be automatically deleted. The data can be encrypted client-side to provide end-to-end security, meaning that the person or organisation operating the server has no ability to read the data. FileSender is a programme of The Commons Conservancy.

GDPR Compliance

In 2016, the European Parliament passed the General Data Protection Regulation (GDPR). It will be the harmonised framework, which will establish the rules regarding the protection of personal data in all European countries. Although the GDPR is directly applicable without needing any law implementing it on national levels, the majority of countries will need to go through a period of adaptation in which the interpretations of the key issues in practice will be crucial (https://edri.org/analysis-flexibilities-gdpr/).

EDRi will provide a series of material, such as a checklist, a technical tool and a set of research papers, to advise Europe's countries on how to translate consent, profiling, access to your data, etc. in practical terms.

GetDNS

Because of the technical complexity of DNSSEC, DANE support has so far been quite complex for developers to work with. The getDNS library is a modern asynchronous DNS library for application developers, with an API vetted by application developers. getdns has especially good stub-resolving capabilities, and has been developed alongside and in close co-operation with recent standards for stub resolving; such as DNS over TLS (RFC7858), and acquiring DNSSEC at stub resolving level. One of the key features of getdns is the ability to deliver DNSSEC as a building block in harsh environments. In this project a number of essential components is implemented to this library, and work on mechanisms to make it easy to integrate the library also at a system level.

GnuTLS

TLS-KDH is a proposed new protocol that combines the security features of TLS with Kerberos. The project aims to upstream the proof-of-concept implementation of the TLS-KDH protocol created previously into GnuTLS. This requires additional code refactoring in both GnuTLS and the TLS-KDH code. GnuTLS is one of the key implementations of TLS, included in all major Linux and Unix distributions. In addition the project will make some additional contributions related to the maintenance of GnuTLS.

Goodforms

The web is ideally suited for questionnaires through online forms, but leaving potentially very sensitive user data with proprietary commercial services is in many cases not an option - and may in fact be illegal. There is a lack of free and open source solutions that can be easily deployed on premises or with a trusted hosting provider. GoodForms is a community-driven free software solution to easily generate questionnairs from a regular OpenDocument spreadsheet, which allows to create elaborate online forms without effort.

Gun

Gun is a realtime, decentralized, offline-first, graph database engine. GUN works peer-to-peer by design, meaning you have no centralized database server to maintain or that could crash. It allows to build decentralized, federated, or centralized apps. The SEA (Security, Encryption, Authorization) framework allows to use the latest native Web Crypto API for cryptographic functions like ECDSA, PBKDF2, AES, and more. With GUN developers can build fully decentralized end-to-end encrypted applications, using a "web of trust" mechanism.

Honeytrap

Honeytrap is an innovative open source honeypot framework with advanced analysis and replay capabilities, written from scratch in Go. It features a server, clients and probes. Honeytrap allows to deploy a large amount agents from a single HoneyTrap Server, where configuration will be downloaded automatically and logging is centralized. The Honeytrap Programme is part of Stichting The Common Conservancy.

Interactive XML / Relax NG

CodeMirror is a very popular code editor for the web. The most valuable tool that is missing is the ability to know if the current XML document is valid and show inline error messages. There is no JavaScript implementation of XML Schema validation and only an incornplete one for Relax NG. There is a widely-used library libxml, that can perform validation with XML Schema and Relax NG. See also the project website. The project successfully ended in 2016.

Internet of Coins

The present cryptocurrency industry is fragmented and potentially at risk of becoming financially and politically centralized. Internet of Coins wants to integrate different token value systems into an interconnected and financially liquid web. As a decentralized open source platform it wants to enable an optimally inclusive financial network, interlinking all digital forms of value. The weavechain is the decentralized network behind Internet of Coins. The weavechain connects the blockchains of cryptocurrencies without the need for a centralized authority. All transactions using Internet of Coins take place on the original blockchain of the cryptocurrency. Data on the weavechain is stored temporarily to communicate between the blockchains. Because of that Internet of Coins allows you to trade digital assets and currencies peer to peer, through a user friendly interface.

Iuh Support in OpenBSC

The open source OpenBSC project is both used for research purposes as well as in empowering rural communities to set up their own communication networks. The project will add 3G support to OpenBSC to be used with off-the-shelf 3G components, creating the first open 3G stack that would allow anyone to set up their own experimental network. See progress at the project website.

Key Management

The life cycle of cryptographic credentials which can be used for servers to serve up services with TLS typically contains a lot of manual steps. This administrative burden is a significant cost factor and built-in delay that needs to be overcome if we want to harden the internet at scale. Especially rollovers are cumbersome and error-prone. Automation is needed to make strong encryption the default on the internet, and this project aims to create a set of integrated open source tools to manage cryptographic keys in a provably correct way. The project stems from the ARPA2 project, and builds on/integrates with the NCSC/NLnet funded TLS Pool from the SecureHub project.

Leap-Torbirdy Integration

The Leap-Torbirdy project will integrate LEAP usage into the well-regarded plug-in TorBirdy to allow easy to use email integration. The integration with LEAP into TorBirdy will allow a "one-click" install for Thunderbird to provide better anonymity and a working email client for the LEAP project. The goal is to achieve the highest-level of anonymity, privacy, and security possible with e-mail.

Magic Wormhole and SPAKE2 in Rust and Haskell

Secure exchange of files is a critical problem of all ages, this solution has potentially disruptive qualities. There are many cases in which a person wants to quickly exchange a file in an untrustworthy environment (say a presentation deck) without running either the risk of an Evil Maid attack or uploading to a trusted server and then giving someone access to that. Most people do not even have such a trusted infrastructure, which forces them to trust their data to third parties. SPAKE2 is a modern academic password-authenticated key exchange mechanism, originally designed by two security researchers from Ecole Normale Superieure. It allows to set up an ad hoc encrypted channel between two users that share a combination of words in real-time. Magic Wormhole is an open source implementation of SPAKE2 (both client and server) that can create a rendez-vous/relay, so it can be used in a LAN, behind firewalls, NATs, etc. In addition to validating the Haskell implementation, and completing the Rust implementation, the project aims to reboot IETF standardisation of SPAKE2. The end result should allow for very user-friendly exchange of files with modern encryption, without the need for anything else.

Make Wifi Fast

Make Wifi Fast is a not-for-profit initiative to develop and promote better technology for wireless internet connectivity. The motto of Make Wi-Fi Fast: Wi-Fi does not need to be slow! The hardware now available for Wi-Fi can accomplish tremendous performance, but it is hobbled by software designs that guarantee high latency under load. This, in turn, dramatically lowers performance in real-world settings (multiple users, home routers, commercial access points) leading to the myth that "Wi-Fi is slow." The goal of the project is to reduce latency on a single access point, develop new packet scheduling and AQM techniques applicable to aggregated, parking lot network types and improving the stack sufficiently for 802.11ac MU-MIMO to actually work.

Making ELF linking more insightful

Software and firmware is known to be a jumble of interdependencies, and developers and integrators easily get lost in what exactly is depending on what. For distribution, files are blobbed together in the "Executable and Linkable Format (ELF)". This small but insightful and useful project wants to make it easy to see exactly which parts of which library are used, and to make it easy to search for dependencies. This can allow for major improvements, such as replacement of broken libraries with newer ones. Without this tool, it is hard to tell if that would not break on some edge case.

MAPPED

The MAPPED project wants to create an inventory of the procedures through which people can get access to the information stored about them, and bring together a statistically significant data set. While it is 'the law' that they can get this information, not much is known about the actual state of affairs. MAPPED builds the infrastructure to get actual data. The project is an academic collaboration between TU Delft and Princeton, with support from EDRi - the umbrella of digital rights organisations in Europe. MAPPED will allow citizens to share the results of their access requests with researchers—in a privacy preserving manner. Researchers will collect replies to access requests, information about the process through which these replies are obtained and citizens' evaluation of the replies. On the basis of this data the researchers will map data practices across sectors and countries and evaluate the effectiveness of the right of access for creating citizen empowerment - under the motto 'The Right of Access as a tool for Privacy Governance'.

Matrix

Matrix.org is one of the more comprehensive open source efforts that emerged in the decentralised application space. It has a healthy community building dozens of satellite open source tools and offers encrypted chat, voice and video communication, document sharing and more. The initial focus on first obtaining strong security capabilities has resulted in mature end to end encryption capabilities (not just among individuals but also extending to group encryption). Now the project needs to make sure that the usability of these encryption and security features is addressed – it is well known that security procedures that are too limiting for users, are typically either circumvented or avoided. Currently it is cumbersome for everyone in a group if users want to allow another device into an encrypted group - everyone must manually validate based on so called fingerprints in a time-consuming and complex process. The project funded by the Internet Hardening Fund is focused on investigating how to optimise the user interaction, creating better usability specifically for adding new encryption keys based on trusted keys as well as user auditing of group memberships. This can serve as an example for other applications.

Namecoin

Namecoin is a blockchain project that provides a decentralized naming system and trust anchor. The flagship use-case is a decentralized top-level domain (TLD) which is the cornerstone of a domain name system that is resistant to hijacking and censorship. Among other things, this provides a decentralized trust anchor for Public Key Infrastructure that does not require third party trust. See progress at the project website

Nixcloud Webservices

NixOS is a Linux distribution with a unique approach to package and configuration management. Built on top of the Nix package manager, it is completely declarative, makes upgrading systems reliable, and has many other advantages. It is used increasingly in complex environments where reproducible behaviour and configurability matter, from desktop systems to some of the top 500 supercomputers. NixOS currently allows only one instance for a particular service, so in order to allow multiple instances, a module needs to have explicit support for it. The web services abstraction solves this by generalizing this to all of its service modules.

P2P collab

The P2P Collab project will design and implement a secure P2P multicast protocol using end-to-end encrypted connections inside communities, based on up to date academic research such as CADET. Secure P2P multicast paves the way for new classes of internet communication applications that are decentralised and automatically provide strong encryption to provide better security and privacy conditions (such as 'forward secrecy') to users. The secure and confidential P2P connectivity it aims to provide among group members will allow to use various pluggable transport mechanisms. The project comes from the GNUnet community, one of the leading alternative internet infrastructure projects.

pEp GNUnet simulation

The official title of the project is "Simulation over GNUnet for large user numbers and different realistic user behavior scenarios". pEp is a serious effort to simplify adding encryption features for normal internet usage by providing client-side open source tools and turnkey infrastructure to help encrypt messages and offer privacy and security without relying on third parties or centralized infrastructure. pEp aims to simplify the use of well-known and established end-to-end cryptographic tools for already existing and widely used written digital communication channels (like email with OpenPGP-compliant encryption or messaging with XMPP/OTR). The ultimate goals is to change the default in written digital communications: from unencrypted, unverified and unanonymized to encrypted, verified and anonymized. This project by p≡p foundation will verify if GNUnet can be realistically be used to contribute to these goals, testing with large user numbers and different realistic user behavior scenarios. The combined ability of securing regular communication traffic between peers with securing the traffic metadata across the network is desirable.

Pitchfork

The PITCHFORK project deals with a simple Cortex-M3 based device for compartmentalizing key material and cryptographic operations in a small and durable USB device in the CPUs flash. It can do post-quantum cryptographic key-exchanges over an embedded radio interface with other PITCHFORKs. And over USB it can send and receive messages using various modern low-level crypto protocols providing different aspects of overall security. See also the project website.

PKCS#11 Standardisation

In 2017 NLnet and the Internet Hardening Fund supported the Pitchfork project to send a representative to the OASIS PKCS#11 TC, to bring about addition of a number of missing algorithms to the upcoming PKCS#11 3.0 standard and later versions. Pitchfork was aiming to support PKCS#11 in its crypto device, until it discovered that the intersection of PKCS#11 supported algorithms and Pitchfork algorithms was empty. In other words: a number of key algoritms was missing. Thus the Pitchforkists received support to help amend this issue, and put forward a number of modern signature mechanisms to the OASIS technical committee - such as ED25519, XEDDSA,VXEDDSA, Sphincs, Curve25519 ECDH, X3DH ECDH, Double Ratchet, Chacha20, Salsa20, Salsa12 and Blake2b.

RaptorJIT

RaptorJIT is a descendant of LuaJIT, with a focus on predictably high performance low-level system programming. LuiJIT is a simple dynamic language that has been used to write network stacks, hypervisors, unikernels, database and more. It offers ubiquitous tracing and profiling to make application performance and compiler behaviour transparent to programmers. LuaJIT Studio offers interactive tools for inspecting and cross-referencing trace and profiler data. RaptorJIT is a community effort, using the same fork-and-merge model used for the Linux kernel. It is developed by the same team behind Snabb Switch.

Redwax

Redwax is a small modular Certificate Authority system written as a set of easy to deploy 'correct by default' apache-httpd modules that require very little configuration and maintenance. This includes not just a pure CA; but also the elements where the 'rubber meets the road' such as CRL and SCEP, the very complex yet practical things needed to make this work with contemporary browsers and devices, such as iPhones and Android. Redwax aims to deliver zero-touch, non-expert-needed, automatic roll out, as well as ongoing maintenance such as CRL distribution and certificate reissuing.

Remote PKCS #11

Setting up an encrypted connection across the internet requires establishing trust between the two endpoints. There are multiple ways, one of which is the use of asymetric keys. However, in many cases there will not be a suitable hardware crypto device available - and storing crypto credentials in userspace on lots of insecure devices (such as mobile phones) is quite risky. Managing and auditing usage of those credentials in such a case is a problem. The project entails two innovative ideas to isolate and organise credentials: Hosted PKCS#11 which allow users to use a trusted remote crypto store instead of a local store (which is of course much easier to audit, assuming that the back end system on which the keys are stored is professionally managed by someone trustworthy), and Layered PKCS#11 which can downgrade or upgrade identities to roles, groups and other attributes of a user (such as "age").

RPKI-RTRlib

The RTRlib is a real-time capable, open-source (MIT licensed) C library that implements the RPKI router part. Basically, it fetches data from an RPKI cache server and allows for prefix origin validation as well as initial steps of BGP path validation (draft 6810bis). The RTRlib can serve as the backend for BGP daemons and monitoring tools in real-world operations, as well as user guidance.

SDR PHY

SDR (Software Defined Radio) allows for a low cost setup to serve a wide variety of changing radio protocols in real time. SDR is gaining popularity in the world of Open Source mobile communications. Thanks to the work of projects like Osmocom and OpenBTS, it is already possible to run a custom GSM network using Open Source software. Moreover, there is a few Open Source projects for LTE, such as OpenLTE, srsLTE and OpenAirInterface. However up to now there was no software defined GSM mobile phone. The "SDR PHY for Osmocom BB" project aims to fill this void. The project is focused on the client side of GSM protocol stack, and bridging the gap between existing GSM stack implementation project and SDR hardware.

Searsia

Searsia is an open source engine and a protocol, created by academic researchers. Using Searsia you can i) manage and share large collections of independent sources; ii) select for each query the most relevant sources; iii) combine sources in an aggregated search interface. Searsia learns over time what kind of information each source provides. To see it in action check this search engine of the University of Twente that combines the results of about 30 sources, including results from Google's web crawl, from Courses, from News, the Telephone directory, the Timetables, as well as results from social media, such as Facebook, Twitter, Pinterest, and Flickr. In addition, Searsia has built a zero-knowledge search solution that works for static websites. Searsia is co-funded by the Vietsch Foundation.

Searx

Searx is a free software internet metasearch engine which aggregates results from a significant amount (currently more than 70) search services. A private (or preferably shared) instance of Searx allow you to escape from the so called 'search bubble' created by overzealous personalisation of your search results. It give you a more diverse (or at least alternatively biased) view on the world, by combining the results of a variety of sources without filtering based on your previous searches. Searx also helps to reduce the amount of tracking and passive observation search users are subject to, by offering a layer of proxying isolation.

Secushare Box

Secushare Box tries to build a framework for 'sufficiently safe' social interaction. It provides an operating system extension for hardware devices that turns them into automatable nodes in a distributed social mesh network, independent of central control. The objective is to offer an alternative to cloud-controlled IoT, empowering the owner of a device instead of its manufacturer. IoT devices are to be cryptographically linked to their owner's smartphones, PCs or other interfaces, using an initial vicinity rendez-vous procedure, akin to how bluetooth devices "pair". This integrates the new IoT device into the owner's social graph as a resource that can potentially be shared with others without the hassle of exchanging unsafe passwords. End-to-end encrypted communication is provided by the mesh service of GNUnet, upon which the multicast channels are built. Pseudonymous users and social places in the system have cryptographical identities &emdash; identified by their public key &emdash; these are mapped to human memorable names using GNS (GNU Name System), where each pseudonym has a zone pointing to its places.

SERVAL iOS

Serval Project's goal is making mobile phones useful, even when there is no cellular network or

internet available. The Serval Project is intended to be useful in disaster and emergency situations anywhere in the world, as well as for people in rural, remote and developing world settings where traditional cellular service may not be available or may be too expensive. The Serval Project's technologies also have obvious application to enabling freedom of speech and communications for people under oppressive regimes.

Serval used to use ad-hoc WiFi on mobile phones to form the mesh network. Traditional focus was on the Android platform, due to the closed nature of other large ecosystems. One such ecosystem (iOS) recently gained an API to allow applications for adhoc communications between devices running iOS. The project tailors the Serval Mesh software to these devices, allowing peer-to-peer mobile telecommunications and internet and bringing mobile mesh communications to the main-stream. See progress at project website.

Shadow Internet (Tribler)

Shadow Internet is an alternative communication infrastructure developed by researchers at Technical University Delft that enables people to distribute videos by copying them from phone to phone wirelessly. So even without an Internet connection you can share content. Specifically crafted to be resilient. The project is specifically targeted for recording and spreading of protest videos. The Shadow Internet ensures people no longer are reliant on commercial websites to view and share content with friends. See progress at ` project website <https://www.tribler.org/ >` __.

SnabbWall

SnabbWall is designed as a modular, application-level (Layer-7) firewall suite built on the foundations of the popular open source SDN Snabb Switch, allowing it to be used with cheap commodity hardware. It will include a complete firewall program out of the box, and components that can be reused in other software defined networking components. As an application-level firewall, it will be able to inspect network traffic and detect flows of related data, and pinpoint which application has produced a certain data flow. It can subsequently be used to filter (drop, reject, or accept) packets using criteria specified in a set of rules.

Steamworks

Distribution and management of domain policies with regards to TLS are currently an open issue - in the vast majority of cases such policies are absent or hardcoded into the application or device. This makes the user fully dependent on the vendor with regards to both trust and agility. The Steamworks project aims to develop a robust, standards-based open source mechanism to propagate and aggregate policies and trust independently from software applications.

Stratosphere IPS

The Stratosphere Project is sophisticated free software Intrusion Prevention System that was researched and partially developed in the CTU University in Czech Republic. It detects and protects users or organizations from the most advanced government-sponsored and botnet-related attacks. The Stratosphere IPS analyzes the behavior of network connections and detects the known malicious patterns. Instead of using anomaly detection techniques or static rules, our technique consists in generating Markov Chain-based models of verified malicious activities that can be later detected in the network. Stratosphere offers a high-level semantic interface to block the traffic. The publication of the Stratosphere software will lower the cost of protection of Internet users against cybercrime and cyberespionage attacks. See progress at the project website.

Stubby

DNSSEC as a technology adds cryptographic signatures to DNS traffic, but does not handle the other axis of security: privacy. Any (passive) observer in the network can see the requests going to the DNS server, leaving a trail that can endanger the user. DNS over TLS is a new approach supported by the DNS software vendor communty which gives it a fair chance of succeeding. The approach allows to encrypt the traffic between a trusted (DNSSEC aware) DNS server and the user in the same way. Stubby allows to use this technology when ones provider does not provide it.

Terms of Service; Didn't Read

"I have read and agree to as Terms" is not as much as it should about actual informed consent from users. The Terms of service for online companies are often too long to read, and yet it is very important for users to understand what is in those carefully crafted legal texts. Their rights online depend on them. ToS;DR is a user rights initiative to rate and label website terms & privacy policies, from very good (Class A) to very bad (Class E). These ratings can help user get informed about their rights. You can check the services you are condidering online, or conveniently get the ratings directly in your browser by installing a web browser add-on.

Tracking Exposed

Algorithms are the technological solution to the information overload: they are as powerful as necessary to manage the overflow of data that reaches us. Unfortunately, they can also conceal the existence and use of assessments and judgments that impact the dissemination of ideas and culture. No one should be allowed to abuse such power over connected people. At this stage, consent is nor informed nor optional. The main objective of the project is to put a spotlight on users' tracking, profiling, on the data market and on the influence of algorithms. As long as these phenomena are shielded from view or understood only by experts, they cannot be tackled with the political determination that problems of such magnitude deserve. The project strives to explain the issue, and to test and promote new solutions developed to benefit the community.

Trusted Boot Module

The Trusted Boot Module project is developing a system for booting trusted OS images on existing, ARM-based systems. It will consist of open hardware and software that allows users to start up Linux systems on off-the-shelf ARM development boards, where the system ensures that the system can be booted in a trusted state by booting only OS images trusted by the vendor and/or the user of the system. The hardware consists of cheap, off-the-shelf components that are simple to analyse and program, and which provide for an easily verifiable solution that does not depend on 'black box' components. The project aims to bring trusted boot to the market of commodity ARM-based servers, thus providing the community a security solution that allows for, for example, affordable distributed hosting and computing.

Unlocking dependency information

NixOS is a Linux distribution that focuses on traceability and reproducibility by for example making the entire dependency chain very explicity. However, it does at the level of a single machine. When deploying NixOS onto more machines, with possibly different installations, it can quickly become cumbersome to track these changes. This project will create a prototype to extract the dependency information from a Nix system and to load it into a graph database, and enrich the graph with additional relevant metadata.

VITA

The Vita project is VPN tunnel software operating on layer 3, which is also a young implementation of IPSEC tunnel mode in user space. Vita is based on Snabb, a high performance open source framework for networking applications running on commodity hardware. Vita can achieve high performance (beyond 10G speeds) on commodity server hardware. Vita is intended to be both simple in terms of code, as well as in terms of deployment, and non-invasive to deploy in existing networks. Vita also strives to be affordable, in terms of both energy footprint and cost of maintenance: its goal is to make the best possible use of commodity hardware while remaining easy to deploy safely. The project aims to mature the current simple but already fast prototype code into a reliable first production release, as a step towards a novel open source VPN option in the high-performance sector.

WireGuard

When an internet user is in an insecure environment, he or she can use a Virtual Private Network (VPN) to create a cryptographically protected tunnel to a trusted point on the internet - and pass all internet traffic through that secure tunnel - thereby protecting it both from snooping and malicious traffic injection. The open source WireGuard project is seen by many as one of the most promising developments in VPN technology in recent years. Wireguard offers higher speeds and more modern cryptography, and has a much smaller, and cleaner codebase compared to the most dominant (but aged) offering OpenVPN. It is also unencumbered by rumours of NSA code injection into implementations of IPsec. It has already being accepted into projects like OpenWRT, Lede, NixOS, Gentoo etc.

WPIA CA infrastructure (Casseopeia/Gigi)

Target of CA Infrastructure project is to provide individuals and organisations with reliable and accountable digital certificates using PKI technique. Certificates should always match the CA/Browser Forum Baseline Requirements and be compatible with ETSI standards. The software built by WPIA covers the feature set of the Baseline Requirements as layed out by the CA/Browser-Forum. The project delivers a number of components: Cassiopeia (signer software), Gigi (frontend), NRE (code used to generate the root certificates that will be used in the CA) and the infrastructure for configuration of the CA systems.Defending digital democracy in the European Union (and beyond) Holland Strikes Back 2018

Annex 2: Presentations, contributions and initiatives in 2018

NLnet and its employees actively participate in various fora and projects regarding the open and free internet, cybersecurity, and the implementation of open standards and open source. A selection of the most prominent contributions:

Participation in various brainstorms and workshops:

TODO

Talks :

TODO

'Radically Open Security' (ROS) is a company around ethical hacking and security founded in 2014 by dr. Melanie Rieback. ROS will donate at least 90% of its proceeds to NLnet foundation for at least the first five years. In 2018 the company continued to build its portfolio of projects and clients, hauling in big names from telecoms, banking, academia and critical infrastructures. The company takes a principled approach which puts transparency, open source, responsible disclosure and ethics first – which together with its idealistic and non-hierarchical model has attracted a talent pool of ethical hackers. Sofar NLnet provided them with two loans to help them grow more rapidly.

In 2018 NLnet continued its membership of Digital Infrastructure Netherlands. DINL is a group of seven institutes, associations and foundations (SIDN, DHPA, DDA, AMS-IX, ISPConnect, Surfnet, Nederland-ICT, VVR and NLnet) that collectively works on important topics in the Netherlands Digital Infrastructure community: promotion, education, cybersecurity, and laws & policy.

NLnet supports the Open Invention Network. Organisations and non-formal organisations like FLOSS communities benefit from the defensive patent pool and from the collective legal support to shield themselves and their users against patent offenses. Open Invention Network has made several donations to NLnet in recognition of its contribution to this initiative.

During 2018 NLnet continued to support Stichting Accessibility. The mission of the Accessibility Foundation is to improve the accessibility of internet and other digital media for all people, including the elderly and people with disabilities. The Foundation was established in 2001 and has about 20 people working in their office in Utrecht. Accessibility has always been funded by the Bartiméus Institute for the blind in the Netherlands. Since early 2016 Accessibility operates entirely independent and is economically healthy, NLnet provided them with a bridging loan to make this possible.

Event sponsoring

On September 27th 2018 NLnet foundation organised the fifth edition of the conference "Holland Strikes Back", together with its DINL partners. The event presented the key Netherlands initiatives against cyber attacks with 17 prominent speakers such as Bill Binney (Pretty Good Knowledge), Jos Weyers (TenneT), Jelle van Haaster (Netherlands Ministery of Defense), and other experts from the sector. The event was presented by Roelof Hemmen.