This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 952702

BIECO

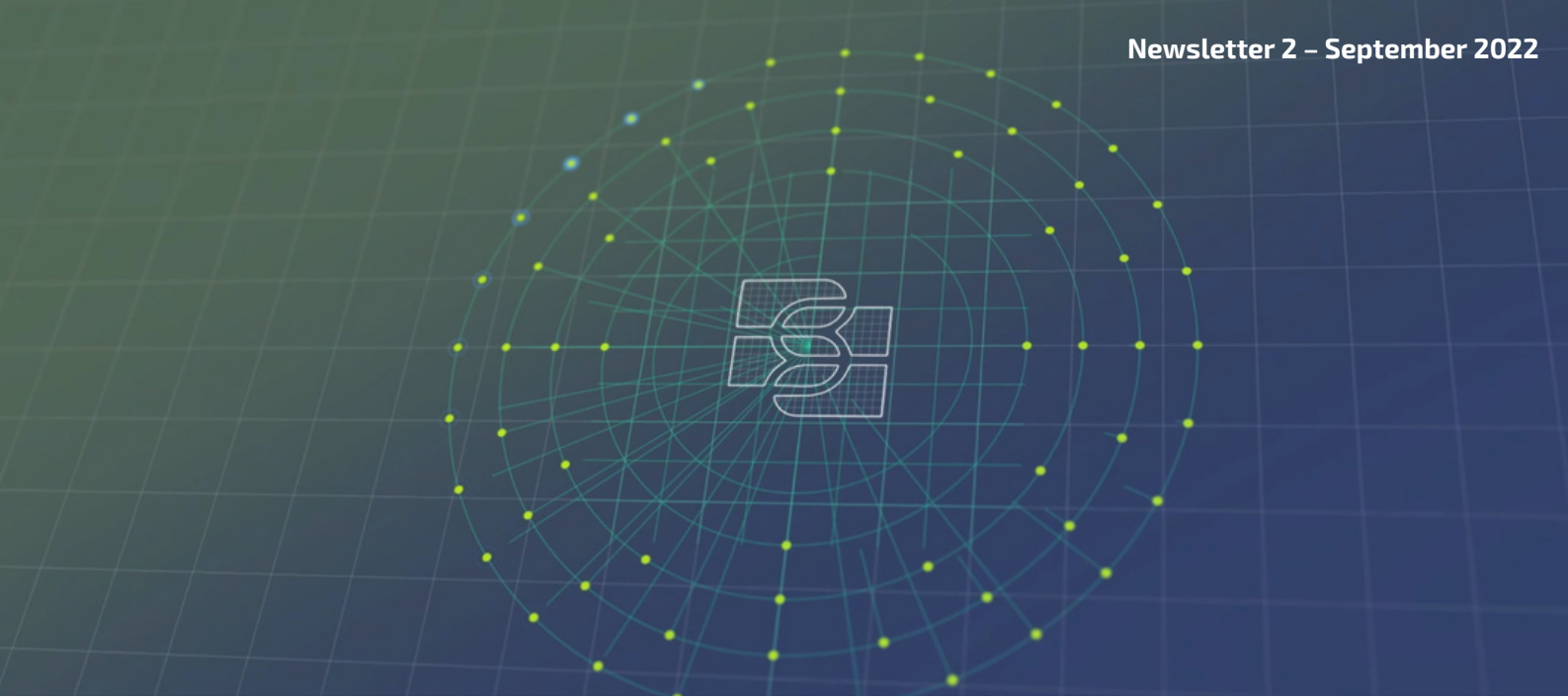
Building Trust in Ecosystems and Ecosystem Components

No. 2

September 2022

IN THIS ISSUE

BIECO
Building Trust in Ecosystems and Ecosystem Components



DEAR READER,

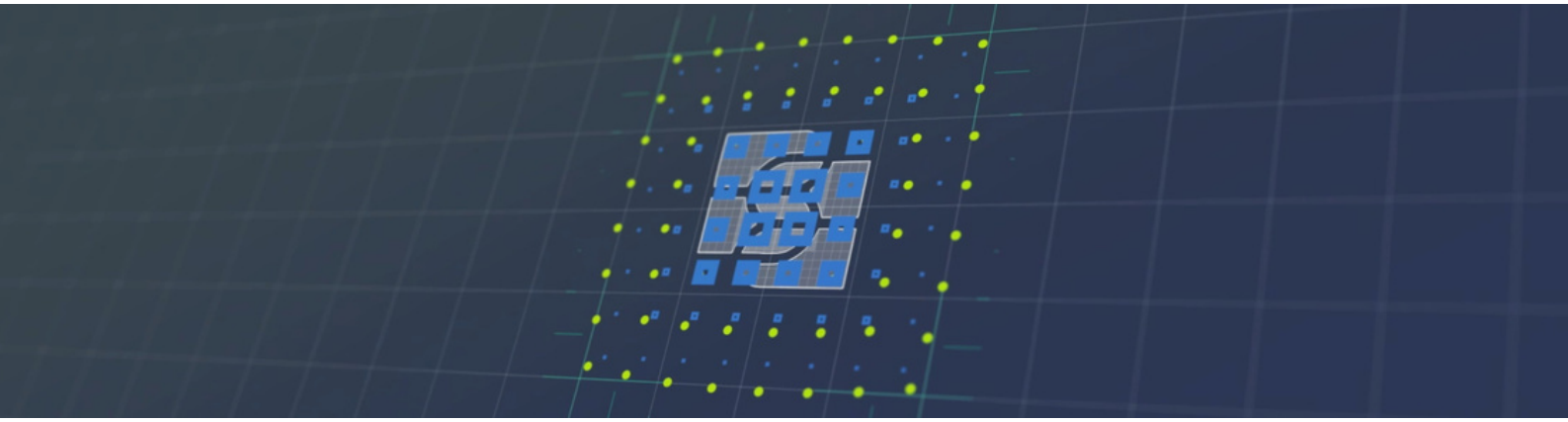
I am extremely proud to present you our second newsletter dedicated to the Horizon 2020 BIECO project.

The consortium involved within the BIECO project made great progresses in achieving all the proposed objectives, milestones, and key outcomes, contributing to our goal to develop a framework that enables measurable, risk-based trust while developing, deploying, and operating complex interconnected ICT systems.

In this newsletter, we present the project status, highlight our important achievements within all our work packages, and the list of publications.

I hope you will enjoy reading our newsletter and invite you to check our website regularly, follow us on social media or contact us directly for more information.

Sincerely yours,
Prof. dr. Jose Barata



BIECO – Objectives of the project

BIECO aims to deliver a framework for increasing trust within ICT supply chains, which comprise different processes, actors (e.g., users, software and hardware providers), technologies and resources. Bieco will provide mechanisms in order to help companies to understand and manage the cybersecurity risks and threats they are subject to when they become part of the ICT supply chain. The framework, composed by a set of tools and methodologies, will address the challenges related to vulnerability management, resilience, and auditing of complex systems.

The specific SMART (Specific, Measurable, Achievable, Realistic, Time-bound) objectives of our project are:

OBJ1 - Providing a framework that allows to reinforce trust in ICT supply chains

In BIECO, a holistic security framework for ensuring trust within ICT supply chains is being developed. The framework will comprise a set of tools and methodologies for vulnerability assessment, auditing, risk analysis, determining the best mitigation strategies, ensuring resilience and certifying the security and privacy properties of the ICT components and the complete supply chain. The tools will be deployed on a cloud platform that will follow the guidelines of the designed reference architecture.

OBJ2 - Performing advanced vulnerability assessment over ICT supply chains

BIECO is developing a set of Machine Learning based tools for advanced vulnerability assessment. The tools allow to detect accurately and forecast vulnerabilities within ICT systems, offering a ranked list of the detected ones which are based on standard metrics such as CVSS (Common Vulnerability Scoring System).

OBJ3 - Achieving resilience in ecosystems formed by unreliable components

BIECO is developing a set of methodologies and tools to improve the resilience mechanisms of ICT supply chains. For that purpose, the framework includes a tool to performs self-checks on the systems, identifying undetected vulnerabilities as well as potential software and hardware failures. In order to address the reliability of the supply chain components, a predictive virtual evaluation tool is being developed, which will allow to forecast the failures of the different components and their impact on the supply chain.

BIECO
Building Trust in Ecosystems and Ecosystem Components

Objectives of the project

OBJ4 - Extending auditing process to evaluate interconnected ICT systems

In BIECO, an extension of the usual auditing procedures is being developed, in order to deal with highly interconnected ICT systems. As in most cases it is not possible to access the individual software or hardware components, making their auditing not an option, the other parties of the supply chain have to rely on trust. To solve this issue, BIECO runs a simulation of the different components of the ICT supply chain, evaluating their behaviour within the ecosystem in a predictive manner and in a virtual environment.

OBJ5 - Provide advanced risk analysis and mitigation strategies that support a view of the complete ICT supply chain

Managing the risks of the supply chain requires ensuring the security, integrity, and resilience of its components. Cyber supply chain risks may include insertion of counterfeits, tampering, theft, insertion of malicious software and hardware, as well as poor development practices that could impact the supply chain. BIECO is developing a tool for automatic and dynamic risk analysis of ICT supply chains that addresses these aspects, and also offer support for cyber-physical systems and the possible impact of their vulnerabilities on safety. The tool can identify those systems/components that are most vulnerable and might cause the greatest organizational impact, if compromised. Furthermore, it visually represents the attack paths, as well as the interactions between components when attacks are exploited. Once the risk analysis is performed, a set of mitigation strategies and measures will be proposed, including security , privacy and accountability aspects.

OBJ6 - Perform evidence-based security assurance and a harmonized certification for ICT systems

BIECO developed a proof-of-concept of a certification methodology based on different security standards such as Common Criteria, ISO 31000 and ISO 27000, providing a set of security claims and objective security metrics to allow mutual recognition and to harmonize the security levels, especially across different sectors. This was achieved by combining risk assessment and testing to perform the assessment, which lead to an evidence-based security measurement of an ICT system. The basis of the certification methodology is an extension of the ARMOUR methodology and defines a series of measurable metrics and security claims. Moreover, the methodology was extended to capture the complexity of ICT systems and it is instantiated using tools developed within the project and open-source tools to automate the process and deal with security changes, leading to a complete security certification framework, able to manage the security during the whole ICT lifecycle.

OBJ7 - Industrial validation of BIECO's framework within IoT ecosystems

The scope of the project is wide reaching and fundamental for the continuous evolution of interconnected ICT systems in general, including IoT ecosystems, and the industries involved in the project in particular. Hence, an important objective is to demonstrate its results in three realistic scenarios, validating BIECO's advances from both a technological and business perspective. Based on the results, the project will demonstrate tangible advances regarding how to ensure security and trust across the whole ICT supply chain. It will also validate the ways in which these advances translate to business benefits for the stakeholders of the energy, finance and industrial sectors.

Project status

WP1 - Project Management

Several technical project committee meetings were organized to ensure that the common vision of BIECO was aligned amongst all partners and to solve any blocking issues throughout the developments of the first 18 months. An initial risk assessment was carried out and a first data management plan was also elaborated.

WP2 - Architecture, Requirements, and Use Case Definition

This work package was successfully concluded at 18 month, with three main outputs being achieved.

These consisted in:

- the definition of the project requirements goals, functional/non-functional requirements and success criteria
- the definition of the three main use cases, along with an additional pre-demonstration use cases for 18 month

two versions of the overall BIECO architecture, the initial version and the finalized version including the entire flow from design to runtime and the specification of the component interactions

WP3 - Vulnerabilities Management

The first two tasks of this WP were concluded, with the main results being:

- the State-of-the-art analysis for vulnerability management
- the Data Collection Tool , in the context software vulnerabilities dataset, which was also already integrated with the BIECO platform for 18 month

The tasks 3.3 and 3.4 are still ongoing, with active developments of the vulnerability forecasting and the vulnerability propagation tools, respectively.

WP4 - Development of Resilient Systems

All the tasks of this work package are still ongoing.

- for task 4.1, a first study of research elements in the area of SafeAI and failure detection has been carried out, which can potentially contribute to the goals of this task. Additionally, a connection to task 3.2 has been identified
- in task 4.2, a method for predictive simulation applicable for multiple trust concerns (including technical and ethical) has been developed, along with a review of failure prediction state-of-the-art models
- in task 4.3 the initial concept for self-adaptation with the support of predictive simulation has been developed, with an initial run over the pre-demonstration scenario of 18 month

Project status

WP5 - Methods and Tools for Auditing complex systems

Both tasks of this Work package are currently ongoing.
The definition of the runtime auditing framework has been carried out, several bi-weekly meetings were organized and the results were compiled in Deliverable 5.1.
Additional work has been carried out to organize the overall auditing knowledge through semantic technology supporting the auditing framework.
This framework had already been integrated with the orchestrator in the BIECO platform and the corresponding interfaces tests through message exchanges.
Furthermore, a first version of the domain-specific language for the development of the digital twin models has been created.

WP6 - Risk Analysis and Mitigation Strategies

Three tasks from this WP have been successfully concluded:

- Methodology for dynamically estimating risks in ICT supply chains
- Visual tools for risk threats and hazard analysis for security and safety
- MUD (Manufacturer Usage Description) files generated

Regarding the task 6.1, the ResilBlockly tool was fully specified in Deliverable 6.1, being capable of threat and hazard analysis, modelling risk-related concepts and visually matching risks to each component while being able to represent attack paths, interactions and when attacks are exploited.
Then, in the task 6.2 a User Guide for the Resilblockly tool was generated in the form of Deliverable 6.2, assisting the user in conducting two complementary risk assessments, one HAZOP-based, more safety oriented, and the other leveraging the integration with online catalogues of threats to security such as CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification), NVD (National Vulnerability Database) and scoring systems like CVSS (Common Vulnerability Scoring System). An early validation of Resilblockly was also carried out, along with a definition of an extended MUD file and its integration with the tool.
Lastly, in the task 6.3 an Integrated dependability assurance methodology was produced, being documented in Deliverable 6.4.
Ongoing work continues in the task 6.4, focusing on a non-repudiation and reliability tool named LogForgeryBlocker.

Project status

WP7 - Security and Privacy Claims

The following two main outputs have been achieved:

- an objective, measurable, testable and general set of security and privacy claims that was collected and reported in Deliverable 7.1, comprising a total of 75 classified into six categories following the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) approach.
- a full security evaluation methodology that was defined and documented in Deliverable 7.2. This methodology enables the evaluation and certification of the security of an ICT system, addressing the weaknesses that current certification and evaluation schemas have.

As far as ongoing work goes, in task 7.3 the developments have been focused on the testing and the risk estimation phases of the methodology. A first prototype of the SecurityScorer tool was implemented to calculate a security score from the outputs of the testing tools: Graphwalker, fuzzing tool and GROOT. GraphWalker is also being improved to generate a test suite automatically from a model, with an initial validation being carried out for the pre-demonstration.

WP8 - Integration, Pilots, and Validation

All the four tasks of this work package are currently ongoing.

- Starting from task 8.1, the main outcome so far has been the specification of BIECO's verification and testing strategy in Deliverable 8.1.
- The BIECO platform has been actively under development in task 8.2, already resulting a mature software infrastructure comprising the BIECO orchestrator and the BIECO User Interface. This infrastructure is being used to integrate the different tools developed in the project as they become available, with several already integrated for the 18 month pre-demonstration Use Case 4.
- While task 8.4 officially started only at 19 month, additional was allocated in the preparation of a pre-demonstration case for 18 monthas a way to support the early validation of the tools developed up until this point, as well as their integration with the BIECO platform and thus facilitating the correction of any potential issues.

WP9 - Dissemination, Communication, and Exploitation

For this work package, one of the main results so far has been the initial version of the dissemination strategy.

Another important result was the deployment of the BIECO website (www.bieco.org) and the social media pages dedicated to BIECO, including Facebook, Twitter, LinkedIn, Instagram and YouTube.

Many communication activities were carried out by the consortium and a detailed initial exploitation plan has been setup which will be later updated by the end of the project.

A number of technical meetings were hold in this first period, as specified in work package 1, concerning Scientific/Technical management.

Publications

BIECO RUNTIME AUDITING FRAMEWORK

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational, CISIS - ICEUTE 2021, Advances in Intelligent Systems and Computing, vol 1400, pp 181–191, 2021
Authors: Antonello Calabrò, Emilia Cioroaica, Said Daoudagh and Eda Marchetti

DEFINING THE BEHAVIOR OF IOT DEVICES THROUGH THE MUD STANDARD: REVIEW, CHALLENGES AND RESEARCH DIRECTIONS

Publication info : IEEE Access, vol. 9, pp. 126265-126285, 2021
Authors: José L. Hernández Ramos, Sara N. Matheu, Angelo Feraudo, Gianmarco Baldini, Jorge Bernal Bernabe, Poonam Yadav, Antonio Skarmeta and Paolo Bellavista

THE CHALLENGES OF SOFTWARE CYBERSECURITY CERTIFICATION

Publication info : IEEE Security & Privacy, vol. 19, no. 1, pp. 99-102, Jan.-Feb. 2021
Authors: José L. Hernández-Ramos, Sara N. Matheu and Antonio Skarmeta

BASIC ASPECTS IN REDUNDANCY-BASED INTRUSION TOLERANCE

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational , CISIS - ICEUTE 2021 , Advances in Intelligent Systems and Computing, vol 1400, pp 192–202, 2021
Authors: Felicita Di Giandomenico, Giulio Masetti (both ISTI-CNR Pisa)

Publications

DATA BASED MESSAGE VALIDATION AS A SECURITY CORNERSTONE IN LOOSE COUPLING SOFTWARE ARCHITECTURE

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational, CISIS - ICEUTE 2021, Advances in Intelligent Systems and Computing, vol 1400, pp 214–223 ,2021
Authors: Oliviu Matei, Rudolf Erdei, Daniela Delinschi, Laura Andreica

A COMPARATIVE STUDY OF THE MOST IMPORTANT METHODS FOR FORECASTING THE ICT SYSTEMS VULNERABILITIES

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational,CISIS - ICEUTE 2021, Advances in Intelligent Systems and Computing, vol 1400, pp 224-233, 2021
Authors: Ovidiu Cosma, Mara Hajdu-Macelaru, Petrica Pop-Sitar, Cosmin Sabo, Ioana Zelina

COMPARISON OF SAFETY AND SECURITY ANALYSIS TECHNIQUES

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational, CISIS - ICEUTE 2021 , Advances in Intelligent Systems and Computing, vol 1400, pp 234–242, 2021
Authors: Emilia Cioroaica, Smruti Ranjan Kar, and Ioannis Sorokos

ON AUTONOMOUS DYNAMIC SOFTWARE ECOSYSTEMS

Publication info : IEEE Transactions on Engineering Management, pp 1-15, 2021
Authors: Rafael Capilla ,Emilia Cioroaica, Barbora Buhnova, Jan Bosch, Göteborg Sweden

Publications

A SURVEY ON THE STATE OF THE ART OF VULNERABILITY ASSESSMENT TECHNIQUES

Publication info : 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational , CISIS - ICEUTE 2021 , Advances in Intelligent Systems and Computing, vol 1400, pp 203-213, 2021
Authors: Eva Sotos Martínez, Nora M. Villanueva ,Lilian Adkinson Orellana

BRIDGING TRUST IN RUNTIME OPEN EVALUATION SCENARIOS

Publication info : Advances in Model and Data Engineering in the Digitalization Era, MEDI 2021 , Communications in Computer and Information Science, vol 1481, pp 112-120, 2021
Authors: Emilia Cioroaica, Barbora Buhnova, Eda Marchetti, Daniel Schneider, and Thomas Kuhn

GOALS WITHIN TRUST-BASED DIGITAL ECOSYSTEMS

Publication info :2021 IEEE/ACM Joint 9th International Workshop on Software Engineering for Systems-of-Systems and 15th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (SESoS/WDES), pp. 1-7, 2021
Authors: Emilia Cioroaica, Akanksha Purohit, Barbora Buhnova, and Daniel Schneider

Published by
Technical University from Cluj-Napoca
Victoriei, nr. 76
Baia Mare
Romania

On behalf of the BIECO consortium

Contact
office@bieco.org

https://www.bieco.org

Building Trust in Ecosystems and Ecosystem Components