



NGI Architects

Selected in the 2020 and 2021
NGI Pointer Open Calls.



Grant Agreement No.: No 871528
Call: H2020-ICT-2019-2
Topic: ICT-24-2018-2019
Type of action: RIA

Index

NGI Architects

2020 -2021 Project Descriptions

Intro	03
-------	----

Core Internet Applications

Nyxt Browser (I)	04
Dream	05
Ltt.rs	06
Lightmeter (LM)	07
Edgeness	08
Garage	09
AP ³	10

Transport Networks

SCE	11
MPTCP5G	12
MPTCP	13
Multipath TCP	14
RIM	15
TA4NGI	16
SPHINX	17
PANAPI	18
TCPLS	19
Nyxt Browser (II)	20
WireGuard	21

Virtualization

Mirage OS	22
-----------	----

Index

NGI Architects

2020 -2021 Project Descriptions

Private-by-design Protocols

Koruza	23
Scuttlebutt	24
DataHop	25
Peergos	26
p2panda	27

Internet Technology Tools

DT4DW	28
Linux Regtracking	29
Libre-SOC	30
P4EDGE	31
LibrEDA	32

New Internet Paradigms

Reowolf (LM)	33
Verified SCION	34
Solid Shape	35

Security

EDGEsec	36
EU Firmware	37
ENViSEC	38

Identity Technology

ID - xover	39
------------	----

Intro **NGI Architects**

2020 -2021 Project Descriptions

What is the Next Generation Internet (NGI)

NGI (ngi.eu) is a European Commission funded programme to evolve the Internet, Internet technologies and uses in a more human centric way. NGI Pointer, NGI Pointer is part of the NGI and seeks brilliant Internet talents – NGI Architects.

Who are NGI Architects?

Historically, the inception of the Internet clearly has key persons behind it. Internet Architects like Vint Cerf, Bob Khan and the inventor of the web Tim Berners-Lee made huge contributions. Technicians, researchers, funders, businesses and policymakers made it happen and scaled it up globally.

However, as the Internet grows in terms of complexity such as technology choices, actors, users and use cases, boundaries become blurred and activities hidden or implicit. Internet governance bodies, such as the Internet Architecture Board and the Internet Engineering Task Force create structure.

But it is the people that everyday evolve and change the Internet through official and unofficial channels, at the core of the architecture or through new applications and uses that are growing rapidly. These people are NGI Architects.

Who are the proto NGI Architects?

NGI Pointer has found their first and second batch of NGI Architects. After the first and second Open Call NGI-Pointer the project received more than 200 applications (proto-NGI Architects) and from which the team selected 37 project beneficiaries that are now NGI Pointer Architects.



NGI POINTER (NGI Program for Open Internet Renovation) has received funding from the European Commission, as part of the Horizon 2020 Research and Innovation Programme, under Grant Agreement No.871528

Core Internet Application

Nyxt Browser

Internet Power Browser



Country:

 Germany

 France

Team:

John Mercouris

Further information:

<https://nyxt.atlas.engineer/>

<https://github.com/atlas-engineer/nyxt>

Contact

<http://john.mercouris.online>

We make Next, a fully extensible power-browser.

It enables sophisticated web document manipulation and processing where users can... e.g.:

- + Switch between tabs by topic, URL, etc.

- + Search all URLs on a page by name, or target.

- + Search through all of their bookmarks with compound queries (e.g. show bookmarks tagged "fish" AND "goldfish" OR "carp")

We wish to extend these capabilities via a number of paradigms/technologies:

- + Strengthen the text and semantic analysis capabilities of Next to allow chaining these operations in workflows for document processing.

- + Graphical, interactive document object model selection and manipulation. This will allow the user to operate on a set of elements simultaneously, to for example, map a download operation on a set of

Further information:

- + Users can persist/retrieve document annotations.

- + "Omni-search" capability allowing users to simultaneously search through their history, notes, and all other sources.

Core Internet Application

Dream

Distributed Replicable Extensible Agency Machine



Country:



Belgium

Team:

Petites Singularités ASBL

Further information:

<https://dream.public.cat/>
[https://gitlab.com/
public.dream](https://gitlab.com/public.dream)

Contact

DREAM Team <dream@public.cat>

DREAM stems from the encounter of P2Pcollab, openEngiAdina, and IN COMMON developers through grassroots community events.

Over time they realized the common interest in systems architecture and values they share to sustain local communities and commons initiatives in the respect for human dignity and human rights, freedom, democracy, equality, and the rule of law.

DREAM aims to advance critical infrastructure parts of our common projects to jump start a long time dream – hence the name – to see converge the best of the Social Web (easy UI, Linked Data), with the best of Peer-to-Peer networking architectures (end-to-end encryption, autonomy, replicability, lack of central control, censorship resistance, privacy-by-design and privacy-by-default).

Together we want to explore and bootstrap the next generation of locally-aware, distributed collaborative Internet protocols and applications to empower citizens to act and find agency together, free from alien interference and disinformation.

Core Internet Application

Ltt.rs

Open Source Email client(JMAP)



Ltt.rs (pronounced "Letters") is a beautiful, user friendly and encrypted by default E-Mail client for Android based on modern standards like JMAP (RFC 8621) and Autocrypt.

Using JMAP instead of IMAP will make the app more maintainable and more reliable on current mobile operating systems due to the build in push capabilities.

Country:



Germany

Team:

Daniel Gultsh

Further information:

GITHUB - <https://github.com/iNPUTmice/ltrs-android>

Contact

<https://gultsch.de/>

Core Internet Application

Lightmeter (LM)

Control of sensitive comms.




Lightmeter will make it easy to run email, servers large and small by visualising, monitoring, and notifying users of problems and opportunities for improved performance and security.

People will regain control of sensitive communications either directly by running their own mailservers, or indirectly via the increased diversity and trustworthiness of mail hosting services.

Country:

 **Germany**

 **Brazil**

 **Albania**

 **France**

Team:

Sam Tuke

Further information:

<https://lightmeter.io/>
<https://twitter.com/lightmeterio>

<https://www.linkedin.com/company/lightmeter>
<https://mastodon.social/@lightmetert>

Contact

@samtuke

Core Internet Application

EDGENESS

Energy Efficiency, Edge and Serverless Computing.



Country:

 **United Kingdom**

Team:

Prof. Karim Djemame
University of Leeds

Contact

K.Djemame@leeds.ac.uk

The project revisits the Internet Architecture by leveraging Software Defined Networks (SDN) with Network Function Virtualisation (NFV) technologies to allow efficient and on-demand placement of Virtual Network Functions (VNF) on a serverless platform for energy-aware function provisioning in edge environments.

Edge computing is seen as critical for supporting the next generation of services and applications that demand high speeds and low-latencies though energy consumption is a matter of concern.

Serverless computing as a paradigm in virtualisation is considered as a low-latency and a rapidly deployable alternative to traditional virtualisation approaches.

Event-triggered serverless functions incentivise energy efficient resource usage and provide granular reporting on a function level.

The project will develop a new building block that satisfies the services performance while reducing the energy consumption in edge environments.

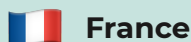
Core Internet Application

Garage

Geo-distributed data store
compatible with the S3 API.



Country:



France

Team:

Deuxfleurs association

Further information:

<https://garagehq.deuxfleurs.fr/>

Contact

ca@deuxfleurs.fr

Garage is a geo-distributed data store notably compatible with the S3 API.

It is developed by Deuxfleurs, an opinionated hosting association pushing to make web hosting more simple, resilient and sustainable for small organisations and society at large. It is already used in production to store and serve Deuxfleurs' websites and media assets.

Garage makes it easy to distribute the storage layer of digital services, supporting multi-cloud and on-premise deployments, even allowing household computers to join the cluster without a hassle.

By replicating hosted data among storage nodes, Garage brings resilience and peace of mind in case of failures. By enabling second-hand hardware to be part of a distributed storage cluster, Garage allows for drastic reductions of one's environmental footprint.

In the future, we plan to support various new kinds of workloads in Garage. In particular, the NGI Pointer grant would allow our team to build a distributed e-mail storage module supporting IMAP.

Core Internet Application

AP³

Advanced privacy-preserving protocols for GNU Taler.



Country:

 **Germany**

Team:

Özgür Kesim

Contact

oec-taler@kesim.org

Further information:

<https://taler.net/>

<https://docs.taler.net/design-documents/013-peer-to-peer-payments.html>

GNU Taler is an existing project that has developed Free Software infrastructure and protocols for privacy-friendly online payments.

Our aim is to extend the GNU Taler protocols with the following new functionalities:

1. Anonymous age verification:
Augmenting coins and corresponding protocols with a scheme to perform anonymous age verification.
2. Anonymous sealed-bid auctions:
Augmenting GNU Taler protocols to run anonymous sealed-bid auctions, based on works by Felix Brandt and Markus Teich.
3. Peer-to-Peer payments: Implementing fully transactional customer-to-customer payments.

Transport Networks

SCE

Some Congestion Experienced.



With support from the NGI Pointer program, our goal is to expand SCE high-fidelity congestion control signaling beyond the edge and into core networks and aggregation points. To accomplish this goal, we will develop a new SCE queueing discipline (qdisc) that can operate using a small and fixed number of FIFO queues, for when fair queueing is not available.

This new qdisc will provide approximate fairness between SCE, RFC3168 ECN and non-ECN flows, some isolation for latency-sensitive flows, and mitigation for unresponsive flows.

Along with the new qdisc, we will develop an expanded suite of tests and tools, addressing an appropriate set of congestion control concerns from RFC5033.

Source code and test results will be added to our open source repositories, and a new I-D (Internet Draft) will be submitted, along with any updates to existing Internet Drafts.

If possible, the results will be presented to the TSVWG (Transport Area Working Group) in the IETF.

Country:

 **Czech Republic**

 **Finland**

Team:

Pete Heist & Jonathan Morton

Further information:

http://sce.dnsmgr.net/downloads/NGI_Supplemental.pdf &
<https://github.com/chromi/sce>

Contact

<https://github.com/heistp/irtt>

Transport Networks

MPTCP5G

Multipath TCP for 5G networks.



Multipath TCP was invented in Europe. It already plays an important role to support Hybrid networks but it will play an even more important one in the Wi-Fi/5G coexistence.

Unfortunately, its deployment remains limited.

This project will bring stable and tested open-source implementations that enable vendors of Linux-based user equipments and servers to leverage all the benefits of this new protocol.

Country:



Belgium

Team:

Tessares S.A.

Further information:

tessares.net

twitter.com/TESSARES_SA

linkedin.com/company/tessares

facebook.com/tessares2015/

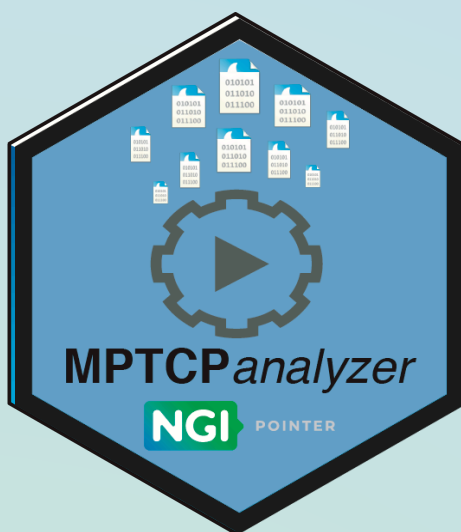
Contact

github.com/gdetal

Transport Networks

MPTCP

Multipath TCP



Multipath TCP (MPTCP) extends the most widely used transport protocol on the internet (TCP) so that it can use several physical paths (e.g., Wifi, cellular, between multihomed servers).

This allows to speed up transfers, smoothly transition from wifi to cellular when leaving one's house or potentially avoid traffic spying.

While the protocol is proven to work well in certain conditions (the fastest TCP connection ever was using MPTCP), it is configuration-sensitive and can degrade badly under adverse conditions (for instance in heterogeneous networks with small buffers).

The aim of this project is to provide the tool to help analyze the performance of a multipath protocol as well as the software to auto-configure the system depending on the application objective and network conditions.

Country:



France

Team:

Matthieu Coudron

Further information:

<https://github.com/ngi-mptcp>

Contact

<http://github.com/teto/>

Transport Networks

Multipath TCP

Fast prototyping of complex Graph Neural Networks for network optimization.



Country:



Team:

**Universitat
Politécnica Catalunya**

Further information:

Website: <https://ignnition.net>

Repository: <https://github.com/BNN-UPC/ignnition>

Contact

Website: <https://bnn.upc.edu/>

Twitter: @BNN_UPC

Despite being a hot-topic, we -the Internet community- have failed to produce marketable AI products for autonomous network operation and control.

The main reason behind this is that state-of-the-art AI techniques can only operate in the same scenarios seen during training. As a result, the vendor needs to train the AI algorithm in each of the production networks where it is planning to deploy it. This strongly limits commercialization since AI training requires using configurations that may break the production network.

Recently, Graph Neural Networks (GNN) emerged as the only AI solution capable of generalizing to unseen networks. This allows a vendor to train a GNN-based AI algorithm and deploy it as is on any operator's network. However, developing a GNN is a heavy task that requires AI experts with deep skills. In this project we aim to address this issue, by allowing the Internet community at large to take advantage of GNN without requiring such skills.

We thus present IGNNITION, a framework for fast prototyping of Graph Neural Networks.

Transport Networks

RIM

Receiver-driven Incoming - traffic Management



Country:



Spain

Team:

**Universidad Carlos III
de Madrid**

Further information:

**[http://
redbat.netcom.it.uc3m.es/](http://redbat.netcom.it.uc3m.es/)**

Contact

Marcelo Bagnulo
- Associate Professor
Telematics Department
University Carlos
III of Madrid

The goal of RIM is to evolve the Internet's resource management approach to enable receivers to execute congestion control functions, taking an active role in determining how the capacity of incoming traffic.

Further information is split among flows. In the current Internet architecture, the distribution of link capacity across multiple flows is determined by the congestion control algorithms running in the senders.

Content consumers play a passive role on the distribution of the capacity of their incoming Further information between flows.

The ambition of the RIM project is to empower end-users to be able to influence the share of capacity that is allocated to different incoming flows according to their preferences.

We propose to achieve this by enabling congestion control functions at the receiver-end of existent transport protocols (TCP/QUIC).

Discover Associate Prof. Marcelo Bagnulo scientific contributions: <https://www.researchgate.net/scientific-contributions/Marcelo-Bagnulo-9200827>

Transport Networks

TA4NGI

Trust and Authentication for Next Generation Internet.



Country:



Germany

Team:

DAASI International GmbH

Further information:

<https://daasi.de/de/>
https://twitter.com/DAASI_Int
<https://www.linkedin.com/company/daasi-international-gmbh/>

Contact

Peter Gietz
<https://www.linkedin.com/in/petergietz/>

TLS-KDH is an evolving standard protocol for high security authentication and transport encryption, which aims at security in a future world of quantum computing.

It combines basically three established technologies to reach this aim: Kerberos, TLS, and Diffie-Hellman key agreement protocol.

Since DH and TLS are used together already, the real innovation of TLD-KDH is the integration of the Kerberos protocol, so that a client can authenticate with a Kerberos ticket instead of using an X509 client certificate, which showed to be hard to manage for many users.

This Project will as proof of concept implement TLS-KDH as authentication mechanism in the form of a microservice plugin to the open source software Satosa.

Satosa is a multi-protocol authentication and authorization proxy that supports both sides of the SSO protocols SAML and OIDC (Identity Provider/ Service provider or OpenID Provider / Relying party). It will also evaluate it's use as transport encryption in the open source application Corteza.

Transport Networks

SPHINX

Standards for Private High Quality Internet Networks.



Country:

 **Switzerland**

Team:

Harry Halpin

Nym Technologies SA

Contact

harry@nymtech.net

The Sphinx packet format provides an essential potentially standardized component for privacy-enhanced networking.

Privacy-enhanced networking works today as an overlay network on top of existing TCP/IP and TLS, but existing implementations are not standardized and so cannot communicate and the lack of a standardized specification leads to difficulty with adoption by enterprise and government.

Our SPHINX project will tackle these problems by producing test-suites, open source code, and standards-ready specifications to make a privacy-enhanced and GDPR compatible internet ready for any European - and beyond! - internet application, including even web browsers.

Transport Networks

PANAPI

Path Aware Networking API



Country:



Germany

Team:

Prof. Dr. David Hausheer

**Otto-von-Guericke Universität
Magdeburg**

Contact

<https://www.netsys.ovgu.de/>

The PANAPI (Path Aware Networking Application Programming Interface Design and Implementation) project will design a sophisticated host-based network-path selection engine on top of the SCION network architecture, and provide it as an open source implementation of the abstract next-generation transport service API currently being drafted in the IETF TAPS Working Group.

PANAPI will provide a powerful and extensible framework for automatic path property measurements, path quality evaluation, and optimized path selection, complete with automatic load balancing and failure recovery in a PAN environment, all hidden behind upcoming standard application-facing API abstractions.

Our work will empower a large community of developers interested in adding PAN support to their applications. Incorporation of developer feedback, permissive open source licensing, close collaboration with PAN architects on the PANAPI implementation, and engagement with the IETF community about front end API compatibility and best practices are among our most important priorities.

Transport Networks

TCPLS

Transport Layer Security Ext. (TLS) 1.3



Country:



Belgium

Team:

Olivier Bonaventure
Université catholique
de Louvain

Contact

Olivier.Bonaventure@
uclouvain.be

TCPLS is an extension to Transport Layer Security (TLS) 1.3 that closely couples TLS with one of the most important Internet protocols: TCP.

This allows a greater extensibility for TCP by overcoming the limits of TCP Options and by limiting middlebox interference.

Our opensource prototype, described in the attached document, demonstrates that this coupling can bring many new features to TCP (support for multiple streams, connection failover and migration, multipathing, ...) while preserving its performance compared to recent protocols such as QUIC.

Since TCPLS is implemented inside TLS libraries, it is easier to deploy than TCP extensions like Multipath TCP that require kernel changes. Within the NGI Pointer programme, we aim at encouraging the adoption of TCPLS through active contributions to the IETF.

In parallel with the improvement of our open-source prototype, we will specify, discuss, and develop the TCPLS protocol within the IETF.

Transport Networks

Nyxt Browser (2)

Internet Power Browser



Country:

 Germany

 France

Team:

John Mercouris

Further information:

<https://nyxt.atlas.engineer/>

<https://github.com/atlas-engineer/nyxt>

Contact

<http://john.mercouris.online>

We make Next, a fully extensible power-browser.

It enables sophisticated web document manipulation and processing where users can... e.g.:

- + Switch between tabs by topic, URL, etc.

- + Search all URLs on a page by name, or target.

- + Search through all of their bookmarks with compound queries (e.g. show bookmarks tagged "fish" AND "goldfish" OR "carp")

We wish to extend these capabilities via a number of paradigms/technologies:

- + Strengthen the text and semantic analysis capabilities of Next to allow chaining these operations in workflows for document processing.

- + Graphical, interactive document object model selection and manipulation. This will allow the user to operate on a set of elements simultaneously, to for example, map a download operation on a set of

Further information:

- + Users can persist/retrieve document annotations.

- + "Omni-search" capability allowing users to simultaneously search through their history, notes, and all other sources.

Transport Networks

WireGuard®

Layer 3 secure network tunnel.



Country:



France

Team:

The WireGuard Project

Further information:

<https://www.wireguard.com>

Contact

team@wireguard.com

WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography.

It is a layer 3 secure network tunnel, originally designed for the Linux kernel, but now making its way into all major operating systems.

It is meant as a more secure replacement for many uses of older protocols like IPsec and OpenVPN, which suffer from countless security design flaws from the 90s.

It uses state of the art cryptography and is designed from the ground up to emphasize a small TCB and defense-in-depth security practices.

WireGuard also aims to be extremely easy to use, having few knobs, and a general notion of being secure by default and misuse resistant. It also has a very small and hardened attack surface, being designed to be placed on the outer-most edge of networks.

Virtualization

MirageOS

Deploying MirageOS unikernels



Country:



Germany

Team:

**Center for the Cultivation
of Technology gGmbH**

Further information:

<https://robur.coop>

Contact

team@robur.coop

A MirageOS unikernel is a virtual machine that provides a single service. It is written in a statically-typed memory-managed functional language.

The language choice avoids several attack vectors, and since a unikernel only contains the required functionality the attack surface is reduced drastically. The resource usage of a MirageOS unikernel is reduced by an order of magnitude compared to a Linux based solution.

Most components are open source under a permissive license (MIT/ISC).

In this project, we will improve and document the deployment story of MirageOS unikernels: establishing a repository of reproducible binary images, enhancing existing MirageOS orchestration tooling, integrate into established orchestration systems, and improve the observability of MirageOS unikernels.

We will as well conduct case studies with external organizations and integrate MirageOS unikernels into their existing infrastructure.

Operators will be able to use MirageOS unikernels instead of relying on commercial cloud solutions. This way they take back control over their data and reduce the carbon footprint.

Private-by-Design Protocols

Koruza

Wireless Optical CommsSystem for Urban Environments.



Country:



Team:

IRNAS – Institute for Development of advanced applied systems Ltd.

Further information:

<https://www.iras.eu/>

<https://www.facebook.com/instituteiras/>

https://twitter.com/institute_iras

<https://www.linkedin.com/company/institute-for-development-of-advanced-applied-systems/>

https://www.instagram.com/institute_iras/

https://medium.com/@institute_iras

Contact

<https://www.linkedin.com/in/luka-mustafa/>

KORUZA is a wireless optical communication system for urban environments, based on the FSO technology, designed for last-mile, 5G and IoT applications.

It uses an eye-safe collimated beam of IR light for point-topoint data transmission through air.

The solution avoids digging up roads, allowing distances up to 150m with fibrelike speeds 1-10 Gbps.

By utilizing mass-produced parts and open-source standards, KORUZA differentiates itself from the competition by dramatically reducing costs, coming at ~ 10/meter, 10x cheaper than other FSO and fibre-based solutions.

The low latency and jitter makes it suitable for 5G networks, last mile network.

Private-by-Design Protocols

Scuttlebutt

The Gossip Protocol [SSB].



Country:

 Denmark

Team:

**Scuttlebutt European
Collective via IOLA ApS**

Further information:

<https://scuttlebutt.nz/>
<https://scuttlebutt.eu/>
[https://github.com/dominictarr/
scuttlebutt](https://github.com/dominictarr/scuttlebutt)

Contact

@thezelf / @zelf

Scuttlebutt (SSB) is an edge computing, peer-to-peer communications protocol.

Originally created by Dominic Tarr in 2015 it is currently developed by an established global community with a variety of implementations, the most wide-spread implementation currently being the main network of ~20,000 nodes.

As one of the frontier protocols in the realms of the Distributed Webs, it shares this space with DAT, IPFS and more.

SSB stands out among its siblings due to its unique network architecture in which data flows opportunistically between nodes and along paths of trust relationships between humans, it is due to this the protocol is called "the gossip protocol", with the network architecture resembling data flows between humans.

The organizational structure behind Scuttlebutt is distributed over several projects globally, in the scale of VC-funded startup apps based on Scuttlebutt to experimental network designs for the Distributed Webs.

Currently all of the Scuttlebutt code base, as developed by different parties, is licensed as MIT and AGPL

Private-by-Design Protocols

DataHop

Incentivised Dissemination of Content at the Network Edge.



DataHop is building a mobile content distribution infrastructure based on smartphone D2D communications.

Content is pushed to source selected mobile users and then hops from device to device (D2D) and spreads in the network to destination nodes. Sources and destinations sync through our unique, data-centric connectivity software solution.

Our revolutionary approach guarantees that content spreads independently of the cellular connection, building a content distribution network that works completely at the edge without depending on the network infrastructure.

Therefore, challenged connectivity and data caps are not a barrier to the distribution of large volumes of data, allowing users to share their unused resources (in our case smartphone memory and available battery) to become an active part of the network, instead of just a consumer.

Country:

 **United Kingdom**

Team:

DataHop Labs Ltd.

Further information:

<http://datahop.network>

[@datahoplabs](https://github.com/datahop)

<https://github.com/datahop>

<https://www.linkedin.com/company/datahoplabs/>

Contact

contact@datahop.network

Private-by-Design Protocols

Peergos

A p2p, secure file storage, social network and application protocol.



Country:

 **United Kingdom**

Team:

Peergos Ltd.

Further information:

<https://peergos.org>

<https://github.com/peergos/peergos>

<https://twitter.com/peergos>

Contact

<https://www.linkedin.com/in/iancpreston>

Peergos is a private-by-design protocol with a global end-to-end encrypted file system at its foundation.

Designed to bring private and secure applications to the web, Peergos respects user privacy - servers cannot see metadata like file names, sizes or directory topology or even who is sharing with whom.

Peergos also gives users portability of their data - since our servers are trustless, users can mirror their data safely on many storage providers.

Finally, Peergos does not depend on DNS or TLS certificate authorities.

With support from NGI-POINTER we built on this foundation to offer a social network protocol, decentralized chat, a bridge to email, several productivity applications (calendar, planning boards, file search), all with our unique privacy and security features.

Peergos is designed to ensure that each user's social graph remains hidden from the server whilst ensuring that users are able to discover each other and the content they post.

Applications served through Peergos are sandboxed so that they cannot track users or exfiltrate data without permission.

Private-by-Design Protocols

p2panda

p2panda + Bamboo + OpenMLS



Country:



Germany



United Kingdom

Team:

Ahrend, Kuna, Dzialocha
GbR

Contact

contributors@p2panda.org

Further information:

<https://p2panda.org>

<https://github.com/p2panda>

p2panda + Bamboo + OpenMLS

p2panda is a user-friendly peer-to-peer communications protocol with browser support, local deletion, fork detection, efficient partial replication, large-scale group messaging encryption and future-proof schema migrations to build secure and user-friendly applications on top.

p2panda has been in development since 2019 with a focus on prototyping and research.

For the next phase we aim at a reference implementation and POC (published under AGPL), while stabilizing the APIs and specifications of related projects:

“Bamboo”, a efficient append-only log data type and “OpenMLS”, an implementation of the MLS protocol for secure group messaging.

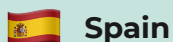
Internet Technology Tools

DT4DW

Developer Tools for Decentralized Web



Country:



Spain

Team:

Tim Perry

Contact

tim@httptoolkit.tech

Further information:

<https://httptoolkit.tech/>

The essential technologies to build a decentralized web are available today, but the wider ecosystem and uptake is still in its infancy. Mainstream web developers are not yet using these technologies to build the production-grade decentralized applications that we need to kickstart the next generation of the internet.

One reason for this is a lack of developer tooling. Moving from traditional client/server architectures to building decentralized applications requires developers to replace many day-to-day debugging & testing tools with manual logging, custom scripts and guesswork. This tooling gap contributes to the significant difficulties of decentralized development today.

By extending HTTP Toolkit and Mockttp (an open-source developer tool and testing library for today's HTTP-powered web) to support IPFS, WebRTC and Ethereum, this project will give developers the tooling they need to debug and test next-generation decentralized web applications.

Internet Technology Tools

Linux Regtracking

Linux kernel regression tracking.



Country:



Team:

Thorsten Leemhuis.

Further information:

<https://linux-regtracking.leemhuis.info/>

Contact

linux@leemhuis.info

Build and integrate mechanisms into the Linux kernel development processes to track all regressions reported by humans or CI systems.

Together with the existing “no regression” rule this will help to make sure new releases with their improved security techniques work as good as their predecessors.

That's important, as the kernel is at the very heart of many devices that drive the internet or connected to it – but many of those use outdated kernel versions with known vulnerabilities, as vendors and admins fear switching to a later version might break something.

The mechanisms built for tracking Linux kernel regressions will include adapting or writing a servicebot tailored to the specific needs of the kernel developers and their email based workflow.

To make sure the solution is practical and accepted in practice the project owner will work it out in close relationship with the maintainers and create procedures on how to use it during development.

The goal is to see the solution properly established to ensure its continued use after this project ends

Internet Technology Tools

Libre-SOC

The Libre-SOC Project



The LibreSOC Project aims to bring to the world an ethically developed privacy respecting power efficient SoC with modern 3D and Video capabilities suited to today's mobile tasks.

Full source to the bedrock. no spying backdoor co-processors. no leaked firmware keys.

Fully transparently developed.

Country:



Team:

Luke Leighton

Libre-SOC

Contact

luke.leighton@gmail.com

Further information:

https://libre-soc.org/about_us/

Internet Technology Tools

P4EDGE

Accessible P4 programmable switches for the edge.

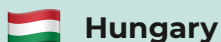


With the advent of P4 and programmable data planes, SDN 2.0 has been born, enabling the deep programmability of networks.

SDN 2.0 will transform networks to programmable end-to-end platforms where all the devices along the packet forwarding path are programmable.

All functions from bottom to top levels will be implemented as software instead of hardware throughout the Internet, enabling rapid prototyping and easy deployment of innovative ideas.

Country:



Hungary

Team:

Sándor Laki
Eötvös Loránd University
ELTE-Soft R&D Nonprofit Ltd.

Contact

lakis@elte.hu

Further information:

<http://p4edge.net>
<https://github.com/P4EDGE>
<https://github.com/P4ELTE/t4p4s>

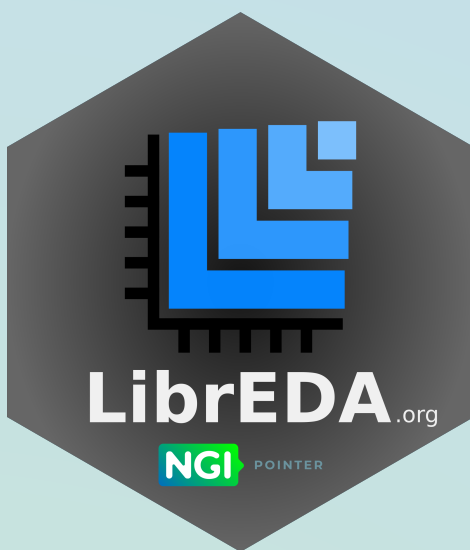
Existing hardware P4-switches were designed for high-speed networks and thus they are far too expensive and powerful for household (or edge) usage.

In this project, we will develop an open-source software stack to enable the creation of accessible P4-switches based on open hardware (e.g., RaspPI, x86/ARM-based router boards) that have low price (~100 USD) and low power consumption, and are accessible for a wide range of edge users (innovators, hobbyists, research, education, industry 4.0) where moderate performance (100Mbps to few Gbps) is only needed.

Internet Technology Tools

LibrEDA

Libre Electronic Design Automation.



Country:

 **Switzerland**

Team:

Thomas Kramer

Contact

contact@libreda.org

Further information:

<https://libreda.org>

LibrEDA is a libre software-framework for the physical design of silicon chips (i.e. turning a gate-level circuit description into layout which can be fabricated).

A strong motivation is democratization of silicon technology by making ASIC toolchains accessible for research, education and hobbyists. Currently the project is funded by NLNet/NGIO (until November 2021).

Generating chip layouts from an abstract circuit description involves many complex tasks which usually can be solved only heuristically.

Hence there are many different approaches for solving each sub-problem like placement or routing. The framework simplifies the implementation and combination of such sub-algorithms.

Currently there are only minimal example implementations of place-and-route algorithms - they do not scale well.

This project wants to bring them to a state which allows to build a usable tool-chain on top of the framework.

New Internet Paradims

Reowolf

Low-level iSockets to High-level Programmable Connectors.



Country:



Germany

Team:

**Stichting Nederlandse
Wetenschappelijk Onderzoek
Instituten - Institute CWI**

Further information:

<https://reowolf.net>

<https://scm.cwi.nl/FM/reowolf>

Contact

reowolf-list@cwi.nl

A major obstacle in the further development of the Internet is that improving quality of service relies on non-standard ad-hoc techniques such as deep packet inspection.

The effectiveness of these techniques is thwarted by the uptake of end-to-end socket encryption (partially caused by EU privacy regulation)!

Funded by NLnet/NGI0, Reowolf 1.0 is a first step to solve these problems, demonstrably by a centralized proof-of-concept implementation, but leaves some major challenges out-of-scope. In this project, Reowolf 2.0 tackles remaining challenges: increasing reliability, trust, standardization, and performance.

Reowolf replaces sockets by connectors which support high-level verification, compilation, and optimization techniques.

Resilience against service disruption is realized by decentralization; we improve security aspects of confidentiality, integrity, and availability (CIA); we draft Internet standards; and we integrate the middleware into the operating system kernel.

New Internet Paradims

Verified Scion

Verified Secure Routing with verified Scion.



Country:

 **Switzerland**

Team:

Anapaya Systems AG

Further information:

<https://www.pm.inf.ethz.ch/research/verifiedscion/NGI.html>

Contact

www.pm.inf.ethz.ch

The Next Generation Internet needs to offer a high degree of security to enable trustworthy communication despite omnipresent adversaries.

Since vulnerabilities are extremely difficult to detect during reviews and testing, the NGI must be based on solid foundations: security properties must be certified through formal proofs.

We will demonstrate the feasibility of developing an NGI that is provably secure by formally verifying strong security properties of the SCION inter-domain routing architecture.

We will formalize SCION's security guarantees and verify that the protocol main.

New Internet Paradims

Solid Shape

Reshaping Linked Data on the Fly with Solid Shape.



In this project, we aim to implement an open-source registry of linked data shapes and forms so we can identify and resolve problems that still remain unclear about these theoretical concepts.

Because a registry of linked data shapes and forms is an essential part of the Solid ecosystem, the execution of this project will accelerate Solid's adoption.

As the Solid specification is designed to improve data privacy, trust and portability, this open-source project matches to a great extent with the vision of NGI and several European values.

Country:



Belgium

Team:

Digita BV

Further information:

<https://digita.ai>

<https://www.linkedin.com/company/digita-ai>

Contact

<https://github.com/digita-ai>

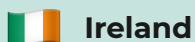
Security

EDGEsec

BSD jail/vm orchestration made easy and free.



Country:



Ireland

Team:

NQMCyber Ltd

Further information:

nqmcyber.com

<https://github.com/nqminds/EDGEsec>

Contact

<https://bit.ly/3yhNr8a>

Internet technologies and current practice does not address security requirements of edge based devices very well.

It is a fact that the "admin page" of most routers, wifi devices and webcams is "unsecured".

It is perhaps not surprise that a recent Symantec study showed that "Routers account for 75% of infected IOT devices " [1]

The problem is that domain resolution on local internets and HTTPS certificates do not work well together.

Also HTTPS certs assume the private key is secure; how do I do this on a small edge device?

EdgeSEC will define innovative user experience, key distribution, key storage and secure service discovery primitives, to address current security shortcomings and provide a new vision for integrated

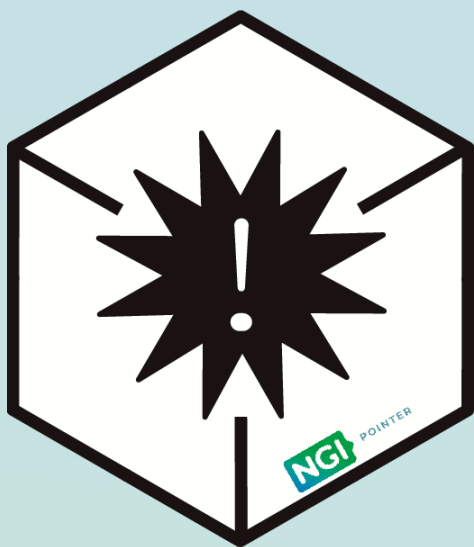
[1] Symantec ISTR - Internet Security Threat Report Volume 24 | February 2019

<https://docs.broadcom.com/doc/istr-24-2019-en>

Security

EU Firmware

European Firmware and App Library.



Country:



Netherlands

Team:

Tjaldur Software Governance Solutions.

Contact

<http://www.binaryanalysis.org/>

<https://github.com/armijnhemel/binaryanalysis-ng>

Current security research for Internet connected devices (consumer electronics, but also industrial IoT and SCADA systems) happens in a haphazard way.

In reporting many vulnerable devices are missed, leading to underreporting of vulnerabilities and a lack of sense of urgency for vendors to fix devices.

By creating a library of firmware files, with analysis reports and the possibility to do further analysis on large collections of firmware files and apps it becomes easier to have more complete reports and pro-actively scan and analyze more amounts of devices and apps.

Security

ENViSEC

AI-enabled Cybersecurity for Future Smart Environments.



Country:



Norway

Team:

Kristiania University College

Further information:

<https://kristiania.no/>
<https://smartseclab.com/envisec/>
<https://github.com/SmartSecLab/ENViSEC>

Contact

Andrii Shalaginov
andrii.shalaginov@kristiania.no

ENViSEC seeks to design new platform-independent Artificial Intelligence-based middleware to ensure cybersecurity in the IoT components present in every layer of Smart Environments.

Modern solutions like anti-virus and intrusion detection systems are not fully deployable on the Edge components due to hardware and software limitations.

The solutions we are proposing are partially dependent on the utilization of asynchronous proposals and balanced Machine Learning off-chip training.

They will ensure cross-platform capabilities that will apply to both non-OS microcontroller devices as well as OS-based single-board microcomputers.

Currently, IoT devices, especially their cybersecurity-related functionality, are solely dependent on the battery and incapable of major computations. Such limitations cause dramatic waste of power and human resources necessary to withstand cyberattacks.

We will ensure that cyber attacks can be detected and prevented across the whole IoT ecosystem.

Identity Technology

ID - xover

InternetWide Identity through Realm Crossover.




A security infrastructure for gaining trust in another realm's identity can be imagined with DNSSEC/DANE and certificates.

Embedding this in actual authentication schemes, with minimal change, is quite a challenge.

We found theoretic options in Kerberos and in SASL; the former scales well and the latter offers migration path for current password users.

Country:

 **Netherlands**

Team:

OpenFortress BV

Further information:

<http://internetwide.org/>
<https://gitlab.com/arpa2>

Contact

<https://gitlab.com/arpa2/>



NGI Architects

Selected in the 2020 and 2021
NGI Pointer Open Calls.



Grant Agreement No.: No 871528
Call: H2020-ICT-2019-2
Topic: ICT-24-2018-2019
Type of action: RIA