CERTIFY NEWSLETTER

WWW.CERTIFY-PROJECT.EU

October 13, 2023

Top News

Kickoff Meeting: Project began with a hybrid meeting at University of Murcia

Project Resource: Project website, social media channels were created

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

Project Resource: Project website, social media channels were created

Newsletter Highlight

We had our project kickoff meeting on 20-21 October 2022 at the University of Murcia. The meeting was chaired by our project coordinator and joined by all partners physically and remotely. Each Project partner presented its relevant tasks, deliverable and milestones.

Inside The Issues

- The CERTIFY project provides IoT stakeholders with mechanisms achieving high-level security. The project began with a kickoff meeting in Murcia.

- CERTIFY will validate the architecture through cutting-edge use-cases in aviation, industry 4.0 and art tracking.

- The objectives and contributions of the CERTIFY project

- A researcher's and a reader's view on CERTIFY

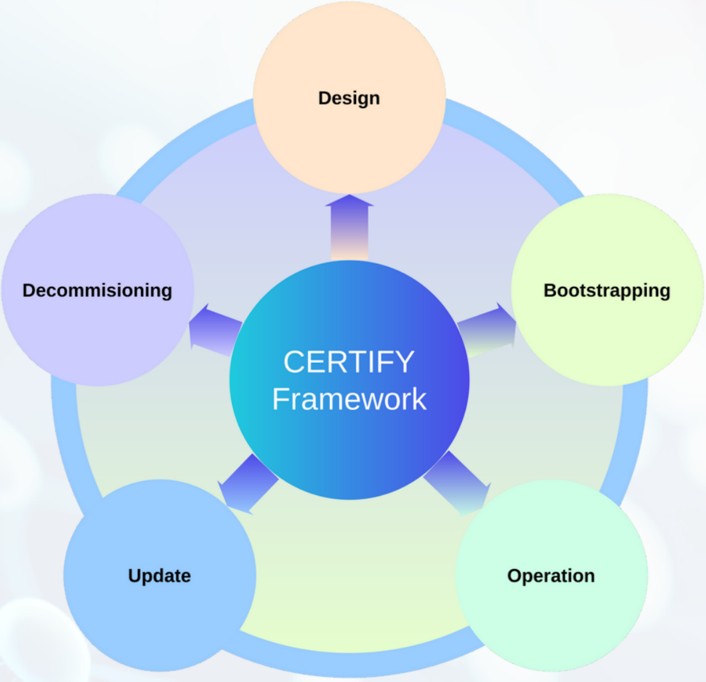
Project Coordinator

Antonio Skarmeta

He received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the PhD degrees in Computer Science from the University of Murcia Spain. Since 2009, he is full professor at the same department and University.

OVERVIEW

To ensure security compliance throughout the lifetime of the device, we propose the design and implementation of a cybersecurity lifecycle management framework for IoT devices. The framework is intended to support device security management by collecting and sharing relevant security information both internally and externally.



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

OBJECTIVES

CERTIFY has SMART (Specific, Measurable, Achievable, Realistic and Timely) specific objectives

- Cybersecurity awareness for IoT enabled environments through a multi-stakeholder sharing of threats and mitigations.
- Secure reconfiguration and maintenance of customizable embedded devices by means of hardware primitives and services.
- Perform security operational management based on bootstrapping and monitoring of attacks and malicious behaviors.
- Run time security compliance and continuous certification methodology via objective metrics.
- Foster knowledge delivery via wide dissemination, capacity building and supporting activities. Build a robust exploitation plan to boost ROI by optimizing current and future EU cybersecurity capabilities.
- Industrial validation of the CERTIFY framework in IoT ecosystems.

AMBITIONS

The main contributions of CERTIFY are as follows, going beyond the state of the art:

- Novel framework to manage security throughout the lifecycle of the IoT device.
- Certification & security evaluation.
- Enhanced open hardware security.
- Secure integration of IoT devices.
- Behavioural profile.
- Security monitoring & detection.
- Information sharing and upgrading.

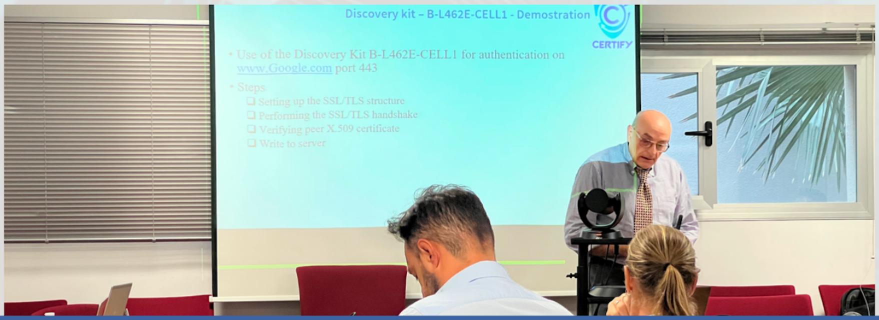
Kickoff

“IoT without security = Internet of Threats”

Stéphane Nappo

The CERTIFY kickoff meeting was in Murcia and was conducted by the University of Murcia. All the project partners presented their technical contributions, their respective tasks and work packages.

Moreover, during the meeting, project partners discussed the overall project goals, mission, administration aspect and created action points to make the project to run smoothly. The meeting ended with Social dinner where everyone get know each other at personal level.


Discovery kit – B-L462E-CELL1 - Demostration
CERTIFY
Use of the Discovery Kit B-L462E-CELL1 for authentication on www.Google.com port 443
Steps:
Setting up the SSL/TLS structure
Performing the SSL/TLS handshake
Verifying peer X.509 certificate
Write to server

CERTIFY

12

Research Partners

8

Countries

36 M

Project duration

USE CASES

The methodologies and tools provided by CERTIFY's framework will be evaluated in 3 use cases from different sectors:

SECURE MANAGEMENT OF DEVICES ENABLING AN INTELLIGENT AND CONNECTED AIRCRAFT CABIN

IoT devices installed in aircraft cabins will be monitored throughout their operations, tested against security requirements, robustness and vulnerability, and will be reconfigured as necessary to detect and mitigate cyber threats in a preventive, corrective or restorative fashion.

SMART MICRO-FACTORIES

The smart micro-factory represents an ongoing evolution from traditional factories to fully connected, flexible and reconfigurable. We will consider the flexible, lightweight and robust authentication, device bootstrapping, threat monitoring, DLT powered software update solutions of CERTIFY to strengthen the security of IIoT devices.

TRACKING AND MONITORING OF ARTWORKS

Cybersecurity is a crucial matter for the monitoring and protection of artworks and concerns issues like user roles, authentication, the integrity and confidentiality of sensitive data. Only entities with authenticated roles should have access to the monitored data and when transmitted only an enciphered and signed format should be used.

FEATURED RESEARCHER

Valerio Senni

Sr Principal Engineer, Product Cybersecurity, Advanced Research & Technology Department

ABOUT

He earned a PhD in applied formal methods in 2008 and worked in several EU research institutions. From 2014, he worked in the industrial research organization of Raytheon Technologies and then in Collins Aerospace, part of Raytheon Technologies. Since 2021, He is a researcher in the Collins Applied Research and Technologies organization (ART). Since 2017, he has been leading cyber-security research projects on applications of formal methods and model-based design to security, implementation of high-assurance network security solutions and embedded security solutions, also based on RISC-V technologies. He represents Collins within the European Cybersecurity Organization (ECSO) and he is author of 35+ conference/journal publications.

ON CERTIFY

IoT devices are becoming pervasive in critical sectors, with a pressing need for secure ecosystems. In Civil Aviation, for example, IoT supports a better cabin experience and predictive health management of aircraft systems. To optimize size/weight/power/cost, we adopt a diversified set of IoT nodes: from extremely low resource to highly capable ones. At the same time, we need a consistent approach to establishing trust in the node, securely integrate it within aviation networks, and keep an up-to-date security posture. CERTIFY is really focusing on addressing our core challenges: covering the whole security lifecycle of the device and providing a uniform security model addressing IoT nodes and capabilities heterogeneity. Collins' role is central on conceptualization of the whole vision, security monitoring services, and IoT security primitives' design. My focus is on the design of the key trusted computing enablers for a RISC-V based system on chip that will enable trusted execution of CERTIFY's security services on lightweight IoT nodes.

READER's VIEW

Mirko Ross is an internationally recognized entrepreneur, expert, speaker, publicist and researcher in the field of cyber security and the Internet of Things. Mirko has been member of the Expert Group on Internet Security of Things of the ENISA and advises the EU Commission and the German Government as an expert. In 2018, he founded asvin.io, a company with the goal of increasing cybersecurity in industry and AI applications.

Mirko Ross

CEO asvin GmbH

STATE OF IOT SECURITY

The state of IoT security remains a significant concern as the number of connected devices continues to proliferate. Many IoT devices are inherently vulnerable due to their limited computing power and resource constraints, making them attractive targets for cyberattacks. Security best practices, such as regular software updates and strong authentication mechanisms, are often overlooked by manufacturers, leaving devices exposed to potential breaches. Furthermore, the diversity of IoT devices, standards, and communication protocols complicates the development of comprehensive security solutions. As a result, there is an ongoing need for industry-wide collaboration and the implementation of robust security measures to safeguard the increasingly interconnected world of IoT.

HOW CERTIFY WILL HELP

CERTIFY project is designed to manage security throughout the lifecycle of the IoT device. It will design and develop novel solution for secure boot-strapping, identity manage-ment, 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 for their IoT devices.

PROJECT PARTNERS

AIR INSTITUTE

Collins Aerospace

University of Zurich UZH

ECS EUROPEAN CYBER SECURITY ORGANISATION

UBITECH ubiquitous solutions

digital worx

UNIVERSIDAD DE MURCIA

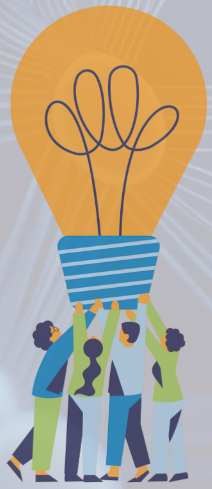
RED ALERT LABS IoT Security

modum

ST life.augmented

ENGINEERING THE DIGITAL TRANSFORMATION COMPANY

TrustUP A PARTHENOPE UNIVERSITY SPIN-OFF



CERTIFY

aCtive sEcurity foR connecTed devIces liFecYcles

FIND US ON

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