NGI ZERO

Open calls on privacy and trust enhancing technology & improving search and discovery

Powered by the European Commission Directorate-General for Communications Networks Content and Technology

825322 / 825310

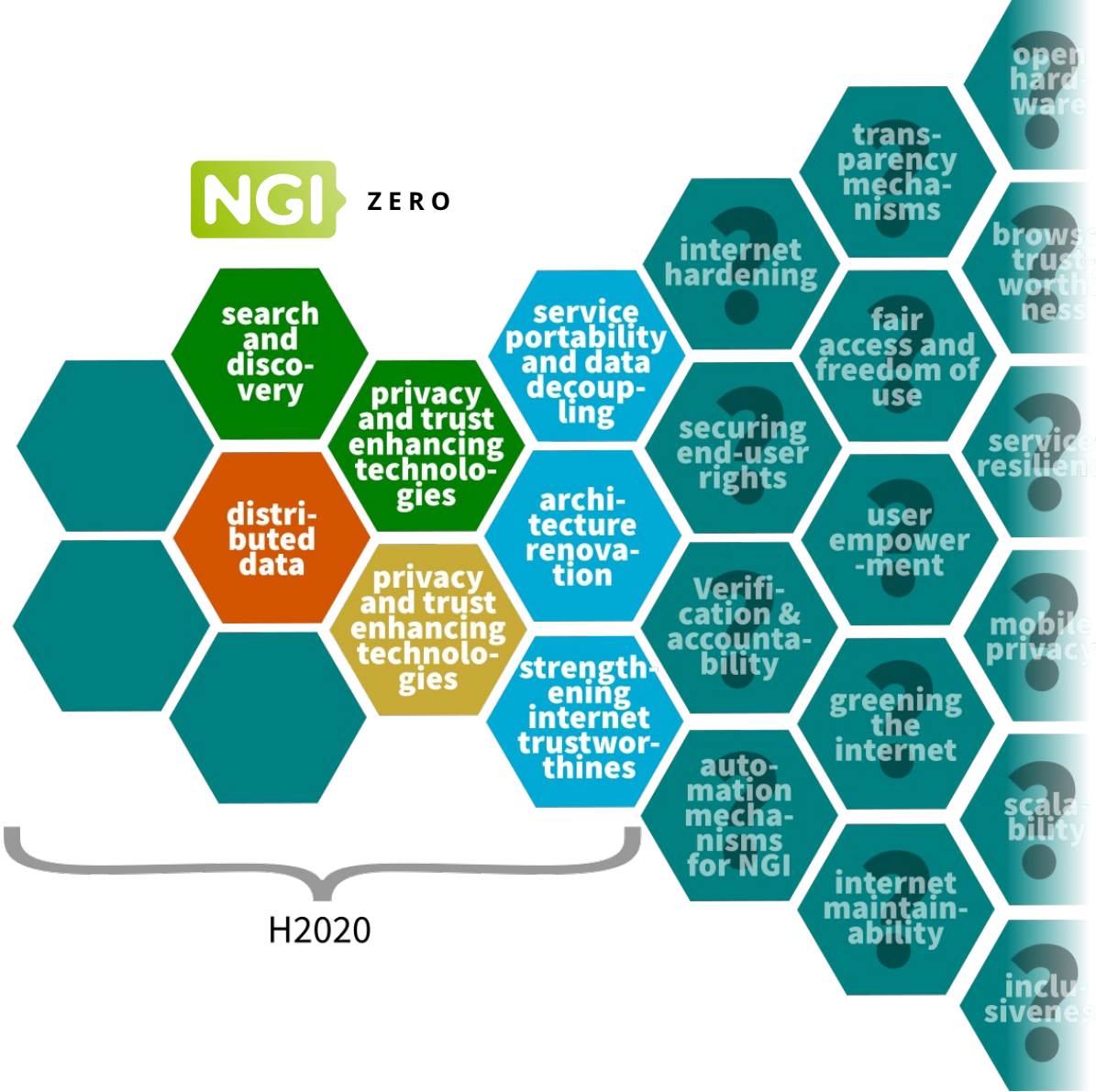
nlnet FOUNDATION

European Commission

NGI Atlantic Webinar

2019-14-05

Next Generation Internet
Research & Innovation actions



Key characteristics

search and discovery

5.6 million euro in small grants between 2018 and 2021

NGI ZERO

Competitive calls every **two months** until the budget is allocated.

Projects between 5k-50k

Walk the talk:

Inclusion
Security
Localisation
Open Standards
Free & Open Source
Deliver to deploy

privacy and trust enhancing technologies

5.6 million euro in small grants between 2018 and 2021

NGI ZERO

Calls: Send in your ideas. Deadline June 1st, 2020.

nlnet FOUNDATION

▸ home ▸ foundation ▸ people ▸ funding possibilities ▸ theme funds ▸ projects we support ▸ press ▸ contact

Welcome to NLnet Foundation

When it comes to important ideas that can help improve our society, there really are no boundaries. The challenge is to turn those *opportunities* into *reality*. Great ideas just come, but they are gone in a breeze as well. Lets make good use of them.

Since 1997 NLnet foundation (after its historical contribution to the early internet in Europe) has been financially support-

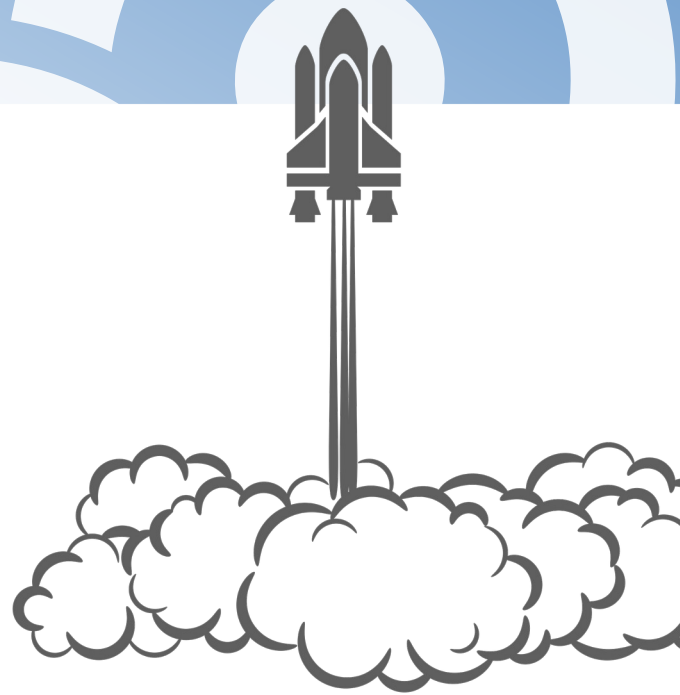
Zero-leak Search

Search

What do you mean with "Zero-leak search"?

Our approach

Design a light-weight and confidential application procedure providing adequate insight into technical capabilities as well as the urgency, relevance and relative cost effectiveness of the projects proposed at a low cost to the **applicants**.



Weight	Criterion
30%	Technical excellence/feasibility
40%	Relevance/Impact/Strategic potential
30%	Cost effectiveness/Value for money

Next Generation Search & Discovery

Next Generation Search & Discovery

The pen may be mightier than the sword, but how does it fare against the search button?

Search should not be a gatekeeper, a black box or a privacy nightmare. If the internet is the equivalent of a global brain, we need creativity and diversity in the pathways across that brain to unlock its true potential. Search and discovery are basic human needs for humans of all ages, and we would like to put powerful new technology in the hands of future generations as building blocks for a fair and democratic society and an open economy that benefits all.

Different layers

- End user applications
  - Searx, Plaudit, Blink RELOAD, Sonar, El Repo, Transparency Toolkit, CoinDiscovery
- Technical building blocks
  - GNU Name System, Software Vulnerability Discovery, IPFS Search, DID Resolver/Registrar
- Community infrastructure
  - StreetComplete, Fediverse.Space, SCION Geotagging, DeltaBot, In Common, SCION-SWARM, Fediverse Space
- Explorative search and discovery
  - Decentralized privacy preserving search

Some sample projects

VariationGraph

Vgteam is pioneering privacy-preserving variation graphs, that allow to capture complex models and aggregate data resources with formal guarantees about the privacy of the individual data sources from which they were constructed. The project will apply formal models of differential privacy to build variation graphs which do not leak information about the individuals whose data was used to construct them. The tools themselves are not limited to the above use cases, and open the doors to many other types of applications both online (web browsing histories, social media usage) and offline.

Some sample projects

Ipv6 Scanning

Scanning is state of the art to discover hosts on the Internet. Today's scanning relies on IPv4 and simply probes all possible addresses. But global IPv6 adoption will render brute-forcing useless due to the sheer size of the IPv6 address space, and demands more sophisticated ways of target generation. Our team developed such an approach that generally allows to probe all subnets in the currently deployed IPv6 Internet within reasonable time. In this project, we will develop a data storage and analysis solution for high-speed IPv6 scanning. It will process the high amount of received data concurrently with scanning, and provide continuous results while scanning for long periods. This effort enables full scans of the IPv6 Internet.

Some sample projects

Librecast Live

The Librecast Live project project contributes to decentralising the Internet by enabling multicast. Multicast is a major network capability for a secure, decentralised and private by default Next Generation Internet. The original design goals of the Internet do not match today's privacy and security needs, and this is evident in the technologies in use today. There are many situations where multicast can already be deployed on the Internet, but also some that are not. This project will build transitional protocols and software to extend the reach of multicast and enable easy deployment by software developers.

Applicant statistics

Entity types

February 2019:
16% foundations, 29% individuals, 43% SME's

April 2019:
5% foundations, 25% individuals, 7% institutes, 46% SME's, 10% universities

June 2019:
7% associations, 10% foundations, 13% individuals, 50% SME's, 10% universities

August 2019:
43% individuals, 8% institutes, 38% SME's

October 2019:
56% individuals, 11% institutes, 33% SME's

Privacy & Trust Enhancing Technologies

Privacy & Trust Enhancing Technologies

Privacy isn't dead, but we lack the right tools to protect our intimacy

Reliability, confidentiality, integrity and security should be the 'new normal' of the internet, something ordinary users should not have to worry about.

Trust is one of the key drivers for the Next Generation Internet, and an adequate level of privacy is a non-negotiable requirement for that.

Different layers of trust

- New end user applications bringing Privacy and Trust to users
  - Conversations, Sylk, Briar, Autocrypt, Cryptpad, Manyverse, Wireguard
- Human-centric middleware/Enablers:
  - IRMA, node-TOR, ValOS, Replicant OS, Rocket CWMP, Mobile Nixos, SCIM, ARPA2 ACL/SASL
- New standards and protocols to solve critical issues “upstream”
  - DID*, GNU Name System*, IMSI Pseudonymisation, TLS-KDH, SASL XMSS, Reowolf
- Technical and fundamental building blocks for trustworthiness
  - e.g. Noise Explorer/Verifpal, Libre-RISCV SoC, IMSI pseudonymisation, Identity Based Encryption, Tor Padding, GNU Mes, ..
- Explorative
  - Distributed private trust, ValOS, Vframe

Some sample projects

Libre-SoC

It is 2019 and it is not possible to buy a mass-produced laptop, tablet or smartphone and replace all of its software (with software that a user can trust) without loss of functionality. Processor boot-loaders are DRM-locked; WIFI, 3D Graphics and Video Processors are proprietary, and Intel's processors contain problematic features and intransparent elements such as the "Management" Engine.

The most logical way to restore and engender trust is to literally make a new processor - one that is developed transparently and may be independently audited to the bedrock. The project develops a low-power, mobile-class, 64-bit Quad-Core RISC-V SoC at a minimum 800mhz clock rate, suitable for tablet, netbook, and industrial embedded systems.

Some sample projects

OTRv4

OTRv4 is the newest version of the Off-The-Record messaging protocol used in for example Jitsi, Psi, etc. It is a protocol where the newest academic research intertwines with real-world implementations. It's aim is to give end-to-end encryption, deniability, authentication, forward secrecy and post-compromise security for any kind of messaging (online or offline). The goal of this new version is to give the most secure privacy and security properties that have a real impact on the world. This new version aims to be available in different desktop clients (that use XMPP or other messaging protocol) and in mobile clients.

Some sample projects

Robur privacy-enhanced DNS resolver and DHCP server

DHCP and DNS are fundamental Internet protocols, DHCP is used for dynamic IP address configuration in a local network, DNS for resolving hostnames to IP addresses. In this project, we develop a robust DHCP server and DNS resolver as a MirageOS unikernel. MirageOS unikernels are self-contained virtual machine images which are composed of the required OCaml libraries, leading to a binary with a minimal trusted code base, and thus minimized attack surface. The choice of the memory-safe, functional, and statically typed language OCaml avoids common attack vectors, such as buffer overflows and double frees.

Applicant statistics

Entity types

February 2019:
18% foundations, 37% individuals, 31% SME's

April 2019:
15% foundations, 35% individuals, 39% SME's, 10% unversities

June 2019:
24% associations, 20% individuals, 42% SME's, 6% universities

August 2019:
37% individuals, 9% association, 11% institutes, 33% SME's

October 2019:
39% individuals, 13% association, 46% SME's

join us and help discover and shape the next generation internet

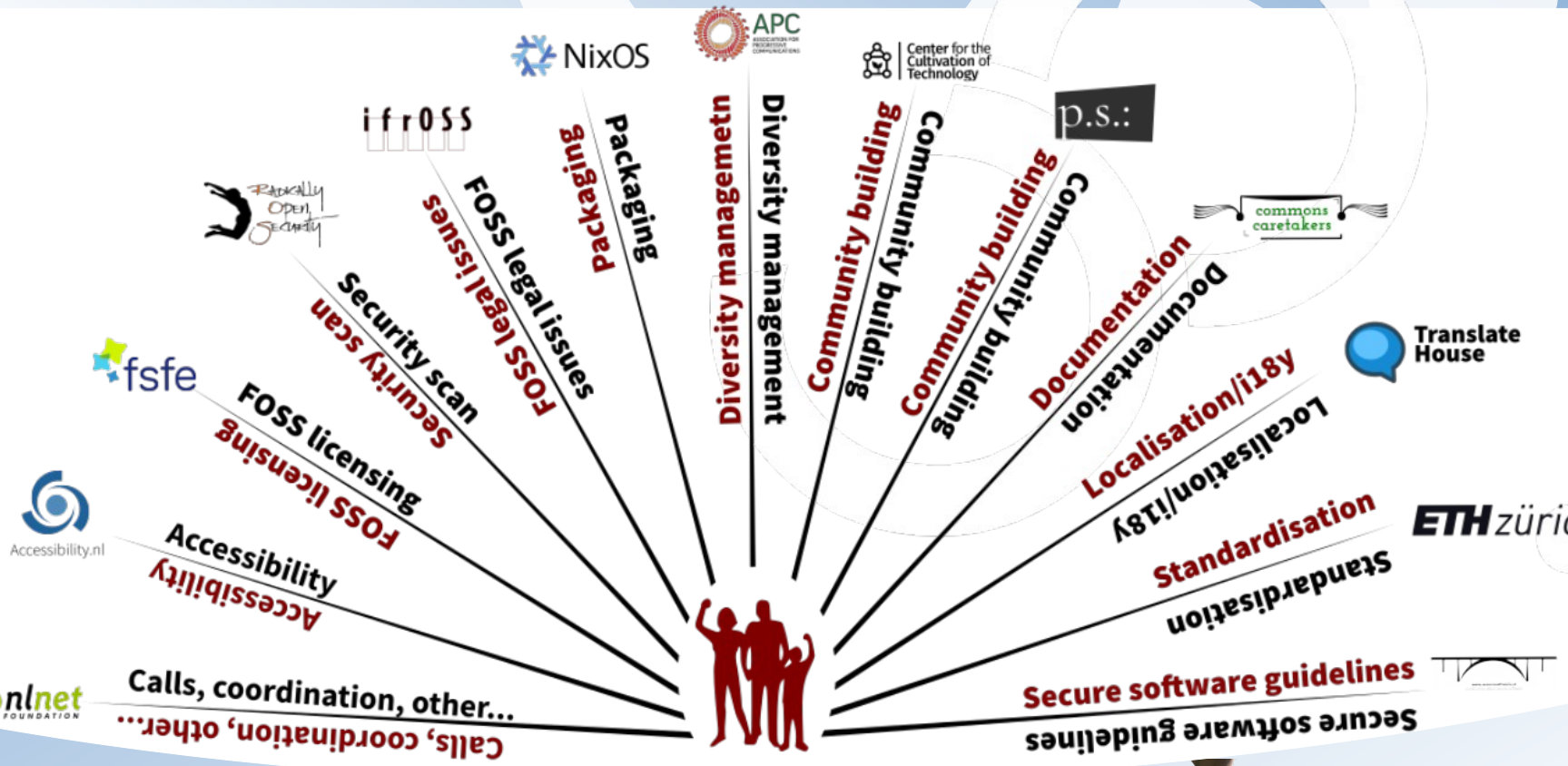
and claim your spot in human history

Full time and part-time paid and unpaid positions available.

Read all about it on
- https://nlnet.nl/discovery
- https://nlnet.nl/PET
- https://ngi.eu

European Commission

We aim to be project-centric



TODAY WE CREATE THE

INTERNET

OF TOMORROW

nlnet FOUNDATION