IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 24 July 2025, accepted 18 August 2025, date of publication 25 August 2025, date of current version 29 August 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3602292

APPLIED RESEARCH

A Knowledge-Driven Approach to Threat Validation and Security Reasoning in Modular Systems

LAURA PANDOLFO, (Member, IEEE), GIORGIO CORONA, DARIO GUIDOTTI, (Member, IEEE), AND LUCA PULINA, (Member, IEEE)
DUMAS, University of Sassari, 07100 Sassari, Italy

Corresponding author: Laura Pandolfo (lpandolfo@uniss.it)

This work was supported by the European Union's (EU) Horizon Europe research and innovation programme under project SECURED "Scaling Up Secure Processing, Anonymization and Generation of Health Data for EU Cross Border Collaborative Research and Innovation," Grant Agreement No. 101095717.

ABSTRACT Modular systems are increasingly employed in critical application domains such as healthcare, smart cities, and Industry 4.0 platforms, where dynamic integration of components poses substantial challenges in ensuring consistent and secure operation. Validating system configurations against known vulnerabilities and threats requires formal, scalable, and explainable approaches. This paper presents a knowledge-driven framework designed to support the validation of modular systems with respect to cybersecurity threats and consistency constraints. Our approach leverages domain-specific ontologies built from well-established threat and vulnerability taxonomies and encodes inference rules to automatically detect potential threats and recommend mitigation strategies. The framework, which includes a reasoning engine and a user-friendly graphical interface providing transparent and traceable explanations for each identified threat, is applied to a modular platform for privacy-preserving, decentralized processing of health data across European institutions. While this composable architecture enables multiple stakeholders to develop, deploy, and maintain specialised components fostering scalability and flexibility, it also introduces critical risks related to architectural coherence and security enforcement. In this context, our framework ensures a human-interpretable assessment of the system's security posture, even in the presence of