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

BIECO

Building Trust in Ecosystems and Ecosystem Components

No. 3
July 2023

DEAR READER,

Welcome to the third newsletter of the BIECO project, exclusively dedicated to the BIECO platform and its array of powerful tools.

BIECO boasts an impressive collection of over 15 distinct tools that comprehensively span the software lifecycle, ranging from initial design to real-time operation. Notably, the majority of these tools have been integrated into a unified platform, that facilitates their interoperability and orchestration in easy deployable toolchains tailored to meet specific business needs.

We trust that the content presented in this newsletter will captivate your interest and offer valuable insights. For more comprehensive information, we encourage you to visit our project website, stay connected with us through social media channels, or contact us directly.

Thank you for your continued support and enthusiasm.

Warm regards,

Prof. dr. Jose Barata

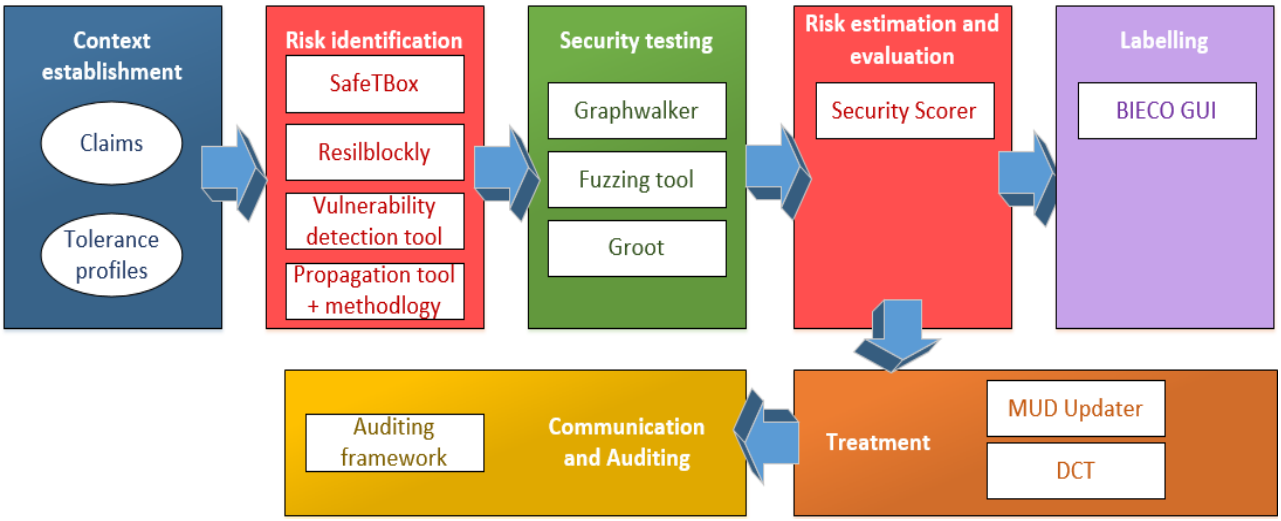
BIECO
Building Trust in Ecosystems and Ecosystem Components

The BIECO Approach

BIECO leverages a combination of state-of-the-art artificial intelligence, digital twins, simulation and static analysis to address the following key areas:

- Vulnerability Assessment and Management
- Risk Assessment and Mitigation
- Resilience Mechanisms
- Security Certification and Testing
- Runtime Auditing of ICT Ecosystems

Given the cross-sectorial nature of the cybersecurity challenges currently faced in Europe, BIECO's validation takes place across three distinct business cases spanning different activity sectors, namely Energy (ICT Gateway from Resiltech, Pisa, Italy), Manufacturing and Electric Mobility (Smart Microfactory from IFEVS, Turin, Italy) and Finance (AI Investment Platform from 7Bulls, Warszawa, Poland).



Security Evaluation Methodology

BIECO defines a security evaluation methodology for complex systems. It is intended to serve as a basis for the security certification, providing the following advantages:

- Basic set of claims from standards and best practices
- Objective, automated, flexible and empirical evaluation combining testing and risk assessment
- Different security for different contexts using tolerance profiles
- Safety, operational, economical, privacy and legislative aspects considered
- Visual and dynamic label to show the results to users
- Security configuration recommended after assessment
- Auditing process to detect suspicious behaviors and restart the evaluation

Vulnerability Detection Tool

The Vulnerability Detection Tool integrated in BIECO detects vulnerabilities within the source code by static analysis and the use of ML techniques.

One of the main factors which can help attackers to corrupt a system is the existence of vulnerabilities in the code. Thus, it is vital to execute a suitable vulnerability assessment to the code in a quick way. The tool allows companies to offer an extra level of security by detecting possible security breaches within the source code in the form of vulnerabilities in an automatic way.

Vulnerability Exploitability Forecasting Tool

The Vulnerability Exploitability Forecasting Tool provides the probability of a known published vulnerability to be exploited in a time window.

Once a known vulnerability is detected within the source code, it is necessary to focus the efforts to mitigate its possible attacks. From BIECO, we are conscious that experts needs to prioritize possible attacks for a more effective results. Thus, the exploitability forecasting tool offers an assessment of a given vulnerability, by indicating if it can be exploited in the next 3, 6 or 12 months from the date of publication.

Vulnerability Propagation Tool

The main goal of the Vulnerability Propagation Tool is to find and indicate the components or elements a single vulnerability can affect and, therefore, its path within the source code.

Sometimes, the most obvious way to reach a vulnerability is by knowing its location. But vulnerabilities can propagate through the source code, offering open doors to cyber attackers to exploit them. Calculating the path affected by a vulnerability helps the cyber security expert to prioritize its mitigation not only directly, but their possible alternative access in the source code.

Fuzzing Tool

The Fuzzing Tool finds through a dynamic analysis, security weaknesses in a REST API which might be related to a possible vulnerability in the system.

The existence of this tool within the BIECO framework allows companies to offer an extra level of security, using the description of the API to analyze which request can lead to an undesired response.

ResilBlockly

ResilBlockly is a tool for Model-Based Design and Safety + Security Assessment of complex System-of-Systems. It supports the early identification of vulnerabilities, it allows prevention and prompt intervention to reduce the likelihood of exploitation by attackers, it supports in activities required for the compliance with security standards.

Some of its new features in BIECO are security threat modelling, risk analysis, and graphical representation of attack paths, integration with open catalogues of vulnerabilities, weaknesses and attack patterns.

Data Collection Tool

The Data Collection Tool (DCT) is a repository of vulnerabilities, weaknesses, exploits, Manufacturer Usage Description (MUD) files and bugs.

The vulnerabilities data structure is modeled based on the Common Vulnerabilities and Exposures (CVE) and Common Platform Enumerations (CPE) from the National Vulnerability Database (NVD), and on the Common Weakness Enumeration from MITRE. The exploits data structure is designed to keep information gathered from the Exploit Database. The DCT has a web interface and communicates with the other BIECO tools through a REST API.

Vulnerabilities Forecasting Tool

The Vulnerabilities Forecasting Tool (VFT) provides an estimation of the number of bugs and vulnerabilities to be expected for the main software components used within complex ICT systems in timeframes of 1, 2, 3, 6 and 12 months. The VFT has a web interface and a REST API.

DAEMON

DAEMON is an ontology that formally models knowledge about Monitoring and System of Systems (SoS) domains. The main objective of DAEMON is to provide stakeholders with functional and non-functional properties of different parts of SoS, and the corresponding definition of concrete monitoring rules.

Failure Prediction Tool

The Failure Prediction Tool (FPT) monitors the logs of the components that make up one or more systems at run time and forecasts their failures. FPT classifies each log message using a neural network model, then calculates an alert level using exponential smoothing. The tool supports model plugins and parameter adjustments.

Runtime Monitoring

The Runtime Monitoring provides runtime evaluation of functional and non-functional properties, notification of properties violations and countermeasures enforcement.

SecurityScorer

SecurityScorer is a tool that analyzes the outputs of the system testing tools and system description to evaluate numerical results describing system safety.

LogForgeryBlocker

LogForgeryBlocker enhances the security of the application logs providing non-repudiation thanks to blockchain technology.

SafeML

SafeML is a collection of statistical measures which evaluate whether samples from two datasets are likely to belong to the same distribution. The measures are based on the Empirical Cumulative Distribution Function and compare in various ways the difference across the two datasets.

GROOT

ICT systems are currently adopting different means of managing personal data. Effective and efficient validation methods must be applied, considering the peculiarity of the reference legal framework, i.e., the General Data Protection Regulation (GDPR). GROOT is based on a combinatorial testing methodology for assessing the compliance with the GDPR in the access control domain.

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