BIECO
Building Trust in Ecosystems and Ecosystem Components

CISIS 2021 - BILBAO (SPAIN)

22-24 SEPTEMBER 2021

Blended Conference - International Joint Conferences
SOCO-CISIS-ICEUTE

SPECIAL SESSION

Building Trust in Ecosystems and Ecosystem Components

TOPICS

- Vulnerability detection
- Vulnerability propagation
- Exploitability forecasting
- Vulnerability forecasting
- Security claims
- Auditing mechanisms
- Predictive simulation
- Runtime monitoring

SESSION CHAIRS

- Oliviu Matei, HOLISUN (RO)
- Jose Barata, UNINOVA (PT)
- Petrica Pop, Technical Univesity of Cluj-Napoca (RO)

Publications

BIECO
Building Trust in Ecosystems and Ecosystem Components

Title: Bridging Trust in Runtime Open Evaluation Scenarios

Authors: Emilia Cioroaica, Barbora Buhnova, Eda Marchetti, Daniel Schneider, and Thomas Kuhn

Abstract:
Solutions to specific challenges within software engineering activities can greatly benefit from human creativity. For example, evidence of trust derived from creative virtual evaluation scenarios can support the trust assurance of fast-paced runtime adaptation of intelligent behavior. Following this vision, in this paper, we introduce a methodological and architectural concept that interplays creative and social aspects of gaming into software engineering activities, more precisely into a virtual evaluation of system behavior. A particular trait of the introduced concept is that it reinforces cooperation between technological and social intelligence.

Title: Goals within Trust-based Digital Ecosystems

Authors: Emilia Cioroaica, Akanksha Purohit, Barbora Buhnova, and Daniel Schneider

Abstract:
Within a digital ecosystem, systems and actors form coalitions for achieving common and individual goals. In a constant motion of collaborative and competitive forces and faced with the risk of malicious attacks, ecosystem participants require strong guarantees of their collaborators' trustworthiness. Evidence of trustworthy behavior derived from runtime executions can provide these trust guarantees, given that clear definition and delimitation of trust concerns exist. Without them, a base for negotiating expectations, quantifying achievements and identifying strategical attacks cannot be established and attainment of strategic benefits relies solely on vulnerable collaborations.
In this paper we examine the relationship between goals and trust and we introduce a formalism for goal representation. We delimit the trust concerns with anti-goals. The anti-goals set the boundaries within which we structure the trust analysis and build up evidence for motivated attacks.

Title: BIECO Runtime Auditing Framework

Authors: Antonello Calabro, Emilia Cioroaica, Said Daoudagh, and Eda Marchetti

Abstract:
Context: Within digital ecosystems avoiding the propagation of security and trust violations among interconnected parties is a mandatory requirement, especially when a new device, a software component, or a system component is integrated within the ecosystem.
Objective: The aim is to define an auditing framework able to assess and evaluate the specific functional and non-functional properties of the ecosystems and their components.
Method: In this paper, we present the concept of predictive simulation and runtime monitoring for detecting malicious behavior of ecosystem components.
Results and Conclusion: We defined a reference architecture allowing the automation of the auditing process for the runtime behavior verification of ecosystems and their components. Validation of the proposal with real use-cases is part of the future BIECO's activities.

Title: Comparison of Safety and Security analysis techniques

Authors: Emilia Cioroaica, Smruti Ranjan Kar, and Ioannis Sorokos

Abstract:
Growing adoption of new technological advancements within the automotive domain is highlighting multiple safety and security concerns. Aiming at reducing the errors humans make on the roads, deployment of novel and intelligent technological solutions are likely to introduce multiple vulnerabilities that can be exploited by attackers. In automated driving scenarios, in particular, vehicles communicating with each other using ad-hoc networks are becoming vulnerable to specialized cyber-physical attacks. A single compromised vehicle will provide an attack entry point for all linked vehicles, putting lives of passengers at risk. In this paper, we present an overview and evaluation of safety and security analysis methods applied on a use case from the automotive domain.

Title: A comparative study of the most important methods for forecasting the ICT systems vulnerabilities

Authors: Ovidiu Cosma, Mara Hajdu-Macelaru, Petrica Pop-Sitar, Cosmin Sabo, Ioana Zelina

Abstract:
Nowadays, companies are facing plenty of IT secure attacks and to guarantee safe, untroubled, and continuous functioning of their business, they should detect and forecast the volume of IT security vulnerabilities and be prepared for future threats. The aim of this paper is to present a comparative study of the most important and promising methods for forecasting the ICT systems vulnerabilities.

Title: Data Based Message Validation as a Security Cornerstone in Loose Coupling Software Architecture

Authors: Oliviu Matei, Rudolf Erdei, Daniela Delinschi, Laura Andreica

Abstract:
Far from being a hype, cybersecurity is one of the most important aspects of our daily lives. Gaining trust in a cyber system is not an easy task, as problems and security hazards can be willingly or unwillingly introduced in it. This paper describes a security-centric architecture of the communication bus in loosely coupled heterogeneous systems. The concept is modular and designed having in mind the fulfillment of the principles of Service Oriented Architecture as well as the common functional and non-functional requirements regarding such communications.