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. 1

October 2021

IN THIS ISSUE

BIECO

Building Trust in Ecosystems
and Ecosystem Components

DEAR READER,

Welcome to the first newsletter of the BIECO project.
We had the kickoff of the BIECO project in September 2020 with the aim to develop a framework that enables measurable, risk-based trust while developing, deploying, and operating complex interconnected ICT systems. We aim to achieve this by handling the reliability and trust aspects of ecosystem participants (ICT systems, ICT system components and actors) within the supply chain. The framework, composed by a set of tools and methodologies, will address the challenges related to vulnerability management, resilience, auditing of complex systems, risk analysis, mitigation strategies and security certification harmonization. The validation of BIECO will be achieved through the application of the tools and methodologies to three use cases (energy, finance, and industry), which include also complex IoT ecosystems.
Since the beginning of our project, we have worked on detailed descriptions of relevant scenarios and the cybersecurity risks and threats encountered in a software supply chain, along with a list of expected improvements, detailed definition and specification of the use cases, and the design of the overall system architecture based on smart production components that is able to support the identification of risks and threats in the software supply chain according to functional requirements.

I hope you 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

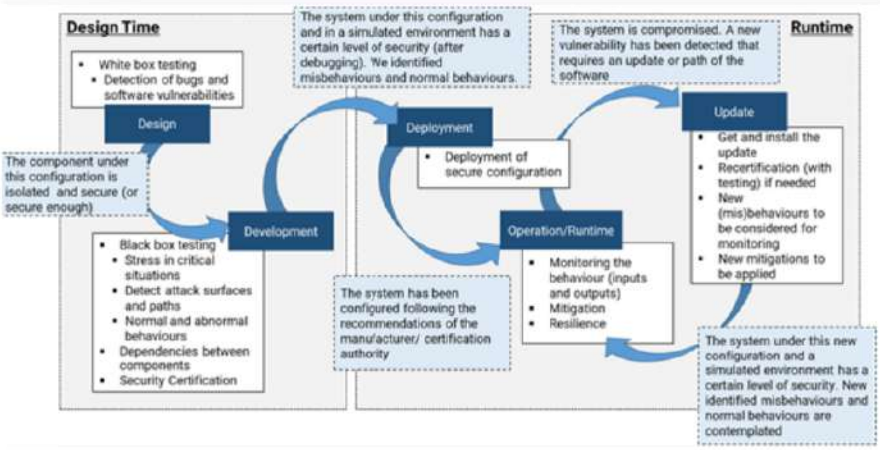
BIECO – Building Trust in Ecosystems and Ecosystem Components

The rationale behind BIECO's concept is to deliver a framework for improving trust and security within ICT supply chains. These are complex ecosystems comprising several heterogeneous technologies, processes, actors (e.g., end-users, software or hardware providers and organizations) and resources, all of which generate or exchange data forming extremely complex information management systems.

We aim to achieve this by handling the reliability and trust aspects of ecosystem participants (ICT systems, ICT system components and actors) within the supply chain.

Project description

The rationale behind BIECO's concept is to deliver a framework for improving trust and security within ICT supply chains. These are complex ecosystems comprising several heterogeneous technologies, processes, actors (e.g., end-users, software or hardware providers and organizations) and resources, all of which generate or exchange data forming extremely complex information management systems.



- White box testing
  - Detection of bugs and software vulnerabilities

The component under this configuration is isolated and secure (or secure enough)

- Black box testing
  - Stress in critical situations
  - Detect attack surfaces and paths
  - Normal and abnormal behaviours
- Dependencies between components
- Security Certification

The system under this configuration and in a simulated environment has a certain level of security (after debugging). We identified misbehaviours and normal behaviours.

- Deployment of secure configuration

The system has been configured following the recommendations of the manufacturer/ certification authority

- Monitoring the behaviour (inputs and outputs)
- Mitigation
- Resilience

The system is compromised. A new vulnerability has been detected that requires an update or path of the software

- Get and install the update
- Recertification (with testing) if needed
- New (mis)behaviours to be considered for monitoring
- New mitigations to be applied

The system under this new configuration and a simulated environment has a certain level of security. New identified misbehaviours and normal behaviours are contemplated

The goal is to instantiate the framework iteratively in order to enable a continuous assessment and improvement of ICT supply chain's security, given the speed at which the cybersecurity landscape evolves with new threats emerging every day.

To realize this vision, BIECO's architecture will thus contain a set of interoperable tools and methodologies capable of ultimately ensuring the trustworthy execution of systems and system components within complex digital ecosystems.

From design to runtime, vulnerabilities and failures are detected, evaluated and mitigated together with prompt reactions that ensure the ultimate trustworthy execution of systems and system components. In order to open the path towards future development and for enabling the possibility to keep up to agile technological progress supported by runtime updates of systems (including safety-critical systems), we further on design the BIECO architecture with expandability in mind.

One possibility in this direction will be that based on detected deviations, runtime updates of systems can be accommodated through a natural extension of the BIECO framework, including the feedback of information to the design time for continuous improvement..

BIECO will offer a holistic approach for building and validating several technologies and methodologies that are specifically oriented to foster security and trust within ICT ecosystems. To better illustrate how BIECO intends to address these challenges along the entire lifecycle of the ICT supply chain, the above figure shows broadly the interaction flow between the different phases of the lifecycle, as well as the core functionalities involved.

Consortium

UNINOVA – INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIAS

UNINOVA Institute is a multidisciplinary, independent, and non-profit research institute employing 180 persons, located in the metropolitan area of Lisbon.

CONSIGLIO NAZIONALE DELLE RICERCHE

The Italian National Research Council (CNR) is the main public research body of Italy, carrying out, promoting and transferring multidisciplinary research through a network of more than one hundred institutes all over the Country.

FRAUNHOFER INSTITUTE FOR EXPERIMENTAL SOFTWARE ENGINEERING IESE

Fraunhofer is Europe's largest application-oriented research organization. The Fraunhofer-Institute for Experimental Software Engineering (FhG IESE) in Kaiserslautern, Germany, founded in January 1996, is led by Prof. Dr. Peter Liggesmeyer.

GRADIANT – ICT R&D CENTER

GRADIANT – Fundación Centro Tecnolóxico de Telecomunicacións de Galicia. Gradiant is a private non-profit foundation that aims to improve the competitiveness of companies by transferring knowledge and technologies in the fields of connectivity, intelligence and security.

Consortium

7BULLS

7BULLS is a private Polish company specializing in software development and integration of IT systems. Founded in 1999, 7bulls was listed among the winners of Deloitte Technology Fast 50 Central Europe in 2012.

RESILTECH

ResilTech is an ICT consultancy company operating in the field of critical systems since early 2008; it is an SME company (approx. 45 employees) that integrates the experiences of R&D in resilient computing with specific industrial skills.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

The Technical University of Cluj-Napoca (UTCN) was founded in 1777 and activates as a higher education institution since 1948. The Technical University of Cluj-Napoca, an "Advanced Research and Education University" is today a tertiary educational institution having both tradition and national and international recognition.

TTTECH

TTTech Auto AG provides solutions for the challenges of future vehicle generations. The company specializes in safe software and hardware platforms for automated driving and beyond, applicable in series production programs.

HOLISUN

Founded in 2001, HOLISUN emerged on the Romanian market as a response to the increasing demand of high quality software products. Following the globalization process and the expansion of world trade, Holisun has developed partnerships with companies all over Europe and America:

UNIVERSIDAD DE MURCIA

The Universidad de Murcia (University of Murcia) (UMU) is a large, international institution which is a reference center for higher education in the Region of Murcia (south-eastern Spain). UMU focuses on academic excellence and plays a very important role in research, teaching and innovation.

Work Packages

WP1 - Project Management

The aim is to ensure timely and efficient project execution, according to the budget and the overall project objectives.

WP2 - Architecture, Requirements, and Use Case Definition

Detailing the requirements of the project together with its Key Performance Indicators. Defining and detailing the use cases that will validate the work to be developed. Designing the architecture.

WP3 - Vulnerabilities Management

Analyze the state of the art to incorporate the latest advances in detection, forecasting and propagation of vulnerabilities. Compile a representative dataset of software vulnerabilities. Provide advanced tools to detect and forecast accurately vulnerabilities in ICT systems and components. Provide an advanced tool to analyze the propagation of vulnerabilities across the ICT supply chain.

WP4 - Development of Resilient Systems

Tools and methods will be developed for supporting creation of resilient systems w.r.t security attacks and vulnerabilities.

WP5 - Methods and Tools for Auditing complex systems

This work package will focus on the development of techniques, methods and tools supporting the audit activity in the BIECO framework. Auditing includes retrieval of data from the field, such as data regarding the usage mode of an ICT system subject to runtime adaptation through delivery of software updates.

WP6 - Risk Analysis and Mitigation Strategies

This work package researches and develops a methodology for continuous risk assessment process on the ICT supply chain, such that the system is continuously analyzed for potential weaknesses, and corresponding mitigation strategies can be enacted using BIECO solutions.

WP7 - Security and Privacy Claims

Identify suitable security and privacy metrics and claims to evaluate the security and privacy of a system. Develop a security certification methodology using the identified security and privacy metrics and claims.

WP8 - Integration, Pilots, and Validation

Develop a cloud platform, according to the reference architecture of WP2, that host the verification and validation activities within BIECO, as well as the applications and datasets of the pilots. Develop the business case implementations.

Provide a set of front-end application.

WP9 - Dissemination, Communication, and Exploitation

Make sure that dissemination of results is pro-actively covered and Data Management is addressed.

Set-up and apply a dissemination strategy to spread BIECO results EU-wide. Identify and implement exploitation mechanisms with the partners and other EU industries.

Use Cases

The methodologies and tools provided by BIECO's framework will be evaluated in four use cases from different sectors.

USE CASE 1: ICT GATEWAY

The ICT gateway is a component intended for Smart Grids that acts as mediator between data sourcing and actuation subsystems and domain applications.

USE CASE 2: INVESTMENT PORTFOLIO OPTIMIZATION PLATFORM

This use case aims at providing security guarantees to a Machine Learning based platform that is used for investment portfolio optimization within a financial ecosystem.

USE CASE 3: SMART MICROFACTORY

The smart microfactory represents an ongoing evolution from traditional factories to a fully connected, flexible and reconfigurable systems that can learn, self-adapt and self-optimize in real or near real-time to frequently changing product and production requirements.

USE CASE 4: AUTONOMOUS NAVIGATION PRE-DEMO

The autonomous navigation use case is meant to serve as a pre-demonstration environment for the internal workshop to be organized around M12. It entails the ensurance of trust and safety in the context of the addition/update of a new module within the navigation environment, more specifically the local planner.

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

BIECO
Building Trust in Ecosystems
and Ecosystem Components