Promoting academia-industry alliances for R&D through collaborative and open innovation platform - All4R&D

Co-funded by the Erasmus+ Programme of the European Union

NPUA/IIAP Cooperative R&D Unit

OPEN CALL FOR PARTICIPATION TO NPUA&IIAP RESEARCH PROJECT

Hardware and Software Cybersecurity Solutions for Internet of Things

Promoting academia-industry alliances for R&D through collaborative and open innovation platform

Project reference number: 598719-EPP-1-2018-1-MK-EPPKA2-CBHE-JP

Project duration: 15 November 2018 – 14 November 2021
EU funding instrument: European Neighbourhood Instrument (Erasmus+: KA2 CBHE)
Erasmus+ (CBHE) grant amount: 531,165.00 €
Partner countries: Armenia, Bosnia and Herzegovina, North Macedonian, Austria, Germany, Finland
Target groups: University management and students, companies, research institutions, intermediaries.
Grant holder: Ss. Cyril and Methodius University in Skopje, North Macedonia
Coordinator: Prof. Elena Dumova-Jovanoska, Ss. Cyril and Methodius University in Skopje

This project has been funded with support from the European Commission. This document reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

NPUA/IIAP Cooperative R&D Unit

Call for Participation opens: 26/09/2022

Deadline for submissions: 31/10/2022

Project summary

One of the top issues regarding the viability of the Internet of Things in the enterprise is how IoT data and devices will be secured. Indeed, IoT introduces several new architecture dynamics that traditional IT security administrators may not be accustomed to on such a large scale. And if security is not properly addressed or implemented, you run the risk of data loss and the possibility of introducing weak points on your network that can be used by hackers to infiltrate your entire infrastructure and gain control over your devices. Studies have shown that IoT device vendors are not taking security all that seriously and, therefore, it is actual to develop hardware and software security solutions at the system and user levels.

Project outcomes

In this project, our own research has led to the development of hardware and software security solutions that can complement modern IoT devices with a sufficient level of security at the system and user levels. This is important because, in the absence of special means of protection against modern threats, the user can become so vulnerable that he may be in serious danger and even refuse to use such devices.

Challenges facing participants (or Who is it for)?

The main challenge is the cross-disciplinary approach aimed at developing such compatible hardware and software cybersecurity solutions for IoT devices that practically do not complicate the use of these devices. We look forward to close cooperation with companies involved in cybersecurity research, as well as organizations in the field of creating smart industrial and household solutions based on IoT.

What will be provided by NPUA/IIAP Cooperative R&D Unit?

Research and development are planned to be carried out mainly on the basis of the Cybersecurity Lab equipped with modern computers, printers and scanners with Wi-Fi capabilities, as well as high-speed access to national and international scientific networks.

Proposals wanted and Criteria for acceptance

The basic criteria for acceptance for individuals and companies are the following:

- Level and type of education: Undergraduate degree in Mathematics, Computer science or Engineering

- Software skills: Windows and mobile OS, Object-Oriented Programming
- Research skills: basic knowledge on IoT, Cybersecurity and Digital Devices

Timeline

- To develop structures of hardware solutions, M8
- To develop suitable algorithm of software solutions, M10
- To develop suitable system solutions, M12

How to participate (or apply)?

The applicant (company or researcher) should send a motivation letter and portfolio/CV to the NPUA/IIAP Cooperative R&D Unit (dtc-rdu-info@polytechnic.am) to state motivation to participate in the project by indicating the technical and scientific experience and competences. Then we will organize in-person interviewing to make final decision.