Future Generation Computer Systems 141 (2023) 462–472

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Ontology-based approach to real-time risk management and cyber-situational awareness

Carmen Sánchez-Zas *, Víctor A. Villagrá, Mario Vega-Barbas, Xavier Larriva-Novo, José Ignacio Moreno, Julio Berrocal

ETSI Telecomunicación, Universidad Politécnica de Madrid, UPM. Av. Complutense 30, 28040 Madrid, Spain

ARTICLE INFO

Article history:
Received 29 July 2022
Received in revised form 25 November 2022
Accepted 2 December 2022
Available online 5 December 2022

Keywords:
Ontology
Cybersecurity
SPARQL Inference Notation
Anomaly
Cyber threat intelligence
Risk management

ABSTRACT

The requirement of continuous risk assessment and management is attracting growing attention because of the need of keeping risk under control. Over the years, companies are dealing with a growing number of malicious actions coming from heterogeneous sources, so risk management must be dynamic in real-time to define action strategies and validate the effectiveness of the safeguards in place. This exposure makes it imperative to use sensor-based systems to detect anomalies or to have an updated catalog of vulnerabilities to understand the situation in which the system finds itself and its level of risk. Such a wealth of heterogeneous information has led to the use of ontologies to organize data, as they allow the extraction of new concepts and behaviors, for instance, measuring the risk level of a system or generating metrics for decision support systems. This paper presents an ontology to describe different types of anomalies, merged with previously developed models for Cyber-Threat Intelligence, becoming a proposal to define real-time risk management in a converged secure environment with physical and logical elements, using these ontologies and SPARQL Rules to infer knowledge and calculate dynamically the risk level of the system.

1. Introduction

In most corporate environments it is essential to be aware of the system's risk situation, specially to keep it under control. Ideally, the objective would be to apply risk assessment and management dynamically, adapting the system response to various types of input based on data received in real time [1]. In real development environments, sources of risk continue to grow, increasing as the study deepens, which means that threat causes are numerous and highly varied, making the analysis truly complex.

According to ISO 31000 [2], which provides guidelines for managing the risk faced by organizations, the main objective of risk assessment is to create and protect value. It must be integrated, customized, inclusive, dynamic, and must consider the best available information, human and cultural factors and continual improvement through learning and experience. The described framework subsumes integration, design, implementation, evaluation, and improvement of the risk management. This process implies the establishment of the context and identifying, analyzing, evaluating, treating, and reporting risks. Following these guidelines, to monitor the system it is necessary to study a heterogeneous environment and obtaining a dynamically adaptive result.

The use of ontologies has become popular in the administration of this type of tasks, driven by the development of Semantic Web and Linked Data, to automate the retrieval of related knowledge [3]. In fact, by means of these techniques, an overview of the whole system can be obtained automatically, inferring the necessary knowledge, and finally estimating the risk level of the system under analysis [4].

For the automatic acquisition of new information, it is necessary to establish the behavioral guidelines or rules that define the objective to be achieved, and how classes should interact with each other [5]. To do so, the most widely used format today is Semantic Web Rule Language (SWRL) [6], which combines OWL and Rule Markup Language. In this approach, the rules are composed of an antecedent and a consequent, so that when the former is fulfilled, the latter is inferred. Another possibility that has been growing over the last years is SPARQL Inference Notation (SPIN) [7], a W3C Recommendation that combines concepts from object-oriented languages, queries, and rule-based systems to describe the object behavior of data.

Following the methodology proposed by Riesco et al. [8] for achieving a framework for dynamic risk management based on

* Corresponding author.
E-mail addresses: carmen.szas@upm.es (C. Sánchez-Zas), victor.villagra@upm.es (V.A. Villagrá), mario.vega@upm.es (M. Vega-Barbas), xavier.larriva.novo@upm.es (X. Larriva-Novo), joseignacio.moreno@upm.es (J.I. Moreno), julio.berrocal@upm.es (J. Berrocal).

https://doi.org/10.1016/j.future.2022.12.006

Threat Intelligence information and the use of reasoners and SWRL, our goal is to go further and broaden the possible threat sources existing in a real heterogeneous environment, considering IoT domains and other cyber-security scenarios [9]. In this regard, anomalies in communications should be considered, both individually and after analyzing their correlation. This modeling implies a previous study of the system environment in a real case, to define the relevant classes, attributes, and relations. Regarding the inference rules, we are proposing a different approach from the base ontology, replacing SWRL by the W3C recommendation, which is more efficient in cases where a large number of individuals must be processed, such as the following [10]. In this way, we aim to achieve a dynamic risk management and cyber-situational awareness system, more comprehensive than the previous, through different sources and SPIN rules.

Briefly, the main contributions of the article are as follows:

- We define an ontology to manage anomalies and infer risk from heterogeneous devices using OWL 2 and SPIN Rules, obtained from a real use case.
- We present an approach to risk management in real-time, by merging our ontology with the methodology from [8], updating the inference rules defined in that research from SWRL to SPIN.
- We present the validation of the ontology and a first approach to an evaluation between both methods (SWRL vs. SPARQL SPIN), selecting SPARQL due to its performance in real time.

To this end, throughout this document we will discuss the previous concepts and define a methodology, presenting the results obtained for a specific use case. In the first section we present this overview of the project and the main purpose. Then we describe other proposals and works related to this field: different approaches to risk management by means of ontology modeling and other applications of SWRL and SPIN to infer knowledge, to finally introduce the base project from which this one arises. Along next section we detail the proposal and the scenario in which the development occurs. To continue, we present the overall system, the ontology created to model different types of anomalies, and the SPARQL rules to infer the relations. Moreover we introduce the validation of the methodology proposed and, finally, we define our conclusions and future lines.

2. Related works

Over the past years, ontologies have grown substantially due to their impact on different areas. This issue has attracted considerable attention from many authors that have described frameworks involving ontologies for their very varied purposes. For this reason, we have analyzed previous studies related to the subject matter of this project, in any of the aspects.

Ontologies have been applied in cybersecurity modeling since 2009. S. Fenz and A. Ekelhart [11] state that the lack of information security knowledge causes inadequate risk-management strategies and therefore, they developed an ontology based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800–12. It is composed by three sub-ontologies: security, enterprise and location, and it is evaluated by a group of experts that analyze its structure and respond a formal competency question set. Also, the importance of modeling a taxonomy to analyze anomalies is a topic that is currently attracting a lot of attention, being approached from different perspectives and environments [12].

One of the main objectives was to detect and act on attacks. In line with this approach, B. Thuraisingham et al. [13] described a framework to collect data and obtain security metrics, to establish the system risk, which may be changing as system conditions do, and to evaluate short- and long-term consequences, with the objective of a dynamic assessment. The followed methodology was to construct a knowledge base with information about the resources under analysis, their vulnerabilities, and the attacks suffered. Then, they defined rules to detect attacks based on context data. In the paper, the authors proposed a model for attackers, user risk, and networks under attack. Following this strategy, and with a number of sources analyzed similar to the one proposed in this project, C. Onwubiko [14] described an ontology to map the information about how cyber incidents are detected, studying the sources, the use of sensors, and how to response and recover from them. The main strengths of this framework were the triggering of alerts and the analysis performed to find the source of the problem, as well as the possibilities for recovery or mitigation. In [15], Yuan et al. described the structure and steps to define a framework based on the study of the environment, to establish different classes and relations to address the problem of reasoning, creating SWRL rules to achieve their objective of modeling the residual risk of a system.

Regarding the analysis of data from sensors, the research work presented in [16] used the assets to control cyber–physical systems. With the emergence of wireless technologies, new exploits, especially affecting IoT field, have appeared. In this sense, Mozzaquatro et al. applied SWRL rules and Pellet reasoner, together with SPARQL to query the information gathered. To validate their proposed ontology, they applied the Software Product Quality Requirements and Evaluation (SQuaRE). To manage vulnerabilities arising from different sources and with the objective to protect the user, Syed R. [17] proposed to construct an ontology and a reasoning system based on SWRL rules and SPARQL queries to evaluate it.

Concerning the language for defining rules, previous studies and research works used SWRL as basis. However, some articles also introduced the development of SPIN rules. In [18], the authors described a risk model for the management and evaluation of possible threats to consider adequate responses. The article focused on including human factors in the risk calculation, using SPIN rules to infer relations, and establishing the human factor profile (experience, training, etc.). Finally, in [19] the authors described the automatic identification of risks to assets in a system, its consequences, and countermeasures. The classes defined are Asset, Threat, Misbehavior and Control. Other classes and the individual's classifications are inferred by means of SPIN rules, to ultimately obtain threat consequences and secondary effects.

On this basis, it would appear to be valid that ontologies provide a primary tool for storing and processing information in any domain, as well as the advantage of using inference rules in these environments, especially when the number of instances to be processed starts to expand.

The baseline for this development is an earlier project, described in [8] by Riesco et al. where the authors proposed a solution where OWL ontologies and SWRL rules are integrated in a layered model based on Threat Intelligence using Pellet reasoner and SWRL rules as algorithms and axioms to support the reasoner. The authors included in the ontology proposed information about cyber threat intelligence, assets, and countermeasures to estimate threats related to the organization or system controlled, and thus be able to infer the risks to which they are subjected and manage them.

3. Scenario

Based on the ontology described above [8], our intention is to extend the sources of threats to include, in addition to assets and cyber threat intelligence information, different anomalies

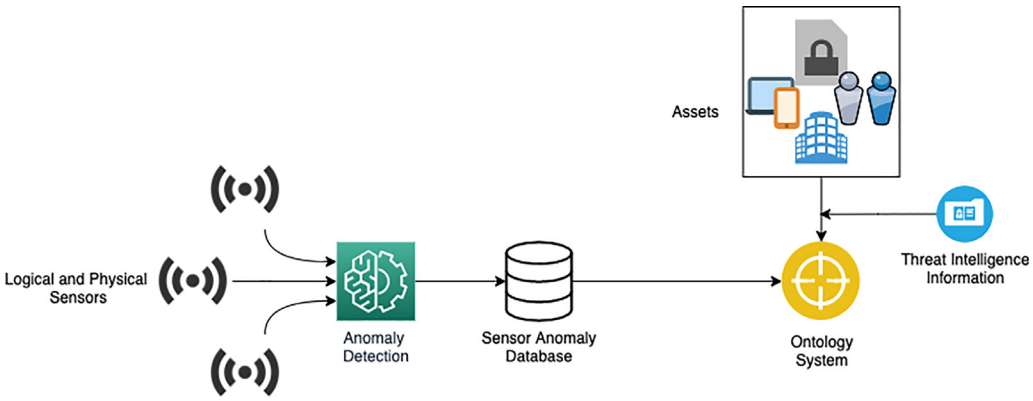

Fig. 1. Project environment, composed by the various sources that feed the ontology.

detected through physical and logical sensors. To describe the new ontology, it is necessary to understand both the environment to be described and the different technologies and tools to be applied.

This project is built on the principles of the Semantic Web [20], which provides technologies to define vocabularies and rules for handling this information. Also known as Web of Linked Data [21], one of the main requirements is to have large amounts of data in a standard format, to access to it and generate relations among the classes. Our ontology is built using the Web Ontology Language (OWL) [22], a W3C Recommendation applied when the gathered data might be processed by applications.

The ontologies that were developed in the previous paper contain information to describe the threat intelligence environment and the Disaster Risk Management data surrounding the system. In the STIX ontology, they attempt to describe domain objects such as Attack Patterns, Campaigns, Course of Action, Indicators, Vulnerabilities, Tools or Threat Actors following the OASIS [23] open standard specification. Additionally, in [8] was presented a DRM ontology, whose vocabulary includes Assets and their Valuation, Context, Incidents, Threats, Safeguards, and a set of risk-related terms: types of risk, Assessment, Impact, Management, Probability, or Severity. Concepts of both ontologies are associated by means of SWRL rules, with the intention of establishing which conditions determine that the monitored system is being threatened, and, in that case, the level of risk associated with that situation and the usefulness of the safeguards that are included, or the possible reactions to be undertaken. Therefore, and due to the characteristics of the environment where the development presented must be deployed (equipped with different types of sensors), we decided to create a new ontology to define the terms related to anomalies in communications. For this purpose, there are systems that, for instance, monitor Wi-Fi and Bluetooth networks, as well as others to control firewalls and Network Traffic, or analyze user behavior. To achieve a real dynamic risk management and awareness system, it is necessary to analyze the records of the different sensors deployed. These data are analyzed using Machine Learning models to predict whether they represent anomalies, and this decision is stored in a database, which feeds the ontology. In addition, the anomalies are studied among themselves, looking for correlations that represent attacks that use different connections. All this information is stored in different classes, establishing properties and relationships between them. Furthermore, the set of assets present in the system must also be recorded in the ontology, as well as the Threat Intelligence information available that affects the environment. All these processes are represented in Fig. 1.

The main drawback of adding anomalies is the increase of individuals to be processed. In this situation, SWRL rules slow down the processing because the reasoner is run beforehand on all instances. For this reason, and to complete the interconnection of these classes, the rules applied to the STIX and DRM ontologies are translated into SPIN, and we also define new rules in this language for anomalies

Thus, after an analysis of the environment in which the prototype is to be deployed, we were able to establish a number of relationships between the anomalies coming from each device and the threats associated with the type of attack represented by that anomaly, obtaining a catalog of threat instances generated from others that represent anomalies or vulnerabilities, with a given value for probability and impact. Moreover, the threats are associated with a type of risk, on which an average value of probability and impact is calculated, and thereby obtaining the risk level.

One of the main requirements facing this development is real-time management. In terms of risk, this is essential, as the effect of an incident on the system has to be assessed at the moment it is detected. The devices that capture and analyze anomalies already work in real time, so we had to focus on the execution of the ontology system, which has to process a large volume of data without being time consuming. As mentioned above, this is the reason for changing the rule definition language because, as will be validated later, it is more efficient in the execution of the rules, so we can keep the risk management in real time.

With all this data, we expect to have a complete view of the sources of threats to which the system is exposed, modeling the different types and the probability and impact values of each one of them. From the threat instances, an inference is made to generate the risk affecting the system, defining the relationships between the different categories of threats and risks. For each one of the latter, a weighted average is calculated, so that the total risk level is obtained as follows: Every threat instance has a probability (P_{Ti}) and impact value (I_{Ti}), with values normalized to be integers between 1 and 10. We group them according to the sub-classes to which they belong, to calculate the total value of probability (P_T) and impact (I_T) for each sub-type, where n_T is the number of instances belonging to each category (Eq. (1)):

$$P_T = \frac{\sum P_{Ti}}{n_T}; \quad I_T = \frac{\sum I_{Ti}}{n_T}. \tag{1}$$

Subsequently, we gather the threats that generate each type of risk, obtaining in the same way as before, a probability (P_R) and an impact (I_R) for every class, which, when multiplied, provide the level of potential risk of that type (PR_R) (Eqs. (2) and (3)), which takes a float value between 0 and 100:

$$P_R = \frac{\sum n_T \cdot P_T}{\sum n_T}; \quad I_R = \frac{\sum n_T \cdot I_T}{\sum n_T}, \tag{2}$$

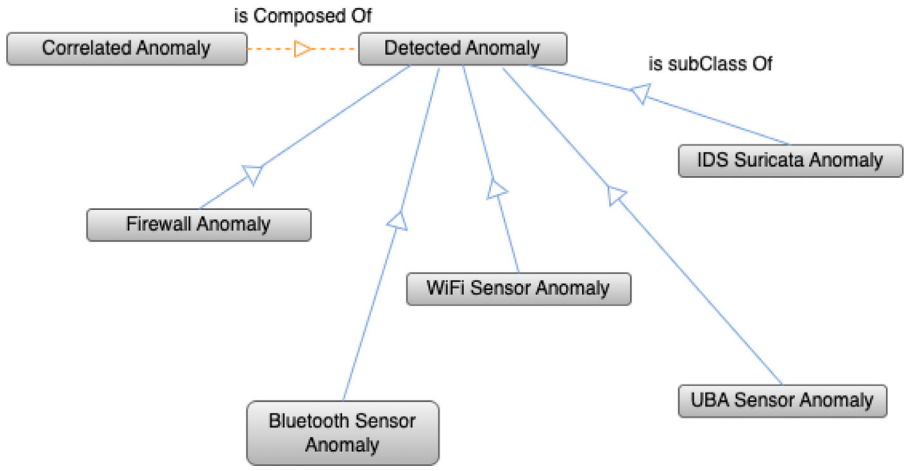

Fig. 2. Sub-classes defined in the ontology for the class *"Detected_Anomaly"* (continuous blue lines) and the relation between Correlated Anomalies and Single Detected Anomalies (orange dashed lines).

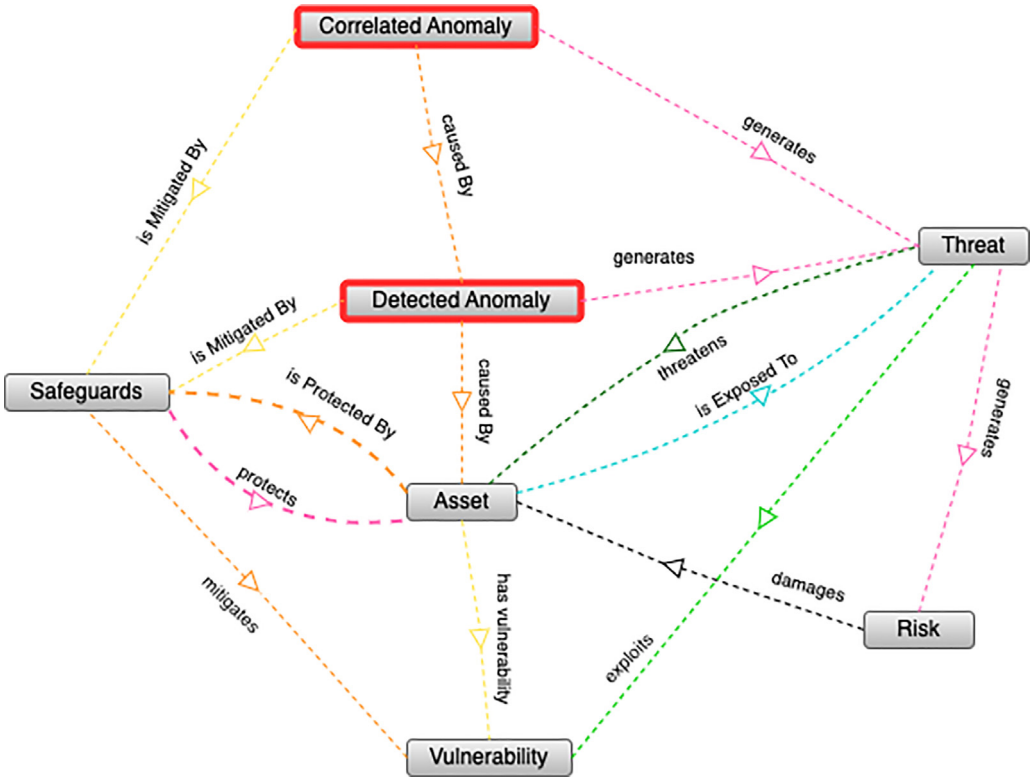

Fig. 3. Relational Graph of the main concepts of the final ontology.

$$PR_R = P_R \cdot I_R. \tag{3}$$

In addition, to consider the effect of the safeguards (S_{Ri}) affecting each class, the residual risk of each type is calculated (RR_R) (Eq. (4)):

$$RR_R = RP_R - \sum S_{Ri}. \tag{4}$$

Finally, the overall system risk level is calculated in terms of potential and residual values (PR_{Total} and RR_{Total}), having n_R as the number of risk types included (Eqs. (5) and (6)):

$$PR_{Total} = \frac{\sum PR_R}{n_R}, \tag{5}$$

$$RR_{Total} = \frac{\sum RR_R}{n_R}. \tag{6}$$

4. Information model proposal

4.1. Threat intelligence ontology and disaster risk management ontology

As mentioned above, the starting points for this research were ontologies [8] already modeled to define Threat Intelligence (STIX) and Disaster Risk Management (DRM) domains. For a better understanding of the development of this work and the rules presented in Section 4.3, we present here an overview of the content of these ontologies:

- **Threat Intelligence (STIX)**. This ontology contains the classes of STIX language elements and their relations: Attack

Pattern, Bundle, Campaign, Course of Action, Cyber Observables (IP Addresses, Domain names, URLs, Artifacts, Network Traffic), Incident, Indicator, Kill Chain Phase, Location, Malware, Relationship or Vulnerabilities.

- **Disaster Risk Management (DRM)**. Assets from the environment, its properties and valuation, Context from the environment and its subtypes, Response (Countermeasure), Risks and its sub-types, Risk Assessment, Risk Impact, Risk Probability, Risk Severity, Risk Management, Risk Scope, Safeguards, Threats and its sub-categories

4.2. Ontology modeling — anomalies

On the basis of the ontologies defined in the previous subsection, and to accomplish the objective of expanding the system to various threat sources, we must develop another to define those concepts and later merge all three. The first step then is to define a concept for a Detected Anomaly. It can be subdivided according to the origin of the anomaly (sensor), and depending on that, each type might have different properties, according to the data obtained from the sensors: power, IP addresses, MAC addresses, frequency, number of bytes/packets, port numbers, etc. Besides, a combination of simple anomalies can generate a correlation, increasing the probability or impact of the threat related. All sub-types of anomalies are presented in Fig. 2.

In a more comprehensive overview, regarding the relations with the other ontologies, we establish that anomalies (*Detected_Anomalies*) could generate correlations (*Correlated_Anomalies*), and might be caused by assets, which may have vulnerabilities. Safeguards mitigate all types of anomalies or vulnerabilities and protect assets. On the other side of the graph, threats could be generated by anomalies, and they could threaten assets by exploiting vulnerabilities. Finally, those threats produce risks, which damages assets. Fig. 3 shows the main existing relationships in the merged ontology between the classes created for this development, highlighted in the figure, and the existing definitions.

4.3. Inference rules

OWL is a standard language that can be used to define classes, properties, and relationships between those classes, and it is the most commonly used in other related works as [24]. Its objective is to give axiomatic definitions, not establishing the computational behavior. To this end, the SPARQL Inference Notation (SPIN) [7] was developed. It combines concepts from object-oriented languages, query languages, and rule-based systems to describe the behavior of web data. One of the basic ideas is to link class definitions with SPARQL queries to capture rules that formalize the expected behavior of those classes. This technology is widely applied in ontologies, as presented in [25].

Once the ontology is populated with individuals of some of the defined classes, the generation of new knowledge can be automated if we correctly define the inference rules. For the development presented here, the ontology already has individuals of various anomalies and Threat Intelligence. On this basis, it is necessary to create related threats and define the risk they pose by establishing these rules using SPARQL language. They are built on the structure of a CONSTRUCT query.

The inferences raised in this document can be diverse. First, the rules already defined in [8] for Threat Intelligence are translated from SWRL to SPIN, without using automatic tools, such as SWRL2SPIN [10], as the ontology of the original project and the present are different, and therefore some modifications in the rule constructions were required. However, in addition, related to the ontology that is developed to model anomalies, new rules are also implemented. The structure of one of the rules for each group used are detailed below as an example:

Enrichment rules to generate more information about the Threat Intelligence environment in which we operate, inferred from the basic data. This is one of the types of rules that were already written in SWRL, so we proceeded to translate them into the new standard. In this case, the purpose of the rule is to relate Domain and IPs to obtain DNS data enrichment:

SWRL
DRM:belongToRefs(?ip, ?ref)
∧ STIX:Domain_Name(?ref)
∧ STIX:IPV4Addr(?ip) − >
STIX:resolves_to_refs(?ref, ?ip)
∧ STIX:Domain_Name(?ref)

SPIN
```
CONSTRUCT {
?ref STIX:resolves_to_refs ?ip.
} WHERE {
?ip a STIX:IPV4Addr.
?ref a STIX:Domain_Name.
?ip DRM:belongToRefs ?ref. }
```

SWRL
DRM:Users(?u)
∧ DRM:dependsOn(?rs, ?new_data)
∧ DRM:dependsOn(?new_data, ?sw)
∧ DRM:dependsOn(?new_data, ?u)
∧ DRM:Risk_Scope(?rs)
∧ DRM:evaluates(?av, ?rs)
∧ DRM:Asset_Valuation(?av)
∧ STIX:Software(?sw)
∧ swrlx:makeOWLThing(?x, ?sw)
∧ DRM:Data(?new_data) − >
DRM:probability(?x, 4.0)
∧ DRM:DelibMaliciousSWDistrib(?x)
∧ DRM:impact(?x, 3.0)
∧ DRM:threatens(?x, ?sw)

SPIN
```
CONSTRUCT {
?x a DRM:DelibMaliciousSWDistrib.
?x DRM:probability 4.
?x DRM:impact 3.
?x DRM:threatens ?sw.
} WHERE {
?u a DRM:Users.
?rs a DRM:Risk_Scope.
?av a DRM:Asset_Valuation.
?av DRM:evaluates ?rs.
?new_data a DRM:Data.
?sw a STIX:Software.
?rs DRM:dependsOn ?new_data.
?new_data DRM:dependsOn ?sw.
?new_data DRM:dependsOn ?u.
BIND(URI(DRM:SWD1) as ?x) }
```

Threat Inventory rules to generate threats (new individuals) depending on some assets and their relations. In this case, the rules must also be translated into SPIN. For the development of these rules, we studied all possible types of assets that may be present in the system, and how they affect each other or as a whole. In the following, the aim is to generate a Malicious Software Distribution Threat with probability 4 and impact 3

when the environment meets a series of conditions in terms of assets and Threat Intelligence Information (Users, Data, Software, their valuation, and risk scope).

Threat Intelligence rules to detect malicious events related to a type of threat. There could be one such rule for each STIX category included in the ontology. We also had to translate this group of rules. The target in this case was to follow re-directions until an executable was found, implying a security event.

SWRL
STIX:redirection(?pl, ?red)
$\wedge$ STIX:dst_payload_ref(?nt, ?pl)
$\wedge$ STIX:dst_ref(?nt2, ?red)
$\wedge$ STIX:Artifact(?pl2)
$\wedge$ swrlx:makeOWLThing(?x, ?nt2)
$\wedge$ STIX:Network_Traffic(?nt)
$\wedge$ STIX:dst_payload_ref(?nt2, ?pl2)
$\wedge$ STIX:URL(?sr)
$\wedge$ STIX:Artifact(?pl)
$\wedge$ STIX:extensions(?pl2, "windows")
$\wedge$ STIX:URL(?red)
$\wedge$ STIX:src_ref(?nt2, ?sr)
$\wedge$ STIX:mime(?pl, "javascript")
$\wedge$ STIX:Network_Traffic(?nt2) $->$
STIX:dst_ref(?x, ?red)
$\wedge$ STIX:related-to(?x, ?nt2)
$\wedge$ STIX:src_ref(?x, ?sr)
$\wedge$ DRM:Security_Events(?x)

SPIN
CONSTRUCT {
?x a DRM:Security_Events.
?x STIX:src_ref ?sr.
?x STIX:dst_ref ?red.
?x STIX:related-to ?nt2.
} WHERE {
?red a STIX:URL.
?sr a STIX:URL.
?nt a STIX:Network_Traffic.
?nt2 a STIX:Network_Traffic.
?pl STIX:Artifact.
?pl2 STIX:Artifact.
?pl STIX:redirection ?red.
?nt STIX:dst_payload_ref ?pl.
?nt2 STIX:dst_payload_ref ?pl2.
?nt2 STIX:src_ref ?sr.
?nt2 STIX:dst_ref ?red.
?pl2 STIX:extensions "windows".
?pl STIX:mime "javascript".
BIND(URI(DRM:SE1) as ?x) }

Anomalies generate Threat. This is the first type of rules defined specifically for this extension of the project by adding data from sensors. At least one is created for each type of sensor, defining the relationship between the anomaly and the associated threat, which is inferred based on the system environment and the possible attacks that can be carried out through the technology monitored by each sensor, modeled in the ONA ontology. For the following example, it has been assumed that an anomaly in WiFi networks generates a Denial-of-Service Threat with a given probability and impact.

CONSTRUCT {
?x a DRM:DenialOfService.
?x a DRM:Threat.
?x DRM:isGeneratedBy ?a.
?a DRM:generates ?x.
?x DRM:probability 5.
?x DRM:impact 8.
} **WHERE** {
?a a ONA:WiFiSensorAnomaly.
BIND(URI(DRM:DoS1) as ?x) }

Threats generate Risk. This set of rules is part of the reasoning core of the proposed project, as it establishes the relationship between threat and risks. Thus, it will be necessary to define at least one rule for each type of threat to be considered, being possible to relate the same instance to several types of risk. One of the considered cases is that Denial of Service threats may entail User Complaint risks.

CONSTRUCT {
?r DRM:isGeneratedBy ?t.
?t DRM:generates ?r.
} **WHERE** {
?t a DRM:DenialOfService.
?r a DRM:UsersComplaintsRisk }

Risk Severity rules to evaluate the risk level and classify them. Rules are generated for all levels: low, medium, high, and extreme. Again, these rules must be translated.

SWRL
swrlx:makeOWLThing(?x, ?rr)
$\wedge$ swrlb:greaterThanOrEqual(?ar, 6)
$\wedge$ DRM:actualRisk(?rr, ?ar)
$\wedge$ DRM:ResidualRisk(?rr)
$\wedge$ swrlb:lessThan(?ar, 8)
$\wedge$ DRM:evaluates(?rr, ?ris) $->$
DRM:drm_value(?x, ?ar)
$\wedge$ DRM:evaluates(?x, ?ris)
$\wedge$ DRM:HighRiskSeverity(?x)

SPIN
CONSTRUCT {
?x a DRM:HighRiskSeverity.
?x DRM:drm_value ?ar.
?x DRM:evaluates ?risk.
} WHERE {
?risk a DRM:Risk.
?rr a DRM:ResidualRisk.
?rr DRM:actualRisk ?ar.
?rr DRM:evaluates ?risk.
FILTER(?ar $>$ 6 AND ?ar $<$ 8)
BIND(URI(DRM:HRS1) as ?x) }

Risk Assessment rules. Using these rules, we generate risk sub-types: Potential and Residual, to differentiate in each category the risk level with and without the effect of the safeguards in place. These rules are used to relate the risks to their corresponding potential/residual risk instances.

```
CONSTRUCT {
?rr a DRM:ResidualRisk.
?pr a DRM:PotentialRisk.
?r DRM:hasAssessmentOf ?rr.
?r DRM:hasAssessmentOf ?pr
} WHERE {
?r a DRM:Risk.
BIND(URI(DRM:RR_1) as ?rr)
BIND(URI(DRM:PR_1) as ?pr) }
```

The risk values are included in each instance of potential/residual risk after the calculation described in other sections above.

Risk Management rules to choose an answer to react to risks. In this case, again, the options implemented in the rules will be Mitigation (Extreme and High-Risk Severity), Investigation (medium risk severity), and Monitoring (low risk severity). This case could be expanded, after an extensive study of the environment, to define more specific measures depending on the risk and context.

```
SWRL
swrlx:makeOWLThing(?x, ?er)
∧ DRM:drm_value(?er, ?sev)
∧ DRM:evaluates(?er, ?risex)
∧ DRM:HighRiskSeverity(?er) − >
DRM:RiskMitigation(?x)
∧ DRM:manages(?x, ?risex)
∧ DRM:drm_value(?x, ?sev)

SPIN
CONSTRUCT {
?x a DRM:RiskMitigation.
?x DRM:drm_value ?sev.
?x DRM:manages ?risk.
} WHERE {
?risk a DRM:Risk.
?er a DRM:HighRiskSeverity.
?er DRM:drm_value ?sev.
?ex DRM:evaluates ?risk.
BIND(URI(DRM:RMS1) as ?x) }
```

There are also more specific rules to define aspects such as Security Policies, that must be translated.

```
SWRL
DRM:Users(?u)
∧ swrlb:greaterThanOrEqual(?a, ?r)
∧ DRM:req_level(?new_data, ?r)
∧ DRM:has_access_level(?u, ?a)
∧ DRM:Data(?new_data) − >
DRM:has_access_to(?u, ?new_data)

SPIN
CONSTRUCT {
?u a DRM:has_access_to ?new_data.
} WHERE {
?u a DRM:Users.
?u DRM:has_access_level ?a.
?new_data a DRM:Data.
?new_data DRM:req_level ?r.
FILTER(?a > ?r) }
```

The ultimate goal of these rules is to infer relationships between the different instances included in the ontology (sensor anomalies, threat intelligence, and assets), and thus obtain an overview of the system and the level of risk in real time, as well as the possible measures to take and the effectiveness of the safeguards.

anomaly	threat	impact	probability
Anomaly_CS_Type_0	DenialOfService_CS_Type_0	"5.0"^^"3.0"^^<ht	
Anomaly_CS_Type_1	DenialOfService_CS_Type_1	"5.0"^^"3.0"^^<ht	

Fig. 4. Result of the Anomaly-Threat rule (SPIN Query).

Fig. 5. Result of the Anomaly-Threat rule (Protégé).

5. Validation of the ontology

To validate the ontology constructed, we used SPARQL queries and the Protégé [26] application to visualize the inference of relations and the calculation of the risk level. For instance, to demonstrate the efficiency of the rules, we queried the ontology to verify the "Anomalies generate threat" rule, obtaining the anomalies introduced in the system, in this case, cyber security sensor anomaly, the threats generated and, when choosing one for better visualization (Denial of Service threat), the associated values of impact and probability (Fig. 4). The results of these queries do not necessarily match the rules used as example in the previous section. The use case of this validation corresponds to Cybersecurity device anomalies.

```
SELECT ?anomaly ?threat ?impact ?prob
WHERE {
?anomaly a ONA:Detected_Anomaly.
?anomaly DRM:generates ?threat.
?threat a DRM:DenialOfService.
?threat DRM:impact ?impact.
?threat DRM:probability ?prob. }
```

This information was also checked in the application (Fig. 5).

risk	riskvalue
PressNegativeImpactRisk_Risk	"10.222222"
TechnicalComplexityDerivedRisk_Risk	"10.54273"
NetworkOutageRisk_Risk	"10.468878"
CorporateBrandImageDamageRisk_Risk	"9.551021"
UntrustworthyRisk_Risk	"13.142858"
DataProtectionComplianceRisk_Risk	"9.540741"
NonIntentionalInformationTamperingRisk_Risk	"12.0"
NonIntentionalInformationDestructionRisk_Risk	"12.0"
DenialOfServiceRisk_Risk	"13.485207"
DeviceTheftRisk_Risk	"4.964286"
DeliberatedRegistersTamperingRisk_Risk	"9.173778"
UsersComplaintsRisk_Risk	"11.298731"
SocialEngineeringRisk_Risk	"6.0"
DeliberatedHWTamperingRisk_Risk	"9.25"
PhysicalFailureRisk_Risk	"10.0"
StrategicObjectiveRisk_Risk	"4.0"
NonIntentionalUserErrorRisk_Risk	"6.0"
DeliberatedMaliciousSWDistributionRisk_Risk	"16.866667"
NonIntentionalMaliciousSWDistributionRisk_Risk	"18.307692"
DeliberatedSWTamperingRisk_Risk	"11.910289"
BadReputationRisk_Risk	"12.108473"
DeliberatedConfigFilesTamperingRisk_Risk	"9.173778"
FireRisk_Risk	"4.0"
DeviceLostRisk_Risk	"4.964286"

Fig. 6. Result of the calculation of risk values.

Following this example, we validated the rules created for this project, for instance, the calculation of the system risks (Fig. 6).

```
SELECT ?risk ?riskvalue
WHERE {
?risk a DRM:Risk.
?risk DRM:hasAssessmentOf ?pr.
?pr a DRM:PotentialRisk.
?pr co:potentialRisk ?riskvalue. }
```

However, another approach for validation was the application of methodologies to evaluate the quality of the ontology, using standardized procedures, such as Ontology Quality Requirements and Evaluation Method and Metrics (OQuaRE) Framework [16,27,28], based on the SQuaRE (Software Product Quality Requirements and Evaluations) [29] methodology.

This framework for evaluating an ontology is an adaptation of the SQuaRE standard for measuring the quality of a software product. In this field, the quality of an ontology is considered to be the degree of conformance to functional and non-functional requirements, if it can be measured.

The Software Product Quality Requirements and Evaluation methodology applied to ontologies implies the definition of quality characteristics:

- Structural: formal and semantic properties.
- Functional Adequacy: capability to provide concrete functions.
- Reliability: ability to maintain a level of performance for a period of time.
- Performance Efficiency: relation between the level of performance and the amount of resources required.
- Operability: effort needed for use.
- Compatibility: ability of two ontologies to exchange information or perform their function when sharing an environment.
- Maintainability: capability to be modified for changes in the environment, requirements of functional specifications.
- Transferability: degree to which the ontology can be transferred from one environment to another.
- Quality in use: degree to which an ontology used by specific users meets their needs to achieve specific goals.

The results obtained when applying the tool [30] to the ontology created were standardized to numbers in the interval from 1 to 5, following the guidance in [31], obtaining an average score considering all indicators of 3,83/5, which is an acceptable result. To continue, we analyzed the individual results for each category. From a structural perspective, it accounts quality factors. The metrics obtained are grouped depending on the indicator to which they relate, obtaining four categories and an average of 2,5 over 5 points. The ontology scored highly on cohesion, but had poorer results in redundancy and tangledness, areas for future improvement. This information, represented in Fig. 7, means that we must identify those concepts that are not informative and design a better distribution of the parent categories.

The indicator for functional adequacy, or the capability to provide certain functions, it improved the average score from the past perspective (3225/5), showing good results on guidance, indexing and linking, among others. However, the results for controlled vocabulary and clustering were also to be improved, so the next action to be taken in this regard will be to unify similar terms, as shown in Fig. 8.

Finally, there were other metrics related to the environment and effort: Compatibility measures, whether two components can exchange information or perform their functions while sharing the same environment, while Transferability is the degree to which the environment could be changed, and Operability represents the effort needed to use the software. Here we obtained very positive results in all of them, scoring over 4 points (Fig. 9).

5.1. Comparison between SWRL and SPIN

Along the development of the project, the ontology we were dealing with started to grow substantially in the number of anomaly's individuals, reaching the thousands range and, using SWRL we evaluated that the execution time soared with the number of instances to process. Therefore, one of the main objectives of the project was to evolve from SWRL to SPIN rules, to verify the efficiency of this proposal, since this is a real-time project, the time needed to complete the execution is one of the main requirements to be met.

Once we decided to make the change in the definition language, we proposed to develop a comparison between both, in order to base the decision on objective metrics. The following is a first approximation of this comparison, taking into account the execution times.

In this regard, it is worth mentioning that SWRL rules are already assumed to be slower because all individuals need to be saved in the ontology to apply the rules defined, meanwhile, SPIN's ontology model allowed us to create the instances and infer from them without the need of saving in a file. Hence, the procedure for saving the last inferences in SWRL is not taken into account, as well as the action to save SPIN ontology in a document. In addition, Fig. 10 shows the number of anomaly instances that are created at the beginning, which cause the rules to be executed and, in some cases, create more individuals, so the final number of ontology instances is significantly higher. The results obtained for SPIN rules were much lower, so that, for

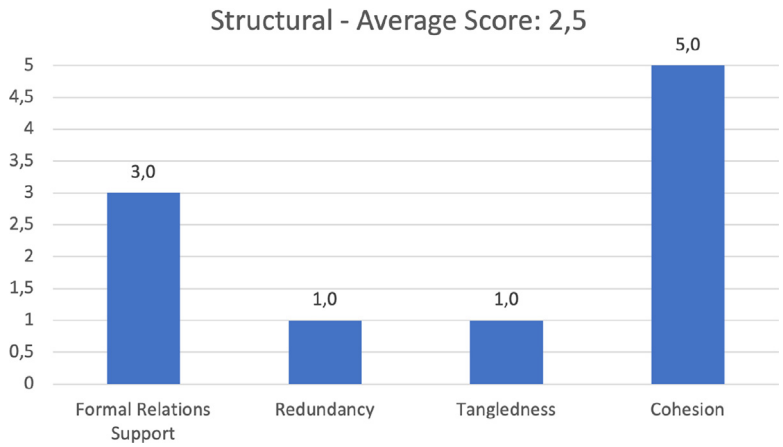

Fig. 7. Structural metrics results obtained with SQuaRE.

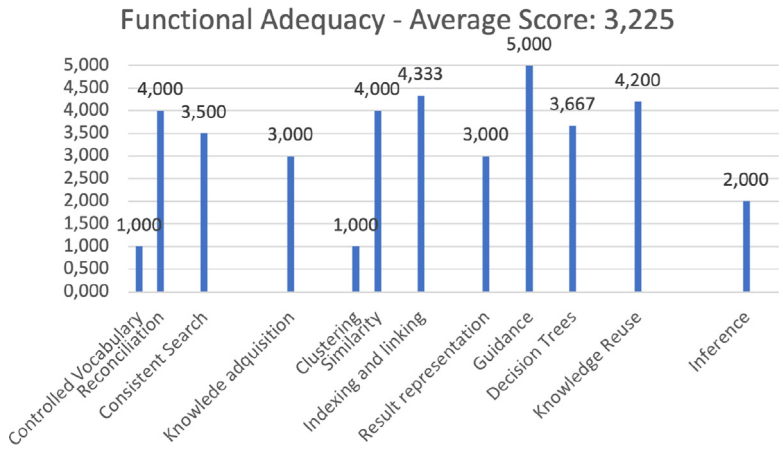

Fig. 8. Functional Adequacy metrics obtained with SQuaRE.

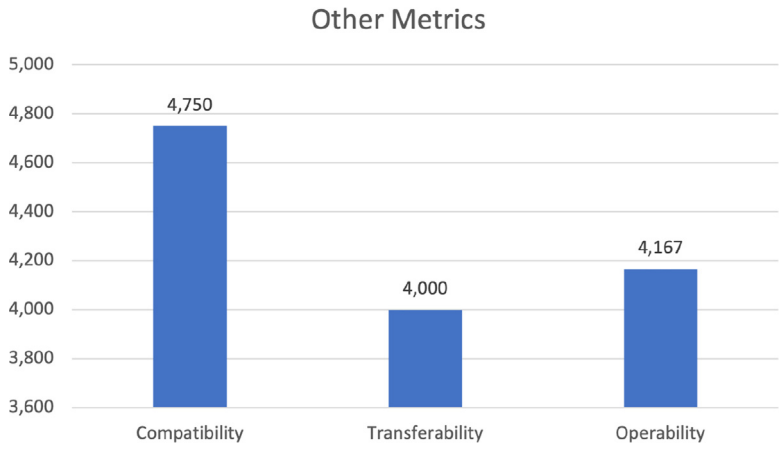

Fig. 9. Other ontology metrics obtained with SQuaRE.

an ontology with a number of individuals around the thousands, those types of rules show a better performance.

To deepen this comparison, the study could be extended to other objective metrics, the resource consumption, interoperability or integration with other programming languages.

5.2. Validation discussion

Having checked the quality of the ontology, identified the points for improvement, and validated the advantage of SPARQL vs. SWRL rules, we can state that the ontology and the rules described could be applied in heterogeneous environments where the risk management must be a priority, so that real time is a mandatory feature, and the effect of SPIN rules sets the difference. The applicability of the ontology and rules model proposed in this research has been tested in the real case described in Section 3. Receiving as input data from heterogeneous devices, and applying the rules described above, a real-time dynamic risk management system is obtained.

Fig. 10. Comparison SWRL and SPIN. Represents the number of instances versus the time required in execution.

6. Conclusions

Given the importance that ontologies are currently gaining, it is essential to have a first-hand and in-depth knowledge of the technology and the different possibilities it offers. Therefore, deciding when it is most efficient to use each language or structure is vital for the development of any project. Trying to meet the need to keep risk under control through continuous risk assessment and management, in this paper, we present a joint ontology to dynamically manage the risk of a system in which threats are presented from logical and physical sources, considering anomalies, assets, and threat intelligence information. For this purpose, we started from an ontology previously developed on Threat Intelligence (STIX), Assets, Threats, and Risk (DRM), and the main objective was to try to extend it to add anomalies (ONA) and new SPIN rules, translating the previous SWRL ones, to calculate the level of risk and support decision making.

The ontology obtained was analyzed using the OQuaRE framework, where an average score of 3.83 out of 5 was obtained among all metrics. The best results were achieved in compatibility (4.75/5), operability (4.167/5) and transferability (4.0/5) metrics, meanwhile the functional adequacy metric obtained an intermediate value on the scale (3.225/5). The poorest results were reached in structural terms (2.5/5), since the metrics that influenced this calculation had very diverging values, from 1.0/5 to 5.0/5, resulting in a very important point of action for the future. Considering these results, the incorporation of classes to model the anomalies, followed by the combination of the three resulting sub-ontologies, represents an extension of the study in the environment of a cyber-situational awareness system, while maintaining levels of ontology quality that are considered acceptable, thus achieving the objective of the project.

We also studied the difference in execution times between both types of rules, obtaining significantly better results for SPIN rules in the case of our project. This calculation was performed under specific conditions, since SWRL required additional time to store all the inferred individuals, and SPIN did not. Therefore, only the number of individuals generated manually at the beginning is considered. The time required by the SWRL rules is considerably longer than in the case of SPIN, having a non-linear growth with the number of instances. It is also noteworthy that, for scenarios above 60 000 instances, no conclusive results were obtained for SWRL, which supported the application of SPIN in this project, where the number of individuals to be processed is substantially high. As a first approximation to a comparison between both types of rules, we can highlight the improvement in the performance that can be extracted from this paper in the conversion and use of SPIN rules.

As mentioned before, the validation performed with the OQuaRE framework has revealed the weak points of our development, such as redundancy and tangledness. In order to improve the construction of the ontology, we must identify concepts that are not informative and design a better distribution of the categories, unifying similar term. Thus, to continue working in the future based on this project, we propose first to analyze and correct the OQuaRE metrics for which we obtained lower metrics, and then to extend the variety of rules to be applied to the data, especially in the case of risk management, or to include other sources of anomalies. In relation to the language of the rules definition, as a main future line to continue in accordance to this work, we propose to extend the comparison to other aspects and metrics, to reinforce the decision to use SPIN rules in an objective way.

CRediT authorship contribution statement

Carmen Sánchez-Zas: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Víctor A. Villagrá:** Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing. **Mario Vega-Barbas:** Formal analysis, Investigation, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing. **Xavier Larriva-Novo:** Data curation, Investigation, Software. **José Ignacio Moreno:** Funding acquisition, Project administration, Resources. **Julio Berrocal:** Funding acquisition, Project administration, Resources.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Victor A. Villagra reports financial support was provided by Government of Spain Ministry of Defense.

Data availability

Data will be made available on request.

Acknowledgment

This work has been partially supported by the Ministerio de Defensa of the Spanish Government within the framework of PLICA project (Ref: 1003219004900-Coincidente)

References

[1] G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, H. Debar, Dynamic risk management response system to handle cyber threats, Future Gener. Comput. Syst. 83 (2018) 535–552, http://dx.doi.org/10.1016/j.future.2017.05.043, URL https://linkinghub.elsevier.com/retrieve/pii/S0167739X17311433.

[2] ISO 31000:2018(en), Risk management — Guidelines, URL https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

[3] K. Munir, M. Sheraz Anjum, The use of ontologies for effective knowledge modelling and information retrieval, Appl. Comput. Inf. 14 (2) (2018) 116–126, http://dx.doi.org/10.1016/j.aci.2017.07.003, URL https://linkinghub.elsevier.com/retrieve/pii/S2210832717300649.

[4] Ontologies - W3C, URL https://www.w3.org/standards/semanticweb/ontology.html.

[5] C. Mercier, L. Roux, M. Romero, F. Alexandre, T. Vieville, Formalizing problem solving in computational thinking : an ontology approach, in: 2021 IEEE International Conference on Development and Learning (ICDL), IEEE, Beijing, China, 2021, pp. 1–8, http://dx.doi.org/10.1109/ICDL49984.2021.9515660, URL https://ieeexplore.ieee.org/document/9515660/.

[6] SWRL: A Semantic Web Rule Language Combining OWL and RuleML URL https://www.w3.org/Submission/SWRL/.

[7] SPIN - Overview and Motivation, URL https://www.w3.org/Submission/spin-overview/.
[8] R. Riesco, V.A. Villagrá, Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL), Int. J. Inf. Secur. 18 (6) (2019) 715–739, http://dx.doi.org/10.1007/s10207-019-00433-2, URL http://link.springer.com/10.1007/s10207-019-00433-2.
[9] X.A. Larriva-Novo, M. Vega-Barbas, V.A. Villagrá, M. Sanz Rodrigo, Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies, IEEE Access 8 (2020) 9005–9014, http://dx.doi.org/10.1109/ACCESS.2019.2963407.
[10] N. Bassiliades, SWRL2SPIN: A tool for transforming SWRL rule bases in OWL ontologies to object-oriented SPIN rules, 2018, arXiv:1801.09061[Cs], URL http://arxiv.org/abs/1801.09061, arXiv:1801.09061.
[11] S. Fenz, A. Ekelhart, Formalizing information security knowledge, in: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ASIACCS '09, Association for Computing Machinery, New York, NY, USA, 2009, pp. 183–194, http://dx.doi.org/10.1145/1533057.1533084.
[12] F. Cauteruccio, L. Cinelli, E. Corradini, G. Terracina, D. Ursino, L. Virgili, C. Savaglio, A. Liotta, G. Fortino, A framework for anomaly detection and classification in Multiple IoT scenarios, Future Gener. Comput. Syst. 114 (2021) 322–335, http://dx.doi.org/10.1016/j.future.2020.08.010, URL https://www.sciencedirect.com/science/article/pii/S0167739X19335253.
[13] B. Thuraisingham, M. Kantarcioglu, K. Hamlen, L. Khan, T. Finin, A. Joshi, T. Oates, E. Bertino, A data driven approach for the science of cyber security: Challenges and directions, in: 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), IEEE, Pittsburgh, PA, USA, 2016, pp. 1–10, http://dx.doi.org/10.1109/IRI.2016.10, URL http://ieeexplore.ieee.org/document/7785719/.
[14] C. Onwubiko, CoCoa: An ontology for cybersecurity operations centre analysis process, in: 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), IEEE, Glasgow, 2018, pp. 1–8, http://dx.doi.org/10.1109/CyberSA.2018.8551486, URL https://ieeexplore.ieee.org/document/8551486/.
[15] J. Yuan, X. Li, K. Chen, M.J. Skibniewski, Modelling residual value risk through ontology to address vulnerability of PPP project system, Adv. Eng. Inform. 38 (2018) 776–793, http://dx.doi.org/10.1016/j.aei.2018.10.009, URL https://linkinghub.elsevier.com/retrieve/pii/S1474034617303063.
[16] B. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, R. Jardim-Goncalves, An ontology-based cybersecurity framework for the internet of things, Sensors 18 (9) (2018) 3053, http://dx.doi.org/10.3390/s18093053, URL http://www.mdpi.com/1424-8220/18/9/3053.
[17] R. Syed, Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system, Inf. Manag. 57 (6) (2020) 103334, http://dx.doi.org/10.1016/j.im.2020.103334, URL https://linkinghub.elsevier.com/retrieve/pii/S0378720620302718.
[18] S. Williams, D. Marriot, Human factors in a computable cybersecurity risk model, in: Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018), Dundee, Scotland, UK, 2018, pp. 214–224.
[19] A. Chakravarthy, S. Wiegand, X. Chen, B. Nasser, M. Surridge, Trustworthy Systems Design Using Semantic Risk Modelling, Coventry, United Kingdom, 2015.
[20] Semantic Web - W3C, URL https://www.w3.org/standards/semanticweb/.
[21] Data - W3C, URL https://www.w3.org/standards/semanticweb/data.
[22] OWL Web Ontology Language Overview, URL https://www.w3.org/TR/owl-features/.
[23] Introduction to STIX, URL https://oasis-open.github.io/cti-documentation/stix/intro.
[24] O.T. Arogundade, A. Abayomi-Alli, S. Misra, An ontology-based security risk management model for information systems, Arab. J. Sci. Eng. 45 (2020) 6183–6198.
[25] M. Eckhart, A. Ekelhart, E. Weippl, Automated security risk identification using automationML-based engineering data, IEEE Trans. Dependable Secure Comput. 19 (3) (2022) 1655–1672, http://dx.doi.org/10.1109/TDSC.2020.3033150.
[26] Protégé, 2022, (Accessed on 07/24/2022) https://protege.stanford.edu/.
[27] OquaRE: A SQUaRE based Quality evaluation framework for Ontologies, URL http://miuras.inf.um.es/evaluation/oquare/Contenido.html.
[28] A. Duque-Ramos, J. Fernandez-Breis, R. Stevens, N. Aussenac-Gilles, OQuaRE: A square-based approach for evaluating the quality of ontologies, J. Res. Pract. Inf. Technol. 43 (2011) 159–176.
[29] W. Suryn, A. Abran, A. April, ISO/IEC SQuaRE. The second generation of standards for software product quality, 2003.
[30] Github to Ontology evaluation project, URL https://github.com/atibaut/ontology-evaluation.
[31] The Quality metrics of OQuaRE, URL http://miuras.inf.um.es/evaluation/oquare/Metrics.html.

Carmen Sánchez-Zas received the M.Sc. degree in Telecommunication Engineering from the Universidad Politécnica de **Madrid (UPM), Spain, in 2020, and currently she** is a Ph.D. student and researcher in ETSI Telecomunicación, Universidad Politécnica de Madrid (UPM), Avda. Complutense 30, 28040 Madrid, Spain. Her research interests include cybersecurity, risk management and different artificial intelligence fields (machine learning, ontologies) for different national and European projects.
Contact: carmen.szas@upm.es.

Víctor A. Villagrá received the Ph.D. degree in computer science from the Universidad Politécnica de Madrid (UPM), Spain, in 1994. He has been an Associate Professor of telematics engineering with UPM, since 1992. He is currently the Director of the UPM Cybersecurity Master degree and Deputy Director and Head of Studies at the ETSI Telecomunicación, UPM, Spain. He has been involved in several international research projects related with network management, advanced services design and network security, and different national projects. He has authored or coauthored over 90 scientific articles and a textbook about security in telecommunication networks. Contact: victor.villagra@upm.es.

Mario Vega-Barbas is an Associate Professor **within UPM. He** received the B.S. and M.S. degrees in computer science from Universidad de Alcalá, Spain (2009) and the Ph.D. degree in telematics and applied medical technology from the UPM, Spain, and the KTH-Royal Institute of Technology, Sweden (2016). He was a Postdoctoral Researcher with the Institute of Environmental Medicine, Karolinska Institute, and Medical Sensors, Signals and Systems, KTH, Sweden. He has authored or co-authored more than 30 publications, including books and chapters. His research interests include data analysis and visualization, ubicomp, pervasive sensitive services, cybersecurity, user-oriented security and IoT solutions. Contact: mario.vega@upm.es.

Xavier Larriva-Novo received the M.Sc. degree in cybersecurity from the Universidad Politécnica de Madrid (UPM), Spain, in 2018, and the Ph.D. degree in telecommunications engineering in 2022. He is currently a Researcher of telematics engineering with UPM. He has been involved in European research projects related with network management, security design in services, network security, machine learning, and high-performance computing as well as different national projects. Contact: xavier.larriva.novo@upm.es.

José Ignacio Moreno received the Ph.D. degree in telecommunication from the Universidad Politécnica de Madrid, in 1996. After more than 20 years as associate professor at UC3M, he is currently Full Professor at UPM. Since 1992, he has been working in international research projects related with protocol design, protocol engineering, network management, advanced networks, and wireless system performance, leading national and European projects on ICT topics with special focus on WSN, Smart Grid and 5G technologies. He has published more than 100 papers in the field of advanced communications in technical books, magazines, and conferences. Contact: joseignacio.moreno@upm.es.

Julio Berrocal is a Full Professor at Universidad Politécnica de Madrid (UPM). He received a Telecommunication Engineer degree in 1983 and a Ph.D. in Telecommunication degree in 1986, both from UPM. He has been involved in several projects of the European Union R&D Programmes in management of telecommunication networks and services, multimedia broadband networks and emergency management. Prof. Berrocal has authored or co-authored 3 books and more than 80 technical papers and reports, in topics such as communication protocol design and implementation, modeling of network management information and cybersecurity. Contact: julio.berrocal@upm.es.