Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

Webinar, 10 September 2021
## Webinar – Agenda

<table>
<thead>
<tr>
<th>Timing</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00 – 10:10</td>
<td>Welcome</td>
</tr>
<tr>
<td></td>
<td>Jean-Luc Dorel, DG Connect, European Commission</td>
</tr>
<tr>
<td>10:10 – 10:20</td>
<td>Introduction</td>
</tr>
<tr>
<td></td>
<td>Alasdair Reid, NGI Trust coordinator, EFIS Centre</td>
</tr>
<tr>
<td>10:20 – 11:35</td>
<td>NGI Trust Funded projects results</td>
</tr>
<tr>
<td></td>
<td>NGI Trust Project managers</td>
</tr>
<tr>
<td>11:35 – 11:55</td>
<td>Round table discussion and exchange - Q&amp;A</td>
</tr>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td>11:55 – 12:00</td>
<td>Wrap-up and close</td>
</tr>
</tbody>
</table>
NGI TRUST in a snapshot

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

Key facts & figures

• 3 open calls:
  - 300 applications;
  - 448 applicants;
  - 36 countries.

• 3rd party funding: €5.6m:
  - 57 funded projects;
  - 84 funded third parties;
  - 20 countries.
NGI TRUST Objectives & Partners

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

Reinforce, structure and develop the community of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies.

Build on the state of the art in privacy and trust enhancing technologies by focusing support for third-party projects in a limited number of priority topics.

Improve user trust and acceptance of emerging technologies by focusing on applications and solutions that develop a more open, robust and dependable Internet and strengthen Internet Governance.

Foster the exploitation and commercialisation of the results of selected third-party projects through a tailored process of coaching and mentoring.
NGI TRUST

57 PROJECTS FUNDED
12 THEMATIC AREAS

- Beyond Passwords
- Better Privacy
- Safer Browsing
- User Control
- Impact of AI
- Human-Centric Internet
- Stronger Tools
- Effective Identity
- Personal Data Management
- Data Ethics
- Securing the Internet of Things
- Advancing Identity
NGI TRUST Funded projects results
Areas: Securing Internet of Things / Advancing Identity

<table>
<thead>
<tr>
<th>Project</th>
<th>Third party</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnonymAI</td>
<td>CELI, ICT Legal Consulting</td>
</tr>
<tr>
<td>IoTrust</td>
<td>Odin Solutions, Digital Worx</td>
</tr>
<tr>
<td>TOTEM</td>
<td>Feron Technologies, ntop</td>
</tr>
<tr>
<td>PRIMA</td>
<td>Cognitive Innovations</td>
</tr>
<tr>
<td>PY/Protect Yourself – PY 2.0</td>
<td>Panga, MyDataBall</td>
</tr>
</tbody>
</table>
AnonymAI
Legally Compliant Anonymization

H-FARM Innovation
What is AnonymAI?

Direct identifiers
- Name
- Surname
- Email address
- ...

National Identifiers
- Codice fiscale
- ID number
- Passport number
- ...

Indirect identifiers
- Civil status
- Nationality
- Age
- ...

Special Categories
- Sexual orientation
- Health related info
- Ethnic origin
- ...
How does AnonymAI work?

Possible Configurations

- Anonymize Everything (A)
  - Max Privacy
  - Min Utility
- Use Rules (B)
  - Only D.I.
- Custom Rules (C)

Machine Learning model

Rule-based component (e.g., regular expressions)

Documents to anonymize

Preprocessing & Language Analysis

Anonymization process

Confidential resolution

Privacy vs Utility Trade-off

Ideal Solution (but impossible)

Bad Data

Possible Trade-off

Low Privacy

Max Privacy

Max Utility

Data Utility
Milad Botros (BTRMDT70P06L425E), rappresentato e difeso da Avv. Matteo Caserio, -parte attrice
Andrea Bolioli (MDRBLM75H65L425G), rappresentata e difesa da Avv. Alessio Bosca, -parte convenuta

<NAME_1> <SURNAME_1> {<FISCAL CODE_1>}, rappresentato e difeso da Avv. <NAME_2> <SURNAME_2>, -parte attrice
<NAME_3> <SURNAME_3> {<FISCAL CODE_2>}, rappresentata e difesa da Avv. <NAME_4> <SURNAME_4>, -parte convenuta
My name is Milad Botros. I was born in Rome but now I live in Turin, which is a city in Italy. I'm 30 years old and I work as a Data Scientist. If you need more information about AnonymAI, please contact me at milad.botros@celi.it or 3333333333.

My name is <NAME_1> <SURNAME_1>. I was born in <BIRTHPLACE_1> but now I live in <RESIDENCE PLACE_1>, which is a city in <COUNTRY/REGION_1>. I'm <AGE_1> years old and I work as a <OCCUPATION_1>. If you need more information about AnonymAI, please contact me at <EMAIL_1> or <PHONE_NUM_1>.
Rafael Marin Perez – ODINS
Mirko Ross - DW

Odin Solutions SL (ODINS) - Spain
Digital Worx GmbH (DW) - Germany
Objectives & Contributions

- **Main Objective:** a trustworthy solution to setup and maintain IoT networks based on the development of novel technologies *(Bootstrapping, Peer-to-Peer and Distributed Ledger)* in order to provide secure initialization of IoT devices, vulnerabilities monitoring and software patching/reprogramming.

- **[O1]** To increase the user trust and application of secure IoT networks in worldwide sectors like Smart Cities, Industry 4.0, etc.

- **[O2]** To achieve trustworthy IoT networks and keep decentralized Internet infrastructure.

- **[O3]** To validate the IoTrust minimum viable product (MVP) using laboratory testbed and real-world pilots.

- **[O4]** To perform dissemination activities and joint exploitation plan.
Results & Deliverables

1. IoTrust Solution based on Novel Standards/Technologies
   1. Bootstrapping: SCHC, COAP-EAP, AAA
   2. Firmware Update Over The Air: Blockchain, IPFS
   3. Trust monitoring & anomaly detection: Machine Learning

2. MVP Testbed & Pilot Validation
   - Smart City Pilot (Spain) - ODINS
   - Industry 4.0 Pilot (Germany) - DW

3. Dissemination and Communication
   - Smart Agrifood Summit 2020
   - Building of Internet of Trust. Feb 2021,
   - Paris Space Week. 10 March 2021
   - Scientific Journal, JCR IF 3.367 Q2LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions
   - Conference paper IEEE International Conference on Smart Internet of Things (SmartIoT 2021)
Next-Steps

- Incorporate new open standards like IETF OSCORE for efficient data exchange protection.

- International Events
  - Web Summit — November 2021
  - LogiMAT — March 2022

- Exploitation Plan

  - SHOWCASE INDUSTRIAL DEMOS
  - FOLLOW AND REACT TO MARKET NEEDS
  - INTEGRATION WITH OPEN-SOURCE PROJECTS
TOTEM
Trust-Enhancing TechnOlogies CommodiTization for IncrEasing Security Awareness in Connected HoMes
FERON TECHNOLOGIES P.C. & ntop

8th Results Webinar, September, 10th, 2021
Antonis Gotsis (FERON) & Luca Deri (ntop)
antonis.gotsis@feron-tech.com & deri@ntop.org
Project Vision & Objectives

Value Proposition: In a connected home with many heterogeneous end-points, we want to simplify, automate and eventually make accessible to tech and non-expert users a set of tools for proper control of end-points and early identification of potential malicious operation.

Objectives

- Empower the home network with network monitoring and enforcing capabilities
- Augment the end-points with advanced monitoring capabilities
- Complement the monitoring capabilities with physical activity tracking & alerting
- Develop an open and fully configurable connected home testing environment
- Bundle the TOTEM tools into a low-cost general-purpose hardware board
## Project Key Results

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Lead Partner</th>
<th>Open-Source Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>A collection of software stacks for transparent home network monitoring and policy enforcing extending ntop's ntopng, nProbe and nDPI tools to the IoT use-case.</td>
<td>ntop</td>
<td><a href="https://github.com/ntop/">https://github.com/ntop/</a></td>
</tr>
<tr>
<td>II</td>
<td>Software library extending FERON's partner IoT codebase, used for embedding cybersecurity-aware device monitoring capabilities in ESP32-based IoT end-points</td>
<td>FERON</td>
<td><a href="https://github.com/insighio/">https://github.com/insighio/</a></td>
</tr>
<tr>
<td>III</td>
<td>Software Plug-in to Home-Assistant for use in connected home devices physical activity monitoring, characterization and end-user alerting</td>
<td>FERON</td>
<td><a href="https://github.com/feron-tech/">https://github.com/feron-tech/</a></td>
</tr>
<tr>
<td>IV</td>
<td>TOTEM testbed for testing project technologies and tools in real-world conditions with the use of COTS connected home devices</td>
<td>Both</td>
<td>-</td>
</tr>
</tbody>
</table>

4 webinars + 4 scientific publications
Project Impact & Next Steps

✓ NGI & Community
- Trust-enhancing technologies as an NGI strategic pillar for human-centric internet
- IoT trust tools (SW, HW, platforms) for increasing trust and cybersecurity awareness in Connected Homes
- Used by technology domain experts (open-source & documentation)
- Or by the general public (automated & user-friendly)

✓ FERON Partner: Full-stack IoT
- Address new markets, such as Smart Homes & IoT Cybersecurity

✓ Ntop: High-quality networking software
- Improve support and focus for IoT and Smart Home Applications

✓ Joint Outcome for Further Exploration
- "TOTEM-in-a-box": A hardware & software bundle of home management and monitoring tools, both in-house and customized 3rd party ones, in a commodity low-cost computing board
List of Publicly Available Output

Open-Source Contributions
1. https://github.com/ntop/ntopng/
2. https://github.com/ntop/nProbe
3. https://github.com/ntop/nDPI
5. https://github.com/feron-tech/ngitotem.sensor-alarming
6. https://github.com/feron-tech/ngitotem-home-assistant

Videos of Presentations, Webinars, Tutorials
1. ntop mini conference 2020: https://youtu.be/TwdRbboERBO
2. FOSDEM 2021: https://youtu.be/CV6-HAQPy3M
3. ntop Webinar on pfSense/OPNsense 2021 https://youtu.be/_FCx6Y1ZD1o
PRIMA - PRPrivacy preserving IoT data analysis using federated MAchine learning protocol

Cognitive Innovations Private Company
Kifisias Av. 125-127, 11524
Athens, Greece
http://cogninn.com/
Challenge addressed

1. **Future Internet** will be able to integrate the ML knowledge from the surrounding environment.

2. **Distributed ML** will be able to train models both to the IoT devices and edge servers.

3. **PRIMA protocol** will specify all the required distributed rules among the IoT and edge computing infrastructures to train ML in a distributed fashion as provided by federated learning.
Results expected

- A federated learning specification for IoT devices, where the edge intelligence with the IoT are integrated in an efficient manner.
- Constrained and non-constrained devices will be considered for the protocol specification and implementation.
- PRIMA will target advanced IoT use cases such as Augmented Reality (AR) services in future smart cities, where the users will be able to integrate knowledge from the surrounding city environment.
- PRIMA will be tested to a Fed4Fire testbed and evaluated in terms of federated training and communication performance.
PY & PY 2.0
Protect Yourself

Personal data protection project carried by french startup PANGA
Objectives & Contributions

How can we protect the average user’s privacy and personal data stemming from their connected devices, with minimal changes in their habits, while respecting their data sovereignty?

PyGuard filters unwanted connections and personal data stemming from connected devices while raising user awareness about privacy.

Main objective:
Industrializing our prototype into a marketable MVP

- Industrializing our PoC & provisioning
- Developing the production chain and distribution channels
- Finding our business model & work on commercialization
- Building trust through standards compliance, tests and certifications
Results

- Evolution in knowledge of ways to protect individuals’ personal data
- Algorithms / IP:
  - Cyberscore
  - Website categorization
  - Personal data categorization
- 2 B2B2C scenarios / business models:
  - Insurers / ISP distribution (first sales)
  - Integration to our Smart Building gateways
- An MVP with its production chain:
  - Edge-computing hardware platform analyzing all network packets in real-time
  - Packaging, inserts, user manual, accessories
  - Software (Web dashboard, web plugin, mobile app (alpha stage))

From concept to prototype to MVP

Web application
PyGuard’s UI demonstration

Plugin

Mobile app (alpha stage)
Next steps

- Focus on first sales
- Fundraising Q1 2022
- External certification with trusted third-parties
- Mobile App launch
- Expand functionalities (SSO, parental control...) and IoT support (cameras, sensors, smart TV, health related connected devices)
- Integration / support with decentralized internet projects by making PyGuard a node (SOLID, DAppNode...)
### Round table discussion and exchange - Q&A

<table>
<thead>
<tr>
<th>Experience and learning from the project – how can the NGI initiative further improve support third-party projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s next: the route to market – or scale-up - what can NGI do to help?</td>
</tr>
<tr>
<td>Future NGI : what should we be focusing on in terms of privacy and trust in future initiatives for a human-centric internet</td>
</tr>
</tbody>
</table>
The NGI_TRUST project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618

More information/contact us

- Project coordinator: Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email: NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki: https://wiki.geant.org/display/NGITrust
- NGI.eu website: https://www.ngi.eu/about/