Grant Agreement N°: 101020259

Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D6.7: Outreach activities report M24

Revision: v.1.0

Work package	WP 6
Task	Task 6.1, 6.4
Due date	30/04/2023
Submission date	05/05/2023
Deliverable lead	Martel
Version	1.0

Abstract

This document offers an overview of the activities carried in T6.1 and T6.4 of Work Package 6 - Dissemination, Communication and Exploitation pursued for awareness creation and engagement of top-notch players. These activities are guided by the Dissemination and Communication Strategy and Plan (D6.1). The activities described in this deliverable focus on communication and dissemination activities carried out between M13 and M24 of the project, including news, content for the website, events and social media animation.

Keywords:

IoT, Dissemination, Communication, Marketing, Online Communication, Communications Task Force, Events, Content, Visual Identity, Web Portal, Social Media, Promotional Material, Newsletter, Presentations, Conferences, Workshops.

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	24/04/2023	ToC and first draft of the deliverable	Martel (Valentin Popescu)
V0.2	27/04/2023	Internal review	E-lex (Carmela Occhipinti)
V0.3	28/04/2023	Final edit	Martel (Valentin Popescu)
V0.4	02/05/2023	SAB review	Cristian Patachia
V1.0	04/05/2023	Final version	Martel (Valentin Popescu), IPN (Sérgio Figueiredo)

Disclaimer

Project co-funded by the European Commission under SU-DS02-2020		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ARCADIAN-IoT project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

This report presents the communication and dissemination activities of the ARCADIAN-IoT project during the reporting period (M13-M24).

Key activities and events include participation in IoT Week 2022, Project to Policy Seminar, TADSummit 2022, Fraunhofer Portugal's "Thursday's with Science," MEDICA Trade Fair 2022, and Lugano Tech Talks November 2022 Meetup. These events allowed the consortium partners to present the project's implementation status, discuss relevant topics, and showcase the ARCADIAN-IoT framework.

The partners have engaged in various communication and dissemination activities, such as participating in local and international events, publishing scientific papers, sharing news through institutional channels, and promoting the project on social media platforms.

To create synergies with other initiatives, the project has reached out to other EC-funded projects and organizations, leading to the establishment of the Communication Task Force. A joint workshop, "EU-made cybersecurity for safe, resilient and trustworthy applications and services," was organized with the participation of multiple projects. The workshop aimed to address the cybersecurity needs of the EU industry and public and provided valuable knowledge and insights to the attendees. Future plans include more joint workshops, publications, and participation in events.

Overall, the ARCADIAN-IoT project engaged in communication and dissemination efforts, creating valuable connections and collaborations with other projects and initiatives in the field of intelligent security and privacy management for IoT systems.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

During the period from M13 to M24 of the project, WP6 was dedicated to implementing an extensive range of tools and initiatives to initially disseminate information and engage with relevant stakeholders. WP6 worked in close collaboration with other WPs in the ARCADIAN-IoT project, the European Commission, and other pertinent H2020 projects. The newly established Communication Task Force (CTF) facilitated coordination with these entities, which consisted of dissemination and communication partners from H2020 projects that were funded under the same call.

1.1 Purpose of the document

The Dissemination and Communication Report for the reporting period (May 2022 - April 2023) presents an overview of the communication and dissemination activities of the ARCADIAN-IoT project.

This deliverable expands upon the strategic framework established in Deliverable 6.1, "Dissemination and Communication Strategy and Plan" and aims to achieve the following objectives:

- Describe the implemented communication and engagement activities, as well as the monitoring and evaluation processes.
- Illustrate how the methods, tools, and promotional materials have been utilized in the project's dissemination and communication efforts
- Provide a comprehensive summary of the communication activities. The report focuses on the key actions carried out during the **second communication phase of the project: Initial dissemination & engagement (M13 – M24)**. This phase aimed to proactively engage target stakeholders, generate interest in ARCADIAN-IoT activities and outcomes, and establish a robust foundation for the planned dissemination activities.

1.2 Structure of the document

The sections of the deliverable at hand are organised in the following manner:

- Section 1 gives the Introduction and overview, with a summary of the main objectives for communication and dissemination for this phase.
- Section 2 presents the various types of dissemination activities and tools used in order to support the project’s dissemination and communication activities.
- Section 3 describes ARCADIAN-IoT’s synergies and interaction with external initiatives.
- Section 4 describes the plan for the third year of the project
- Section 5 depicts the metrics for the evaluation of the dissemination and communication activities.
- Section 6 concludes the document and presents the most relevant next steps.

2 DISSEMINATION AND COMMUNICATION FOR ARCADIAN-IOT

2.1 Dissemination and communication objectives

The main aim of ARCADIAN-IoT is to foster a stronger, more innovative, and more resilient European industry by providing a reliable and advanced framework for trust, security, and privacy management in IoT systems. WP6 manages dissemination and communication activities in close collaboration with all ARCADIAN-IoT tasks and work packages as appropriate, which includes refining branding and visual identity, animation of the web portal, social media channels, promotional materials, and main communication tools.

WP6 leads a set of dedicated dissemination and communication actions with the following objectives:

- Ensure broad visibility and awareness of ARCADIAN-IoT, promoting project knowledge and establishing a recognizable identity to support promotional and marketing efforts.
- Engage and stimulate a critical mass of relevant stakeholders to effectively showcase project results, leading to validation and further adoption of the developed technologies.
- Contribute significantly to relevant scientific domains and standardization bodies as appropriate and relevant to planned exploitation plans and project outcomes.
- Establish liaisons and ensure close collaboration with relevant initiatives in the industry and R&I domains, particularly those launched as a result of the Horizon 2020 LEIT ICT, other similar initiatives, and projects being funded in SU-DS02-2020.

2.2 ARCADIAN-IoT target stakeholders

Throughout the activities performed in the reporting period, ARCADIAN-IoT tried to reach a large community of target stakeholders such as

- **Cybersecurity industry group**
- **Related domains' industry group**
- **Research communities' group**
- **H2020 projects group**
- **Products and service providers group**
- **Standardisation bodies initiatives group**
- **Policy makers**
- **Citizens and civil society**

The extended list as well as the measures to reach these stakeholders are detailed in D6.1.

2.3 Communication phases

In the reporting period, dissemination and communication activities were carried out related to the **second phase of communication and dissemination** activities, as defined in D6.1: **Dissemination and Engagement (M13 - M24),** according to Figure 1.

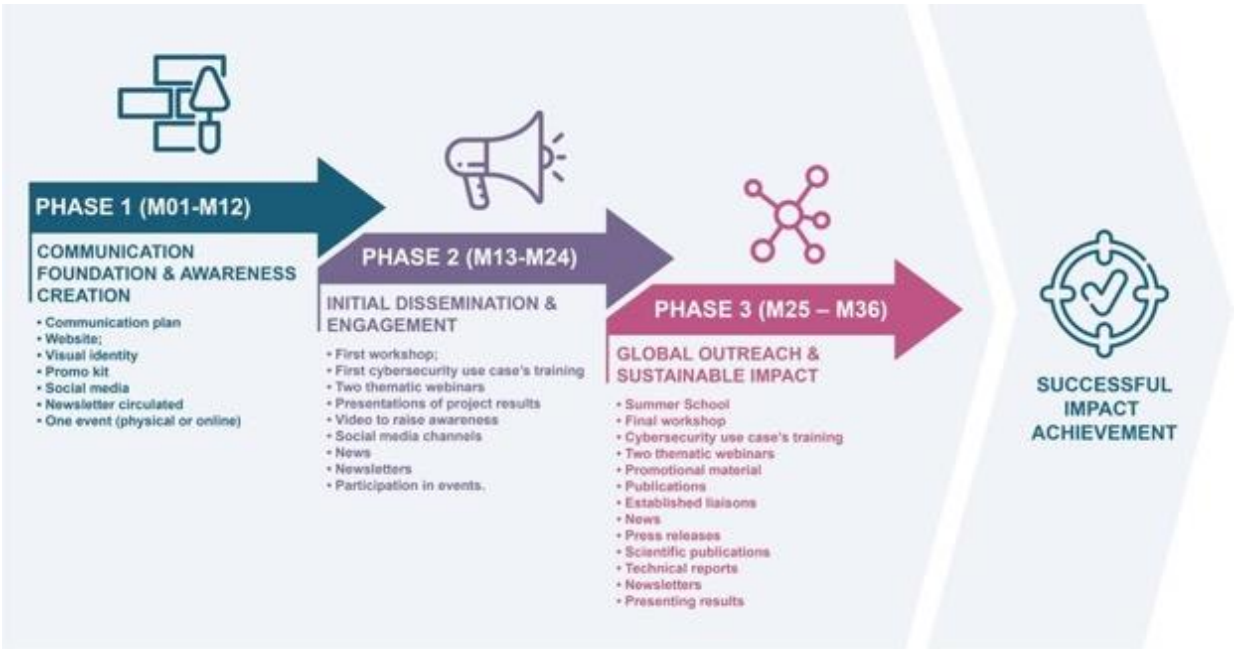


Figure 1: ARCADIAN-IoT communication phases

In this second phase, the primary focus was on engaging target stakeholders and present the result of the project. dissemination activities. The following communication strategy and activities were carried out:

- Organizing the first workshop: ARCADIAN-IoT organized an event co-located with a relevant conference (i.e. IoT Week), to maximize outreach and collaboration opportunities.
- Presenting project results: ARCADIAN-IoT showcased the initial outcomes and milestones at various events and conferences.
- Producing videos to raise awareness: These promotional video were created to highlight the project's objectives, achievements, and impact.
- Animating social media channels: The project team actively engaged with stakeholders and the public through various social media platforms.
- Publishing news items on the project website and media: Regular updates were posted to keep stakeholders informed about the project's progress.
- Distributing newsletters: Periodic newsletters were sent out to stakeholders to maintain interest and update them on project milestones.
- Participating in events: Team members attended events to network, share knowledge, and promote the project.

3 DISSEMINATION AND COMMUNICATION IN ACTION

3.1 Active Communication and Dissemination of Key Content

In order to engage with its target audience and stakeholders, ARCADIAN-IoT employs a diverse range of communication and dissemination methods. The ARCADIAN-IoT website serves as the primary information hub for the community, while social media channels, newsletters, news articles, blogs, and curated stories are also utilized. Content is strategically shared through specialized channels to maximize reach.

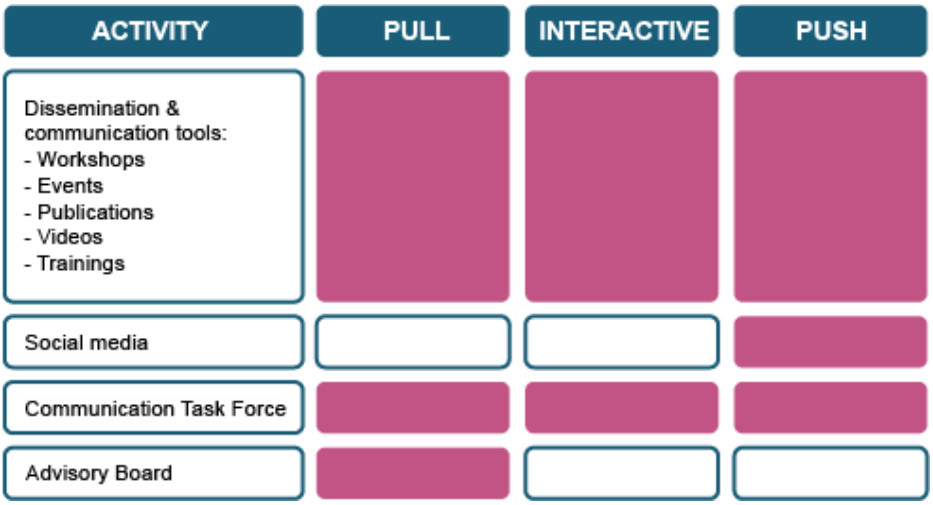


Figure 2: The communication activities and their relations to the communication and dissemination mix

3.2 Web Portal

The fully functional ARCADIAN-IoT website (https://www.arcadian-iot.eu) represents the entry point that enables the project to reach to all stakeholders involved. All relevant information about projects, outcomes, events, milestones, developments, etc., are exposed and accessible via the dedicated areas the portal has been structured around.

As described in D6.1, the website has a clear and clean communication interface that is easily navigable, containing all relevant project related public information. The website also offers direct access to the most relevant documents produced by the consortium.

Since its launch, the website was updated, and the content improved with **new pages added:**

- **Domain 1 - Emergency and Vigilance:** https://www.arcadian-iot.eu/emergency-and-vigilance/
- **Domain 2 - Industrial Control Systems:** https://www.arcadian-iot.eu/industrial-control-systems/
- **Domain 3 - Medical IoT:** https://www.arcadian-iot.eu/medical-iot/
- **Blog section**: https://www.arcadian-iot.eu/blog/
- **Synergies with other projects/initiatives:** https://www.arcadian-iot.eu/synergies/ (more details in section 5 of this deliverable)
- **Summer School:** a dedicated page to offer the information about the Summer School RISE plans to organise in September 2023 https://www.arcadian-iot.eu/summerschool/
- **Videos:** this page contains all the videos related to the activity of ARCADIAN-IoT project (besides the dedicated Youtube channel): https://www.arcadian-iot.eu/videos/
- **Publications:** this page gives the opportunity to view all the scientific publications from ARCADIAN-IoT: https://www.arcadian-iot.eu/publications/

During the reporting period, several news items were published on the website:

- News item related to the participation of the project at IoT Week 2022: https://www.arcadian-iot.eu/arcadian-iot-at-iot-week-2022/
- ARCADIAN-IoT participates in the discussion on the new EU policy on cybersecurity: https://www.arcadian-iot.eu/arcadian-eu-cybersecurity/
- Digital Europe Programme: Call for large-scale pilots for cloud-to-edge based service solutions: https://www.arcadian-iot.eu/digital-europe-programme-call-for-large-scale-pilots-for-cloud-to-edge-based-service-solutions/
- ARCADIAN-IoT 4th consortium meeting: https://www.arcadian-iot.eu/arcadian-iot-4th-consortium-meeting/
- Harnessing cyber threat intelligence for a secure IoT ecosystem: https://www.arcadian-iot.eu/harnessing-cyber-threat-intelligence-for-a-secure-iot-ecosystem/
- Enhancing data security with Hardened Encryption: https://www.arcadian-iot.eu/enhancing-data-security-with-hardened-encryption/
- Report on the Joint Workshop on EU-made cybersecurity: https://www.arcadian-iot.eu/report-on-the-joint-workshop-on-eu-made-cybersecurity/
- Exploring the self-recovery component of the ARCADIAN-IoT framework: backup, security, and privacy: https://www.arcadian-iot.eu/exploring-the-self-recovery-component-of-the-arcadian-iot-framework-backup-security-and-privacy/
- Newly published paper presents breakthrough in communication-efficient and robust peer-to-peer Federated Learning: https://www.arcadian-iot.eu/newly-published-paper-presents-breakthrough-in-communication-efficient-and-robust-peer-to-peer-federated-learning/
- IoT Security with Permissioned Blockchain: https://www.arcadian-iot.eu/iot-security-with-permissioned-blockchain/

ARCADIAN-IoT website analytics

In the reporting period (May 2022 - April 2023), the ARCADIAN-IoT website had 334 unique visitors and 1,434 page views.

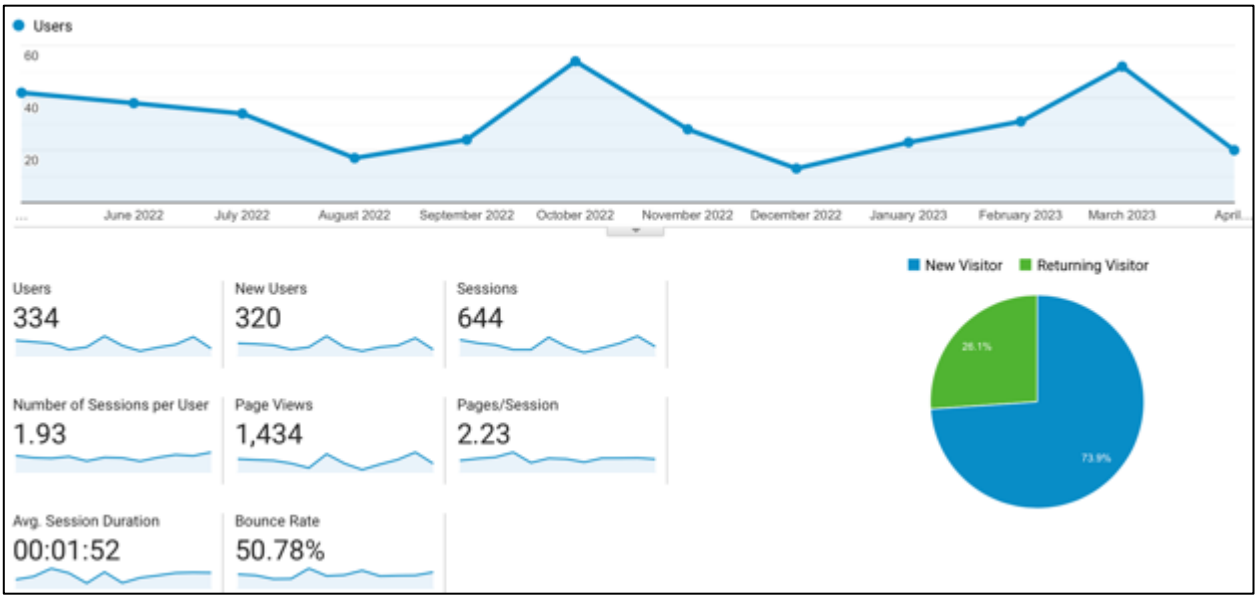


Figure 3: ARCADIAN-IoT website audience

The most visited pages of the website are:

	Page	Page Views	Unique Page Views
		1,439 % of Total: 100.00% (1,439)	1,243 % of Total: 100.00% (1,243)
1.	/	398 (27.66%)	323 (25.99%)
2.	/the-project/	139 (9.66%)	126 (10.14%)
3.	/events/	78 (5.42%)	63 (5.07%)
4.	/consortium/	72 (5.00%)	68 (5.47%)
5.	/deliverables/	59 (4.10%)	55 (4.42%)
6.	/publications/	53 (3.68%)	49 (3.94%)
7.	/news/	51 (3.54%)	38 (3.06%)
8.	/blog/	46 (3.20%)	39 (3.14%)
9.	/industrial-control-systems/	45 (3.13%)	40 (3.22%)
10.	/vision-strategy/	41 (2.85%)	37 (2.98%)

Figure 4: Most visited pages on the website

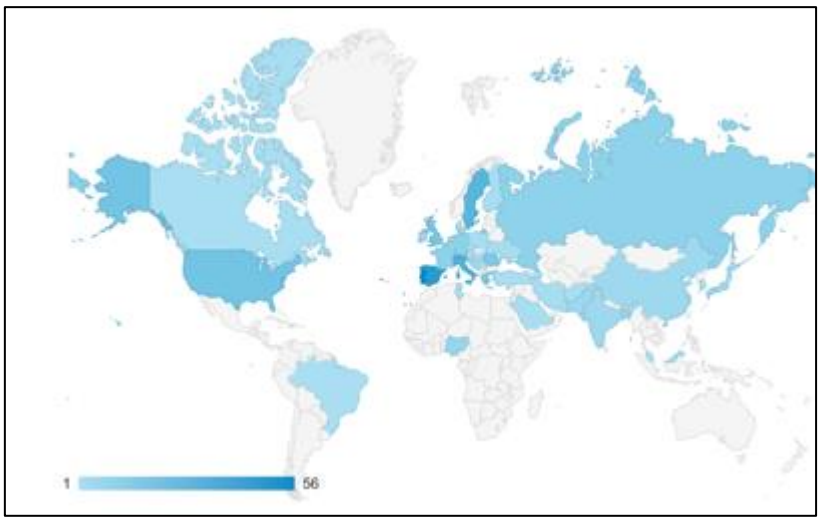


Figure 5: Geographical distribution of the visitors of the ARCADIAN-IoT website

The most visits are from Portugal, Spain, Sweden, Greece, Italy, Switzerland, Romania, United Kingdom. This reflects, in part, the composition of the consortium and the communication activities undertaken by partners.

Based on the provided analytics data for the ARCADIAN-IoT website for the period of May 2022 to April 2023, we have the following traffic sources:

- **Direct: 253 (64.71%):** Direct traffic occurs when users type the website's URL directly into their browser's address bar, access it through browser bookmarks, or click on a link in an email or a document (e.g., a PDF). This traffic source often reflects users who are already familiar with the project or have visited the website before.
- **Organic Search: 82 (20.97%):** Organic search traffic refers to users who found website through a search engine (e.g., Google, Bing, Yahoo) by entering relevant keywords.
- **Social: 36 (9.21%):** Social traffic comes from users who find and visit the website through social media platforms (e.g., Facebook, Twitter, LinkedIn, Instagram).

- **Referral: 20 (5.12%):** Referral traffic is generated when users visited the website by clicking on a link from another website. This can include links in blog posts, news articles, or online directories.

Measures to improve website traffic:

1. **Enhance Organic Search Traffic:** Organic search accounts for 20.97% of the total traffic, indicating that there is significant room for improvement. To boost organic search traffic, we will focus on:

- Conducting thorough keyword research and incorporating relevant keywords into your website's content.
- Improving on-page SEO by optimizing metadata (title tags, meta descriptions, header tags, etc.) and creating high-quality, informative content that engages visitors.
- Utilizing internal and external links to improve site navigation and build a strong backlink profile.
- Regularly updating and maintaining your website to ensure optimal performance and user experience.

2. **Strengthen Social Media Presence:** Social media contributes 9.21% of the total traffic, indicating potential growth in this area. To increase social traffic, we will consider:

- Developing a consistent and engaging social media strategy that includes regular content updates, audience engagement, and promotion of the website.
- Leveraging various social media platforms such as Twitter and LinkedIn to reach a wider audience.
- Creating shareable content (e.g., blog posts, infographics, videos) to encourage our audience to share your content on their social media profiles.

3. Boost Referral Traffic: With referrals accounting for only 5.12% of the total traffic, there's room to increase this metric. To enhance referral traffic, we will consider:

- Establishing partnerships with relevant industry websites, blogs, or online communities.
- Engaging in guest posting on authoritative websites in your niche.
- Offering valuable resources, such as whitepapers or webinars, that can be shared by other websites.

4. **Direct Traffic:** Direct traffic constitutes the majority of the website's traffic (64.71%). It is important to understand the source of this traffic and identify potential growth opportunities. We will consider:

- Ensuring that your website is easily accessible through clear navigation, fast loading times, and mobile-friendly design.
- Encouraging repeat visitors by offering valuable content.

By focusing on these recommendations, you can work towards a more balanced traffic acquisition strategy and increase the overall performance of your ARCADIAN-IoT website.

3.3 Social Media

Twitter, LinkedIn and Youtube social media channels were established as communication tools in order to promote activities and outputs of the project on a regular basis, while also encouraging a wider discussion on the topics related to the project's activities. So far, ARCADIAN-IoT created an active presence on the most popular social media channels, such as Twitter and LinkedIn, which are linked to the project's website. In addition, the YouTube channel was opened, and it features videos from the events where ARCADIAN was presented, interviews with the consortium partners and animated video showcasing the use cases.

3.3.1 Twitter

ARCADIAN-IoT has established its Twitter account @ArcadianIoT (https://twitter.com/ArcadianIoT) in April 2021 and since then has used the social medium to inform and engage the relevant audience and create awareness about the project.

The Twitter account is used for promoting and disseminating the development of ARCADIAN-IoT, including news, events, outcomes, etc. Moreover, re-tweets are made of relevant and interesting content from disparate sources.

By the time of writing this report, ARCADIAN-IoT has 291 followers and has posted, on average, one tweet a week, beside the regular retweets from other followed accounts. The number of impressions in the reporting period exceeds 11,000 and the number of times users visited the ARCADIAN-IoT profile page exceeds 8,700.

Figure 6: Examples of top tweets from the ARCADIAN-IoT account

Measure to boost the Twitter channel:

1. Increase posting frequency: We will aim for at least a tweet per day to increase visibility and engagement and share a mix of informative content, news, updates, and promotional materials to maintain variety and interest.
2. Use relevant hashtags: We will continue to Incorporate popular and relevant hashtags in your tweets to increase discoverability and reach a larger audience interested in IoT topics.

3. Share visual content: We will use images, infographics, and videos to make the tweets more engaging and shareable.
4. Schedule tweets for optimal times: We will analyze our audience's activity patterns and schedule tweets for when your followers are most active. This can lead to increased engagement and impressions.
5. Run targeted ad campaigns: We will consider using Twitter's advertising options to promote our content and reach a broader audience.

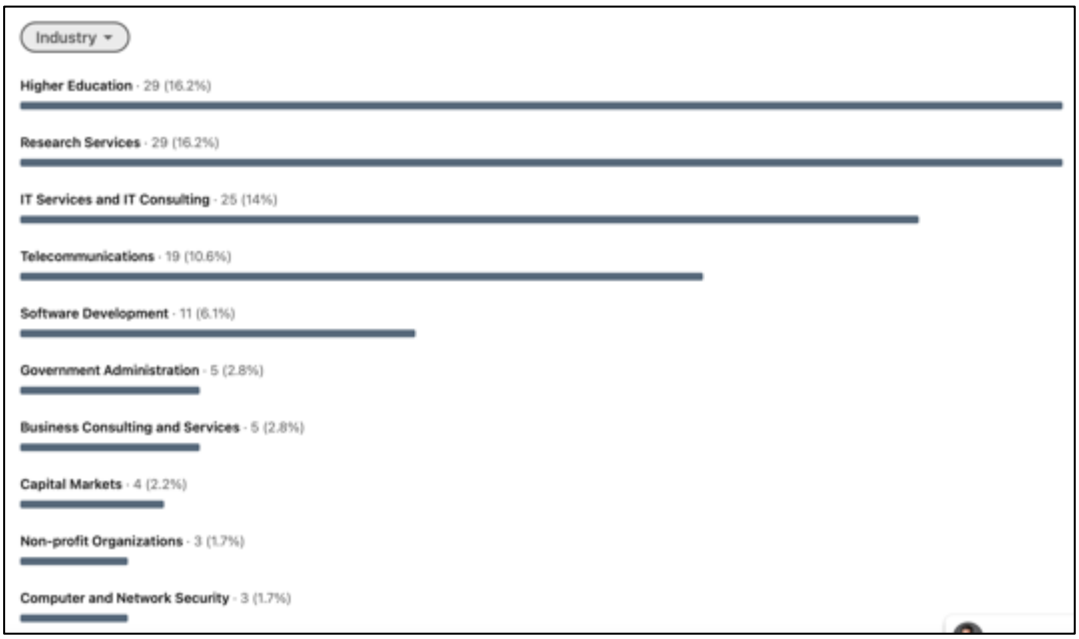
By implementing these recommendations, we can boost the performance of your ARCADIAN-IoT Twitter channel, attract more followers, and increase overall engagement.

3.3.2 LinkedIn

LinkedIn is a business-oriented professional networking tool that is used by many as a source of information and inspiration, therefore, it serves as a solid tool to amplify the news shared on the website. It is an important platform for discussions relevant to ARCADIAN-IoT, among experts in the area and various stakeholders in general.

The ARCADIAN-IoT LinkedIn page (https://www.linkedin.com/company/arcadian-iot/) allows reaching a professional audience with more elaborated news and/or specific events highlights. The page was established in April 2021, ahead of the project's start, and has at the time of writing this report (April 2022) 178 followers.

Below, a few key figures regarding the LinkedIn account:



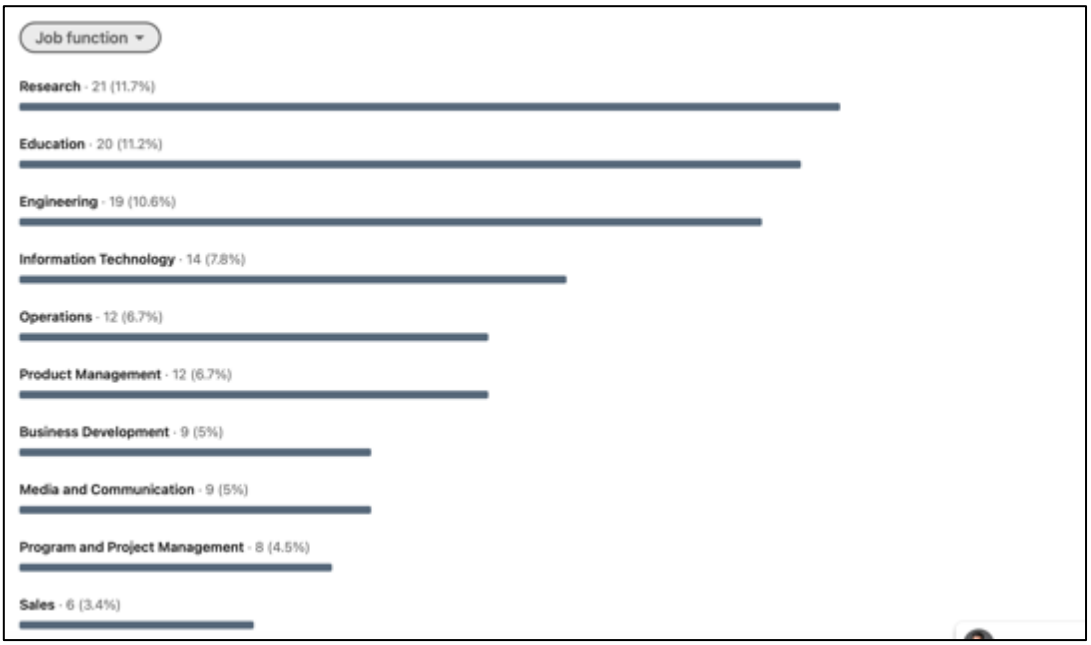


Figure 7: Industries and functions of the visitors of ARCADIAN-IoT Linkedin account

During the reporting period, the Linkedin page had over 16,200 impressions.

ARCADIAN-IoT also contributes to the NGIoT LinkedIn Group "Next Generation Internet of Things" (https://www.linkedin.com/groups/8774065/) that has more than 280 members (April 2023) and allows the publication (and moderation) of contents of multiple players. It is very active and allows multiple voices and contributions. Group members may publish the news directly in the LinkedIn group, which aims to attract professionals and industry players and invites group members to publish their own updates and open interesting subjects, relevant for the whole community.

Based on the analytics provided by LinkedIn, the most engaging content are the blog post. As such, we will continue to create this kind of content and promote it on this social network.

Harnessing Cyber Threat Intelligence for a secure IoT ecosystem - ARCADIAN-IoT Posted by Valentin Popescu 2/8/2023 Boost	Article	All followers	353

Enhancing data security with Hardened Encryption - ARCADIAN-IoT Posted by Valentin Popescu 2/19/2023 Boost	Article	All followers	291

Figure 8: Examples of impressions for the blog post shared on LinkedIn page

3.4 YouTube

The YouTube channel was established in February 2022: https://www.youtube.com/channel/UCJRCUJktsmglj8ngQmPCavA. The Youtube channel has 34 subscribers. In the reporting period, the videos had 521 views in total and generated 9,600 impressions.

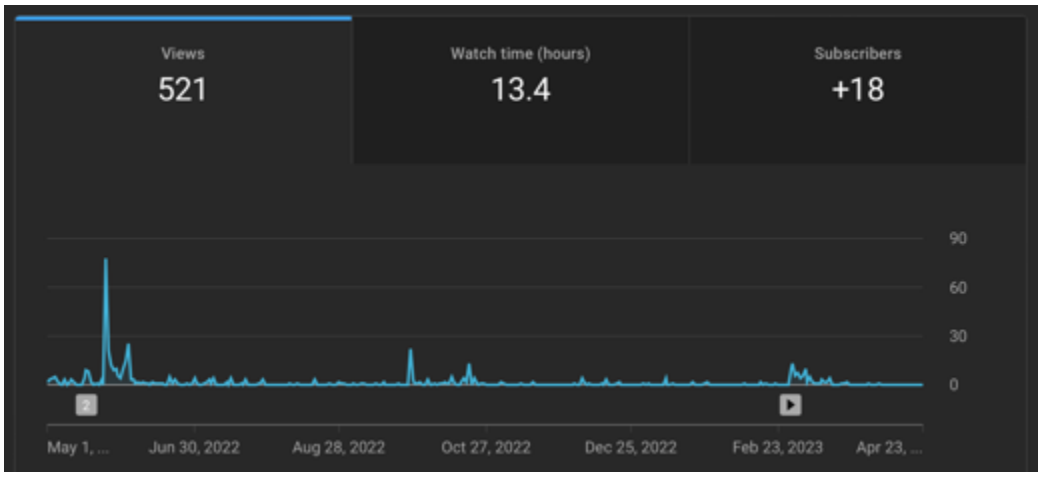


Figure 9: Analytics for the ARCADIAN-IoT Youtube channel

The channel features the presentations ARCADIAN-IoT partners had at different events, such as Digital Around the World 2021 (https://www.youtube.com/watch?v=miq7kUYVVTk&t=2002s) but also the explainer videos related to the use cases, recordings of events and interviews with ARCADIAN-IoT partners:

- Medical IoT explainer video : https://www.youtube.com/watch?v=eD6G01ITuus
- Emergency Surveillance explainer video: https://www.youtube.com/watch?v=kgm7wIqyoag
- Recording of the Joint Workshop: EU-made cybersecurity for safe, resilient and trustworthy applications and services: https://youtu.be/yIcpyISGUAI
- ARCADIAN-IoT by University of the West of Scotland, interview with Jose Alcaraz-Calero: https://youtu.be/fOIHdId7aKo
- ARCADIAN-IoT by TRUPHONE, interview with Joao Casal: https://youtu.be/9lru8N-OTgw
- ARCADIAN-IoT by Sérgio Figueiredo, project coordinator, Instituto Pedro Nunes: https://youtu.be/P6aBcvX3EJM

3.5 Publications

In this Outreach Report, we will highlight the significant scientific publications produced by the ARCADIAN-IoT team, showcasing the cutting-edge research and innovations that are driving the development of secure, trustworthy, and privacy-centric IoT systems for various industries and

applications.

Scientific publications in journals:

1. **Illumination-aware image fusion for around-the-clock human detection in adverse environments from Unmanned Aerial Vehicle**. *Expert Systems with Applications*. Authors: Gelayol Golcarenarenji, Ignacio Martinez-Alpiste, Qi Wang, Jose Maria Alcaraz-Calero. https://doi.org/10.1016/j.eswa.2022.117413
2. **XDP-Based SmartNIC Hardware Performance Acceleration for Next-Generation Networks.** *Journal of Network and Systems Management volume 30, Article number: 75 (2022).* Authors: Pablo Salva-Garcia, Ruben Ricart-Sanchez, Enrique Chirivella-Perez, Qi Wang, Jose M. Alcaraz-Calero. https://doi.org/10.1007/s10922-022-09687-z
3. **Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks.** *Computer Networks, Volume 222, February 2023.* Authors: Pablo Benlloch-Caballero, Qi Wang, Jose M. Alcaraz Calero https://doi.org/10.1016/j.comnet.2022.109526
4. **Lightweight Certificate Revocation for Low-power IoT with End-to-end Security.** *Journal of Information Security and Applications (Elsevier).* Authors: Joel Höglund, Martin Furuhed, Shahid Raza. https://doi.org/10.1016/j.jisa.2023.103424
5. **SparSFA: Towards Robust and Communication-Efficient Peer-to-Peer Federated Learning.** *Elsevier Computer & Security*. Authors: Han Wang, Luis Muñoz-González, Muhammad Zaid Hameed, David Eklund, Shahid Raza. https://doi.org/10.1016/j.cose.2023.103182
6. **Non-invasive, plug-and-play pollution detector for vehicle on-board instantaneous CO2 emission monitoring.** *Internet of Things (Elsevier).* Authors: David Tena-Gago, Qi Wang, Jose M. Alcaraz-Calero. https://doi.org/10.1016/j.iot.2023.100755

Conference publications:

1. **Enabling Autonomous Trust, Security and Privacy Management for IoT.** *GIoT Summit, June 2022, Dublin.* Authors: Sérgio Figueiredo, Paulo Silva, Alfonso Iacovazzi, Vitalina Holubenko, João Casal, Jose M Alcaraz Calero, Qi Wang, Pedro Colarejo, Shahid Raza, Ross Little Armitt, and Giacomo Inches. https://www.arcadian-iot.eu/wp-content/uploads/sites/76/2022/12/GIoTS-WISP.pdf
2. **An Intelligent Mechanism for Monitoring and Detecting Intrusions in IoT Devices.** *IEEE Consumer Communications & Networking Conference, 8–11 January 2023, Las Vegas, NV, USA.* Authors: Vitalina Holubenko, Paulo Silva and Carlos Bento. **https://doi.org/10.1109/CCNC51644.2023.10060443**
3. **Ensemble of Random and Isolation Forests for Graph-Based Intrusion Detection in Containers.** *2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 30-37***.** Authors: Alfonso Iacovazzi, Shahid Raza. https://doi.org/10.1109/CSR54599.2022.9850307
4. **Towards Automated PKI Trust Transfer for IoT.** *2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA).* Authors: Joel Höglund, Martin Furuhed, Shahid Raza. https://doi.org/10.1109/PKIA56009.2022.9952223
5. **BLEND: Efficient and blended IoT data storage and communication with application layer security.** *2022 IEEE International Conference on Cyber Security and Resilience (CSR).* Authors: Joel Höglund, Shahid Raza. https://doi.org/10.1109/CSR54599.2022.9850290
6. **On the Resilience of Machine Learning-Based IDS for Automotive Networks.** *2023 IEEE Vehicular Networking Conference (VNC).* Authors: Ivo Zenden, Han Wang, Alfonso Iacovazzi, Arash Vahidi, Rolf Blom, Shahid Raza. doi: not yet available
7. **CHARRA-PM: An Attestation Approach Relying on the Passport Model**. *9th International Conference on Information Systems Security and Privacy - ICISSP, 349-356, 2023, Lisbon, Portugal.* Authors: António Marques, Bruno Sousa. https://doi.org/10.5220/0011623600003405

8. **An Intelligent Mechanism for Monitoring and Detecting Intrusions in IoT Devices.** *The 1st International Workshop on Smart Living and Communications for the Next Generations Networks - SLICO 2023*. Authors: Vitalina Holubenko and Paulo Silva. https://doi.org/10.1109/CCNC51644.2023.10060443
9. **Towards Cyber Threat Intelligence for the IoT.** *4th International Workshop on Security and Reliability of IoT Systems.* Authors: Alfonso Iacovazzi, Han Wang, İsmail Bütün, and Shahid Raza. doi: not yet available.
10. **Key Update for the IoT Security Standard OSCORE**. *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. Authors: Rikard Höglund, Marco Tiloca, Simon Bouget, Shahid Raza. doi: not yet avaiable

3.6 Promotional Material

With the resumption of events with physical presence, the consortium produced the first promotion materials to be used and distributed. For the IoT Week 2022, that took place in Dulin, ARCADIAN-IoT had a roll-up and flyers that were used for the promotion of the project among the participants.

Figure 10: ARCADIAN-IoT Rollup

Figure 11: ARCADIAN-IoT flyer – front and back

3.7 Newsletter

ARCADIAN-IoT produces e-newsletters on a quarterly basis, which provide regular updates on the project, future events, as well as news from project partners and stakeholders upon subscription and news availability. In the reporting period, three editions were developed and distributed. The ARCADIAN-IoT e-Newsletters are uploaded to the project website: https://www.arcadian-iot.eu/newsletter/

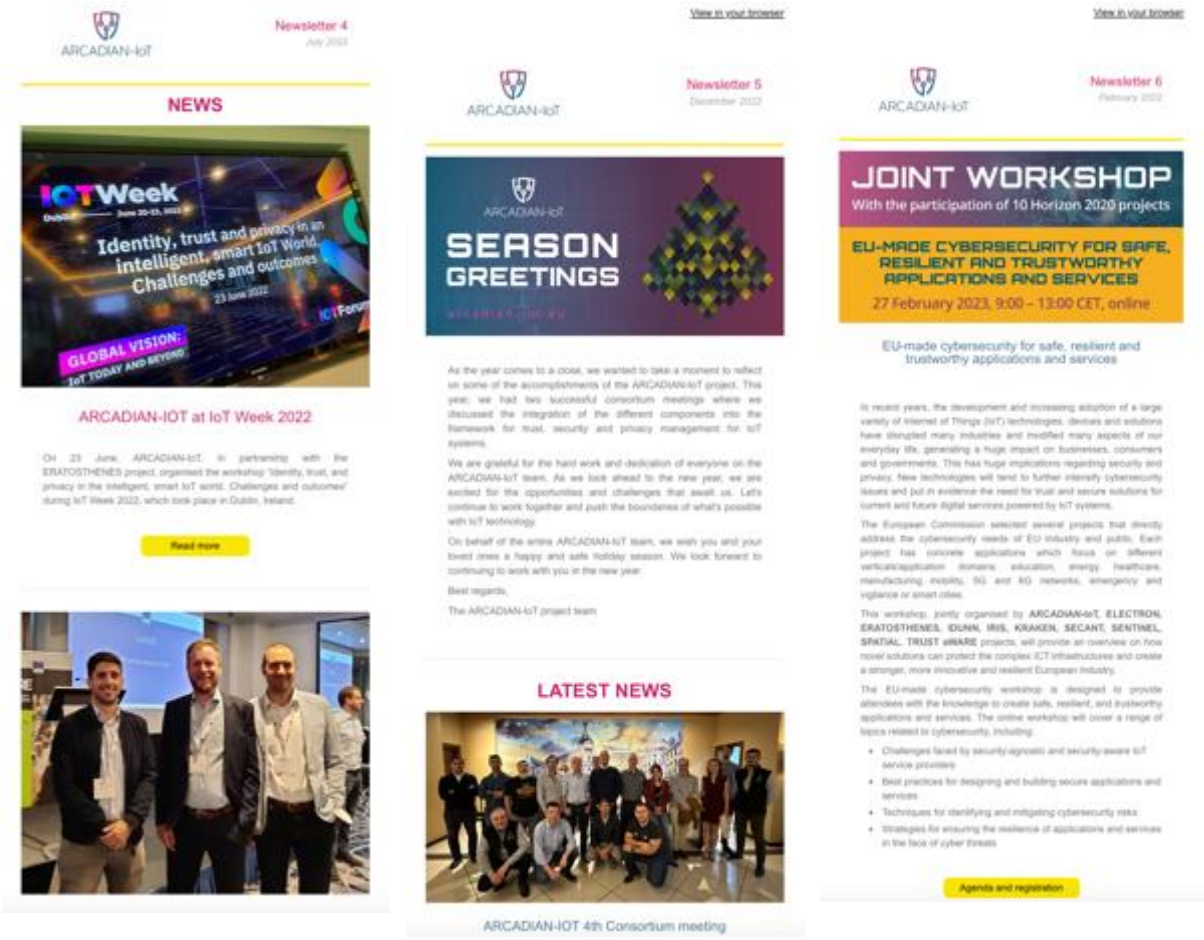


Figure 12: Snapshots of the ARCADIAN-IoT Newsletter

3.8 Media Relations and Engagement

In the reporting period, one press releases was distributed. The topic of the press release the joint workshop on EU-made cybersecurity for safe, resilient, and trustworthy applications and services that took place on 27 February 2023, from 9:00 – 13:00 CET.

The press release was distributed to the partners for further dissemination and to journalists Europe-wide.

EU-MADE CYBERSECURITY FOR SAFE, RESILIENT AND TRUSTWORTHY APPLICATIONS AND SERVICES

27 February 2023, 9:00 – 13:00 CET, online

PRESS RELEASE

Ten European projects join forces to enhance the cybersecurity of the European ICT infrastructures

2023-02-21

The development and increasing adoption of a variety of Internet of Things (IoT) technologies, devices, and solutions have disrupted many industries and modified many aspects of our everyday life, generating a huge impact on businesses, consumers, and governments. This has huge implications regarding security and privacy. New technologies tend to further intensify cybersecurity issues and put in evidence the need for trust and secure solutions for current and future digital services powered by IoT systems.

To address these issues, ten European projectsare hosting a joint workshop on EU-made cybersecurity for safe, resilient, and trustworthy applications and services on 27 February 2023, from 9:00 – 13:00 CET.

The workshop will cover a range of topics related to cybersecurity, including best practices for designing and building secure applications and services, techniques for identifying and mitigating cybersecurity risks, and strategies for ensuring the resilience of applications and services in the face of cyber threats.

The workshop, which is jointly organised by ARCADIAN-IoT, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SENTINEL, SPATIAL, TRUST aWARE projects, will provide an overview of how novel solutions can protect the complex ICT infrastructures and create a stronger, more innovative and resilient Europeanindustry.

Each project has concrete applications which focus on different verticals/application domains: education, energy, healthcare, manufacturing mobility, 5G and 6G networks, emergency and vigilance or smart cities. The workshop is designed to provide attendees with the knowledge to create safe, resilient, and trustworthy applications and services.

Figure 13: Snapshot of the ARCADIAN-IoT press release

3.9 Events

During the reporting period, ARCADIAN-IoT took part in several events:

1. **ARCADIAN-IoT workshop at IoT Week 2022 in Dublin**

On 23 June 2022, ARCADIAN-IoT organised a workshop co-located with IoT Week 2022. The title of the workshop was ***"Identity, trust, and privacy in the intelligent, smart IoT word. Challenges and outcomes".*** https://www.arcadian-iot.eu/arcadian-iot-at-iot-week-2022/

Description of the session:

The Internet and the recent connectivity leap are shaping every aspect of our lives, becoming more intelligent and connected. As IoT evolves, it changes how we interact with the internet and it with us. However, the enormous penetration of IoT into our day-to-day life has created a similarly large attack surface that includes high security and privacy risks. The IoT ecosystem now integrates a broad set of technologies leading profound transformation across a variety of sectors. IoT, alongside AI, Blockchain, is pushing the boundaries of existing identity, trust and security aspects and brings the need for a new vision and way forward that will shape Europe's digital

future while support recent efforts on the Cybersecurity Act, along with GDPR and the NIS directive, conforming the three main pillars of the EU perspective on cybersecurity. This workshop will showcase how Europe's Research and Innovation community is addressing the issues of identity, trust, security, and privacy for IoT devices and network systems. The way we address these aspects will impact Europe's collective resilience against cyber threats so that citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The workshop hosted around 12 EC, research projects.

Agenda of the workshop

Welcome and Workshop Opening:

- Konstantinos Loupos, INLECOM Innovation
- Sérgio Figueiredo, Instituto Pedro Nunes

Session 1: Trust and lifecycle management in the IoT World

- Chair: Sérgio Figueiredo, Instituto Pedro Nunes

Presentations:

- ARCADIAN-IoT - Autonomous Trust, Security and Privacy Management Framework for IoT, Sérgio Figueiredo Instituto Pedro Nunes, ARCADIAN-IoT project coordinator
- ERATOSTHENES - Secure lifecycle management of IoT Devices, Konstantinos LouposINLECOM InnovationERATOSTHENES project coordinator
- BIECO - Building trust in the design phase: Security validation and certification, Antonio SkarmetaUniversity of Murcia
- TRUST aWARE: a holistic Security & Privacy framework to enhance software trust and regulatory compliance, Javier Gutiérrez MeanaTRUST aWARE project coordinator
- Session Conclusions

Session 2: AI and ML technologies as enablers for a more secure IoT

- Chair: Konstantinos Loupos, INLECOM Innovation

Presentations:

- Keynote: Orchestration of intelligence. Empowering IoT beyond microservices, Edgar RamosEricsson
- SCOTT and InSecTT - Bringing Internet of Things and Artificial Intelligence together – But is it Trustworthy?, Michael KarnerVirtual Vehicle Research GmbH
- SPATIAL - Security and Privacy Accountable Technology Innovations, Algorithms, and machine Learning, Jose GonzálezAUSTRALO
- IDUNN: Securing the Computing Continuum, Cristobal Arellano IKERLANIDUNN project coordinator
- CONCORDIA - Threat Intelligence for 5G IoT, Thanh van DoTelenor – Oslo Metropolitan University
- Session Conclusions

Session 3: Trustworthiness and Tailored applications

- Chair: Antonio Skarmeta, University of Murcia,

Presentations:

- EU-IoT - EU-IoT trustworthiness and security aspects for sustainable IoT end-to-end systems, Rute C. SofiaFortiss GmbH

- CyberSec4Europe - Privacy-preserving solutions on verticals in the context of CyberSec4Europe, Antonio SkarmetaUniversity of Murcia
- SealedGRID - Scalable, highly trusted and interoperable Smart Grid Security Platform - Pilot Progress and Results, Christos XenakisUniversity of Piraeus
- SENTINEL - Affordable and tailor-made cybersecurity and data protection for SMEs and Miroenterprises, George Bravos ITML, SENTINEL project coordinator
- ELECTRON - Security and Privacy for Resilient and Self-healed Electrical Power Nanogrid, Panagiotis SarigiannidisUniversity of Western Macedonia
- SECANT - Security and privacy protection in IoMT ecosystems-The SECANT paradigm, Dimitris KavallierosInformation Technologies Institute
- IOTAC - The IoT security concept of IoTAC , Mert NakipInstitute of Theoretical and Applied Informatics, Polish Academy of Sciences
- Session Conclusions,

Key-takeaways and Session Closing

- Konstantinos Loupos, INLECOM Innovation
- Sérgio Figueiredo, Instituto Pedro Nunes

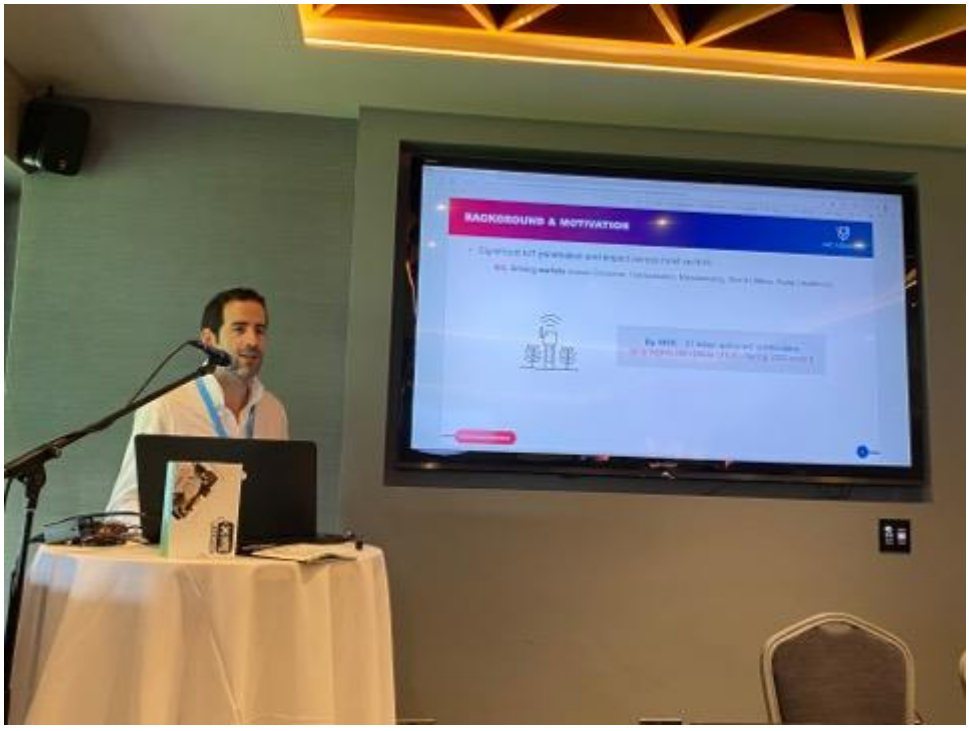


Figure 14: Sérgio Figueiredo, ARCADIAN-IoT project coordinator opens the IoT Week 2022 workshop

2. Project to Policy Seminar

From 30 June – 1 July, ARCADIAN-IoT attended the Project to Policy Seminar organised by the European Research Executive Agency (REA) and the Directorate-General for Migration and Home Affairs (DG HOME), together with Directorate-General for Communications Networks, Content and Technology (DGCNET), in Brussels.

The purpose of this in-person event was to gather EU Security Research and Innovation (R&I) Projects newly launched last year. Our consortium partners from Instituto Pedro Nunes and Martel Innovate attended the specific session on Digital security (DS). With the other projects funded under the same call attending the session, we had the

opportunity to provide feedback about the importance of the NIS2 Directive: the proposal for a Directive on measures for a high common level of cybersecurity across the Union.

During the seminar, ARCADIAN-IoT presented the project's implementation status and participated in the discussion on the Privacy and cybersecurity certification for software and devices, how to mitigate users' scepticism in AI, and how EU policies could help in increasing trust in AI and ML.

Figure 15: From left to right Paulo Silva (IPN), Juuso STENFORS (PO) and Giacomo Inches (Martel Innovate) at the Project to Policy Seminar

3. TADSummit 2022 (Telecom Application Developers Summit 2022)

TADSummit is the thought-leadership event in programmable communications for ten years. The audience includes CxOs from many of the programmable communication companies, open source leaders, and telecom operators. It's a strategic and technology event. Many of TADSummit's sponsors go on to be acquired.

ARCADIAN-IoT was represented by João Casal**, Head of R&D at Truphone in the session on** eSIM as Root of Trust for IoT security:

- ARCADIAN-IoT: Research with eSIM as key element of a novel IoT security framework
- SIM: Proven secure element
- Leveraging cellular network authentication for zero-touch authentication of IoT devices in third-party services
- The eSIM ecosystem role in new security mechanisms for IoT
- IoT connectivity and IoT security: 2 faces of the same coin

Figure 16: João Casal, Head of R&D at Truphone, presents at TADSummit 2022

4. Talk @ Fraunhofer Portugal's "Thursday's with Science"

On 30 June 2022, IPN was invited to do a presentation on its ongoing R&D activities at the Fraunhofer Portugal's "Thursday's with Science" online event. Sérgio Figueiredo presented both ARCADIAN-IoT and another national R&D project where IPN is involved.

5. MEDICA Trade Fair 2022

RGB Medical participated in MEDICA Trade Fair, the world's largest event for the medical sector, that took place in Dusseldorf, Germany in November 2022. This is the most important international Fair in the world, with over 175.000 visitors. RGB has presented the ARCADIAN project in HAll15 Booth K03 of Medica exhibition in Dusseldorf.

Figure 17: Ricardo Ruiz Fernandez, from RGB Medical at the MEDICA Trade Fair 2022

6. Lugano Tech Talks November 2022 Meetup

Giacomo Inches from MARTEL presented at the Lugano Tech Talks November 2022 Meetup the open source multi- platform tool for data owners to retain sovereignty over their data developed within the framework of the ARCADIAN-IoT project. The presentation introduced the technical details of this flexible Policy Enforcement solution, that makes it easier to reuse security policies for a given resource across different services, leveraging open source solutions such as Envoy, OPA, FIWARE and various reference standards e.g. W3C WAC, W3C ODRL, OAUTH2.

Figure 18: Giacomo Inches, from Martel, presenting ARCADIAN-IoT framework at Lugano Tech Talks

7. Energy Crisis and Cybersecurity International Event

On 5-7 December 2022, ARCADIAN-IoT partners, BOX2M and MARTEL, took part in the international event on Energy Crisis and Cybersecurity. Alexandru Gliga, BOX2M presented ARACADIAN-IoT in the 2nd Session of H2020/Horizon Projects: ARCADIAN-IoT: Autonomous trust, security, and privacy management framework for IoT, with a focus on the second use case of the project and Valentin Popescu, from MARTEL, presented the "Communication Task Force: tool for creating synergies to amplify outreach"

Figure 19: Visual of the Energy Crisis and Cybersecurity International Event

8. Privacy Simposium 2023

Shahid Raza, from RISE, presented ARCADIAN-IoT at the 2023 Privacy Symposium in Venice. The conference took place on April 17 to 21 2023 and focused on international cooperation and convergence in data protection regulations, emerging technologies and compliance with data protection, as well as Health and data protection compliance.

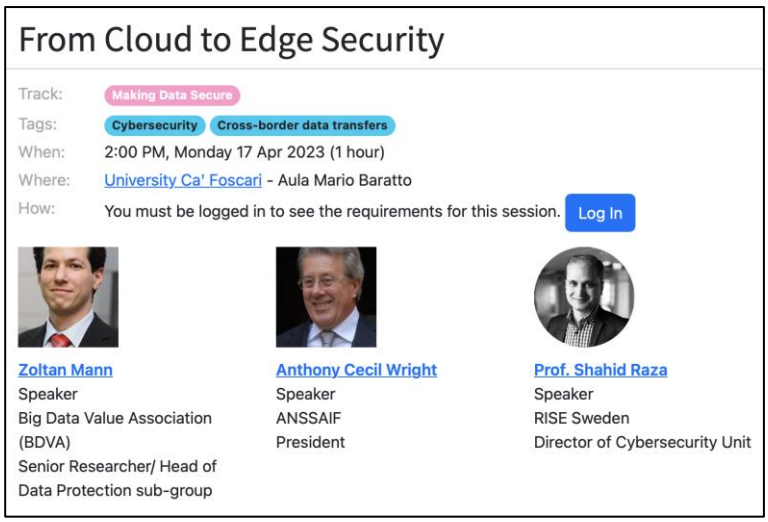


Figure 20: The session "From Cloud to Edge Security" at the 2023 Privacy Symposium

3.10 Vehicles for communication and dissemination

Below find an overview of the key structures providing access to the networks and supporting the dissemination of the ARCADIAN-IoT project.

3.10.1 ARCADIAN-IoT Advisory Boards

ARCADIAN-IoT Advisory Board (AB), Security Advisory Board (SAB) and the Ethics Board (EB) are composed of world- renowned experts that will providing effective means to optimise and fine-tune the project development.

The AB is constituted by six experts:

- Prof. Dr. Kai Rannenberg, Goethe University Frankfurt, Germany;
- Prof. Dr. Emil Lupu, Imperial College London, UK;
- Prof. Dr. Luis Gonçalves, is the head of CyberSecurity, IT Risk & Compliance at Banco de Portugal and Founder of Cloud Security Alliance Portugal;
- Prof. Dr. Elena Ferrari is a full professor of Computer Science at the University of Insubria, Italy;
- Cristian Patachia, Development & Innovation Manager for Orange Romania;
- Dr. Cade Wells, CENSIS, the Innovation Centre for sensing, imaging and Internet of Things (IoT), UK;

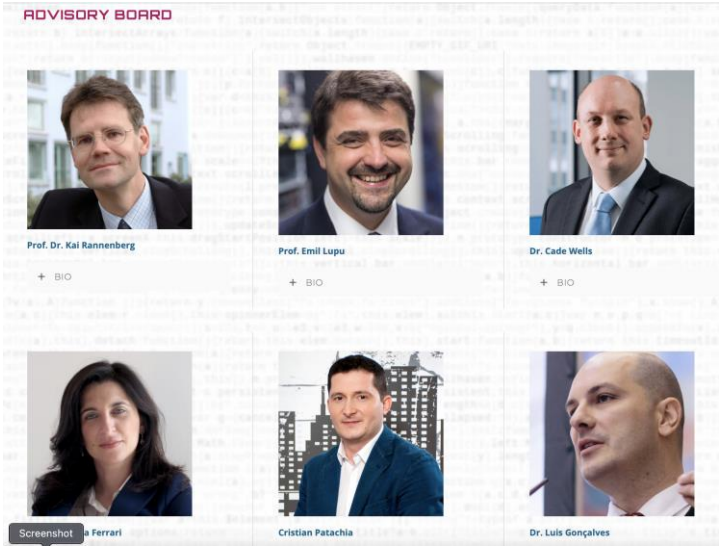
The SAB is constituted by three experts:

- Arthur van der Wees, managing director of ALBV, Netherlands
- Rafael Aranha, Head of Cybersecurity for REN, Portugal
- Cristian Patachia, Development & Innovation Manager for Orange Romania;

The EB is constituted by three experts:

- Arthur van der Wees - managing director of ALBV
- Giovanni Maria Riccio – E-lex
- José Ricardo Aguilar - IPN

They have been invited to send their brief biography and picture in order to present them on the ARCADIAN-IoT website: https://www.arcadian-iot.eu/advisory-board/



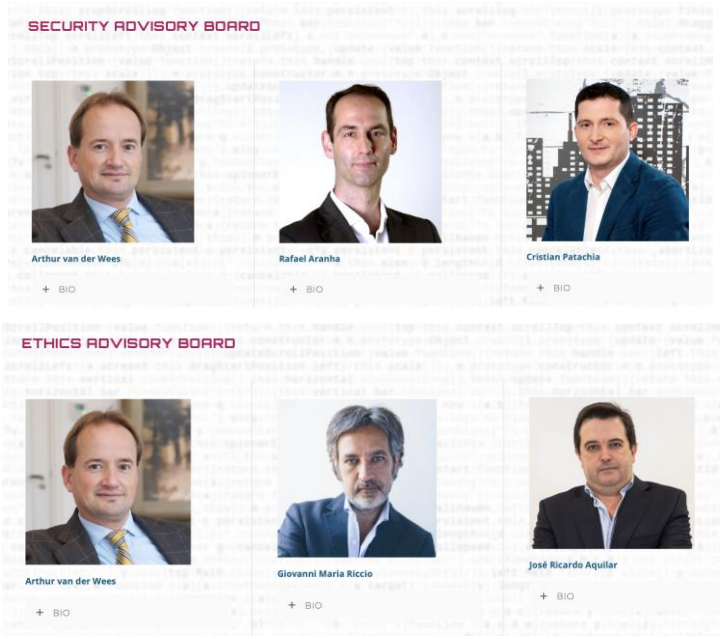


Figure 21: Advisory Board, Security Advisory Board and Ethics Board on the ARCADIAN-IoT website

As part of the Dissemination and communication strategy and plan, WP6 engaged the AB and SAB members by producing blog posts that feature on the website and were promoted on social media and in the on the topics related to the project.

The following blog posts from the AB and SAB member feature on the website:

- Trust, security and privacy management for IoT systems, Dr Cade Wells: https://www.arcadian-iot.eu/trust-security-and-privacy-management-for-iot-systems/
- Human-centric systems thinking & doing, in this digital age, Arthur van der Wees: https://www.arcadian-iot.eu/next-generation-iot-integrity-of-trust-human-centric-systems-thinking-doing-in-this-digital-age/

3.10.2 Communication Task Force

In line with T6.4 - Synergies and interaction with external initiatives, ARCADIAN-IoT started the preparations to establish a Communication Task Force (CTF) that gathers the projects funded under the same call - H2020 SU-DS02-2020.

This Communication Task Force (CTF) has been set up by WP6 to address specific plans and activities around communication and dissemination. The main objective of the CTF is to coordinate and create synergies to amplify outreach and increase the impact of activities.

It is formed by representatives of the various projects to align on why, what, where, when and how to brand, communicate and disseminate cybersecurity, privacy news/events. Currently it gathers representatives from:

- ELECTRON
- ERATOSTHENES
- IDUNN
- IRIS
- KRAKEN
- SECANT
- SENTINEL
- SPATIAL
- TRUST aWARE

ARCADIAN-IoT organises and supports CTF monthly conference calls, maintenance of common plans and actions, leading coordinated participation at selected events, ensuring proper synchronisation of presentations and promotion of exchange programmes, and other news and activities. In the reporting period, 12 meetings took place.

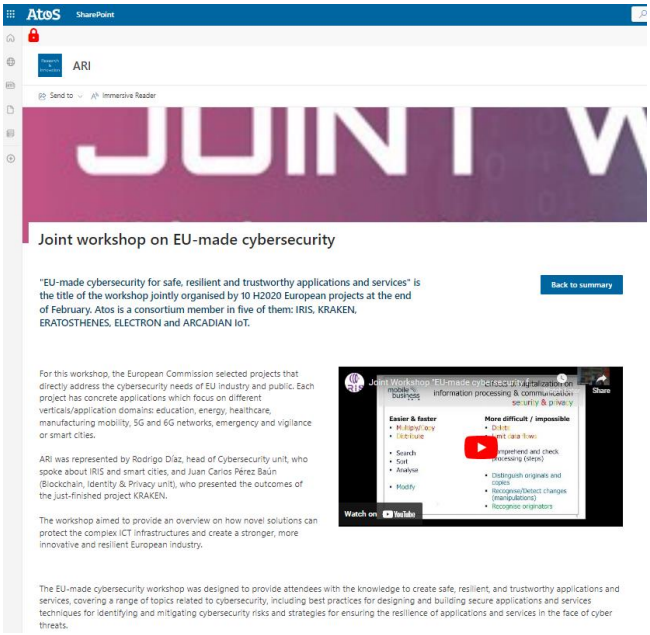
3.10.3 Partners' communication and dissemination activities

Table 1: Involvement of partners in C&D activities

Partner	Activities
IPN	• Communication of the project in 2 local newspapers and at least 3 tech news' web sites; • Communication of key project events (Kick-off and other consortium meetings) through Linkedin • Dissemination of the project's objectives and scope in Digital Around the World event, session "Intelligent trust and identity management towards a secure IoT world – research challenges and outcomes" • Participation in several events: IoT Week 2022 and Fraunhofer Portugal's "Thursday's with Science" Journals and conferences scientific publications: • Enabling Autonomous Trust, Security and Privacy Management for IoT. GIoT Summit, June 2022, Dublin. Authors: Sérgio Figueiredo, Paulo Silva, Alfonso Iacovazzi, Vitalina Holubenko, João Casal, Jose M Alcaraz Calero, Qi Wang, Pedro Colarejo, Shahid Raza, Ross Little Armitt, and Giacomo Inches. https://www.arcadian-iot.eu/wp-content/uploads/sites/76/2022/12/GIoTS-WISP.pdf • An Intelligent Mechanism for Monitoring and Detecting Intrusions in IoT Devices. IEEE Consumer Communications & Networking Conference, 8–11 January 2023, Las Vegas, NV, USA. Authors: Vitalina Holubenko, Paulo Silva and Carlos Bento. https://doi.org/10.1109/CCNC51644.2023.10060443 • An Intelligent Mechanism for Monitoring and Detecting Intrusions in IoT Devices. The 1st International Workshop on Smart Living and Communications for the Next Generations Networks - SLICO 2023. Authors: Vitalina Holubenko and Paulo Silva.
UC	Journals and conferences publications: CHARRA-PM: An Attestation Approach Relying on the Passport Model. 9th International Conference on Information Systems Security and Privacy - ICISSP, 349-356, 2023, Lisbon, Portugal. Authors: António Marques, Bruno Sousa. https://doi.org/10.5220/0011623600003405
TRU	• Internal communication of the project in several channels, from online general chats to dedicated meetings, including kick-off sessions and status meetings with different audiences (management, business, and engineering), and 2 mentions in the company's newsletter. ARCADIAN-IoT internal communication in TRU reached all the company's group - over 500 employees in 14 countries. • Presentation of the project to the chair of GSMA IoT SAFE working group in a dedicated meeting. • Presentation of the project to the members of GSMA IoT SAFE working

	group using the mailing list and in a plenary meeting.
	• Participation at TADSummit 2022
	• Dissemination of the project in the company website:
	  ○ https://www.truphone.com/security/
	  ○ https://web.truphone.com/about/newsroom/ensuring-the-security-of-iot/)

MARTEL	• Dissemination of the project's objective and activities through its own channels (news items on the website, newsletters) • Cross-promotion of the posts published on the ARCADIAN social media accounts. • Production and promotion of the two animated videos showcasing ARCADIAN-IoT domains and several video interviews with the consortium partners.
UWS	Journals and conferences publication: • Illumination-aware image fusion for around-the-clock human detection in adverse environments from Unmanned Aerial Vehicle. Expert Systems with Applications. Authors: Gelayol Golcarenarenji,Ignacio Martinez-Alpiste,Qi Wang,Jose Maria Alcaraz-Calero. https://doi.org/10.1016/j.eswa.2022.117413 • XDP-Based SmartNIC Hardware Performance Acceleration for Next-Generation Networks. Journal of Network and Systems Management volume 30, Article number: 75 (2022). Authors: Pablo Salva-Garcia, Ruben Ricart-Sanchez, Enrique Chirivella-Perez, Qi Wang, Jose M. Alcaraz-Calero. https://doi.org/10.1007/s10922-022-09687-z • Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Computer Networks, Volume 222, February 2023. Authors: Pablo Benlloch-Caballero, Qi Wang, Jose M. Alcaraz Calero https://doi.org/10.1016/j.comnet.2022.109526 • Non-invasive, plug-and-play pollution detector for vehicle on-board instantaneous CO2 emission monitoring. Internet of Things (Elsevier). Authors: David Tena-Gago, Qi Wang, Jose M. Alcaraz-Calero. https://doi.org/10.1016/j.iot.2023.100755 • ARCADIAN-IoT project was also presented at ITU Focus Group on Autonomous Networks (FG-AN). • Dissemination of the project's objectives and activities through Beyond5GHub (B5GH) website. • Dissemination of the project's activities and media such as consortium meetings, dissemination events held by UWS e.g., lab tours for visitors, and surveys at B5GH LinkedIn account. • Cross-promotion of the posts published on the ARCADIAN-IoT social media accounts.
LOAD	• Dissemination of LOAD involvement in the project's activities through its own channels (blog on the website, newsletters, facebook and linkedin posts). • Sharing of the posts published on the ARCADIAN social media accounts through LOAD's own social media accounts. • References to the ARCADIAN-IoT project and Domain A use-cases in some LOAD's presentations in IoT and AI related workshops.

RGB	• Dissemination of the project's objective and activities through its own communication channels with distributors. Promotion of the animated video showcasing ARCADIAN-IoT domain C. • Participation and presentation of ARCADIAN-IoT in MEDICA Trade Fair 2022.
XLAB	• Dissemination of the project through the publication of news on website. • Cross promotion on social media channels.
BOX2M	• Participation in the demo session at the ARCADIAN-IoT workshop at IoT Week 2022 • Participation in the international event on Energy Crisis and Cybersecurity
UNAV	• Project dissemination through UNAV's internal channels (website and newsletter).
E-LEX	• Dissemination of the project activity through its own institutional channels and social media accounts
ATOS	• Internal communication of the project in several channels • Cross promotion on socila media • Internal communication of the project in several channels; mention in internal newsletter March-April 2023 of joint EC workshop  *Figure 22: ATOS internal newsletter March-April 2023*
RISE	• Dissemination of the project's objective and activities through its own channels; • Sharing of latest outcomes to RISE's partners in RISE open house's poster session; • Cross-promotion of the posts published on the ARCADIAN-IoT social media accounts. • ARCADIAN-IoT project was also presented at the 2023 Privacy

	Symposium Conference Journals and conferences publications: • Lightweight Certificate Revocation for Low-power IoT with End-to-end Security. Journal of Information Security and Applications (Elsevier). Authors: Joel Höglund, Martin Furuhed, Shahid Raza. https://doi.org/10.1016/j.jisa.2023.103424 • SparSFA: Towards Robust and Communication-Efficient Peer-to-Peer Federated Learning. Elsevier Computer & Security. Authors: Han Wang, Luis Muñoz-González, Muhammad Zaid Hameed, David Eklund, Shahid Raza. https://doi.org/10.1016/j.cose.2023.103182 • Ensemble of Random and Isolation Forests for Graph-Based Intrusion Detection in Containers. 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 30-37. Authors: Alfonso Iacovazzi, Shahid Raza. https://doi.org/10.1109/CSR54599.2022.9850307 • Towards Automated PKI Trust Transfer for IoT. 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). Authors: Joel Höglund, Martin Furuhed, Shahid Raza. https://doi.org/10.1109/PKIA56009.2022.9952223 • BLEND: Efficient and blended IoT data storage and communication with application layer security. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). Authors: Joel Höglund, Shahid Raza. https://doi.org/10.1109/CSR54599.2022.9850290 • On the Resilience of Machine Learning-Based IDS for Automotive Networks. 2023 IEEE Vehicular Networking Conference (VNC). Authors: Ivo Zenden, Han Wang, Alfonso Iacovazzi, Arash Vahidi, Rolf Blom, Shahid Raza. doi: not yet available • Towards Cyber Threat Intelligence for the IoT. 4th International Workshop on Security and Reliability of IoT Systems. Authors: Alfonso Iacovazzi, Han Wang, İsmail Bütün, and Shahid Raza. doi: not yet available. • Key Update for the IoT Security Standard OSCORE. 2023 IEEE International Conference on Cyber Security and Resilience (CSR). Authors: Rikard Höglund, Marco Tiloca, Simon Bouget, Shahid Raza. doi: not yet available

4 SYNERGIES WITH OTHER PROJECTS AND INITIATIVES

In Task 6.4, ARCADIAN-IoT's goals is to create synergies with other initiatives. To this end, we reached out to other EC-funded projects and organisations, informing them about ARCADIAN-IoT's aims and objectives and inviting them to share information on their project with us. Below is a list of the projects approached for collaboration.

The objective for creating these connections is to facilitate a cross dissemination of both actions via shared-blog entries, cross-referral on the project websites, mutual social network interaction and event sharing perspective and to have a constant flow of communication between the initiatives in order to promote additional points for collaboration which may emerge in the short and mid-term.

Thanks to these efforts, the **Communication Task Force** among the EU- funded projects in the field of Intelligent security and privacy management was established.

4.1 Joint events

In the reporting period, one of the main outcomes of the T6.4 was the organisation of the **Joint Workshop** "**EU-made cybersecurity for safe, resilient and trustworthy applications and services"** on 28 February 2023: https://www.arcadian-iot.eu/report-on-the-joint-workshop-on-eu-made-cybersecurity/

Figure 23: Visual of the Joint Workshop "EU-made cybersecurity for safe, resilient and trustworthy applications and services"

The workshop was initiated by ARCADIAN-IoT and organized with ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SENTINEL, SPATIAL, and TRUST aWARE projects, with the aim of addressing the cybersecurity needs of the EU industry and public. The workshop focused on the security challenges posed by the increasing adoption of Internet of Things (IoT) technologies, devices, and solutions.

The workshop provided attendees with the knowledge to create safe, resilient, and trustworthy applications and services. It covered a range of topics related to cybersecurity, including challenges faced by security-agnostic and security-aware IoT service providers, best practices

for designing and building secure applications and services, techniques for identifying and mitigating cybersecurity risks, and strategies for ensuring the resilience of applications and services in the face of cyber threats.

The workshop was designed to provide attendees with the knowledge to create safe, resilient, and trustworthy applications and services. The virtual event was attended by professionals and experts from the EU industry, government, and academia. The event was considered a success in terms of the valuable knowledge and insights it provided to attendees.

The main outcome of the workshop was a **Policy Brief** (that can be found in the Appendix).

The event had 79 participants from Austria, Azerbaijan, Bulgaria, Finland, Germany, Greece, Ireland, Italy, Malta, Netherlands, Peru, Poland, Portugal, Romania, Spain, Sweden, Switzerland, Ukraine, United Kingdom, and United States.

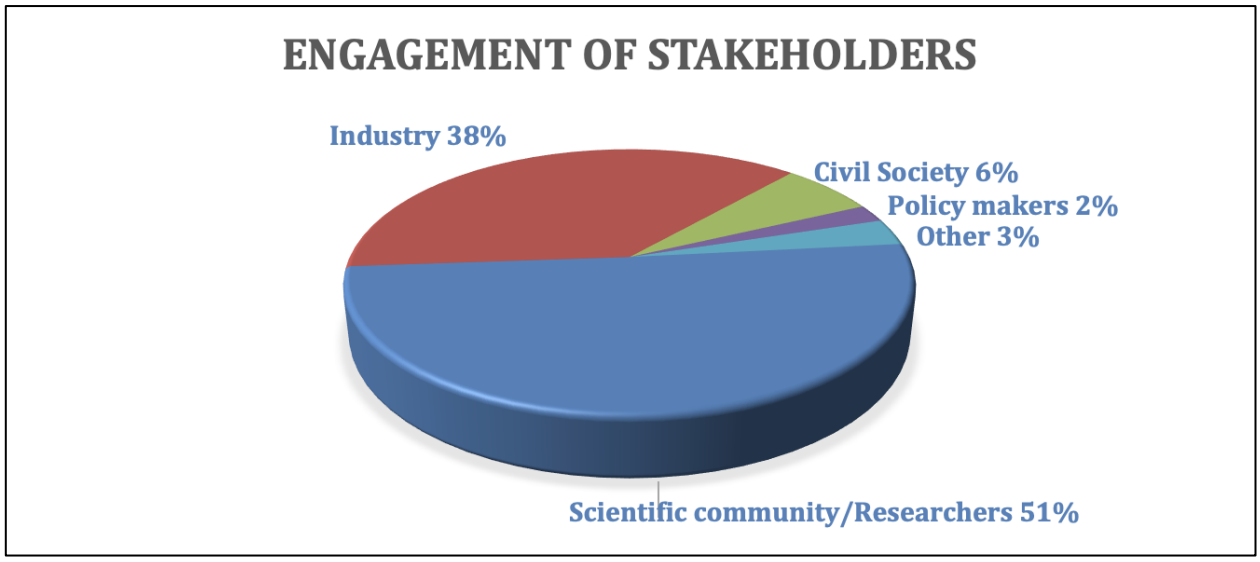


Figure 24: : Engagement of stakeholders in the Joint Workshop

In the next period, ARCADIAN-IoT and the other projects have plans for:

- Other join workshops (September or October 2023).
- Joint publications.
- Joint participation in events.

5 IMPACT CREATION MONITORING

5.1 Dissemination and Communication KPIs

The following metrics are used to monitor and assess the progress of the dissemination and communication activities and provide some measurable outcomes related to their impact created (as far as this is feasible from a quantitative point of view).

Table 2: Dissemination and Communication KPIs

Measure	Indicators and Target (M36)	Results at M24
Flyers Posters / roll-ups	*Nº of flyers *:* 6 *Nº of posters/roll-ups *:* 4	1 (IoT Week 2022) 2
Project Website	*Nº of unique visitors to the website:* 1,500 (average per year)	2,454
Social Networks	*Nº followers on Twitter:* 300 *Nº followers on LinkedIn:* 200 *Nº of views on YouTube:* 300	*Nº followers on Twitter:* 292 *Nº followers on LinkedIn:* 178 *Nº of views on YouTube:* 521
Press Releases* / publication in press*	*Nº of press releases issued to specialized and general media channels:* 6	2 press releases
Videos	*Nº of videos published on the project website and social media:* 3 videos per year *Average number of views:* 60 views /video	Nº of videos: 6 Average number of views: 107
Participation to events and presentations	*Nº of external events partners attended to promote the project:* at least 4 events per year	12
Workshops (2)	*Average Nº of participants: At least 30 participants each*	1 workshop with 79 participants
Cybersecurity Training (6, 2 per use case)	*Average Nº of participants:* At least 20 participants each	Planned for later in the project (refer to D5.6)
4 thematic webinars in (M20,24,30,36)	*Average Nº of participants:* At least 50	Planned for later in the project
Scientific publications	*Nº of peer-reviewed publications in journals:* At least 10. *Nº of peer-reviewed publications in conferences and workshops:* At least 14	6

		10
Newsletters	*Nº of newsletters: 9 (every 4 months)*	6
Summer School (1, M32-M36).	*Nº of participants:* At least 25 participants	Summer School planned to take place between 4-8 September 2023

5.2 Dissemination and Communication Deliverables and Milestones

Table 3: ARCADIAN-IoT Communication Deliverables

No	Deliverable name	Lead	Type	Level	Delivery date (in months)	Status at M12
D6.1	Dissemination and communication strategy and plan	MAR	PU	R	M03	Submitted
D6.4	Outreach activities report	MAR	PU	R	M12	Submitted
D6.7	Outreach activities report	MAR	PU	R	M24	Current document
D6.8	Outreach activities report	MAR	PU	R	M36	Planned

6 CONCLUSIONS AND NEXT STEPS

The ARCADIAN-IoT project has made significant progress in its communication and dissemination activities during the reporting period. As the project enters its third phase of communication, Stage 3 - ARCADIAN-IoT global outreach and sustainable impact (M25-M36). The consortium will focus on actively engaging and supporting the adoption and deployment of the concepts and tools offered by ARCADIAN-IoT through dedicated promotional activities.

To achieve this, the project will participate in events, organise the cybersecurity training to educate stakeholders on the project's outcomes, organise thematic webinars to present the project's results and foster liaisons with relevant initiatives, and organise a Summer School to engage the research community in the ARCADIAN-IoT project.

In parallel, further promotional materials, news item, newsletters will be created and distributed. At the same time, the partners will continue to publish scientific publications in renowned journals and conferences.

1. Technical reports showcasing the project's progress.
2. Additional e-newsletters' editions to keep stakeholders informed.
3. Presenting results and lessons learned at relevant events and platforms.

By focusing on these activities and measures, the ARCADIAN-IoT project aims to create a lasting, sustainable impact on the IoT security and privacy landscape, fostering innovation and promoting the adoption of its concepts and tools across various sectors.

APPENDIX A - POLICY BRIEF

April 2023

POLICY BRIEF

The cybersecurity needs of the EU industry

Editors *(alphabetical order)*

- **Blanca Arregui, AUSTRALO, SPATIAL project**
- **Panagiotis Sarigiannidis, University of Western Macedonia, ELECTRON project**
- **Theodoros Rokkas, InCites, ELECTRON project**

GENERAL SCENE SETTER

Projects that were funded under the H2020-SU-DS-2020: Intelligent security and privacy management call of the EU have formed a Communication Task Force to better share the knowledge among the projects and the external audience. As part of these activities, the Joint Workshop: EU-made cybersecurity for safe, resilient and trustworthy applications and services was organized on 27/02/2023 with the participation of representatives from ten projects. This policy report summarises the views of the different projects based on the presentations and discussions that were made during this joint workshop.

The cybersecurity requirements of the EU industry are critical in today's interconnected and digital world. As businesses and industries increasingly rely on digital infrastructure and data, they face significant cyberattack threats that could compromise their operations, sensitive data, and

financial stability.

EU industries must address various scientific and technical challenges to ensure robust cybersecurity. One of the most significant challenges/issues is the rapid evolution of cybersecurity threats, which requires continuous monitoring and adaptation to new risks. This requires a comprehensive understanding of the latest cybersecurity technologies and strategies, as well as ongoing investment in research and development.

Another challenge/issue is the growing complexity of IT infrastructure, which includes a wide range of interconnected systems and devices. This complexity makes it difficult to secure all aspects of the network, leaving vulnerable areas that cybercriminals can exploit.

Moreover, the lack of qualified cybersecurity professionals is also a significant challenge/issue for EU industries. There is a shortage of skilled professionals capable of managing complex cybersecurity operations, making it challenging to maintain a secure infrastructure and defend against cyber threats effectively.

Main Text

The increasing reliance on digital infrastructure and data in EU industries makes cybersecurity a critical priority. **Most policy-relevant findings** are:

- Cyber threats are constantly evolving, which requires continuous monitoring and adaptation to new risks.
- The lack of qualified cybersecurity professionals is a significant challenge for the EU industry. There is a shortage of skilled professionals capable of managing complex cybersecurity operations.
- The growing complexity of IT infrastructure makes securing all aspects of the network challenging, leaving vulnerable areas that cybercriminals can exploit.
- Insufficient investment in cybersecurity is a major problem in many EU industries. Organisations must allocate sufficient resources to cybersecurity to ensure they can defend against cyber threats effectively.
- Cybersecurity breaches can have severe consequences, such as data breaches, financial loss, damage to reputation, and legal and regulatory repercussions.
- Collaboration and sharing of information between organisations, governments, and cybersecurity experts can help to identify and address emerging threats.
- Adoption of best practices, such as using strong passwords, regularly updating software, and implementing two-factor authentication, can significantly enhance cybersecurity.
- Emerging technologies, such as artificial intelligence and machine learning, can be used to improve cybersecurity and automate routine security tasks.
- The limited project synergies such as data exchange and conducting common pilot and lab experiments.

Recommendations

There are several **policy recommendations** that could be considered to improve cybersecurity needs in the future. Here are a few options:

- Increase funding for research and development in cybersecurity: The EU could increase its investment in cybersecurity research and development to create new technologies and approaches to protect against cyber threats. This could lead to the development of more advanced cybersecurity tools and systems that are better equipped to address emerging threats.

- Improve cross-border collaboration: The EU could encourage greater collaboration between member states on cybersecurity issues. This could involve sharing information about cyber threats and best practices for addressing them, as well as coordinating responses to cyber-attacks. Improved collaboration could strengthen the EU's overall cybersecurity posture.
- Develop common standards and regulations: The EU could develop common standards and regulations for cybersecurity to ensure consistency and improve the effectiveness of cybersecurity measures across the region. This could reduce vulnerabilities and improve the overall resilience of the EU's digital infrastructure.
- Promote cybersecurity education and training: The EU could invest in cybersecurity education and training programs to develop a stronger workforce of cybersecurity professionals. This could address the skills gap in the cybersecurity industry and ensure that the EU has the expertise it needs to effectively address cyber threats.
- Encourage the private sector to prioritize cybersecurity: The EU could encourage private sector companies to prioritize cybersecurity by providing incentives such as tax breaks or other benefits. This helps ensure that private sector organisations are taking cybersecurity seriously and investing in the necessary measures to protect their systems and data.
- Encourage the synergies amongst project having common cybersecurity objectives, while creating/funding the environment of exchanging datasets, output results, pilot experiments results, and lessons learnt. Legal issues could be resolved by fostering the exchange of trained AI and machine learning models, instead of pure datasets, e.g., by encouraging the use of federated learning techniques.

By implementing these policy recommendations, the EU could improve its overall cybersecurity posture and better protect its digital infrastructure against cyber threats. For example, increased funding for cybersecurity research and development could lead to the developing of new tools and technologies that are better equipped to address emerging threats. Improved cross-border collaboration and the development of common standards and regulations could ensure consistency and effectiveness in cybersecurity measures across the region. Meanwhile, promoting cybersecurity education and training and encouraging the private sector to prioritize cybersecurity could help to address the skills gap in the industry and ensure that organisations are taking cybersecurity seriously.

Policy Implications

By staying vigilant and proactive, companies can protect themselves from cyber threats and ensure the safety of their data and operations. The current cybersecurity needs of the EU industry are complex and multifaceted, with various causes and effects. Here are some of the main factors contributing to this situation:

Causes:

- Rapidly evolving cyber threats: With the increasing sophistication of cyberattacks, industries face significant challenges in keeping their systems and data secure.
- Lack of cybersecurity expertise: There is a shortage of skilled cybersecurity professionals, making it challenging for industries to implement effective cybersecurity measures.
- The growing complexity of IT infrastructure: As digital systems become more complex, it becomes more difficult to secure them adequately.
- Insufficient investment in cybersecurity: Many businesses do not allocate sufficient resources to cybersecurity, leaving them vulnerable to attacks.

Effects:

- Data breaches: Cyberattacks can result in the loss of sensitive data, which can have serious consequences for organisations, businesses and customers.
- Financial loss: A cyberattack can result in significant financial losses, such as through the disruption of operations or the theft of funds.
- Damage to reputation: A cybersecurity breach can damage a business's reputation, leading to a loss of customers and revenue.
- Legal and regulatory repercussions: Organisations may face legal and regulatory repercussions if they fail to protect their data adequately.

Perspectives for solutions:

- Increased investment in cybersecurity: Organisations need to allocate sufficient resources to cybersecurity to ensure they can defend against cyber threats effectively.
- Improved cybersecurity education and training: There needs to be an increased focus on educating and training cybersecurity professionals to address the shortage of skilled experts.
- Collaboration and sharing of information: Greater collaboration between businesses, governments, and cybersecurity experts can help to identify and address emerging threats.
- Adoption of best practices: Businesses should adopt best practices for cybersecurity, such as using strong passwords, regularly updating software, implementing two-factor authentication, etc.
- Embracing new technologies: Emerging technologies, such as artificial intelligence and machine learning, can be used to improve cybersecurity and automate routine security tasks.

There are **several potential disadvantages and barriers** to implementing cybersecurity within the EU. Some of the most significant ones include:

- Funding: One of the biggest challenges cybersecurity faces in the EU is funding. Securing the necessary funding to support cybersecurity initiatives can be difficult, especially during economic uncertainty. This can lead to delays in project implementation and a lack of resources to effectively address cybersecurity threats.
- Fragmented regulatory environment: The EU has a fragmented regulatory environment for cybersecurity, with different countries having different approaches to cybersecurity regulation. This can make implementing consistent cybersecurity measures across the EU difficult, leaving some countries more vulnerable to cyber threats than others.
- Lack of real-world datasets: There is a lack of real-world datasets, especially related to critical infrastructure. The availability of open and public datasets could be of paramount importance to enhance the validity, credibility, and transparency of various protocols, algorithms and processes related to AI and machine learning, e.g., anomaly detection, risk analysis, and deep packet inspection.
- Federated-based techniques & legal barriers: exchanging real data amongst different business domains, projects, and pilots become quite difficult and tough mostly due to legal issues. By exchanging federated models instead of data, as an output of related machine learning and AI techniques like federated learning could speed up the process of exchanging important information and experience amongst different actors, without exposing sensitive information or creating legal issues and obstacles.
- Lack of skilled professionals: Another barrier to cybersecurity projects in the EU is the lack of skilled professionals. There is a shortage of qualified cybersecurity experts, which makes it difficult to implement and maintain effective cybersecurity measures.

- Cultural barriers: Different countries within the EU may have different attitudes towards cybersecurity, making it difficult to implement consistent cybersecurity measures across the entire region. For example, some countries may prioritize privacy over security, while others may prioritize security over privacy.
- Technological barriers: Technological barriers can also challenge cybersecurity organisations in the EU. As technology continues to evolve rapidly, it can be difficult to keep up with new threats and implement effective cybersecurity measures that are capable of protecting against them.

Conclusions

In summary, the cybersecurity needs of the EU industry require comprehensive policies that address the challenges of the rapidly evolving cyber landscape. Policies must include measures to address the shortage of skilled cybersecurity professionals, increase investment in cybersecurity, adopt best practices, and embrace emerging technologies. Collaboration and information sharing between businesses, governments, and cybersecurity experts are also critical for addressing emerging threats. In conclusion, this policy brief recommends the following actions:

- EU could increase funding for research and development in the area of cybersecurity.
- EU could encourage greater collaboration to improve the cross-border sharing of information.
- EU could encourage the development of real-world datasets stemming from critical infrastructure[1].
- EU could assist in the development of common standards and regulations.
- EU could foster the development of federated-based model exchange, e.g., federated learning instead of dataset exchange amongst different domains, projects, and pilots.
- EU should promote cybersecurity education and training with emphasis on designing AR/VR training scenarios.
- EU should encourage the private sector to prioritize cybersecurity.
- EU should further encourage the synergies amongst project, highlighting the exchange of critical information, e.g., by using MISP nodes, or fostering the exchange of trained models instead of data by using appropriate technologies like federated learning.

Project Identity

The European Commission selected several projects that directly address the cybersecurity needs of the EU industry. Each project has concrete applications which focus on different verticals/application domains: education, energy, healthcare, manufacturing, mobility, 5G and 6G networks, emergency and vigilance or smart cities, and all these projects joined in a Communication Task Force:

ARCADIAN-IoT: This project aims to develop innovative and advanced security and privacy

[1] Indicative datasets developed from the project participating in the Joint Workshop:
https://ieee-dataport.org/documents/dnp3-intrusion-detection-dataset
https://ieee-dataport.org/documents/iec-60870-5-104-intrusion-detection-dataset

management mechanisms and technologies that can seamlessly be integrated into various contexts and applications.

ELECTRON: This project to aims at delivering a new-generation EPES platform capable of empowering the resilience of energy systems against cyber, privacy, and data attacks.

ERATOSTHENES: This project aims to solve critical obstacles considering "Security of Things" as core to the future IoT success. The project envisions developing a decentralized and contextual Trust and Identity Management Framework for resource-restricted IoT environments following a self-sovereign approach.

IDUNN: This project focuses on adding the trust ingredient to any business by making its ICT systems resilient to cyber-attacks. It will create a security shield through tools, methodologies, microservices and initial standards compatible with any ICT supply chain.

IRIS: This project aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI provisions and their learning/decision-making algorithms.

KRAKEN: This project aims to enable the sharing, brokerage, and trading of potentially sensitive personal data by returning the control of this data to citizens (data providers) throughout the entire data lifecycle.

SECANT: This project focuses on enhancing the capabilities of organisations' stakeholders, implementing (a) collaborative threat intelligence collection, analysis and sharing; (b) innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem; (c) cutting-edge trust and accountability mechanisms for data protection and (d) security awareness training for more informed security choices.

SENTINEL: This project aims to bridge the security and personal data protection gap for European SMEs/MEs by raising awareness and boosting their capabilities in the domain through innovation at a cost-effective level.

SPATIAL: This project tackles the identified gaps of data issues and black-box AI by designing and developing resilient accountable metrics, privacy-preserving methods, verification tools and system solutions that will serve as critical building blocks for trustworthy AI in ICT systems and cybersecurity.

TRUST aWARE: This project aims to provide a holistic and effective digital Security & Privacy (S&P) framework comprising a set of novel and integrated tools and services co-created by citizens and stakeholders to identify, audit, analyse, prevent, and mitigate the impact of the various S&P threats associated with citizen's digital activities in a timely manner, while enhancing software trust and regulatory compliance.

1. ARCADIAN-IoT

Project name: Autonomous trust, security and privacy management framework for IoT (ARCADIAN-IoT)

Coordinator: Instituto Pedro Nunes (Portugal)

Consortium:

- Atos It Solutions and Services (Spain)
- Box2m Engineering (Romania)
- E-Lex (Italy)
- Instituto Pedro Nunes (Portugal)

- Load Interactive (Portugal)
- Martel (Switzerland)
- RGB Medical Devices (Spain)
- Rise Research Institutes Of Sweden (Sweden)
- Truphone (Portugal)
- Universidad De Navarra (Spain)
- University of the West of Scotland (United Kingdom)
- Xlab (Slovenia)

Funding scheme: RIA

Duration: 36 months

Budget: €5.894.106,27

Website: www.arcadian-iot.eu

More information:
- Sérgio Figueiredo: sfigueiredo@ipn.pt
- Mónica Ferreira: mferreira@ipn.pt

Further reading:
1. Enabling Autonomous Trust, Security and Privacy Management for IoT
2. ARCADIAN-IoT requirements
3. ARCADIAN-IoT architecture
4. Horizontal plane of ARCADIAN-IoT framework
5. Vertical plane of ARCADIAN-IoT

2. ELECTRON

Project Name: ELECTRON - rEsilient and seLf-healed EleCTRical pOwer Nanogrid

Coordinator: NETCOMPANY - INTRASOFT

Consortium:

- ALTER TECHNOLOGY TUV NORD SA (Spain)
- ATOS IT SOLUTIONS AND SERVICES IBERIA SL (Spain)
- AZERBAYCAN DOVLET NEFT VE SENAYE UNVERSITETI (Azerbaijan)
- CHECKWATT AB (Sweden)
- COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (Romania)
- CYBERLENS BV (Netherlands)
- DIETHNES PANEPISTIMIO ELLADOS (Greece)
- EIGHT BELLS LTD (Cyprus)
- ENERFIN SOCIEDAD DE ENERGIA SL (Spain)
- ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (Greece)
- FUNDACION TECNALIA RESEARCH & INNOVATION (Spain)
- G.E. PUKHOV INSTITUTE FOR MODELINGIN ENERGY ENGINEERING OF THE NATIONAL ACADEMY OF SCIENCES OF UKRAINE (Ukraine)

- GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS (Greece)
- IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD (Israel)
- IDENER RESEARCH & DEVELOPMENT AGRUPACION DE INTERES ECONOMICO (Spain)
- INCITES CONSULTING SA (Luxembourg)
- INDEPENDENT POWER TRANSMISSION OPERATOR SA (Greece)
- INTEGRATED SOLUTIONS LLC (Ukraine)
- ISOTROL SA (Spain)
- JOINT-STOCK COMPANY PRYKARPATTYAOBLENERGO (Ukraine)
- LOGOS RICERCA E INNOVAZIONE (Italy)
- METAMIND INNOVATIONS IKE (Greece)
- NETCOMPANY – INTRASOFT (Belgium)
- NETCOMPANY-INTRASOFT SA (Luxembourg)
- NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU (Norway)
- PANEPISTIMIO DYTIKIS MAKEDONIAS (Greece)
- PUBLIC POWER CORPORATION S.A. (Greece)
- SCHNEIDER ELECTRIC ESPANA SA (Spain)
- SCHNEIDER ELECTRIC FRANCE SAS (France)
- SIDROCO HOLDINGS LIMITED (Cyprus)
- SOCIETATEA ENERGETICA ELECTRICA SA (Romania)
- THALES DIS FRANCE SAS (France)
- TUV AUSTRIA ROMANIA SRL (Romania)
- UBITECH ENERGY (Belgium)
- UNIVERSIDAD DE MURCIA (Spain)
- UNIVERSITATEA POLITEHNICA DIN BUCURESTI (Romania)
- UNIVERSITY OF CYPRUS (Cyprus)

Funding scheme: IA

Duration: 36 months

Budget: €10,312,814.69

Website: https://electron-project.eu/

More information:

- Panagiotis Sarigiannidis: psarigiannidis@uowm.gr
- Andreas Zalonis: Andreas.ZALONIS@netcompany-intrasoft.com
- Kostas Thivaios: Kostas.THIVAIOS@netcompany-intrasoft.com

Further reading:

- https://electron-project.eu/publications/
- https://ieee-dataport.org/documents/dnp3-intrusion-detection-dataset
- https://ieee-dataport.org/documents/iec-60870-5-104-intrusion-detection-dataset
- https://zenodo.org/record/7348493#.ZCfxHnZBw7c
- https://zenodo.org/record/7108614#.ZCfxHXZBw7c
- https://electron-project.eu/electron-international-event-baku/
- Simos, M., Bouzinis, P. S., Diamantoulakis, P. D., Sarigiannidis, P., & Karagiannidis, G. K. (2022, October). Hierarchical Federated Learning for the Next Generation IoT. In *2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 198-203). IEEE.

- Diamantoulaki, I., Diamantoulakis, P. D., Bouzinis, P. S., Sarigiannidis, P., & Karagiannidis, G. K. (2022, August). Health Risk Assessment with Federated Learning. In *2022 International Balkan Conference on Communications and Networking (BalkanCom)* (pp. 57-61). IEEE.
- Siniosoglou, I., Argyriou, V., Lagkas, T., Moscholios, I., Fragulis, G., & Sarigiannidis, P. (2022, May). Unsupervised Bias Evaluation of DNNs in non-IID Federated Learning Through Latent micro-Manifolds. In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-6). IEEE.
- Siniosoglou, I., Argyriou, V., Lagkas, T., Tsiakalos, A., Sarigiannidis, A., & Sarigiannidis, P. (2021, December). Covert distributed training of deep federated industrial honeypots. In *2021 IEEE Globecom Workshops (GC Wkshps)* (pp. 1-6). IEEE.
- Kelli, V., Argyriou, V., Lagkas, T., Fragulis, G., Grigoriou, E., & Sarigiannidis, P. (2021). Ids for industrial applications: A federated learning approach with active personalization. *Sensors*, *21*(20), 6743.

3. ERATOSHHENES

Project Name: ERATOSTHENES

Coordinator: INLECOM INNOVATION

Consortium:

- AIRBUS CYBERSECURITY SAS (FRANCE)
- ATOS IT SOLUTIONS AND SERVICES IBERIA SL (SPAIN)
- DBC EUROPE (BELGIUM)
- DIGITAL WORX GMBH (GERMANY)
- ENGINEERING – INGEGNERIA INFORMATICA SPA (ITALY)
- EULAMBIA ADVANCED TECHNOLOGIES MONOPROSOPI ETAIRIA PERIORISMENIS EFTHINIS (GREECE)
- IDIADA AUTOMOTIVE TECHNOLOGY SA (SPAIN)
- KATHOLIEKE UNIVERSITEIT LUEVEN (BELGIUM)
- SINTEF AS (NORWAY)
- TECHNISCHE UNIVERSITAET GRAZ (AUSTRIA)
- TELLU IOT AS (NORWAY)
- UNIVERSITY OF MURCIA (SPAIN)
- UNIVERSITY OF PIRAEUS RESEARCH CENTER (GREECE)

Funding scheme: RIA

Duration: 42 months

Budget: €5,999,920.00

Website: www.eratosthenes-project.eu

More information:

- Konstantinos Loupos (konstantinos.loupos@inlecomsystems.com)

Further reading:

- https://eratosthenes-project.eu/results/publications-white-papers/

4. IDUNN

Project name: IDUNN – A cognitive Detection System for Cybersecure Operational Technologies
Coordinator: Cristobal Arellano (Ikerlan)
Consortium (alphabetically, followed by the country)

BITTIUM WIRELESS (Finland)
COSYNTH GMBH (Germany)
DIN DEUTSCHES INSTITUT FUERNORMUNG (Germany)
FAGOR ARRASATE (Spain)
GAIA (Spain)
GRUPO S 21SEC GESTION (Spain)
IKERLAN (LEADER) (Spain)
MONDRAGON ASSEMBLY (France)
OFFIS (Germany)
OULUN YLIOPISTO (Filand)

Funding scheme: Horizon 2020
Duration: 36 months (From September 2021)
Budget: 4.909.745 €
Website: https://www.idunnproject.eu/
More information mitxelena@gaia.es, carellano@ikerlan.es
Further reading:

1. **Backdoor Attacks on Spiking NNs and Neuromorphic Datasets https://dl.acm.org/doi/10.1145/3548606.3563532**
2. **DoS Attack Detection Using Unsupervised Federated Learning for 5G Networks and Beyond, 2023 European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (in review) (UOULU)**
3. **Cyber threat hunting using unsupervised federated learning and adversary emulation, 2023 IEEE CSR. (in review) (UOULU)**
4. **Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security, Augmented Humans Conference 2023 (UOULU)**
5. **Using smart glasses for monitoring cyber threat intelligence feeds, 2021 ASONAM (UOULU)**

5. IRIS

Project Name: artificial Intelligence threat Reporting and Incident response System (IRIS)

Coordinator: INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal

Consortium:

- ATOS, Spain
- CEA, France
- CEL, Italy
- CERTH, Greece
- CISCO SPAIN, Spain
- CLS, Netherlands
- DNSC Romania
- ECSO, Belgium
- FVH, Finland
- ICCS, Greece
- IMI BCN, Spain
- INTRA, Luxembourg
- INOV, Portugal
- KEMEA, Greece

- SID, Cyprus
- TalTech, Estonia
- THALES, France
- TU Delft, Netherlands
- UPC, Spain

Funding scheme: IA

Duration: 36 months (September 2021 – August 2024)

Budget: EU Contribution: €4,918,790

Website: www.iris-h2020.eu

More information:

goncalo.cadete@inov.pt/ coordinator@iris-h2020.eu,

maria.tsirigoti@iccs.gr

Further reading:

- Fine-Grained Coverage-Based Fuzzing NDSS Symposium 2022
- IRIS Advanced Threat Intelligence Orchestrator- A Way to Manage Cybersecurity
- Challenges of IoT Ecosystems in Smart Cities IoT Week 2022
- Passtrans: An Improved Password Reuse Model Based on Transformer ICASSP 2022.
- WordMarkov: A New Password Probability Model of Semantics, ICASSP 2022

6. SECANT

Project name: SECurity And privacy protectioN in IoT devices (SECANT)

Coordinator: Monica Caballero (NTTDATA)

Consortium:

- Adrestia, GR
- Axon Logic, GR
- Business and IoT Integrated solutions, CY
- Centrul National de Raspuns la incidente de securiate cibernetica, RO
- Exalens, NL
- Eight bells, CY
- Ethniko Kentro Erevnas kai technologikis anaptyxis, GR
- Fundacio Privada I2Cat, ES
- Fundacio TICSALUT, ES
- Ianus Consulting, CY
- Infolysis, GR
- Karolinska Institutet, SE
- NTT DATA, ES
- Polaris, RO
- Security Labs, IE
- Software Imagination and Vision, RO
- Thales, FR
- Ubitech, CY
- University of Surrey, UK

Funding scheme: IA

Duration: 3 years

Budget: €6.567.958,75

Website: https://secant-project.eu/

More information:

monica.caballero.galeote@nttdata.com
Further reading:

https://zenodo.org/record/7041087#.ZAcEK3bP1D8
https://zenodo.org/record/7674017#.ZAcEZHZBxD8

7. SENTINEL

Project name: SENTINEL - Bridging the security, privacy and data protection gap for smaller enterprises in Europe- coordinator: ITML

Consortium:

- AEGIS, Germany
- AIRBUS CYBERSECURITY, France
- CENTRE FOR EUROPEAN CONSTITUTIONAL LAW, Greece
- CLINGENICS, United Kingdom
- FOCAL POINT, Belgium
- IDIR, Ireland
- ITML, Greece
- LIST, Luxembourg
- NETCOMPANY-INTRASOFT, Luxembourg
- SPHYNX, Switzerland
- TRISTONE INVESTMENT GROUP, Malta
- UNINOVA, Portugal
- TELECOMMUNICATION SYSTEMS INSTITUTE, Greece

Funding scheme: RIA
Duration: 36 Months
Budget: 5304732,50€
Website: Home | SENTINEL (sentinel-project.eu)
More information: George Bravos gebravos@itml.gr, Siranush Akarmazyan siranush@itml.gr
Further reading:
https://sentinel-project.eu/publications/
https://sentinel-project.eu/deliverables/
https://sentinel-project.eu/dissemination-materials/

8. SPATIAL

Project name: SPATIAL Project (Security and Privacy Accountable Technology, Innovations, Algorithms, and Machine Learning)

Coordinator: Aaron Ding (Netherlands)

Consortium:

- AUSTRALO (Spain)
- Delft University of Technology (Netherlands)

- Erasmus University Rotterdam (Netherlands)
- Fraunhofer Fokus (Germany)
- Mainflux (Serbia)
- Minnalearn (Finland)
- Montimage (France)
- NEC Europe Laboratories (Germany)
- Telefónica I+D (Spain)
- University College Dublin (Ireland)
- University of Tartu (Estonia)
- Withsecure (Finland)

Funding scheme: RIA

Duration: 36 months

Budget: € 4,961,976.25

Website: www.spatial-h2020.eu

More information:
- Aaron Ding: Aaron.Ding@tudelft.nl
- Marcus Westberg: M.Westberg@tudelft.nl

Further reading:

- Aaron Yi Ding, Marijn Janssen, Jon Crowcroft, "Trustworthy and Sustainable Edge AI: A Research Agenda", in Proceedings of the Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021.
- Wiebke Toussaint, Akhil Mathur, Aaron Yi Ding, and Fahim Kawsar. 2021. "Characterising the Role of Pre-Processing Parameters in Audio-based Embedded Machine Learning". In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21).
- M.D. Nguyen, V. H. La, R. Cavalli and E. M. de Oca, "Towards improving explainability, resilience and performance of cybersecurity analysis of 5G/IoT networks (work-in-progress paper)," 2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Valencia, Spain, 2022
- Wiebke Toussaint, Aaron Yi Ding. 2022. "Towards Trustworthy Edge Intelligence: Insights from Voice-activated Services". In Proceedings of the 19th IEEE International Conference on Services Computing (SCC '22).
- Abdul-Rasheed Ottun, Pramod C. Mane, Zhigang Yin, Souvik Paul, Mohan Liyanage, Jason Pridmore, Aaron Yi Ding, Rajesh Sharma, Petteri Nurmi, Huber Flores, "Social-aware Federated Learning: Challenges and Opportunities in Collaborative Data Training", in IEEE Internet Computing, 2023.

9. TRUST aWARE

Project name: TRUST aWARE “Enhancing digital security, privacy and trust in software”

Coordinator: TREE TECHNOLOGY (Dr Javier Gutiérrez)

Consortium:

- Abilab – Centro di Ricerca e Innovazione per la Banca - IT
- Asociata Infocons – RO
- Centre National de la Recherche Scientifique – FR
- E-Seniors – FR
- Fondazione Mondo Digitale – IT
- Fundación Cibervoluntarios – ES
- Fundación IMDEA Networks – ES
- IOT Lab Association – CH
- Tree Technology – ES
- Trilateral Research – IE
- Universidad Carlos III – ES
- WithSecure – FI

Funding scheme: Innovation Action

Duration: 36 months

Budget €5,244,997.50

Website: https://trustaware.eu/

More information:
- Anna Brekine (abrekine@iotlab.com)
- Javier Gutiérrez (javier.gutierrez@treetk.com)

Further reading:

https://cordis.europa.eu/project/id/101021377/results