Onto-CARMEN: Ontology-driven approach for Cyber-Physical System Security Requirements meta-modelling and reasoning

Carlos Blanco[1,2][0000−0001−9001−0904], David G.Rosado[2][0000−0003−4613−5501], Ángel Jesús Varela-Vaca[3][0000−0001−9953−6005], María Teresa Gómez-López[3][0000−0002−3562−875X], and Eduardo Fernández-Medina[2][0000−0003−2553−9320]

[1] ISTR Research Group. Dept. de Ingeniería Informática y Electrónica, Universidad de Cantabria, Spain
Carlos.Blanco@unican.es

[2] GSyA Research Group, Dpto. Tecnologías y Sistemas de Información, Universidad de Castilla-La Mancha, Ciudad Real, Spain
David.GRosado@uclm.es, Eduardo.Fdezmedina@uclm.es

[3] IDEA Research Group, Universidad de Sevilla, Escuela Técnica Superior de Ingeniería Informática, Dpto. Lenguajes y Sistemas Informáticos, Sevilla, Spain
ajvarela@us.es,maytegomez@us.es

Keywords: Cyber-Physical System, Cybersecurity, Security, Configuration Models, Security Requirements, Security Verification, Diagnosis

Published in: Internet of Things, Vol. 24, pp. 100989, 2023

Impact Factor: JCR: 5,9 (Q1) - Position: 35/158 - Area: Computer Science / Information Systems. SJR (SCImago Journal and Rank): 1,474 (Q1)

DOI: https://doi.org/10.1016/j.iot.2023.100989

Abstract. In the last years, Cyber-physical systems (CPS) have attracted substantial mainstream, especially in the industrial sector, since they have become the focus of cyber-attacks. CPS are complex systems that encompass a great variety of hardware and software components with a countless number of configurations and features. For this reason, the construction, validation, and diagnosis of security in CPS become a major challenge. An invalid security requirement for the CPS can produce partial or incomplete configuration, even misconfigurations, and hence catastrophic consequences. Therefore, it is crucial to ensure the validation of the security requirements specification from the earlier design stages. To this end, OntoCarmen is proposed, a semantic approach that enables the automatic verification and diagnosis of security requirements according to the ENISA and OWASP recommendations. Our approach provides a mechanism for the specification of security requirements on top of ontologies, and automatic diagnosis through semantic axioms and SPARQL rules. The approach has been validated using security requirements from a real case study.

Summary

Figure 1 shows an overview of our proposal. Initially, it is necessary to describe the security requirements involving the Cyber-Physical System (CPS) components and security aspects. For this purpose, a semantic model for CPS security requirements is formalized. The ontology allows the creation of individuals as new instances of security requirements.

Validation of these requirements is then performed through semantic rules, identifying the validity of the requirement as valid (OK) or invalid (KO). In the case of an invalid security requirement, the semantic rules allow a diagnosis providing corrective actions to transform it into valid.

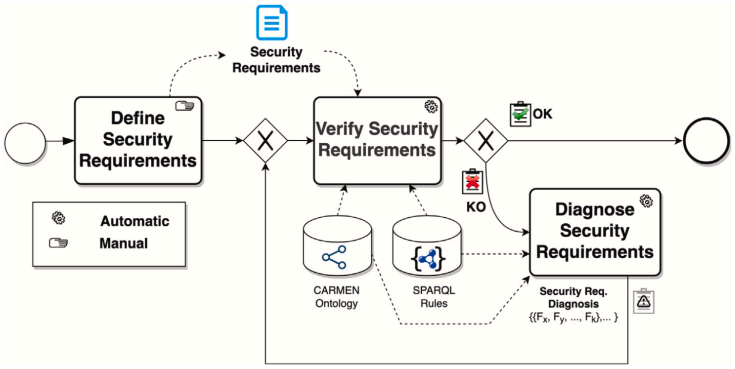

Fig. 1. Overview

The main components of the proposal are briefly presented below.

Ontology

It provides a framework for defining and classifying CPS security requirements. It uses OWL (Web Ontology Language) to formally represent the elements and their relationships. This ontology includes classes such as "Security Requirement", "Asset", "Security Feature", and properties to connect these elements. In addition, it includes axioms to impose constraints and logical rules. Figure 2 shows the main classes and relationships of the ontology.

Reasoning Framework

It uses SPARQL rules to verify and diagnose safety requirements at design time. These rules allow to evaluate whether the security requirements are valid and, if not, to provide corrective actions.

Figure 3 shows an example of a SPARQL rule used to ensure that all security features using Camellia encryption are assigned a medium security level. If a security feature using Camellia has a different security level, the rule will update it to "MediumSecurityLevel".

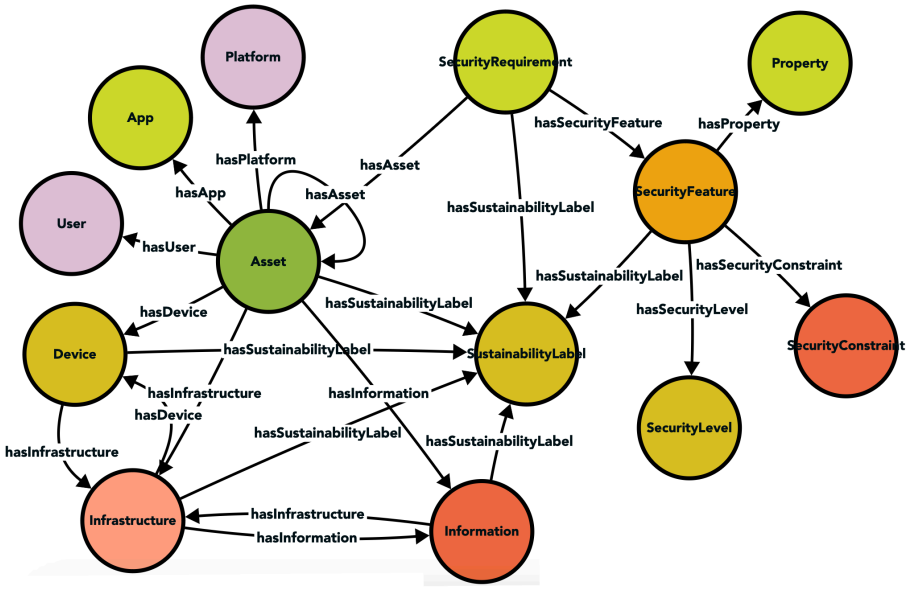

Fig. 2. Ontology

Example

We see an example (Figure 4) with the definition of a security requirement (SR1). The requirement states that the wireless communication between the temperature sensor and the microcontroller must be encrypted to maintain a high level of confidentiality. To achieve this, we have defined the Confidentiality property, which is associated with a specific type of encryption (Camellia) and a secure communication channel (HTTPS). This security feature is applied to a set of assets including the temperature sensor and the Arduino, which communicate with each other over a WLAN network using BLE or RFID. This relationship between the safety feature and the set of assets is called secure communication.

We show how the SPARQL rule discussed above is applied to the SR1 security requirement, detecting an invalid situation (since it presents a high security level) and how, after applying the rule, the security level has been changed to medium.

CamelliaRequiresMediumSecurityLevel SPARQL rule

```
DELETE {
   ?sf ontocarmen:hasSecurityLevel ?sl .
}

INSERT {
   ?sf ontocarmen:hasSecurityLevel
   ontocarmen:MediumSecurityLevel .
}

WHERE{
  ?sf a ontocarmen:SecurityFeature .
  ?sf ontocarmen:hasSecurityLevel ?sl .
  FILTER (?sl != ontocarmen:MediumSecurityLevel) .
  ?sf ontocarmen:hasSecurityConstraint ?sc .
  ?sc a ontocarmen:CamelliaCipher .
}
```

Fig. 3. Example rule

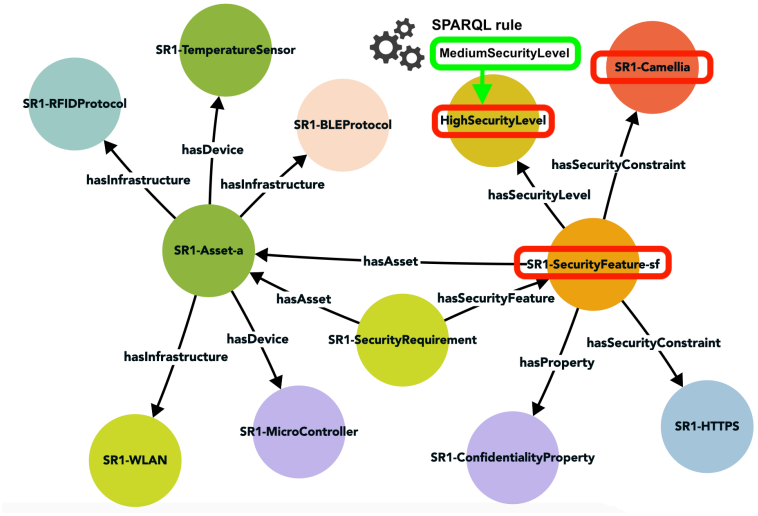

Fig. 4. Example of security requirement definition and rule application