

CERTIFY NEWSLETTER #2

WWW.CERTIFY-PROJECT.EU



February 6, 2024

Top News

1st Plenary Meeting: Project discussion in a hybrid meeting at [Engineering Ingegneria Informatica](#), Rome

Project Progress: Technical outcomes, conferences, dissemination

CERTIFY

defines a methodological, technological, and organizational approach towards IoT security lifecycle management based on

- security by design support
- continuous security assessment and monitoring
- timely detection, mitigation, and reconfiguration
- secure Over-The-Air software update
- steady security information sharing



1st PLENARY MEETING



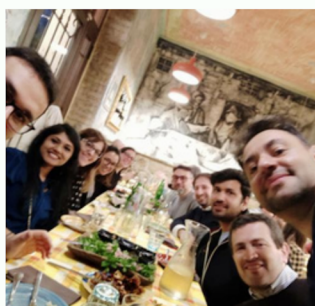
"If you think that the internet has changed your life, think again. The Internet of Things is about to change it all over again!"

Brendan O'Brien



1st plenary meeting of CERTIFY was held in Rome from 18 to 19 April 2023 and was conducted by the Engineering Ingegneria Informatica. During the meeting work package and task leaders took the lead and presented activities and their results since kickoff meeting.

The format of the meeting included presentations by the work leaders followed by open discussion on tasks, results and next step of work package. Meeting minutes and action points for each partner were prepared.



12

Research Partners

8

Countries

36 M

Project duration

DELIVERABLE

SECURITY REQUIREMENTS

Stringent security requirements dictate the need for robust encryption, multi-factor authentication, and periodic security assessments to fortify the project against potential vulnerabilities.

Compliance with industry standards and regulations, coupled with continuous monitoring, ensures that security requirements evolve in tandem with emerging threats, fostering a resilient project environment. In the CERTIFY project, we have worked with partners to derive requirements from 3 pilots in the task T1.1 in work package 1. They will be documented in the deliverable D1.1



THREATS MODELS

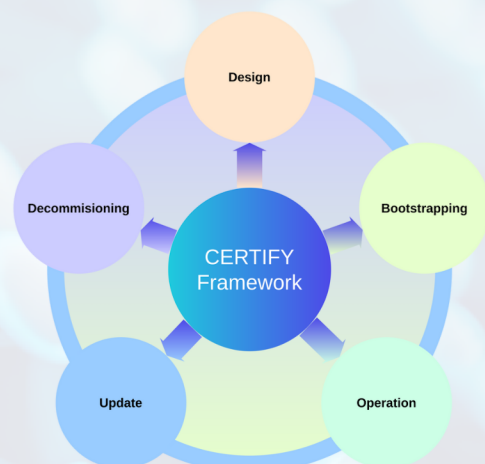
Crafting a comprehensive threat model involves identifying potential risks, assessing their impact, and developing proactive strategies to mitigate vulnerabilities, enabling a preemptive defense against cyber threats.

The threat model serves as a dynamic blueprint, evolving alongside the project to anticipate and neutralize potential risks, thereby fortifying the project's resilience in an ever-changing threat landscape. We have used STRIDE model to perform threat analysis of Pilots. We will describe in detail about identified threats, potential threat scenarios, threat scores and mitigation plan in deliverable D1.1

INITIAL CERTIFY LIFECYCLE MANAGEMENT

In the initial certification lifecycle management, a meticulous assessment of the project's security controls and protocols has been conducted to meet established standards and compliance criteria.

We have submitted deliverable D7.1 which establishes the project management and quality procedures and tools for efficient coordination and communication between partners, as well as the project's data management procedures



DISSEMINATION

Conferences play a pivotal role in projects by providing a platform for knowledge exchange, fostering collaboration, and staying abreast of industry trends. These gatherings not only enhance project visibility but also offer invaluable opportunities for networking, idea generation, and partnerships critical for project success.



On 28 March, 2023, there was a workshop titled, Sensibilisierung-Schulung Verfassungsschutz, was organised by the [asvin GmbH](#). The objective of the workshop was to increase awareness about cybersecurity and present security landscape of Germany. On this occasion, Rohit Bohara from digital worx GmbH presented CERTIFY project'S objectives and technologies. It was a hybrid event where around 23 people joined physically and online.

On February, 10th, a project clustering meeting was organized in Trento, to create synergies among projects funded within the context of call [HORIZON-CL3-2021-CS-01](#). CERTIFY participated to the meeting, where Luigi Coppolino from [Trust Up](#) presented the approach CERTIFY has taken to provide protection of IoT devices throughout their lifecycle. The representative of the [CROSSCON](#) project, namely Matjaz Breskvar from Beyond Semiconductor, presented CROSSCON activities.



[CERTIFY](#) contributed to this year's edition of the [European Network for Cybersecurity \(NeCS\) PhD School](#) from 6th to 10th Feb 2023. The school was launched six years ago, in response to the increasing need of highly qualified experts in cyber-security. Luigi Romano from TrustUp gave a lecture titled: "Hardware-assisted Trusted Computing: State of The Art and Emerging Use Cases".

In [CNSM 2022](#) (31 Oct to 4 Nov), the [keynote](#) was delivered by Professor Antonio Skarmeta from the University of Murcia who is project coordinator of the CERTIFY project. The CNSM 2022 is a selective single-track conference, covering all aspects of the management of networks and services, pervasive systems, enterprises, and cloud computing environments. CNSM 2022 is technically co-sponsored by the [IEEE](#) Communications Society, IFIP, and ACM's in-Cooperation support.



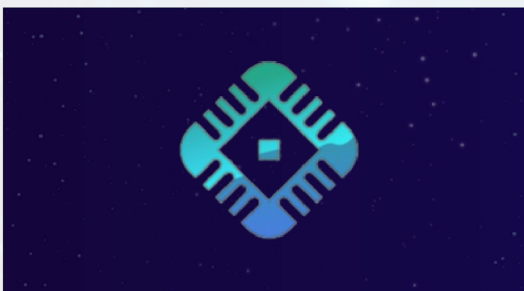
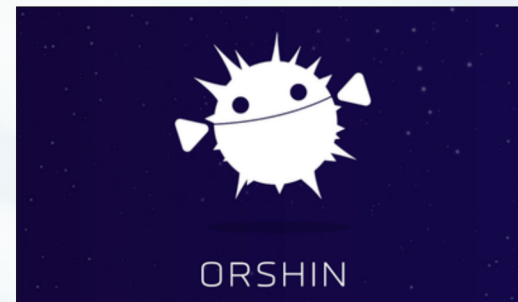
COLLABORATION

In order to maximize impact, promote innovation, and accelerate progress in the R&D environment, collaboration with other R&D projects is essential. Researchers can better address difficult issues by collaborating with other initiatives to pool varied viewpoints, resources, and skills. We have collaborated with other EU funded projects with the objective to exploit synergy and disseminate results together.



REWIRE envisions a holistic framework for continuous security assessment of open-source and open-specification hardware and software for IoT devices and the development of cybersecurity certification in accordance with the requirements and guidelines of recent EU regulation Cyber security Act.

ORSHIN is creating the first generic and integrated methodology, called trusted lifecycle, to develop secure network devices based on open-source components while managing their entire lifecycle. ORSHIN's trustworthy lifecycle consists of different phases (design, implementation, evaluation, installation, maintenance and retirement) that form a chain of trust.



CROSSCON will implement a security baseline across the whole IoT system to avoid "easy" entry points for attackers. CROSSCON aims at addressing all these issues by designing a new open, modular, highly portable, and vendor-independent IoT security stack that can run on a wide range of devices that may use heterogeneous hardware architectures

The EU-funded ENTRUST project will seek to tackle the lack of cybersecurity implementations in connected medical devices without limiting their wide applicability. The proposed trust management architecture will dynamically and holistically manage the lifecycle of connected medical devices, strengthening trust and privacy in the entire medical ecosystem.



FEATURED RESEARCHER



Roberto Nardone


*Assistant Professor
University of Naples Parthenope*

ABOUT

Roberto Nardone is an Assistant Professor at the University of Naples Parthenope and a consultant for TrustUp, specializing in Computer Science. His research, enriched by both national and international collaborations, focuses on the functional and non-functional properties of critical complex systems, emphasizing security. He is part of the FITNESS research group, delving into cybersecurity and the reliability of distributed computer systems. His expertise includes security, dependability, maintainability, and performability of systems, developed through his involvement in various EU-funded projects such as CERTIFY. He is passionate about enhancing the security and efficiency of critical infrastructures through innovative research.

ON CERTIFY

CERTIFY marks a significant leap in IoT security, exciting me greatly with its promise to deliver advanced protection mechanisms for stakeholders. This project stands out for its innovative approach to detect, respond, and support security throughout the IoT lifecycle. Its pioneering architecture, validated through cutting-edge pilots, is set to revolutionize security across various IoT environments.



His role in CERTIFY, coupled with TrustUp's leadership in the architecture definition and validation work package, allows for the practical application of advanced methodologies and technologies. We are integral in integrating diverse tools and services, thus shaping a collaborative deployment environment for the entire system. TrustUp's contribution to an innovative SIEM-SOAR system, performing aggregated event analysis and orchestrating responsive actions, underscores our commitment to enhancing IoT security. This involvement not only aligns with his professional passions but also positions us at the forefront of technological innovation in IoT security.

READER'S VIEW

Rob van Kranenbourg is an internationally recognized expert, speaker, publicist and researcher in the field of cyber security and the Internet of Things. In 2009 I founded the Internet of Things Council (theinternetofthings.eu) and in 2010 the IoTDay (iotday.org) in order to bring IoT to a general audience. He is working as Chief Innovation officer in asvin GmbH.



Rob van Kranenbourg

CIO asvin GmbH



STATE OF IOT SECURITY

The day is not far off when all people will have some tool, call it a wallet, a router, a phone, a crypto mining device (maybe all of that) that runs all computation locally on that device and gives out only contextual, time-limited and scope-based information; a companion to assist you in educating yourself and others in living together on a small planet that is tumbling about in vast space. In fact, the 1976 novel *Woman on the Edge of Time* by Marge Piercy, describes this tool in her 'utopia' of a society combining local bio food and resilient communities running on high tech renewable and distributed ledgers provisioning services. Maybe it was not a utopia but just a vision? She calls the device a *kenner*.

HOW CERTIFY WILL HELP


I am closely following the CERTIFY project. Its aim to manage security throughout the lifecycle of the IoT device is quite ambitious and will have great impact. It will design and develop novel solution for secure boot-strapping, identity management, trust score generation, threat monitoring, intrusion detection and authentication. These tools and processes will address the existing security issues and will enable the IoT stack holders in achieving high level security.



ABOUT US



aCtive sEcurity foR connecTed devlces liFecYcles

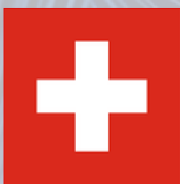
OCT 2022 | SEP 2025 

Project Partners



FIND US ON

- WWW.CERTIFY-PROJECT.EU
- WWW.TWITTER.COM/CERTIFY_PROJECT
- WWW.LINKEDIN.COM/COMPANY/CERTIFY-PROJECT



This project has received funding from the European Union's Horizon CL3 Increased Cybersecurity 2021 under grant number agreement number 101069471 and from the Swiss State Secretariat for Education, Research and Innovation (SERI) under grant agreement numbers 22.00165 and 22.00191